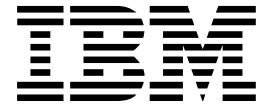


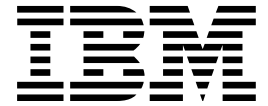
Nways Multiprotocol Access Services



# Consulta de configuración y supervisión de protocolos Volumen 2 Versión 3.4



Nways Multiprotocol Access Services



# Consulta de configuración y supervisión de protocolos Volumen 2 Versión 3.4

**Nota**

Antes de utilizar este documento, lea la información general del apartado "Avisos" en la página xix.

**Segunda edición (octubre de 1999)**

Este manual es la traducción del original inglés *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference Volume 2 (SC30-3885-06)*.

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

Puede realizar el pedido de publicaciones a través del representante de IBM o de la sucursal de IBM de su localidad. Las publicaciones no se suministran en la dirección que aparecerá a continuación.

IBM agradece sus comentarios. Al final de esta publicación se proporciona una hoja de comentarios del lector. Si no se encuentra la hoja mencionada, puede dirigir sus comentarios a:

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

Además, puede escribir comentarios acerca de la documentación así como de otro soporte del producto en la siguiente dirección de la Web:

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

Cuando envía información a IBM, otorga a IBM un derecho no exclusivo a utilizar o distribuir la información del modo que considere apropiado sin incurrir en ninguna obligación con el remitente.

---

# Contenido

<b>Avisos</b> . . . . .	xix
<b>Marcas registradas</b> . . . . .	xxi
<b>Prefacio</b> . . . . .	xxiii
A quién va dirigido este manual . . . . .	xxiii
Obtención de información adicional . . . . .	xxiii
Acerca del software . . . . .	xxiii
Convenios utilizados en este manual . . . . .	xxiv
Visión general de la biblioteca . . . . .	xxv
Resumen de los cambios para la biblioteca de software de IBM 2216 . . . . .	xxvii
Network Utility . . . . .	xxix
Funciones de software soportadas por Network Utility . . . . .	xxix
Cómo obtener ayuda . . . . .	xxxi
Cómo salir de un entorno de nivel inferior . . . . .	xxxi
<b>Utilización de APPN</b> . . . . .	1
¿Qué es APPN? . . . . .	1
Comunicaciones de igual a igual . . . . .	1
Tipos de nodos APPN . . . . .	1
¿Qué funciones de APPN están implementadas en el direccionador? . . . . .	4
Funciones opcionales de nodo de red APPN . . . . .	7
Direccionamiento de alto rendimiento . . . . .	8
Petionario de LU dependientes (DLUR) . . . . .	11
Redes de conexiones APPN . . . . .	15
Branch Extender . . . . .	16
Nodos Extended Border Node . . . . .	17
Branch Extender frente al Extended Border Node . . . . .	20
Gestión de un nodo de red . . . . .	21
Posibilidades de punto de entrada para alertas relacionadas con APPN . . . . .	22
Posibilidades de SNMP para MIB APPN . . . . .	23
Base de datos de topología con Garbage Collection . . . . .	23
Cola de alertas retenidas configurable . . . . .	24
Punto focal implícito . . . . .	24
Soporte del Enterprise Extender para el HPR sobre IP . . . . .	24
DLC soportados . . . . .	24
Proceso de configuración del direccionador . . . . .	25
Cambios de la configuración que necesitan el reinicio de la función de APPN . . . . .	26
Requisitos de la configuración para APPN . . . . .	26
Configuración del direccionador como nodo de red APPN . . . . .	27
Configuración del Branch Extender . . . . .	31
Configuración de nodos Extended Border Node . . . . .	32
Direccionamiento de alto rendimiento . . . . .	37
DLUR . . . . .	38
Configuración de puntos focales . . . . .	38
Configuración del tamaño de la cola de alertas retenidas . . . . .	38
Definición de características de grupo de transmisión (TG) . . . . .	38
Cómo calcular rutas de APPN utilizando características de TG . . . . .	39
Opciones de CoS . . . . .	40
Ajuste de nodo APPN . . . . .	41

Servicio de nodo (rastreos)	42
Estadísticas de contabilidad y nodos	42
Algoritmo de reintentos de DLUR	43
Implementación de APPN en el direccionador con DLSw	46
Implementación de una red de conexiones APPN BAN Frame Relay	47
Listas de parámetros de nivel de puerto	51
Listas de parámetros de nivel de enlace	51
Lista de parámetros de LU	52
Listas de parámetros de nivel de nodo	52
Notas de configuración de APPN	52
Configuración de un circuito permanente con RDSI	52
Configuración de APPN sobre circuitos de marcación bajo pedido	55
Configuración del redireccionamiento de WAN	59
Configuración de la restauración de WAN	66
Configuración de V.25 bis	68
Configuración de APPN sobre ATM	69
Configuración de APPN con SDLC	72
Configuración de APPN sobre X.25	79
Configuración de APPN sobre Frame Relay	84
Configuración de APPN sobre BAN Frame Relay	85
Configuración de APPN sobre MPC+	86
Configuración del soporte del Enterprise Extender para el HPR sobre IP	87
Configuración de redes de conexiones sobre HPR sobre IP	87
Configuración de un Extended Border Node	88
<b>Utilización de TN3270</b>	<b>89</b>
Visión general	89
Colocación de la función de servidor TN3270	90
Función de servidor TN3270E	90
Colocación en antememoria de Host On-Demand Client en TN3270	93
Configuración general del servidor TN3270E	94
Carga del código de servidor TN3270	94
Cómo configurar TN3270 bajo el protocolo APPN	94
Dirección IP de servidor	95
Puertos TCP de servidor	95
Definición de PU	96
Definición de LU	97
LU configuradas	98
Definición dinámica de LU dependientes (DDDLU)	99
Definición dinámica iniciada por sistema principal de LU dependientes (HIDLU)	102
Correlación de cliente con LU	103
Correlación de dirección IP de cliente con LU/grupación	104
Asociación de puerto TCP de servidor con agrupación	107
Combinación de correlación de puerto y correlación de dirección IP	108
Equilibrio de carga entre diversas PU	109
Configuraciones de ejemplo	109
Configuración de TN3270 con DLUR	110
Configuración de TN3270E con conexión de subárea	113
Otras configuraciones de ejemplo	116
<b>Configuración y supervisión de APPN</b>	<b>119</b>
Acceso al proceso de configuración de APPN	119
Resumen de los mandatos de configuración de APPN	119

Información detallada sobre los mandatos de configuración de APPN . . . . .	121
Enable/Disable . . . . .	121
Set . . . . .	121
Add . . . . .	157
Delete . . . . .	219
List . . . . .	219
Activate_new_config . . . . .	219
TN3270E . . . . .	220
Supervisión de APPN . . . . .	232
Acceso a los mandatos de supervisión de APPN . . . . .	232
Mandatos de supervisión de APPN . . . . .	232
Información detallada sobre los mandatos de supervisión de APPN . . . . .	237
Mandatos de supervisión de TN3270E . . . . .	276
Deactivate LU . . . . .	276
List . . . . .	277
Soporte de la reconfiguración dinámica de APPN . . . . .	288
Mandato Delete Interface de CONFIG (Talk 6) . . . . .	288
Mandato Activate Interface de GWCON (Talk 5) . . . . .	288
Mandato Reset Interface de GWCON (Talk 5) . . . . .	288
Mandatos Reset de GWCON (Talk 5) del componente . . . . .	288
Mandatos Activate de CONFIG (Talk 6) . . . . .	289
<b>Utilización de AppleTalk Phase 2 . . . . .</b>	<b>291</b>
Procedimientos básicos de la configuración . . . . .	291
Habilitación de parámetros de direccionador . . . . .	291
Establecimiento de parámetros de red . . . . .	292
AppleTalk sobre PPP . . . . .	292
Filtros de zona de AppleTalk 2 . . . . .	293
Información general . . . . .	293
Razón de los filtros de nombre de zona . . . . .	293
¿Cómo se añaden los filtros? . . . . .	294
Procedimientos de la configuración de muestra . . . . .	294
<b>Configuración y supervisión de AppleTalk Phase 2 . . . . .</b>	<b>299</b>
Acceso al entorno de configuración de AppleTalk Phase 2 . . . . .	299
Mandatos de configuración de AppleTalk Phase 2 . . . . .	299
Add . . . . .	300
Delete . . . . .	301
Disable . . . . .	302
Enable . . . . .	304
List . . . . .	305
Set . . . . .	307
Acceso al entorno de supervisión de AppleTalk Phase 2 . . . . .	308
Mandatos de supervisión de AppleTalk Phase 2 . . . . .	308
Atecho . . . . .	309
Cache . . . . .	310
Clear Counters . . . . .	310
Counters . . . . .	311
Dump . . . . .	311
Interface . . . . .	312
<b>Utilización de VINES . . . . .</b>	<b>313</b>
Visión general de VINES . . . . .	313
VINES sobre protocolos e interfaces de direccionador . . . . .	313

Nodos de servicio y clientes	313
Protocolos de capa de red VINES	314
VINES Internet Protocol (VINES IP)	314
Routing Update Protocol (RTP)	316
Internet Control Protocol (ICP)	319
VINES Address Resolution Protocol (VINES ARP)	319
Procedimientos básicos de la configuración	321
Ejecución de Banyan VINES en el direccionador con función de puente	321
Ejecución de Banyan VINES sobre enlaces WAN	321
<b>Configuración y supervisión de VINES</b>	<b>323</b>
Acceso al entorno de configuración de VINES	323
Mandatos de configuración de VINES	323
Add	323
Delete	324
Disable	324
Enable	325
List	325
Set	326
Acceso al entorno de supervisión de VINES	327
Mandatos de supervisión de VINES	327
Counters	328
Dump	329
Route	331
<b>Utilización de DNA IV</b>	<b>333</b>
Visión general de DNA IV	333
Terminología y conceptos de DNA IV	334
Direccionamiento	335
Tablas de direccionamiento	336
Direccionadores de áreas	336
Configuración de parámetros de direccionamiento	337
Implementación de DNA IV por parte de IBM	337
Gestión del tráfico mediante el control del acceso	338
Gestión del tráfico mediante filtros de direccionamiento de áreas	342
Configuración de DNA IV	346
<b>Configuración y supervisión de DNA IV</b>	<b>351</b>
Mandatos de configuración y supervisión de DNA IV	351
Define/Set	352
Purge	362
Set	362
Show	363
Show/List	365
Zero	371
<b>Utilización de OSI/DECnet V</b>	<b>373</b>
Visión general de OSI	373
Sistema de dirección NSAP	374
IDP	375
DSP	375
Formato de sistema de dirección IS-IS	375
NSAP del GOSIP Versión 2	376
Direcciones de vertimiento múltiple	376



Direccionamiento de OSI . . . . .	377
Protocolo IS-IS . . . . .	377
Áreas IS-IS . . . . .	378
Dominio IS-IS . . . . .	378
Mensaje hello de IS a IS (IIH) . . . . .	380
Mensaje IIH de L1 . . . . .	380
Mensaje IIH de L2 . . . . .	381
Mensaje IIH punto a punto . . . . .	381
IS designado . . . . .	381
Bases de datos de estado de los enlaces . . . . .	382
Tablas de direccionamiento . . . . .	383
Codificación de prefijos de dirección . . . . .	386
Contraseñas de autenticación . . . . .	387
Protocolo ESIS . . . . .	387
Mensaje hello . . . . .	388
Mensaje hello de sistema final (ESH) . . . . .	388
Mensajes hello de sistema intermedio (ISH) . . . . .	388
Circuitos X.25 para DECnet V/OSI . . . . .	388
Circuitos de direccionamiento . . . . .	388
Filtros . . . . .	389
Plantillas . . . . .	389
Inicialización del enlace . . . . .	390
Configuración de OSI/DECnet V . . . . .	390
Procedimiento básico de la configuración . . . . .	390
Configuración de OSI sobre una LAN Ethernet o Red en Anillo FDDI . . . . .	391
Configuración de OSI sobre X.25 ó Frame Relay . . . . .	391
Configuración de un direccionador de DNA V para un entorno de DNA IV . . . . .	391
Consideraciones sobre los algoritmos de DNA IV y DNA V . . . . .	392
<b>Configuración y supervisión de OSI/DECnet V . . . . .</b>	<b>393</b>
Acceso al entorno de configuración de OSI . . . . .	393
Mandatos de configuración de OSI/DECnet V . . . . .	393
Add . . . . .	394
Change . . . . .	401
Clear . . . . .	403
Delete . . . . .	404
Disable . . . . .	406
Enable . . . . .	407
List . . . . .	407
Set . . . . .	414
Acceso al entorno de supervisión de OSI/DECnet V . . . . .	421
Mandatos de supervisión de OSI/DECnet V . . . . .	421
Addresses . . . . .	422
Change Metric . . . . .	423
CLNP-Stats . . . . .	423
Designated-router . . . . .	425
DNAV-info . . . . .	425
ES-Adyacencias . . . . .	426
ES-IS-Stats . . . . .	426
IS-Adyacencias . . . . .	429
IS-IS-Stats . . . . .	429
L1-Routes . . . . .	431
L2-Routes . . . . .	431
L1-Summary . . . . .	432

L2-Summary	433
L1-Update	433
L2-Update	434
Ping-1139	435
Route	435
Send (Echo Packet)	436
Subnets	436
Toggle (Alias/No Alias)	437
Traceroute	437
<b>Utilización de NHRP</b>	<b>439</b>
Visión general de Next Hop Resolution Protocol (NHRP)	439
Ventajas de NHRP y la implementación por parte de IBM	440
Características del rendimiento	441
Ejemplos de configuraciones de NHRP	442
Implementación de NHRP	446
Parámetros de configuración	448
<b>Configuración y supervisión de NHRP</b>	<b>455</b>
Acceso al proceso de configuración de NHRP	455
Mandatos de configuración de NHRP	455
Enable NHRP	456
Disable NHRP	456
Advanced Config	456
List	456
Mandatos de configuración avanzada de NHRP	457
Add	458
Delete	459
Change	460
List	461
Set	462
Acceso al proceso de supervisión de NHRP	466
Mandatos de supervisión de NHRP	466
Box Status	466
Interface Status	467
Statistics	467
Cache	468
Server_purge_cache	468
MIB	468
LANE Shortcuts	469
CONFIG Parameters	470
Reset	471
Rastreo de paquetes de NHRP	472
Soporte de la reconfiguración dinámica de servidor de NHRP	473
Mandato Delete Interface de CONFIG (Talk 6)	473
Mandato Activate Interface de GWCON (Talk 5)	473
Mandato Reset Interface de GWCON (Talk 5)	473
<b>Utilización de IP Versión 6 (IPv6)</b>	<b>475</b>
Visión general de IPv6	475
Comparación de IPv6 con IPv4	475
Sistema de dirección IPv6	476
Formato de dirección IPv6	476
Representación textual de los prefijos de dirección	477

Formato de cabecera de IPv6	477
Tamaño mínimo de MTU en IPv6	477
Necesidad de Path MTU Discovery en IPv6	477
Necesidad de la Seguridad en IPv6	478
Neighbor Discovery Protocol (NDP) en IPv6	478
Descubrimiento de direccionadores y prefijos	478
Configuración automática de direcciones	479
Resolución de direcciones	479
Detección de inasequibilidad de contiguo	479
Redireccionamiento	479
Función de túnel de IPv6 sobre IPv4	479
Protocol Independent Multicast (PIM)	480
<b>Configuración y supervisión de IPv6</b>	<b>481</b>
Acceso al entorno de configuración de IPv6	481
Mandatos de configuración de IPv6	481
Add	482
Change	489
Delete	489
Disable	489
Enable	490
List	490
Move	493
Set	493
Update	497
Mandatos de Update Packet-filter	497
Acceso al entorno de supervisión de IPv6	502
Mandatos de supervisión de IPv6	502
Access-control	503
Cache	504
Counters	504
Dump routing tables	504
Interface addresses	505
Internal address	505
Mcast	505
Mld	506
Reset	506
Route	506
Sizes	506
Sniffer	507
Static routes	507
Packet-filter	507
Path-mtu	508
Ping6	508
Traceroute6	509
Tunnels	510
Soporte de la reconfiguración dinámica de IPv6	510
Mandato Delete Interface de CONFIG (Talk 6)	510
Mandato Activate Interface de GWCON (Talk 5)	510
Mandato Reset Interface de GWCON (Talk 5)	510
Mandatos Reset de GWCON (Talk 5) del componente	511
Mandatos de CONFIG (Talk 6) de cambio inmediato	511
<b>Configuración y supervisión de Neighbor Discovery Protocol (NDP)</b>	<b>513</b>

Acceso al entorno de configuración de NDP	513
Mandatos de configuración de NDP	513
Add	514
Change	516
Delete	518
Disable	518
Enable	519
List	519
Set	519
Acceso al entorno de supervisión de NDP	520
Mandatos de supervisión de NDP	520
DHCPv6-Relay	520
Dump	521
List	521
Ping6	521
Soporte de la reconfiguración dinámica de NDP6	521
Mandato Delete Interface de CONFIG (Talk 6)	521
Mandato Activate Interface de GWCON (Talk 5)	522
Mandato Reset Interface de GWCON (Talk 5)	522
Mandatos Reset de GWCON (Talk 5) del componente	522
<b>Configuración y supervisión del protocolo de direccionamiento Protocol Independent Multicast (PIM)</b>	
Utilización de PIM	525
Acceso al entorno de configuración de PIM	526
Mandatos de configuración de PIM	527
Delete	527
Disable	527
Enable	527
List	528
Set	529
Acceso al entorno de supervisión de PIM	532
Mandatos de supervisión de PIM	532
Dump routing tables	533
Clear	534
Interface	534
Join	535
Leave	535
Mcache	535
Mgroups	536
Mstats	536
Neighbor	538
PIM	539
Summary PIM	539
Ping	540
Reset	540
Traceroute	540
Variables	540
Soporte de la reconfiguración dinámica de PIM	541
Mandato Delete Interface de CONFIG (Talk 6)	541
Mandato Activate Interface de GWCON (Talk 5)	541
Mandato Reset Interface de GWCON (Talk 5)	542
Mandatos Reset de GWCON (Talk 5) del componente	542
Soporte de la reconfiguración dinámica de PIM para IPv6	542

Mandato Delete Interface de CONFIG (Talk 6) . . . . .	542
Mandato Activate Interface de GWCON (Talk 5) . . . . .	542
Mandato Reset Interface de GWCON (Talk 5) . . . . .	543
Mandatos Reset de GWCON (Talk 5) del componente . . . . .	543
Soporte de la reconfiguración dinámica de Multicast Forwarding Cache . . . . .	543
Mandato Delete Interface de CONFIG (Talk 6) . . . . .	543
Mandato Activate Interface de GWCON (Talk 5) . . . . .	544
Mandato Reset Interface de GWCON (Talk 5) . . . . .	544
Mandatos no reconfigurables dinámicamente . . . . .	544
Soporte de la reconfiguración dinámica de Multicast Forwarding Cache V6 . . . . .	544
Mandato Delete Interface de CONFIG (Talk 6) . . . . .	544
Mandato Activate Interface de GWCON (Talk 5) . . . . .	544
Mandato Reset Interface de GWCON (Talk 5) . . . . .	545
Mandatos no reconfigurables dinámicamente . . . . .	545
<b>Configuración y supervisión de Routing Information Protocol (RIP6) . . . . .</b>	<b>547</b>
Acceso al entorno de configuración de RIP6 . . . . .	547
Mandatos de configuración de RIP6 . . . . .	547
Add . . . . .	548
Change . . . . .	548
Delete . . . . .	551
Disable . . . . .	551
Enable . . . . .	553
List . . . . .	554
Set . . . . .	554
Acceso al entorno de supervisión de RIP6 . . . . .	557
Mandatos de supervisión de RIP6 . . . . .	558
Dump . . . . .	558
List . . . . .	558
Ping6 . . . . .	559
Reset . . . . .	559
Traceroute6 . . . . .	559
Soporte de la reconfiguración dinámica de RIP6 . . . . .	559
Mandato Delete Interface de CONFIG (Talk 6) . . . . .	559
Mandato Activate Interface de GWCON (Talk 5) . . . . .	559
Mandato Reset Interface de GWCON (Talk 5) . . . . .	560
Mandatos Reset de GWCON (Talk 5) del componente . . . . .	560
Mandatos de CONFIG (Talk 6) de cambio inmediato . . . . .	560
Mandatos no reconfigurables dinámicamente . . . . .	560
<b>Configuración y supervisión de BGP6 . . . . .</b>	<b>561</b>
Acceso al entorno de configuración de BGP6 . . . . .	561
Mandatos de configuración de BGP6 . . . . .	561
Add . . . . .	562
Attach . . . . .	569
Change . . . . .	569
Delete . . . . .	571
Disable . . . . .	573
Enable . . . . .	573
List . . . . .	574
Move . . . . .	576
Set . . . . .	577
Update . . . . .	577
Acceso al entorno de supervisión de BGP6 . . . . .	579

Mandatos de supervisión de BGP6	579
Disable Neighbor	580
Dump Routing Tables	581
Enable Neighbor	581
List	581
Neighbors	584
Parameter	586
Paths	586
Ping6	587
Policy-List	587
Reset Neighbor	588
Sizes	588
Traceroute6	589
Soporte de la reconfiguración dinámica de BGP6	589
Mandato Delete Interface de CONFIG (Talk 6)	589
Mandato Activate Interface de GWCON (Talk 5)	589
Mandato Reset Interface de GWCON (Talk 5)	589
Mandatos Reset de GWCON (Talk 5) del componente	589
Mandatos de GWCON (Talk 5) de cambio temporal	590
Mandatos no reconfigurables dinámicamente	590
<b>Apéndice A. Tamaños de los paquetes</b>	591
Datos generales	591
Límites de tamaño específicos de las redes	591
Límites de tamaño específicos de los protocolos	592
Longitudes de paquete de IP	592
Cómo cambiar los tamaños máximos de los paquetes	593
<b>Apéndice B. Lista de Abreviaturas</b>	595
<b>Glosario</b>	605
<b>Índice</b>	633

---

## Figuras

1.	Conectividad del Extended Border Node	19
2.	Flujo de datos de una configuración de APPN con puerto DLSw	46
3.	Vista lógica con soporte de red de conexiones BAN/trama de puente de Frame Relay	47
4.	Red de conexiones APPN BAN/trama de puente de Frame Relay	48
5.	Red de conexiones individual que utiliza BAN con 1 puerto Frame Relay	49
6.	Red de conexiones individual que utiliza BAN con diversos puertos Frame Relay	49
7.	Diversas redes de conexiones que utilizan BAN	49
8.	Red de conexiones individual que utiliza la función de puente con un puerto Frame Relay	50
9.	Red de conexiones individual que utiliza la función de puente con diversos puertos Frame Relay	50
10.	Diversas redes de conexiones que utilizan la función de puente	51
11.	Ejemplo de filtración de zonas	296
12.	Ejemplo de filtración de redes	298
13.	Tabla de direccionamiento de muestra	317
14.	Tabla de contiguos de muestra	318
15.	Ejemplo del control del acceso inclusivo	340
16.	Ejemplo del control del acceso exclusivo	341
17.	Ejemplo del filtro de direccionamiento de áreas para la seguridad	343
18.	Ejemplo de la combinación de dominios DECnet	346
19.	Red OSI	373
20.	Estructura de una dirección NSAP	374
21.	Interpretación del sistema de dirección NSAP en IS-IS	375
22.	Formato de dirección GOSIP	376
23.	Dominio OSI	379
24.	Áreas sinónimas	380
25.	Métricas del direccionamiento interna y externa	386
26.	Visión general de Next Hop Resolution Protocol (NHRP)	439
27.	NHRP en un entorno de IP clásico	442
28.	NHRP en un entorno de IP clásico con dispositivo sin NHRP	443
29.	NHRP en un entorno de ELAN	444
30.	NHRP en un entorno de ELAN con conmutadores de LAN	445
31.	NHRP en un entorno mixto de IP clásico y ELAN	445
32.	NHRP para un direccionador de salida	446
33.	Utilización de atajos de direccionador a direccionador anulados	451





## Tablas

1.	Funciones de código soportadas en el 2216 Modelo 400 y en Network Utility . . . . .	xxix
2.	Implementación de funciones de nodo de red APPN . . . . .	4
3.	Tipos de puertos soportados para el direccionamiento de APPN . . . . .	25
4.	Valores de tipo de dispositivo/modelo . . . . .	102
5.	Resumen de los mandatos de configuración de APPN . . . . .	119
6.	Lista de parámetros de configuración - Direccionamiento de APPN . . . . .	121
7.	Lista de parámetros de configuración - Direccionamiento de alto rendimiento (HPR) . . . . .	128
8.	Lista de parámetros de configuración - Opciones de temporizadores y reintentos de HPR . . . . .	128
9.	Lista de parámetros de configuración - Peticionario de LU dependientes . . . . .	131
10.	Lista de parámetros de configuración - Ajuste de nodo APPN . . . . .	134
11.	Lista de parámetros de configuración - Opciones de configuración de rastreo . . . . .	139
12.	Lista de parámetros de configuración - Rastros de nivel de nodo . . . . .	140
13.	Lista de parámetros de configuración - Rastros de señales interprocesos . . . . .	144
14.	Lista de parámetros de configuración - Rastros de entrada y salida de módulos . . . . .	147
15.	Lista de parámetros de configuración - Rastros generales de nivel de componente . . . . .	149
16.	Lista de parámetros de configuración - Rastros varios . . . . .	153
17.	Lista de parámetros de configuración - Gestión de nodo APPN . . . . .	155
18.	Lista de parámetros de configuración - Soporte para el registro del ISR de APPN . . . . .	156
19.	Lista de parámetros de configuración - Configuración de puerto . . . . .	158
20.	Lista de parámetros de configuración - Configuración de puerto para ATM . . . . .	161
21.	Lista de parámetros de configuración - Definición de puerto . . . . .	166
22.	Lista de parámetros de configuración - Características de TG de puerto por omisión . . . . .	170
23.	Lista de parámetros de configuración - Características de LLC de puerto por omisión . . . . .	175
24.	Lista de parámetros de configuración - Valores por omisión de alteración temporal de HPR . . . . .	178
25.	Lista de parámetros de configuración - Estación de enlace - Información detallada . . . . .	179
26.	Lista de parámetros de configuración - Configuración de estación para ATM . . . . .	189
27.	Lista de parámetros de configuración - Modificación de características de TG . . . . .	193
28.	Lista de parámetros de configuración - Modificación del Servidor de LU dependientes . . . . .	195
29.	Lista de parámetros de configuración - Modificación de características de LLC . . . . .	196
30.	Lista de parámetros de configuración - Modificación de valores por omisión de HPR . . . . .	198
31.	Lista de parámetros de configuración - Nombre de LU de nodo final LEN . . . . .	200

32.	Lista de parámetros de configuración - Red de conexiones - Información detallada . . . . .	201
33.	Lista de parámetros de configuración - Configuración de red de conexiones para ATM . . . . .	203
34.	Lista de parámetros de configuración - Características de TG (Red de conexiones) . . . . .	206
35.	Lista de parámetros de configuración - COS de APPN - Correlación de nombre de modalidad con nombre de COS - Información detallada . . . . .	209
36.	Lista de parámetros de configuración - Puerto adicional APPN para red de conexiones . . . . .	210
37.	Lista de parámetros de configuración - Punto focal implícito APPN . . . . .	211
38.	Lista de parámetros de configuración - PU local de APPN . . . . .	211
39.	Lista de parámetros de configuración - Configuración de lista de direccionamiento . . . . .	214
40.	Lista de parámetros de configuración - Configuración de tabla de correlación de COS . . . . .	217
41.	Resumen de los mandatos de configuración de TN3270E . . . . .	220
42.	Lista de parámetros de configuración - Establecimiento de TN3270E . . . . .	220
43.	Lista de parámetros de configuración - Adición de agrupación implícita de TN3270E . . . . .	223
44.	Lista de parámetros de configuración - Adición de LU de TN3270E . . . . .	225
45.	Lista de parámetros de configuración - Adición de correlación de TN3270E . . . . .	228
46.	Lista de parámetros de configuración - Adición de puerto TN3270E . . . . .	229
47.	Lista de parámetros de configuración - Supresión de LU de TN3270E . . . . .	230
48.	Lista de parámetros de configuración - Supresión de agrupación implícita de TN3270E . . . . .	230
49.	Lista de parámetros de configuración - Supresión de correlación de TN3270E . . . . .	231
50.	Lista de parámetros de configuración - Supresión de puerto TN3270E . . . . .	231
51.	Resumen de los mandatos de supervisión de APPN . . . . .	232
52.	Resumen de los mandatos de supervisión del Servidor TN3270E . . . . .	236
53.	Distintivos . . . . .	237
54.	Descripción de la salida de APING . . . . .	238
55.	Descripción de la salida de List appc_sessions . . . . .	240
56.	Descripción de la salida . . . . .	241
57.	Descripción de la salida de List dlur-dlus . . . . .	242
58.	Descripción de la salida de List dlur lu . . . . .	243
59.	Descripción de la salida . . . . .	244
60.	Descripción de la salida . . . . .	246
61.	Descripción de la salida . . . . .	246
62.	Descripción de la salida . . . . .	247
63.	Descripción de la salida . . . . .	248
64.	Descripción de la salida . . . . .	249
65.	Descripción de la salida . . . . .	250
66.	Descripción de la salida . . . . .	250
67.	Descripción de la salida . . . . .	252
68.	Descripción de la salida . . . . .	253
69.	Descripción de la salida . . . . .	254
70.	Descripción de la salida . . . . .	255
71.	Tabla de asociados . . . . .	256
72.	Tabla de conexiones . . . . .	257
73.	Descripción de la salida . . . . .	259
74.	Descripción de la salida . . . . .	261

75.	Descripción de la salida	261
76.	Descripción de la salida	262
77.	Descripción de la salida	264
78.	Descripción de la salida	264
79.	Descripción de la salida	265
80.	Descripción de la salida	266
81.	Sintaxis del submenú <b>Log view</b>	267
82.	Descripción de la salida (la página de resumen, de izquierda a derecha)	268
83.	Descripción de la salida (la información detallada de un suceso)	269
84.	Descripción de la salida	270
85.	Descripción de la salida	273
86.	Descripción de la salida	274
87.	Resumen de los mandatos de supervisión de TN3270E	276
88.	Descripción de los distintivos	277
89.	Descripción de la salida	278
90.	Descripción de la salida	279
91.	Descripción de la salida	280
92.	Descripción de la salida	281
93.	Descripción de la salida	281
94.	Descripción de la salida	283
95.	Descripción de la salida	283
96.	Descripción de la salida	284
97.	Descripción de la salida	286
98.	Descripción de la salida	286
99.	Resumen de los mandatos de configuración de AppleTalk Phase 2	300
100.	Resumen de los mandatos de supervisión de AppleTalk Phase 2	309
101.	Resumen de los campos de cabecera de Vines IP	315
102.	Estados de los nodos clientes y los nodos de servicio VINES ARP	320
103.	Resumen de los mandatos de configuración de VINES	323
104.	Resumen de los mandatos de supervisión de VINES	327
105.	Consideraciones sobre los algoritmos de DNA IV y DNA V	347
106.	Mandatos de configuración y supervisión del NCP	351
107.	Direcciones de vertimiento múltiple en IS-IS	377
108.	Resumen de los mandatos de configuración de OSI	393
109.	Resumen de los mandatos de supervisión de OSI/DECnet V	421
110.	Resumen de los mandatos de configuración de NHRP	455
111.	Resumen de los mandatos de configuración avanzada de NHRP	458
112.	Resumen de los mandatos de supervisión de NHRP	466
113.	Resumen de los parámetros de configuración de NHRP	470
114.	Resumen de los mandatos de configuración de IPv6	482
115.	Resumen de los mandatos de configuración de Update Packet-filter	497
116.	Resumen de los mandatos de supervisión de IPv6	503
117.	Resumen de los mandatos de configuración de NDP	514
118.	Resumen de los mandatos de supervisión de NDP	520
119.	Resumen de los mandatos de configuración de PIM	527
120.	Resumen de los mandatos de supervisión de PIM	533
121.	Resumen de los mandatos de configuración de RIP6	548
122.	Resumen de los mandatos de supervisión de RIP6	558
123.	Resumen de los mandatos de configuración de BGP6	562
124.	Resumen de los mandatos de supervisión de BGP6	580
125.	Tamaño máximo por omisión de paquete específico de la red	592



---

## Avisos

Es posible que en otros países IBM no ofrezca los productos, servicios o funciones que se describen en este documento. Consulte al representante local de IBM para obtener información sobre los productos y servicios actualmente disponibles en su localidad. Las referencias a un producto, programa o servicio de IBM no pretenden afirmar ni implicar que sólo pueda utilizarse el mencionado producto, programa o servicio de IBM. En su lugar, puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no vulnere ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patentes pendientes que cubran los temas tratados en este documento. La entrega de este documento no otorga ninguna licencia sobre estas patentes. Puede enviar consultas sobre licencias, por escrito, a:

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

Para las consultas sobre licencias referentes a información del juego de caracteres de doble byte (DBCS), póngase en contacto con el Departamento de la Propiedad Intelectual de IBM de su país o envíe consultas, por escrito, a:

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

El párrafo siguiente no es aplicable al Reino Unido ni a ningún país en el que tales disposiciones sean incompatibles con la legislación local: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGUNA CLASE, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VIOLACIÓN DE DERECHOS, COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN DETERMINADO. Algunos estados no permiten, en determinadas transacciones, la declaración de limitación de responsabilidad respecto a garantías explícitas o implícitas, por lo que es posible que esta declaración no sea aplicable en su caso.



---

## Marcas registradas

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

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

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

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

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

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

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





---

## Prefacio

Este manual pertenece a la biblioteca de productos descrita en el apartado “Visión general de la biblioteca” en la página xxv y describe un grupo de los protocolos soportados por el 2216 y el programa Network Utility. Es posible que un 2216 o Network Utility específicos no den soporte a todos los protocolos descritos en estos manuales. Si un protocolo o una función son específicos de un dispositivo, se indica esta restricción en el manual correspondiente o en el prefacio del manual *Guía del usuario de software*. Consulte el prefacio del manual *Guía del usuario de software* para ver la tabla que muestra todas las funciones y protocolos soportados por el programa Network Utility.

En este manual, el 2216 viene referido como “el direccionador” o como “el dispositivo”. Los ejemplos de la biblioteca representan la configuración de un 2216, pero la salida real que visualice puede ser diferente. Utilice los ejemplos como una directriz de lo que puede visualizar mientras configure el dispositivo.

---

## A quién va dirigido este manual

Este manual está pensado para las personas que instalan redes de sistema y se sirven de éstas. Aunque es útil estar familiarizado con el hardware y software de redes de sistema, no es necesaria experiencia en programación para utilizar el software de protocolo.

---

## Obtención de información adicional

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

---

## Acerca del software

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

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

El código base viene instalado de fábrica en el 2216.

- El Programa de configuración para IBM Nways Multiprotocol Access Services (denominado en este manual: *Programa de configuración*) es una interfaz

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

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

También puede obtener el Programa de configuración para IBM Nways Multiprotocol Access Services a partir de la página de presentación del soporte técnico de la red de IBM. Consulte el manual *Guía del usuario del programa de configuración para Nways Multiprotocol and Access Services*, GC10-3430, para obtener la dirección de servidor y los directorios.

---

## Convenios utilizados en este manual

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

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

reload

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

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

mandato [palabraclave1 o palabraclave2]

Elija una de las palabras clave como valor del parámetro.

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

time host ...

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

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

Media (UTP/STP) [UTP]

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

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

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

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

6. Los nombres de las teclas del teclado que se pulsán se indican así: **Intro**

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

---

## Visión general de la biblioteca

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

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

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

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

### Planificación

GA27-4105 *IBM 2216 Introduction and Planning Guide*

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

### Instalación

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

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

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

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

### Diagnósticos y mantenimiento

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

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

### Gestión de red y operaciones

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

SC10-3434 *Guía del usuario de software*

En este manual se explica cómo:

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

SC10-3429 *Utilización y configuración de las características*

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

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

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

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

SC10-3431 *Guía de mensajes del sistema para el registro cronológico de sucesos*

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

## **Configuración**

GC10-3430 *Guía del usuario del programa de configuración para Nways Multiprotocol and Access Services*

Este manual describe cómo utilizar el Programa de configuración.

## **Seguridad**

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

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

## **Marketing**

La siguiente página Web de IBM proporciona información sobre el producto:

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

---

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

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

- Mejoras en Frame Relay:
  - Soporte de un nuevo Manejador de tramas (FH)
  - Regulación de PU para manejar las ráfagas de tráfico en soporte de los controladores 3745
  - Nuevo tipo de interfaz (subinterfaz Frame Relay) para permitir interfaces virtuales en la misma interfaz física
  - Soporte de IP sin número
- Mejoras en VPN:
  - Mejoras en CPE:
    - La información de las políticas de los servidores LDAP se almacena localmente.
    - Configuración rápida de las políticas.
    - Comprobación de la coherencia de las políticas.
    - Ahora la información de las políticas puede recuperarse a partir de los servidores LDAP dentro de un dominio administrativo.
    - Acción de ping para túneles de IPsec.
  - Mejoras en IP:
    - Mejoras en el direccionamiento de voz:
      - Compresión de cabeceras de IP en PPP (RFC 2507, 2508, 2509)
      - Intercalación de tráfico de voz entre paquetes de datos fragmentados en PPP de multienlace
      - Intercalación de tráfico de voz entre paquetes de datos fragmentados en Frame Relay
      - Se ignoran la compresión de paquetes de PPP o Frame Relay y el cifrado para el tráfico de voz
    - Dirección de bucle de retorno IP  
Este soporte permite que los usuarios definan direcciones IP en una interfaz especial para dar soporte a los requisitos de la Pasarela de TN3270, de Network Dispatcher y de IPsec.
    - IPv6
      - Se proporciona una función de direccionamiento interdominios (BGP4+) para IPv6 que da soporte a información sobre el direccionamiento y el sistema de dirección IPv6 y utiliza TCP6 para el transporte.
      - Se da soporte al tráfico de IPv6 sobre la emulación de LAN de ATM Ethernet sin encapsulación ni función de túnel.
    - Diversas vías de acceso de reenvío  
El direccionamiento de IP puede utilizar hasta cuatro rutas estáticas de igual coste para dar soporte a diversos enlaces paralelo con una dirección y una máscara determinadas.
    - Agregación de ruta IP
    - Mejoras en el vertimiento múltiple:

## Resumen de los cambios

- Protocol Independent Multicast-Dense Mode (PIM-DM) para IPv4.
- Ahora los administradores de red pueden controlar el flujo de datos de vertimiento múltiple de IP hacia dentro y hacia fuera de las redes utilizando filtros de tráfico de entrada y de salida.
- Área NSSA (Not-so-stubby area)

OSPF da soporte al área NSSA (Not-so-stubby area) tal como se ha definido en RFC 1587 y ahora está soportado el borrador de Internet más reciente.
- Random Early Detection (RED)
- Mejoras en la supervisión de los servicios diferenciales
- Mejoras en VRRP:
  - Puede utilizarse la dirección MAC de hardware en lugar de una dirección MAC virtual para identificar una pasarela redundante; esto puede ofrecer una mejora del rendimiento.
  - Cuando hay más de una elección disponible como reserva, pueden configurarse opciones de adelantamiento.
  - Para seleccionar el direccionador de IP maestro, pueden utilizarse criterios adicionales, como, por ejemplo, la ruta o la interfaz de red disponibles, con el fin de dar soporte a funciones que son diferentes de IP.
- Interfaz alternativa de marcación bajo pedido para el redireccionamiento de WAN
- Mejoras en TN3270
  - Selección de LU
  - Equilibrio de carga de las agrupaciones de LU
  - Desconexión de Talk 5 de las sesiones TN3270
  - Información de notificación adicional
  - Soporte de las direcciones 1 y 255
- Mejoras en Network Dispatcher
  - Anuncio de las direcciones de cluster de asignador de tareas de red mediante protocolos de direccionamiento
  - Un nuevo SSL Advisor
- Soporte de PU1 en SDLC con DLSw
- Soporte de encapsulación de Ethernet para el tipo II de Ethernet (valor por omisión) y para Ethernet 802.3 de forma simultánea en la misma interfaz
- Mejoras en DHCP:
  - Copia de seguridad de disco fijo de la información sobre alquileres
  - Soporte de diversas direcciones IP para las interfaces DHCP
  - Soporte de alquiler corto
- Mejoras en RADIUS
  - Escalabilidad de Radius
  - Inicio de sesión del último recurso
- Escalabilidad de L2TP

- Mejora en Thin Server  
Conexión con un servidor maestro de reserva o alternativo
- Mejoras en la recuperación de archivos de servicio

## Network Utility

El producto Network Utility consta de varios modelos del 2216. Proporciona varios subconjuntos de las funciones del 2216, tal como muestra la Tabla 1.

## Funciones de software soportadas por Network Utility

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

<i>Tabla 1 (Página 1 de 3). Funciones de código soportadas en el 2216 Modelo 400 y en Network Utility</i>				
<b>Función o protocolo</b>	<b>Disponible para el 2216 Modelo 400 Base</b>	<b>Disponible para la WSC del 2216 Modelo 400</b>	<b>Disponible para Network Utility Modelo TN1</b>	<b>Disponible para Network Utility Modelo TX1</b>
TN3720E	Sí <sup>1</sup>	—	Sí <sup>1</sup>	—
Antememoria de IBM eNetwork Host on-Demand Client en TN3720E	Sí <sup>1</sup>	—	Sí <sup>1</sup>	—
Definición de LU dinámica iniciada por sistema principal para TN3720E	Sí <sup>1</sup>	—	Sí <sup>1</sup>	—
Múltiples SA de PU sobre DLSw para TN3720E	Sí <sup>1</sup>	—	Sí <sup>1</sup>	—
Network Dispatcher	Sí	Sí	Sí	Sí
Server Advisor (o Network Dispatcher Advisor) para TN3720E	Sí	Sí <sup>2</sup>	Sí	Sí <sup>2</sup>
Reserva de ancho de banda y puesta en cola según prioridad	Sí	Sí	Sí	Sí
Fragmentación de paquetes de Frame Relay	Sí	Sí	Sí	Sí
Reenvío de paquetes de Voz sobre Frame Relay	Sí	Sí	Sí	Sí
Filtración del MAC	Sí	Sí	Sí	Sí
Restauración de WAN	Sí	Sí	—	—
Redireccionamiento de WAN	Sí	Sí	—	—
Compresión de datos	Sí	Sí	Sí	Sí

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

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



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

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

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

## Cómo obtener ayuda

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

## Cómo salir de un entorno de nivel inferior

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

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

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

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



---

## Utilización de APPN

Este capítulo describe APPN® e incluye los apartados siguientes:

- “¿Qué es APPN?”
- “¿Qué funciones de APPN están implementadas en el direccionador?” en la página 4
- “Funciones opcionales de nodo de red APPN” en la página 7
- “DLC soportados” en la página 24
- “Proceso de configuración del direccionador” en la página 25
- “Notas de configuración de APPN” en la página 52

---

### ¿Qué es APPN?

Advanced Peer-to-Peer Networking® (APPN) supone una extensión de la arquitectura SNA al permitir que los nodos de tipo 2.1 (T2.1) se comuniquen directamente sin que necesiten los servicios de un sistema principal SNA.

### Comunicaciones de igual a igual

Los nodos T2.1 pueden activar conexiones con otros nodos T2.1 y establecer sesiones de LU-LU con otros nodos. La relación entre un par de nodos T2.1 viene referida como *relación de igual* porque cualquier parte puede iniciar la comunicación.

Antes de APPN, un nodo T2.1 podía comunicarse directamente con otro nodo T2.1, pero necesitaba los servicios de un sistema principal SNA centralizado para ubicar a su asociado y cualquier recurso relacionado. Todas las rutas entre los dos nodos estaban predefinidas. APPN ha mejorado la función de un nodo T2.1 de la siguiente manera:

- Haciendo necesario que cada recurso de red sólo esté definido en el nodo en que se ubique
- Distribuyendo información sobre estos recursos por toda la red según se necesite
- Generando rutas dinámicamente entre los nodos que utilicen la información actual sobre la topología de la red y la clase de servicio que desean

### Tipos de nodos APPN

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

- Nodos de red APPN
- Nodos finales APPN
- Nodos finales de red de entrada baja (LEN)
- Nodos de PU 2.0 soportados por la función DLUR

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

### Nodo de red APPN

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

- Los recursos locales que posee el nodo
- Un punto de control (CP), que gestiona los recursos del nodo
- Los recursos que poseen los nodos finales APPN y nodos finales LEN que utilizan los servicios del nodo de red

Los nodos de red APPN también:

- Intercambian información sobre la topología de la red. Esta información se intercambia cada vez que los nodos de red establecen una conexión o cuando hay un cambio en la topología de la red (por ejemplo, cuando se desactiva un nodo de red, cuando entra en línea o cuando se congestiona o falla un enlace). Cuando un nodo de red recibe una actualización de topología, difunde esta información a los otros nodos activos y de red con los que tiene sesiones de CP-CP.
- Actúan como nodos intermedios recibiendo datos de sesión de un nodo adyacente y pasando estos datos al siguiente nodo adyacente de la ruta.

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

#### Servicios de directorio

El nodo de red, comunicándose con otros nodos de red, puede ubicar un recurso de la red en nombre de un nodo final APPN. El nodo de red también mantiene un directorio local de recursos de nodo final APPN y LEN en el que puede realizar búsquedas en nombre de un nodo final APPN conectado, un nodo final LEN conectado u otros nodos de red.

#### Servicios de topología y direccionamiento

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

#### Servicios de gestión

El nodo de red puede pasar condiciones de *alerta* a un punto focal designado para permitir una gestión centralizada de los problemas. El nodo de red tiene la responsabilidad de procesar condiciones de alerta para todos los recursos de su dominio. La sección “Gestión de un nodo de red” en la página 21 describe este proceso.

### Nodos finales APPN

Un nodo final APPN proporciona servicios limitados de directorios, direccionamiento y gestión para las unidades lógicas (LU) asociadas con el nodo. Un nodo final APPN selecciona un nodo de red para que sea su servidor de nodos de red. Si el nodo de red acepta actuar como servidor del nodo final APPN, el nodo final puede registrar sus recursos locales con el nodo de red. Esto permite que el servidor de nodos de red intercepte y pase peticiones de búsqueda de recursos ubicados en el nodo final APPN.

El nodo final APPN y su servidor de nodos de red se comunican estableciendo sesiones de CP-CP. Un nodo final APPN puede conectarse con varios nodos de red, pero solamente uno de éstos actúa como servidor del nodo final APPN en cualquier momento.

El nodo final APPN remite todas las peticiones de recursos desconocidos al servidor de nodos de red. El servidor de nodos de red, a su vez, utiliza sus servicios de búsqueda para ubicar el recurso solicitado y calcular una ruta del nodo final APPN al recurso.

### **Nodos LEN**

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

Puesto que un nodo LEN no puede establecer sesiones de CP-CP con un servidor de nodos de red APPN, no puede registrar sus recursos con el servidor ni solicitar que el servidor busque un recurso y calcule dinámicamente una ruta hacia este recurso. Un nodo LEN puede utilizar indirectamente el directorio y los servicios de direccionamiento de un nodo de red si se predefinen LU remotas (propiedad de nodos no adyacentes) como si se ubicaran en un nodo de red APPN, aunque la ubicación real pueda ser cualquier parte de la red. Cuando el nodo LEN tiene que iniciar una sesión con la LU remota, envía una petición de activación de sesión (BIND) para la LU al nodo de red. En este caso, el nodo de red actúa como servidor de nodos de red del nodo LEN localizando el recurso solicitado, calculando una ruta y reenviando la BIND a su destino correcto.

Cuando configure el nodo de red direccionador, puede especificar los nombres de LU que estén asociados con un nodo final LEN conectado. Estos nombres de LU residen en el directorio local del nodo de red direccionador. Si el nodo de red direccionador recibe una petición para que busque uno de estos recursos de nodo final LEN, podrá buscar la LU en su directorio local y devolver una respuesta positiva al nodo que ha originado la búsqueda. Con el fin de reducir el número de nombres de LU que tenga que especificar para un nodo final LEN conectado, el direccionador da soporte al uso de nombres de LU genéricos, que permiten que un carácter comodín represente una parte de un nombre de LU.

### **Nodos de PU 2.0**

Un nodo de PU 2.0 es un nodo de tipo T2.0 que contiene LU dependientes. Los nodos de PU 2.0 están soportados por la función Peticionario de LU dependientes (DLUR) que implementa un nodo de red o nodo final APPN. Los nodos de PU 2.0 necesitan los servicios de un punto de control de servicios del sistema, que está disponible por medio del nodo APPN con habilitación de DLUR. Tenga en cuenta que los nodos APPN pueden contener LU dependientes soportadas por la función DLUR. No obstante, el direccionador no contiene LU dependientes.

## ¿Qué funciones de APPN están implementadas en el direccionador?

El direccionador implementa las funciones de la arquitectura APPN Release 2 base definidas en el manual de consulta de Systems Network Architecture para APPN. Las funciones de nodo de red APPN implementadas por el direccionador están resumidas en la Tabla 2. Después de la tabla, siguen unas notas sobre funciones específicas. Para obtener una descripción de los servicios de gestión de APPN soportados por el direccionador, consulte la sección “Gestión de un nodo de red” en la página 21.

APPN utiliza protocolos de LU 6.2 para proporcionar conectividad de igual entre los asociados a una sesión de CP-CP. El nodo de red direccionador implementa los protocolos de LU 6.2 necesarios para las sesiones de CP-CP y los que se utilizan en las sesiones entre un CP de nodo de red y su punto focal de gestión de red. La implementación de APPN en el direccionador no proporciona una interfaz de programas de aplicación para dar soporte a programas de LU 6.2 escritos por el usuario.

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

<b>Función de APPN</b>	<b>Sí</b>	<b>No</b>	<b>Notas</b>
<b>Funciones de soporte y servicios de sesiones</b>			
Diversas sesiones de CP-CP	X		
Correlación de nombre de modalidad con clase de servicio (CoS)	X		1
Estaciones de enlace de recursos limitados	X		2
Segmentación y reensamblaje de BIND	X		3
Seguridad de nivel de sesión	X		4
<b>Direccionamiento de sesiones intermedias</b>			
Direccionamiento de sesiones intermedias	X		
Direccionamiento de sesiones de LU dependientes	X		
Ritmo de nivel de sesión fijo y adaptable	X		
Segmentación y reensamblaje de RU	X		5
<b>Servicios de directorio</b>			
Búsquedas generalizadas	X		
Búsquedas dirigidas	X		
Colocación de directorios en antememoria	X		
Almacenamiento seguro de la antememoria de servicios de directorio		X	6
Servidor de directorios central		X	7
Cliente de directorios central	X		7
Registro de LU de EN APPN con servidor de nodos de red	X		
Definición de LU de nodo LEN en servidor de nodos de red	X		
Utilización de comodines para definir recursos de nodo LEN conectado	X		
Aceptación de diversas condiciones “recurso encontrado”	X		
Servidor de nodos de red para EN DLUR - Conjunto de opciones	X		

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

<b>Función de APPN</b>	<b>Sí</b>	<b>No</b>	<b>Notas</b>
<b>Servicios de topología y direccionamiento</b>			
Intercambio de información de topología	X		
Difusiones periódicas sobre topología	X		8
Mantenimiento de la base de datos de topología	X		9
Conocimiento de la topología en sesiones de CP-CP	X		
Cálculo de ruta aleatorio	X		10
Árboles de direccionamiento colocados en antememoria	X		11
Almacenamiento seguro de la base de datos de topología	X		
Garbage Collection Enhancements	X		
<b>Conectividad</b>			
Definición de red de conexiones	X		12
Diversos grupos de transmisión	X		
Grupos de transmisión paralelo	X		
<b>Servicios de gestión</b>			
Soporte de diversos dominios (MDS)	X		
Punto focal explícito	X		
Punto focal implícito	X		
Alertas retenidas	X		
Sesiones de SSCP-PU con puntos focales		X	
Datos de diagnóstico de problemas de los SNA/MS en las alertas	X		

**Notas:**

1. Pueden definirse nuevos nombres de modalidad en el direccionador utilizando la interfaz de línea de mandatos. Estos nuevos nombres de modalidad pueden correlacionarse con nombres de definición de clase de servicio (CoS) existentes o con nuevas definiciones de CoS, que pueden establecerse utilizando la herramienta de configuración.
2. Las estaciones de enlace de recursos limitados están soportadas para:
  - enlaces de red de conexiones
  - enlaces de SVC X.25
  - enlaces PPP en ejecución sobre RDSI, V.25 bis o V.34
  - enlaces Frame relay en ejecución sobre RDSI
  - SVC ATM
  - enlaces Red en Anillo
  - enlaces Ethernet
3. Cuando el direccionador activa un TG para un nodo adyacente, negocia con este nodo el tamaño máximo de mensaje que puede enviarse a través del TG. Si un mensaje BIND sobrepasa el tamaño de mensaje negociado, el direccionador segmenta el mensaje BIND. La segmentación sólo se produce si el nodo adyacente puede volver a ensamblar el BIND. El direccionador da soporte al reensamblaje de BIND.

4. Puede habilitarse una función de seguridad de nivel de sesión para las conexiones entre el nodo de red direccionador y un nodo adyacente. Los dos asociados de la conexión necesitan una clave hexadecimal coincidente que permita que cada nodo realice una verificación de su asociado antes de establecer la conexión.
5. Cuando se direccionan datos de sesión a un nodo adyacente, el direccionador segmenta una unidad de petición/respuesta (RU) si la unidad de mensaje sobrepasa el tamaño máximo de mensaje que puede enviarse a través del grupo de transmisión. Si el direccionador recibe una RU segmentada, el nodo la vuelve a ensamblar.
6. Después de localizar satisfactoriamente un recurso de la red APPN, el direccionador almacena o *coloca en antememoria* esta información en su base de datos de directorios local para utilizarla más adelante. No obstante, el direccionador no guarda estas entradas de directorio de antememoria en un soporte de almacenamiento permanente, como, por ejemplo, un disco, para facilitar la recuperación en el caso de que el nodo falle.
7. El direccionador no puede utilizarse como servidor de directorios central para una red APPN. No obstante, el direccionador puede utilizar un servidor de directorios central para obtener información de directorio sobre la ubicación de un recurso en la red.
8. Para evitar que otros nodos de red desechen información sobre el direccionador de sus bases de datos de topología, el direccionador crea una actualización de base de datos de topología (TDU) sobre sí mismo y los grupos de transmisión que posee localmente cada 5 días y difunde esta TDU a los nodos de red.
9. Está asociado un temporizador de intervalos con cada entrada de recurso de la base de datos de topología de red del direccionador. Si el direccionador no recibe información sobre un recurso en 15 días, desecha la entrada correspondiente a este recurso de la base de datos.
10. Si hay más de una ruta de las de menor peso entre una LU de origen y una LU de destino para una clase de servicio determinada, el direccionador selecciona aleatoriamente una de estas rutas para la sesión. Esta forma de actuar ayuda a distribuir el flujo de tráfico de la red.
11. El direccionador mantiene una copia de la base de datos de topología de red. La base de datos identifica las rutas disponibles hacia otros nodos de red para una clase de servicio en particular. Cuando el direccionador tiene que calcular una ruta hacia un nodo de red o hacia un nodo final adyacente respecto a este nodo de red, utiliza información de la base de datos de topología con el fin de generar un árbol de direccionamiento para este nodo de red. El árbol de direccionamiento identifica las rutas óptimas hacia el nodo de red para la clase de servicio necesaria.

Cuando el direccionador genera un nuevo árbol de direccionamiento, almacena aquel árbol en antememoria. Cuando el direccionador recibe una petición de servicios, comprueba esta antememoria en primer lugar para ver si hay una ruta calculada. La utilización de la antememoria reduce el número de cálculos de ruta necesarios. Cuando el direccionador recibe información de topología que invalida un árbol de direccionamiento, desecha el árbol. El direccionador vuelve a calcular el árbol de la manera necesaria y coloca en antememoria el nuevo árbol.



12. El direccionador puede definirse como miembro de una red de conexiones en puertos Ethernet, puertos Red en Anillo, puertos BAN Frame Relay, el soporte del Enterprise Extender para el HPR sobre IP y puertos ATM.

---

## Funciones opcionales de nodo de red APPN

Además de funciones de la arquitectura APPN base, el direccionador también implementa las siguientes series de conjuntos de opciones y nuevas funciones:

- 087** Garbage Collection Enhancements
- 1002** Nombre de estación de enlace adyacente
- 1007** TG paralelo\*
- 1012** Nombre de LU = Nombre de CP
- 1016** Extended Border Node
- 1061** Prerrequisitos de SS Extensions para el soporte de NNS
- 1063** Soporte de NNS en SS Extensions
- 1067** Peticionario de LU dependientes
- 1071** Uso generalizado de ODAI
- 1101** Antememoria de directorios precargados
- 1107** Registro de recursos central (de LU)
- 1116** Soporte de servidor de nodos de red para el registro de LU servidas por un DLUS
- 1119** Informe de topología de rama para un gestor
- 1120** Conocimiento de ramas
- 1121** Branch Extender
- 1124** Reserva de Branch Extender de configuración automática
- 1200** Colocación de árboles y de TG en antememoria
- 1201** Soporte de almacenamiento permanente
- 1400** Direccionamiento de alto rendimiento (HPR)
- 1401** Rapid Transport Protocol (RTP)
- 1402** Control de los flujos sobre RTP
- 1405** HPR Border Node
- Ajuste de rendimiento de nodo
- Rastros de servicio de nodo
- Conjunto de estadísticas de contabilidad y nodos

**\*Nota::** Cuando defina TG paralelo, si utiliza la asignación dinámica de números de TG, debe definir TODOS los enlaces entre los dos nodos o no definir NINGUNO.

### Direccionamiento de alto rendimiento

El HPR es una mejora para la arquitectura APPN que proporciona un mayor rendimiento por lo que respecta a los enlaces de baja proporción de errores y gran velocidad que utiliza el hardware existente. El HPR sustituye el direccionamiento de sesiones intermedias (ISR) normal de APPN por una Capa de control de red (NCL) que contiene un nuevo tipo de función de direccionamiento de origen denominado direccionamiento de red automático (ANR). En el paquete de ANR está contenida la ruta completa de HPR, lo que permite que los nodos de direccionamiento intermedio direccionen los paquetes con menos actividad general de proceso y almacenamiento.

El HPR también elimina los procedimientos de recuperación de errores y control del flujo/congestión (ritmo de nivel de sesión) para cada enlace entre los nodos y desplaza tales procedimientos a los puntos finales de una conexión de HPR. Los puntos finales de la conexión de HPR utilizan una capa de transporte que se sirve de un nuevo procedimiento de recuperación de errores denominado Rapid Transport Protocol (RTP). Los nodos intermedios de HPR no tienen conocimiento de sesiones ni conexiones con RTP. Esta nueva capa de transporte contiene:

- Un procedimiento de recuperación de errores de retransmisión selectivo
- Segmentación y reensamblaje
- Un mecanismo de control del flujo y de la congestión basado en la velocidad adaptable (ARB) que franquea los datos de una ruta y permite una utilización eficaz de los recursos de red mientras se minimiza la congestión. El método ARB utiliza una aproximación preventiva antes que reactiva para el control del flujo y de la congestión.
- Una función de conmutación de la vía de acceso de no interrupción (NDPS) que redirecciona automáticamente el tráfico alrededor de las anomalías de un nodo o enlace sin interrumpir las sesiones de usuario final.
- Detección de conjunto de bits de notificación de congestión explícita hacia adelante (FECN), que permite que el algoritmo de control del flujo y de la congestión basado en la velocidad adaptable de RTP ajuste la velocidad de emisión de datos. Este algoritmo evita ráfagas y congestión en el tráfico, con lo cual mantiene un alto nivel de productividad.

El direccionador implementa el direccionamiento ANR y Rapid Transport Protocol. Por lo tanto, el direccionador puede funcionar como nodo de direccionamiento intermedio de HPR y también como nodo de punto final de conexión de HPR.

### Interoperatividad

El HPR utiliza funciones de control de red de APPN que incluyen el cálculo de ruta de menor peso basado en la clase de servicio (CoS) y la prioridad de transmisión. El HPR interopera sin disrupciones con el ISR de APPN:

- La red se adapta automáticamente a la presencia de nodos con posibilidad de HPR y enlaces con habilitación de HPR.
- Una red APPN puede tener cualquier mezcla de enlaces de ISR y HPR, aunque se aprovecha la mayor ventaja que supone el HPR cuando la red tiene tres o más nodos con habilitación de HPR y dos o más enlaces entre éstos con posibilidad de HPR. Con ello, el nodo medio de HPR podrá ser un nodo intermedio de HPR y utilizar solamente el direccionamiento ANR, lo que permitirá que los datos de sesión se direccionen a través del nodo medio que sólo utiliza la NCL.

- Una ruta de sesión determinada puede estar compuesta por una combinación de enlaces de ISR y HPR.
- El HPR utiliza las mismas características de TG y nodo para el cálculo de ruta de menor peso que el ISR de APPN. No se da otra consideración especial a los nodos o enlaces con posibilidad de HPR que sus características potencialmente mejoradas (como, por ejemplo, a mayor velocidad de un enlace, mayor efectividad).

### Tipos de tráfico

El ISR de APPN utiliza el protocolo de QLLC para el control de enlace de datos directo de X.25, el protocolo del tipo 2 de LLC de IEEE 802.2 para Red en Anillo, Ethernet, PPP y Frame Relay, y el protocolo de SDLC para el control de enlace de datos SDLC. El HPR de APPN, que está soportado en Red en Anillo, Ethernet, PPP, MPC+, LSA y Frame Relay, no utiliza el protocolo del tipo 2 de LLC, pero sí algunas funciones de una estación de enlace APPN para el XID y el valor de tiempo de espera excedido respecto a la inactividad. Por lo tanto, se utiliza una sola estación de enlace APPN para el ISR o el HPR. Se utilizan diferentes mecanismos para distinguir entre tráfico de ISR y tráfico de HPR, que dependen del tipo de DLC:

- Para los puertos LAN Red en Anillo y Ethernet:

Cada protocolo que utiliza un puerto debe tener una dirección de SAP exclusiva, con la excepción de DLSw (que puede utilizar la misma dirección de SAP que otros protocolos porque las tramas de DLSw no se destinarán a la dirección MAC local, sino a una dirección MAC de DLSw). Una dirección de SAP exclusiva identifica la estación de enlace APPN para el tráfico de HPR (parámetro de dirección de SAP de HPR local). Si se destina tráfico de ISR a una estación de enlace, debe utilizarse una dirección de SAP diferente (parámetro de dirección de SAP de APPN local). El tráfico de ISR utiliza tramas de LAN del tipo 2 de LLC. El tráfico de HPR se maneja de forma similar con tramas de LAN del tipo 1 de LLC y debe tener una dirección de SAP diferente.

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

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

- Para los puertos Frame Relay:

El tráfico de ISR de APPN y el tráfico de HPR de APPN transferidos por una conexión de enlace de datos Frame Relay dan soporte al formato de trama de puente de RFC 1490/2427 y al formato de trama de ruta de RFC 1490/2427.

- Formato de trama de ruta de RFC 1490/2427

El tráfico de ISR de APPN se transferirá por una conexión de enlace de datos Frame Relay que utilice el método de encapsulación de múltiples protocolos de orientación a las conexiones definido en RFC 1490/2427 con:

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

El tráfico de HPR de APPN transferido por una conexión de enlace de datos frame-relay no utiliza el LLC de IEEE 802.2. Utiliza una encapsulación de múltiples protocolos diferente definida en RFC 1490/2427 con:

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

El HPR de APPN no utiliza ningún SAP para el tráfico transferido con el formato de trama de ruta de RFC 1490/2427 porque no hay ningún protocolo de capa 2.

- Formato de puente de RFC 1490/2427

El HPR de APPN utiliza un SAP para el tráfico transferido con el formato de trama de puente de RFC 1490/2427.

- Para los puertos PPP:
  - El tráfico de ISR de APPN utiliza el LLC de 802.2 por la conexión PPP.
  - Puesto que no se utiliza ningún protocolo de capa 2 en la encapsulación de RFC 1490/2427 del HPR, no se utiliza ningún SAP para el tráfico de HPR.
- Para los puertos ATM:
  - El tráfico de ISR de APPN no está soportado en los puertos ATM nativos. No obstante, se da soporte a dos tipos de tráfico de APPN definidos en RFC 1483:
    - Durante el arranque de la estación de enlace, se transportan XID con el siguiente formato de trama:
      - NLPID = X'09'
      - ID de protocolo de capa 2 = X'4C80' (cabecera del LLC de 802.2 presente)
      - ID de protocolo de capa 3 = X'7083' SNA-APPN (FID2) con inclusión del XID3
    - El tráfico de HPR se transporta con el siguiente formato de trama:
      - NLPID = X'09'
      - ID de protocolo de capa 2 = X'4C80' (cabecera del LLC de 802.2 presente)
      - ID de protocolo de capa 3 = X'7085' SNA-APPN/HPR (NLP)
- Para los puertos MPC+:
  - Se da soporte al HPR. Sólo se da soporte a una estación de enlace por puerto MPC.
- Para los puertos LSA:
  - Se da soporte al HPR.
- FDDI
- Soporte del Enterprise Extender para el HPR sobre IP

Consulte la Tabla 3 en la página 25 para obtener una lista de los DLC que dan soporte al HPR.

**Nota:** El HPR no está soportado en los puertos SDLC, X.25 ó DLSw.

## Peticionario de LU dependientes (DLUR)

La opción DLUR hace extensivo el soporte de dispositivos T2.0 ó T2.1 que contienen LU dependientes a los nodos APPN. La función DLUR de un nodo de red APPN o nodo final APPN se desarrolla junto con un servidor de LU dependientes (DLUS) en una red mixta de subárea/APPN. La función DLUS puede residir en una parte de la red mixta que no sea la de la función DLUR.

Los flujos de LU dependientes (SSCP-PU y SSCP-LU) se encapsulan en un conducto de LU 6.2 (CP-SVR) establecido entre el nodo APPN DLUR y el SSCP de DLUS. El conducto CP-SVR consta de un par de sesiones de LU 6.2 que utilizan una nueva modalidad CPSVRMGR entre el DLUR y el DLUS. Este conducto lleva la función del SSCP (del DLUS) al nodo APPN DLUR, donde puede volverse disponible para los nodos T2.0/T2.1 conectados que contienen LU dependientes.

Las LU dependientes aparentarán ubicarse dentro del dominio del SSCP que sirve. Se emularán flujos de iniciación de sesión desde el DLUS, pero las vías de acceso de enlace lógico y datos de sesión se calcularán directamente entre la LU dependiente y su asociado de la sesión. Esta vía de acceso puede pasar o no por el nodo DLUS que sirve.

Establezca el parámetro de tipo de nodo adyacente en PU 2.0 Node cuando defina una estación de enlace como nodo adyacente T2.0 que contiene LU dependientes. Establezca el parámetro de tipo de nodo adyacente en APPN end node o LEN end node cuando defina una estación de enlace como nodo adyacente T2.1 que contiene LU dependientes.

Vea la Tabla 3 en la página 25 si desea obtener los tipos de puertos soportados que proporcionan conexión con la PU de sentido directo (DSPU).

## Funciones soportadas

La opción DLUR de APPN incluye las funciones siguientes:

- Soporte para nodos T2.0 de sentido directo conectados por SDLC que contienen LU dependientes que no dan soporte al intercambio de XID.
- Soporte para nodos T2.0 de sentido directo que contienen LU dependientes que responden con el tipo 0 de XID y el tipo 1 de XID.
- Soporte para nodos T2.1 de sentido directo que contienen LU dependientes que responden con el tipo 3 de XID.
- Soporte para LU dependientes que equivale al soporte proporcionado por el entorno de subárea con el fin de:
  - Activar PU y sus LU
  - Ubicar y permitir la ubicación a otras LU de una red de subárea o APPN
  - Determinar las características de LU
  - Permitir que los operadores de terminal se conecten a aplicaciones de redes de subárea y APPN
  - Posibilitar la entrada en función de un SSCP
  - Permitir sesiones de LU-LU sin interrupciones si falla el DLUS (SSCP) de soporte

- Permitir la inicialización de SLU, PLU y terceros

### Restricciones

La opción DLUR, tal como está implementada en el nodo de red direccionador, tiene las siguientes restricciones funcionales:

- La función DLUR sólo puede dar soporte a LU secundarias (SLU). Una LU soportada por la función DLUR no puede funcionar como LU primaria (PLU). Por lo tanto, la unidad física de sentido directo (DSPU) debe configurarse como secundaria.
- Puesto que sólo se da soporte a SLU, el Recurso de direccionamiento de red (NRF) y la Opción de terminal de red (NTO) no reciben soporte.
- El recurso de recuperación extendida (XRF) y el XRF/CRYPTO no reciben soporte.
- Debe poder establecer una sesión de sólo APPN o sólo APPN/HPR entre el DLUS y el DLUR. La sesión de CPSVRMGR no puede pasar por una red de subárea.

### Consideraciones de VTAM para el DLUR

A continuación, se muestran definiciones de ejemplo de VTAM® Switched Major Node para el DLUR. Debe tener en cuenta que las sentencias PATH sólo son necesarias si es VTAM el que va a iniciar la conexión con la DSPU.

Debe consultar el manual *IBM VTAM Resource Definition Reference* si desea obtener información detallada sobre las sentencias de parámetros de DLC para las definiciones de Switched Major Node.

```

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

```

## Utilización de APPN

```
*****
* Below is Frame Relay
*****
*A20RT  PATH  PID=2,
*          DLURNAME=GREEN,
*          DLCADDR=(1,C,FRPVC),
*          DLCADDR=(2,X,4652303033),      2 **nombre de puerto
*          DLCADDR=(3,X,04),              3 **dirección de SAP
*          DLCADDR=(4,X,0024)            4 **DLCI
*****
* Below is Frame Relay BAN
*****
*A20RT  PATH  PID=3,
*          DLURNAME=GREEN,
*          DLCADDR=(1,C,FRPVC),
*          DLCADDR=(2,X,4652303033),      2 **nombre de puerto
*          DLCADDR=(3,X,04),              3 **dirección de SAP
*          DLCADDR=(4,X,0024),            4 **DLCI
*          DLCADDR=(6,X,40000000001)      5 **dirección MAC
*****
* Below is DLSw
*****
*A20RT  PATH  PID=3,
*          DLURNAME=GOLD,
*          DLCADDR=(1,C,TR), 7
*          DLCADDR=(2,X,444C53323534),    2 **nombre de puerto
*          DLCADDR=(3,X,04),              3 **dirección de SAP
*          DLCADDR=(4,X,40000000001)      6 **dirección MAC
*
*****
** Below is Token Ring
*****
*PATHT20 PATH  PID=1,
*          DLURNAME=RED,
*          DLCADDR=(1,C,TR),
*          DLCADDR=(2,X,5452303030),      2 **nombre de puerto
*          DLCADDR=(3,X,04),              3 **dirección de SAP
*          DLCADDR=(4,X,400000011088)     6 **dirección MAC
*****
** Below is Ethernet
*****
*PATHE20 PATH  PID=1,
*          DLURNAME=PURPLE,
*          DLCADDR=(1,C,ETHERNET),
*          DLCADDR=(2,X,454E303030),      2 **nombre de puerto
*          DLCADDR=(3,X,20),              3 **dirección de SAP
*          DLCADDR=(4,X,400000011063)     6 **dirección MAC
*****
* Below is X25 SVC
*****
*A20RT  PATH  PID=3,
*          DLURNAME=GREEN,
*          DLCADDR=(1,C,X25SVC),
*          DLCADDR=(2,X,583235303033),    2 **nombre de puerto
*          DLCADDR=(4,X,C3),              3 **identificador de protocolo
*          DLCADDR=(21,X,000566666),     9 **dirección de DTE de destino
*****
* Below is X25 PVC
*****
*A20RT  PATH  PID=3,
*          DLURNAME=GREEN,
*          DLCADDR=(1,C,X25PVC),
*          DLCADDR=(2,X,583235303033),    2 **nombre de puerto
*          DLCADDR=(3,X,0001)            10 **número de canal lógico
*****
```



```

*****
*****
* LU statements
*****
*PU21LU1 LU LOCADDR=2 11
*PU21LU2 LU LOCADDR=3
*PU21LU3 LU LOCADDR=4
*****

```

**Notas:**

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

Consulte "Utilización de TN3270" en la página 89 para ver un ejemplo de una sentencia de vía de acceso de PU interna.

## Redes de conexiones APPN

Cuando los nodos se conectan a un recurso de transporte de acceso compartido (SATF), es posible la conectividad de cualquiera con cualquiera. Esta conectividad de cualquiera con cualquiera permite las conexiones directas entre dos nodos cualesquiera, lo que elimina el direccionamiento a través de nodos de red intermedios y el paso repetitivo de los datos correspondientes por el SATF. No obstante, para conseguir esta conectividad directa, deben definirse TG en cada nodo para todos los otros posibles asociados.

La definición de conexiones entre todos los pares posibles de nodos conectados al SATF da como resultado un gran número de definiciones (con un aumento del orden del cuadrado del número de nodos implicados) y también el flujo de un gran número de actualizaciones de base de datos de topología (TDU) en la red APPN. Con el fin de solucionar estos problemas, APPN permite que los nodos se conviertan en miembros de una red de conexiones para representar su conexión a un SATF. El tráfico de las sesiones entre dos nodos que se han definido como miembros de una red de conexiones puede direccionarse directamente, sin pasar por un nodo de red (consigue la conectividad directa). Para convertirse en un miembro de una red de conexiones, debe "conectarse" un puerto del nodo APPN a una Red de conexiones mediante la definición de una interfaz de red de conex-

iones. Cuando se define el puerto, se crea un TG de Red de conexiones mediante el componente de APPN para identificar la conexión directa del puerto al SATF (es decir, la red de conexiones). Este TG no es un TG convencional como en el caso de las estaciones de enlace definidas, sino que representa la conexión a la Red de conexiones en la base de datos de topología.

**Nota:** Los TG para los nodos finales no se encuentran en la base de datos de topología de red, sino en la base de datos de topología local del nodo. No fluyen TDU a través de la red cuando se establece una conexión a través de una Red de conexiones o cuando un nodo final se hace miembro de una Red de conexiones.

Puesto que está representada la conectividad mediante un TG de un nodo determinado a una Red de conexiones, pueden utilizarse los servicios normales de topología y direccionamiento (TRS) para que el servidor de nodos de red calcule la vía de acceso directa entre dos nodos cualesquiera conectados al SATF (con TG para la misma Red de conexiones). El nodo de destino devuelve información de señalización de DLC durante el proceso normal de Locate para permitir que el nodo de origen establezca una conexión directamente con el nodo de destino.

Por lo tanto, para conseguir la conectividad directa en un SATF, en lugar de que cada nodo del SATF se defina (o conecte) con otro, cada uno de ellos se conecta a una Red de conexiones. La Red de conexiones se visualiza a menudo como un nodo virtual del SATF al que se conectan todos los otros nodos. Este modelo se utiliza frecuentemente y, de hecho, se intercambian a menudo los términos Nodo de direccionamiento virtual (VRN) y Red de conexiones.

Cuando se define una red de conexiones, recibe un nombre. Este nombre se convierte en el nombre del CP del VRN y debe seguir todos los requisitos de cualquier nombre de CP. Vea la Tabla 25 en la página 179 para obtener una lista de estos requisitos.

### Restricciones

- Puede definirse la misma red de conexiones (VRN) en una sola LAN. No obstante, puede definirse el mismo VRN en diversos puertos que tengan características iguales y relativas a una sola LAN.
- Sólo hay un TG de red de conexiones de un puerto determinado al VRN de una red de conexiones determinada.
- Puesto que el VRN no es un nodo real, no pueden establecerse sesiones de CP-CP con o a través de un VRN.
- Cuando se define una red de conexiones en el nodo de red direccionador, se especifica un nombre calificado al completo para el parámetro *connection network name*. Sólo pueden definirse redes de conexiones que tengan el mismo ID de red que el nodo de red direccionador. El ID de red del VRN es, pues, el mismo que el ID de red del nodo de red direccionador.

## Branch Extender

La función Branch Extender (BrNN) está diseñada para optimizar la conexión de una sucursal a una red troncal WAN APPN. El BrNN aísla todos los nodos finales de una o más LAN sucursales de la WAN troncal. El dominio de un BrNN puede contener nodos finales y BrNN en cascada solamente. El dominio de un BrNN no contiene nodos de red ni nodos con la función DLUR.

Al configurar un BrNN, configure las estaciones de enlace para la red troncal como enlaces superiores. Esto hace que el BrNN aparezca como un nodo final convencional ante la red troncal. Desde la perspectiva de la red troncal, todos los recursos del dominio del BrNN aparentan ser propiedad del BrNN, lo que oculta la topología del dominio del BrNN respecto a la red troncal y reduce el número de peticiones Locate difundidas en la red troncal.

Un BrNN presenta una interfaz de nodo de red convencional sobre los enlaces inferiores. Los nodos finales del dominio del BrNN registran sus recursos con el BrNN y lo utilizan como servidor de nodos de red convencional.

Un BrNN lleva a cabo:

- Una reducción del número de nodos de red en una red APPN grande.
- La ocultación de la topología de la sucursal respecto a la WAN y la ocultación de la topología de la WAN respecto al BrNN.
- Una comunicación directa de igual a igual entre las ramas definidas que están conectadas a la misma red de conexiones.
- Una reducción del tráfico de las sesiones de CP-CP en el enlace de WAN.

Las siguientes son limitaciones del Branch Extender:

- Los nodos de red sólo pueden conectarse sobre los enlaces que un BrNN define como enlaces superiores.
- Sólo pueden conectarse a un enlace inferior de BrNN nodos finales o BrNN en cascada. Los nodos de frontera que actúan como nodos finales y los nodos DLUR no pueden conectarse a un enlace inferior de BrNN.
- Un nodo no puede conectarse a un Branch Extender sobre un enlace superior y un enlace inferior al mismo tiempo.
- Un BrNN puede tener sesiones de CP-CP con un solo nodo de red cada vez.

Es posible configurar dos o más BrNN iguales en una sola rama, cada uno de los cuales servirá a un conjunto de EN en la rama. Cuando uno de estos BrNN pierde conectividad con su servidor de nodos de red preferente, es conveniente que uno de los otros BrNN tome posesión del servicio de los EN del primer BrNN.

Puede configurar BrNN iguales que actúen de reserva entre sí automáticamente en esta situación pasando de una configuración de igual a una configuración de BrNN en cascada.

## Nodos Extended Border Node

Los nodos Extended Border Node (BN) permiten que redes con diferentes ID de red se conecten entre sí. Se establecerán sesiones de CP-CP a través de las fronteras de red y podrá expandirse por las redes interconectadas el establecimiento de sesiones y flujos de servicios de directorio. No se intercambiará información de topología a través de la frontera de red. Esto permite que redes con diferentes ID de red establezcan sesiones de CP-CP y proporciona el aislamiento de las topologías entre las diferentes redes.

Además de permitir que redes con diferentes ID de red se interconecten, los BN proporcionan un mecanismo para subdividir las redes con el mismo ID de red en "subredes con topología" más pequeñas. Esta subdivisión proporciona el ais-

lamiento de las topologías entre las dos subredes mientras permite que se expandan por las fronteras de subred sesiones y flujos de servicios de directorio.

Debe haber un BN a un lado de la frontera de subred para utilizar esta función. Cuando un BN se conecta con un NN no nativo, el BN aparece como un EN ante el NN no nativo aunque en realidad el BN sea un NN.

Puede haber dos BN, uno a cada lado de la frontera, cooperando para realizar esta función. Cuando se conecten dos BN a través de una frontera de subred, el BN aparecerá como un NN ante el BN no nativo.

Un BN aparentará ser el servidor de NN para todos los recursos no nativos accesibles a través del BN. Esto permite que se desarrollen las funciones APPN existentes de cálculo de ruta y colocación de directorios en antememoria mientras posibilita que el BN intercepte y modifique todos los flujos de Locate y BIND que pasan por un TG intersubredes (ISTG).

Los BN implementan un cálculo de ruta de sesión óptima relativo a su parte. Cada subred calcula su propia parte del vector de control de selección de ruta (RSCV) de la sesión respecto al punto de entrada de la siguiente subred no nativa. Mientras que el RSCV será óptimo a través de la subred nativa, no hay garantía de que sea óptima la vía de acceso de sesión de final a final.

### **Ejemplo de topología de red**

La Figura 1 en la página 19 muestra muchas de las opciones de conectividad que proporciona la función BN. En general, puede ir de cualquier red a cualquier otra red, con la excepción de que la Red F sólo puede acceder a la Red E y ésta es la única red que puede acceder a la Red F.

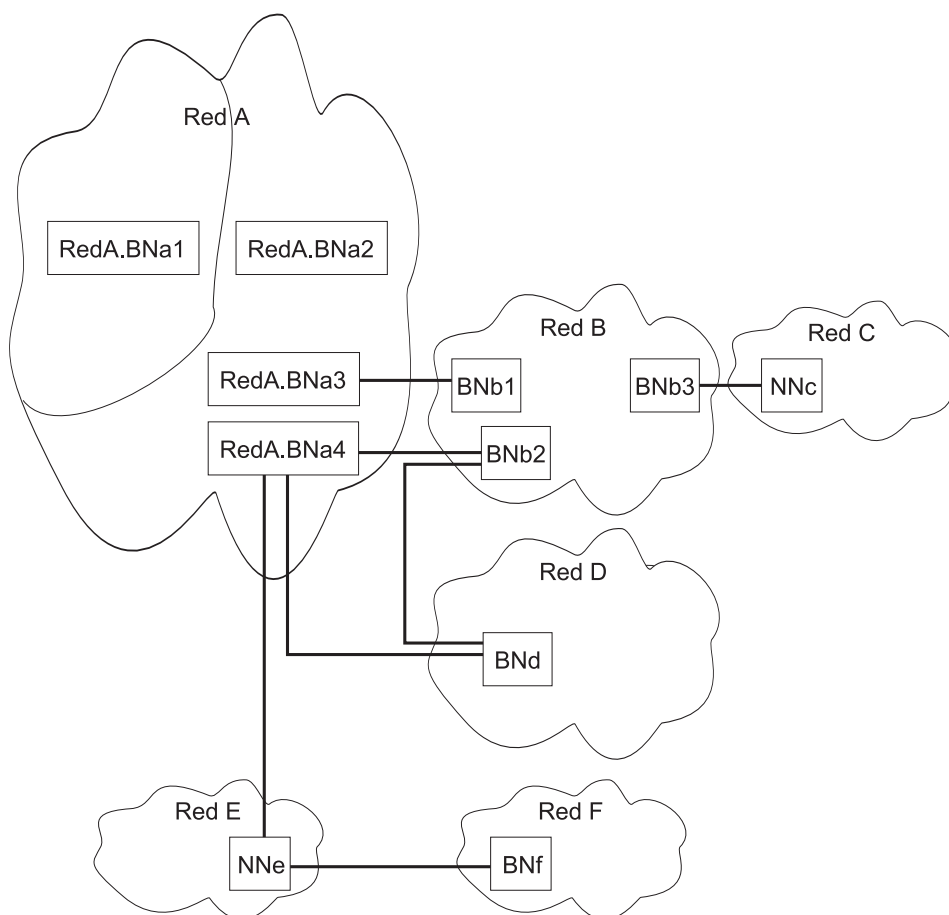


Figura 1. Conectividad del Extended Border Node

**Nota:** Los TG intersubredes se representan mediante líneas uniformes.

En esta figura:

- El ID de red RedA con subredes se ha dividido en subredes con topología. La subred con topología localizada más a la izquierda contiene el BNa1, que está conectado a través de un TG intersubredes con el BNa2, situado en la subred con topología de la derecha. El ID de red del BNa1 y del BNa2 es RedA.
- El BNa1 es no nativo para todos los otros nodos de frontera extendida, incluido el de la RedA2.
- El BNa2, el BNa3 y el BNa4 son todos nodos nativos para la subred con topología de la derecha de la REDA, y son no nativos para las otras redes, incluida la subred que contiene el BNa1.
- Un BN puede interconectar diversas redes tal como el BNa4 conecta una subred con topología de la RedA a la RedB y la RedD.
- Diversos enlaces pueden conectar dos redes tal como la subred con topología de la derecha de la RedA y la RedB están conectadas por BNa3/BNb1 y BNa4/BNb2.
- Los dos extremos de un enlace interredes deben ser BN a menos que una de las redes sea una red periférica. En este caso, la red periférica puede utilizar

un nodo de red convencional que no sea un BN para la conexión con el BN de la red adjunta. Esto se muestra en la conexión de la red periférica RedC a la RedB mediante el NNc.

- Cualquier LU de las redes RedA, RedB, RedC, RedD o RedE puede acceder a cualquier otra LU de cualquiera de estas redes. La RedC y la RedE se han conectado utilizando nodos de red convencionales que no son BN.
- La RedE está conectada mediante el nodo de red convencional que no es un BN NNe con los BN de la RedA2 y la RedF. No puede hacer que un nodo de red interconecte redes no periféricas, por lo que no es posible ir de la RedF a ninguna red que no sea la RedE.
- Puede ir de la RedA2 a la RedE y de la RedE a la RedA2 porque el NNe se encuentra en una red periférica. Del mismo modo, puede ir de la RedF a la RedE y de la RedE a la RedF.

### Session Services Extensions (SSE) para el soporte de NNS

La función SSE de un direccionador se habilita cuando se habilita éste para APPN. Sucede así aunque no se habilite la función Extended Border Node. Esto significa que el direccionador puede actuar como servidor de nodos de red para un nodo final VTAM. Como tal, puede manejar funciones de NNS para los nodos finales que realizan peticiones de sesiones iniciadas por SLU, sesiones iniciadas por terceras partes, puesta en cola de peticiones de sesiones, inicio de sesión automático, peticiones de liberación de sesión y registro de vector de TG de EN.

La función SSE no se utiliza cuando el direccionador actúa como Branch Extender porque no se permiten VTAM de sentido directo en dicha configuración.

### Requisitos de red

No hay requisitos para los otros nodos APPN de una red mientras no se conecten directamente con un BN a través de una frontera de topología. Los nodos APPN que se conecten con un BN a través de una frontera de topología (a través de un ISTG) deben cumplir con uno de estos requisitos:

- APPN Ver1 con el conjunto de opciones 1013, Interoperatividad con nodo de frontera extendida periférico
- APPN Ver2, en que el conjunto de opciones 1013 forma parte del software base.

Los nodos conectados mediante ISTG que no cumplan con ninguno de estos requisitos generarán alertas y no manejarán algunos de los nuevos flujos asociados con los BN. No obstante, si están disponibles otras vías de acceso en la red, todavía puede conseguirse conectividad de final a final.

## Branch Extender frente al Extended Border Node

Tanto el Branch Extender como los nodos Extended Border Node sirven para minimizar la topología de la red. La elección de cuál utilizar depende de la red.

Un **extensor de rama** es la elección adecuada cuando dispone de una sola red con uno o más grupos de nodos finales en que cada grupo de nodos finales normalmente tiene que comunicarse con los otros nodos finales de aquel grupo, y sólo ocasionalmente tiene que interactuar con la red troncal.

Ninguno de los dispositivos de sentido directo del extensor de rama puede ser un nodo de red, DLUR, VTAM o nodo final VTAM.

Con el extensor de rama, la visión que tiene la red troncal de éste consiste en que es un nodo final gigante que posee todas las LU de sentido directo. La red troncal no tiene conocimiento de la topología de sentido directo del extensor de rama, lo cual reduce la actividad general de intercambios de topologías. A la inversa, el servidor de nodos de red del extensor de rama, servidor que forma parte de la red troncal, tendrá conocimiento de todas las LU propiedad del extensor de rama si éste se configura para el registro de recursos. Esto sirve para reducir el número y tamaño de búsquedas difundidas y actualizaciones de topología.

Un **nodo de frontera extendida** es la elección adecuada cuando tiene diversas redes que desea relacionar entre sí o cuando tiene una red grande que desea subdividir sin restricciones acerca de qué tipos de nodos se permiten en las partes de la subdivisión. No existe el concepto de sentido directo o inverso y puede tener nodos de frontera extendida adicionales, nodos de red, nodos finales, DLUR, VTAM o nodos finales VTAM ubicados en cualquier parte de la red. A diferencia del extensor de rama, un nodo de frontera extendida no puede registrar recursos con otra red.

## Gestión de un nodo de red

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

Puede utilizar SNMP para acceder a estas MIB estándares de IETF:

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

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

- IBM APPN Memory
- Contabilidad de IBM
- NCL de HPR de IBM
- Prueba de Ruta de HPR de IBM
- IBM Branch Extender Node
- IBM TN3270 Connection Rejection

### Posibilidades de punto de entrada para alertas relacionadas con APPN

El nodo de red direccionador puede servir de punto de entrada APPN para alertas relacionadas con el protocolo de APPN. Como punto de entrada, el direccionador tiene la responsabilidad de remitir alertas genéricas de APPN y LU 6.2 sobre sí mismo y sobre los recursos de su dominio a un *punto focal* para el proceso centralizado. Un punto focal es un punto de entrada que proporciona gestión y control centralizados para otros puntos de entrada en una o más categorías de gestión de red.

**Nota:** Si un punto focal no está disponible para recibir una alerta del dispositivo, éste retiene (almacena) la alerta.

Los puntos de entrada que se comunican con un punto focal componen la *esfera de control* de este punto focal. Si un punto focal define explícitamente los puntos de entrada de su esfera de control e inicia la comunicación con los mismos, es un *punto focal explícito*. Si un punto focal está designado por sus puntos de entrada, que inician la comunicación con el punto focal, éste es un *punto focal implícito*. El punto focal del direccionador puede ser un punto focal explícito o implícito.

Los direccionadores configurados como nodos extensores de rama tienen una flexibilidad adicional. Como con los nodos de red convencionales, el punto focal puede establecer directamente una relación explícita con el nodo extensor de rama. Como también ocurre con los nodos de red convencionales, puede configurar uno o más puntos focales implícitos en el nodo extensor de rama.

A diferencia de los nodos de red convencionales, los nodos extensores de rama pueden, como alternativa, tener información del punto focal a partir de su servidor de nodos de red. Cuando el servidor de nodos de red establezca una relación con el punto focal, explícita o implícitamente, informará a todos sus nodos finales servidos, incluidos los nodos extensores de rama servidos, del nombre del punto focal.

Si la sesión entre el punto de entrada direccionador y su punto focal primario falla, el direccionador puede iniciar una sesión con un punto focal de reserva designado. Antes de iniciar una sesión con un punto focal de reserva, el punto de entrada direccionador realiza el intento de restablecer la comunicación con su punto focal primario si se ha asignado al direccionador la responsabilidad del restablecimiento de sesión. Si falla este intento, el direccionador pasa al punto focal de reserva.

**Nota:** El direccionador intentará establecer una sesión con el punto focal de reserva o intentará restablecer la sesión con el punto focal primario solamente si el direccionador tiene una alerta para enviar.

Después de pasar a un punto focal de reserva, el direccionador intentará periódicamente restablecer su sesión con el punto focal primario. El intervalo entre los intentos se dobla cada vez que falla un intento hasta que se alcanza el intervalo máximo de un día. A partir de este punto, el intento se realiza a diario.

#### Notas:

1. Si el punto focal es explícito y el punto focal explícito retiene la responsabilidad del restablecimiento para sí mismo, se inhabilita este mecanismo de reintentos.
2. Si el punto focal es explícito y asigna la responsabilidad del restablecimiento al direccionador, éste intentará restablecer la comunicación hasta el siguiente reinicio de APPN en el direccionador.



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

El componente servicios de gestión de punto de control (CPMS) maneja los procesos de gestión del punto de control del direccionador. El componente CPMS del nodo de red direccionador reúne datos no solicitados de gestión de problemas a partir de recursos del dominio del direccionador y remite estos datos al punto focal adecuado.

### Unidades de mensajes soportadas

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

#### Unidad de mensaje Descripción

<b>CP-MSU</b>	Unidad de servicios de gestión de punto de control. Esta unidad de mensaje se genera mediante el CPMS y contiene información de alerta que remite el punto de entrada direccionador. El CPMS pasa unidades de mensajes CP-MSU al MDS.
<b>MDS-MU</b>	Unidad de mensaje de soporte de diversos dominios. Esta unidad de mensaje se genera mediante el MDS. Encapsula las CP-MSU para el transporte entre los nodos.

## Posibilidades de SNMP para MIB APPN

Un operador o una aplicación de una estación de gestión de red SNMP puede consultar objetos de las MIB APPN (utilizando los mandatos de SNMP **get** y **get\_next**) para recuperar información de estado y estadísticas de nodos de APPN. Puede modificarse un subconjunto de los objetos de MIB APPN mediante el mandato de SNMP **set**. Sólo puede accederse a las MIB APPN mediante SNMP.

## Base de datos de topología con Garbage Collection

Fluye información entre los NN APPN para que éstos estén informados acerca de recursos de la red. Cada NN mantiene una base de datos de topología compuesta por los nombres y las características de estos recursos. Cuando se elimina un recurso de la red, también puede suprimirse de la base de datos de topología de cada NN. Cuando un NN detecte que un recurso de su base de datos de topología está obsoleto, el nodo difundirá información indicando que debe recogerse el recurso para desecharlo. Si los NN que reciben esta información dan soporte a Enhanced Garbage Collection, deben suprimir este recurso de su base de datos de topología. En realidad, no se recoge el registro para desecharlo hasta el siguiente ciclo de recogida para desecho. Un NN examina cada recurso de su base de datos de topología una vez al día.

### Cola de alertas retenidas configurable

La función de cola de alertas retenidas configurable le permite configurar el tamaño de la cola de alertas retenidas. Si no está disponible un punto focal, la cola de alertas retenidas guarda las alertas de APPN. Cuando se vuelve disponible el punto focal, se envían las alertas retenidas. Si llegan más alertas de las que pueden retenerse, se desechan las alertas de mayor antigüedad.

**Nota:** Si configura un valor grande para el Held Alert Queue Size, hay que contar con la memoria adicional. Se puede hacer dejando que el algoritmo de ajuste calcule automáticamente el valor de Maximum Shared Memory. Consulte la sección “Ajuste de nodo APPN” en la página 41 para obtener información adicional sobre el algoritmo de ajuste del nodo.

### Punto focal implícito

Un punto focal es un nodo con responsabilidad de gestión centralizada. El nodo gestor puede contactar con el nodo gestionado (direccionador) y establecer una sesión de gestión. El nodo gestor es entonces un punto focal explícito. Cuando el nombre del nodo gestor está configurado en el direccionador y éste puede iniciar una sesión de gestión, el nodo gestor es un punto focal implícito. Puede configurar un solo punto focal implícito primario con un máximo de ocho puntos focales implícitos de reserva, donde cada punto focal es un nombre de red calificado al completo. El direccionador intentará contactar con cada punto focal por orden hasta que se establezca una sesión de gestión satisfactoria.

Si la sesión de gestión es con un punto focal implícito de reserva, el dispositivo intentará periódicamente restablecer su sesión con el punto focal implícito primario. El intervalo entre los intentos se dobla cada vez que falla un intento hasta que se alcanza el intervalo máximo de un día. A partir de este punto, el intento se realiza a diario.

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

### Soporte del Enterprise Extender para el HPR sobre IP

El soporte del Enterprise Extender para el HPR sobre IP permite que se ejecuten aplicaciones de HPR/APPN sobre una red troncal IP y se aprovechen de la clase de servicio de APPN. El HPR sobre IP encapsula datos de HPR en un paquete de UDP/IP para la entrega sobre la red IP.

---

### DLC soportados

La Tabla 3 en la página 25 muestra los puertos DLC soportados por el dispositivo sobre APPN:

Tabla 3. Tipos de puertos soportados para el direccionamiento de APPN

Tipo de puerto	Norma	HPR	ISR	DLUR <sup>1</sup>
Ethernet	Versión 2	Sí	Sí	Sí
Ethernet	IEEE 802.3	Sí	Sí	Sí
TR	802.5	Sí	Sí	Sí
PPP serie		Sí	Sí	No
FR serie (de puente y ruta) <sup>2</sup>		Sí	Sí	Sí
BAN Frame Relay		Sí	Sí	Sí
Función de puente de LAN serie		ND	ND	ND
SDLC		No	Sí	Sí
X.25	CCITT X.25	No	Sí	Sí
DLSw		No	Sí	Sí
APPN/PPP/RDSI		Sí	Sí	No
APPN/FR/RDSI		Sí	Sí	Sí
APPN/PPP/V.25 bis		Sí	Sí	No
APPN/PPP/V.34		Sí	Sí	No
LANE	Adaptación al Forum	Sí	Sí	Sí
ATM		Sí	No	Sí
MPC+ <sup>3</sup>		Sí	No	Sí
LSA <sup>3</sup>		Sí	Sí	Sí
FDDI		Sí	Sí	Sí
HPR sobre IP		Sí	No	Sí
Ethernet a 100 Mbps		Sí	Sí	Sí
TR a 100 Mbps	802.5	Sí	Sí	Sí

## Proceso de configuración del direccionador

Este apartado describe el proceso de configuración del direccionador e incluye detalles sobre los parámetros.

<sup>1</sup> Esta columna hace referencia al puerto que proporciona la conexión con la PU de sentido directo (DSPU).

<sup>2</sup> Utilice el formato de puente cuando tenga dos dispositivos conectados por Frame Relay y uno de ellos no tenga APPN. De lo contrario, utilice el formato de ruta debido a su mejor rendimiento.

<sup>3</sup> Consulte el capítulo titulado "Planificación y configuración del Adaptador de Canal Paralelo y ESCON" de la publicación *Nways Multiprotocol Access Services Guía del usuario de software* para obtener información sobre MPC+ y LSA.

### Cambios de la configuración que necesitan el reinicio de la función de APPN

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

Consulte el apartado “Soporte de la reconfiguración dinámica de APPN” en la página 288 para obtener información detallada sobre los cambios dinámicos que puede efectuar en la configuración de APPN.

### Requisitos de la configuración para APPN

El direccionamiento de APPN se configura en los adaptadores individuales que dan soporte al DLC que se desea. Para utilizar el direccionamiento de APPN, debe configurarse y habilitarse, como mínimo, uno de los DLC siguientes:

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

El código talk 6 necesario para configurar APPN o TN3270 reside en el módulo de carga correspondiente (archivo .ld), y este módulo no está cargado si no se ha

habilitado la función correspondiente. Si utiliza el Programa de configuración para configurar el dispositivo, se llevará a cabo automáticamente. Si utiliza mandatos `talk 6` para configurar el dispositivo, debe emitir uno de los siguientes mandatos, o los dos, y luego rearrancar para poder invocar los mandatos `talk 6` de APPN o TN3270:

- `Config> load add package appn`
- `Config> load add package tn3270`

## Configuración del direccionador como nodo de red APPN

Puede configurar el direccionador como nodo de red APPN siguiendo uno de los tres métodos siguientes, elección que depende del nivel de conectividad que desee con los otros nodos.

- Configuración mínima
- Configuración para el inicio de las conexiones
- Configuración para el control de las conexiones

### Configuración mínima

Este grupo de pasos de configuración de APPN:

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

Si elige los pasos de configuración mínima, los nodos adyacentes deben definir conexiones con el nodo de red direccionador para asegurar la conectividad. Puesto que los nodos APPN pueden iniciar sesiones de CP-CP con el nodo de red direccionador, no hay necesidad de definir estos nodos en la configuración del direccionador. En general, al configurar APPN en el direccionador, puede simplificar la tarea de modo considerable permitiendo que el nodo de red direccionador acepte peticiones de conexión de cualquier nodo. Si configura el nodo de red de esta manera, eliminará la necesidad de definir información sobre los nodos adyacentes, excepto en los casos siguientes:

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

En estos casos, debe especificar información sobre el nodo adyacente cuando habilite el direccionamiento de APPN en el puerto específico que vaya a utilizar para conectarse con el nodo adyacente, y debe seguir los pasos de configuración descritos en la sección “Configuración para el inicio de las conexiones” en la página 28.

Utilice el procedimiento siguiente para los pasos de configuración mínima:

1. Si va a configurar APPN utilizando un puerto DLSw:
  - a. Habilite la función de puente en el nodo
  - b. Habilite DLSw en el nodo
  - c. Defina el puerto DLSw con una dirección MAC administrada localmente para DLSw.

2. Habilite el direccionamiento de APPN en el puerto.  
**Nota:** Puesto que la opción Service Any está habilitada por omisión, el nodo acepta cualquier petición de conexión que reciba de otro nodo.
3. Habilite el Nodo de red APPN.
4. Configure los parámetros siguientes:
  - ID de red
  - Nombre del punto de control
5. Defina el número de XID para el parámetro de conexiones de subárea del nodo de red APPN (opcional).
6. Acepte todos los otros valores por omisión.
7. Realice las acciones siguientes opcionalmente:
  - Modifique parámetros del Direccionamiento de alto rendimiento
  - Configure el Peticionario de LU dependientes
  - Defina redes de conexiones
  - Defina correlaciones de nuevos nombres de CoS o nombres de modalidad
  - Ajuste el rendimiento de este nodo
  - Ejecute diagnósticos de rastreo de servicio de nodo
  - Reúna estadísticas para este nodo de red

### Notas:

1. El direccionamiento de APPN debe definirse y habilitarse en los puertos específicos que configure para que los utilice el nodo de red direccionador.
2. Deben habilitarse la función de puente y DLSw en los puertos de adaptador específicos que desee que utilice el nodo de red del dispositivo.

### Configuración para el inicio de las conexiones

Este grupo de pasos de configuración de APPN:

- Permite que el nodo de red acepte cualquier petición que reciba de otro nodo para establecer una conexión.
- Habilita el nodo de red para iniciar conexiones con otros nodos que especifique el usuario, incluidos nodos finales LEN.

Puesto que los nodos APPN pueden iniciar sesiones de CP-CP con el nodo de red direccionador, no hay necesidad de definir estos nodos en la configuración del direccionador, excepto en los casos siguientes:

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

Si ninguno de estos casos se aplica a su configuración, debe seguir los pasos de configuración descritos en la sección "Configuración mínima" en la página 27.

Utilice el procedimiento siguiente si desea la configuración para el inicio de las conexiones:

1. Si va a configurar APPN utilizando un puerto DLSw:

- a. Habilite la función de puente en el nodo
  - b. Habilite DLSw en el nodo
  - c. Defina el puerto DLSw con una dirección MAC administrada localmente para DLSw.
2. Seleccione los puertos sobre los que va a iniciar conexiones con nodos adyacentes. Los siguientes son los tipos de puertos DLC soportados por APPN:
    - Puerto LAN Red en Anillo
    - Puerto LAN Ethernet
    - Puerto serie Frame-relay
    - Puerto serie PPP
    - X.25
    - SDLC
    - MPC+
    - DLSw
    - Puerto IP
    - FDDI
  3. Habilite el direccionamiento de APPN en los puertos APPN con el parámetro *enable APPN routing on this port*.
 

**Nota:** Puesto que la opción Service Any está habilitada por omisión, el nodo acepta cualquier petición de conexión que reciba de otro nodo.
  4. Defina estaciones de enlace APPN en los puertos DLC seleccionados para los nodos adyacentes con los que este nodo de red puede iniciar una conexión.
 

**Nota:** No tiene que definir estaciones de enlace en cada puerto, sino sólo en aquellos sobre los que desea iniciar conexiones con nodos adyacentes.
  5. Habilite el nodo de red APPN.
  6. Configure los parámetros siguientes para el nodo de red APPN:
    - a. ID de red
    - b. Nombre del punto de control
  7. Defina el número de XID para el parámetro de conexiones de subárea del nodo de red APPN (opcional).
  8. Acepte todos los otros valores por omisión.
  9. Realice las acciones siguientes opcionalmente:
    - Modifique parámetros del Direccionamiento de alto rendimiento
    - Configure el Peticionario de LU dependientes
    - Defina redes de conexiones
    - Defina correlaciones de nuevos nombres de CoS o nombres de modalidad
    - Ajuste el rendimiento de este nodo
    - Ejecute diagnósticos de rastreo de servicio de nodo
    - Reúna estadísticas para este nodo de red

### Configuración para el control de las conexiones

Este grupo de pasos de configuración de APPN:

- Permite que el nodo de red acepte peticiones sólo de los nodos que especifique el usuario.
- Habilita el nodo de red para iniciar conexiones con otros nodos que especifique el usuario, incluidos nodos finales LEN.

Esta configuración proporciona un nivel de seguridad superior porque el usuario define explícitamente qué nodos APPN pueden comunicarse con este nodo de red direccionador. Una petición de conexión de un nodo adyacente sólo se aceptará si se ha configurado el parámetro de su nombre de CP calificado al completo en este nodo de red. Este grupo de pasos de configuración le permite opcionalmente tener un enlace seguro con cada nodo adyacente configurando la función de seguridad de nivel de sesión para cada enlace.

Utilice el procedimiento siguiente si desea la configuración para el control de las conexiones:

1. Seleccione los puertos sobre los que desea establecer conexiones con nodos adyacentes entre los siguientes tipos de puertos DLC soportados por APPN:
  - Puerto LAN Red en Anillo
  - Puerto LAN Ethernet
  - Puerto serie Frame-relay
  - Puerto serie PPP
  - X.25
  - DLSw
  - SDLC
  - MPC+
  - Puerto IP
  - FDDI
2. Defina los puertos seleccionados como puertos APPN directos con los parámetros siguientes:
  - Habilite *APPN routing on this port*
  - Inhabilite el parámetro de puerto *Service any*
3. Si va a configurar APPN utilizando un puerto DLSw:
  - Habilite la función de puente en el nodo
  - Habilite DLSw en el nodo.
  - Defina los puertos DLSw con el parámetro siguiente:
    - Defina una dirección MAC administrada localmente para DLSw
    - Inhabilite el parámetro *Service any node*
4. Habilite el direccionamiento de APPN en el puerto.
5. Defina estaciones de enlace APPN en los puertos DLC seleccionados para los nodos adyacentes:
  - que pueden iniciar una conexión con este nodo de red.
  - con los que desea que este nodo de red direccionador inicie una conexión.Especifique los siguientes parámetros de estación de enlace:
  - Nombre de CP calificado al completo del nodo adyacente (necesario)
  - Cualquier parámetro de direccionamiento necesario para el nodo adyacente
  - Y opcionalmente:
    - Seguridad de nivel de sesión de CP-CP
    - Clave de cifrado de seguridad
6. Habilite el nodo de red APPN.
7. Configure los parámetros siguientes para el nodo de red APPN:
  - ID de red



- Nombre del punto de control
8. Defina el número de XID para el parámetro de conexiones de subárea del nodo de red APPN (opcional).
  9. Acepte todos los otros valores por omisión.
  10. (Opcional) Configure las siguientes opciones de nodo de red direccionador:
    - Modifique parámetros del Direccionamiento de alto rendimiento
    - Configure el Peticionario de LU dependientes
    - Defina redes de conexiones
    - Defina correlaciones de nuevos nombres de CoS o nombres de modalidad
    - Ajuste el rendimiento de este nodo
    - Ejecute diagnósticos de rastreo de servicio de nodo
    - Reúna estadísticas para este nodo de red

## Configuración del Branch Extender

Para configurar el Branch Extender, establezca los parámetros de configuración siguientes de acuerdo con lo que corresponda a la red.

1. Utilice el mandato **set node** para:
  - a. Responder 1 para el Branch Extender a la pregunta Enable Branch Extender or Border Node. Si responde 0, no aparecerá ninguna de las siguientes preguntas sobre el Branch Extender.
  - b. Responder Full, Partial o None a la pregunta *Enable Branch Awareness Support* en función de si desea limitar el flujo de información topológica sobre los TG entre NN y BrNN.
  - c. Responder yes o no a la pregunta Permit search for unregistered LUs en función de si desea permitir o no búsquedas de la red troncal relativas a LU que no se hayan registrado con el servidor de nodos de red.
  - d. Su respuesta a la pregunta Branch uplink determinará el valor por omisión para la pregunta de nivel de enlace análoga.
2. Utilice el mandato **add link** para:
  - a. Responder yes a la pregunta *Branch uplink* si desea que el direccionador aparezca como un nodo final en este enlace. Un nodo final es para los enlaces con nodos de red de la red troncal. Tenga en cuenta que esta pregunta no aparece y queda forzada a yes si ha definido que la estación de enlace adyacente sea un nodo de red en una de las solicitudes de configuración anteriores. Responda no si desea que el direccionador aparezca como un nodo de red en este enlace. Un nodo de red es para los enlaces con nodos finales.
  - b. La pregunta Is uplink to another Branch Extender node sólo aparece si este enlace se ha definido como un recurso limitado y también se ha definido como enlace superior de Branch Extender. Responda yes si el nodo adyacente es otro Branch Extender.
  - c. La pregunta Preferred network node server sólo aparece si el nodo adyacente es un nodo de red y se da soporte a sesiones de CP-CP en este enlace. Puesto que sólo puede tener un servidor de nodos de red preferido, ya no le aparecerá esta pregunta una vez que se haya establecido en yes en cualquier enlace.

### Configuración de nodos Extended Border Node

Para configurar un nodo de frontera extendida, debe configurar uno de estos parámetros o más:

- Set node
- Add port
- Add link
- Add routing\_list
- Add cos\_mapping\_table

#### Set node

La solicitud utilizada anteriormente para habilitar el extensor de rama se ha expandido para permitirle elegir la función de extensor de rama, la función de nodo de frontera extendida o ninguna de las dos. Únicamente si habilita la función de nodo de frontera extendida aparecerá cualquiera de las otras solicitudes de nodo de frontera extendida.

Subnetwork visit count es la primera solicitud. Este parámetro define el número máximo de subredes con topología por las que puede expandirse una sesión. El valor definido aquí se utiliza como el valor por omisión para el nodo de frontera extendida. Puede especificar valores diferentes para subnetwork visit count cuando añada puertos, enlaces o listas de direccionamiento.

Cache search time es la siguiente solicitud de nivel de nodo. Especifica el número de minutos durante los cuales el nodo de frontera extendida retendrá información de búsquedas en diversas subredes. El propósito es ser el mecanismo primario para limitar el tamaño de esta antememoria. No obstante, también puede utilizarse el siguiente parámetro para controlar el tamaño de esta antememoria.

A continuación, aparece Maximum search cache size. Controla la misma estructura de datos controlada por el parámetro anterior. Si se establece en cero, el tamaño máximo es ilimitado. Sólo se desecharán entradas después de que haya caducado el tiempo de la antememoria de búsquedas. Si prefiere fijar un tamaño máximo para la antememoria de búsquedas, especifíquelo aquí. Si se alcanza este tamaño máximo antes de que ninguna entrada sobrepase el límite de tiempo, se desechan las entradas menos recientes.

List dynamics es la siguiente solicitud y le permite controlar cómo determina el nodo de frontera extendida los siguientes saltos posibles cuando intenta ubicar recursos (LU). La lista temporal de CP de siguiente salto posible se crea dinámicamente por medio del código operativo siempre que el nodo de frontera intenta ubicar un recurso. Este parámetro especifica los orígenes de los nombres de CP de siguiente salto que el nodo de frontera extendida puede utilizar para crear esta lista dinámica temporal de nombres de CP.

Después de que se haya creado la lista temporal, siempre se ordena de manera que los CP de siguiente salto configurados vayan en primer lugar seguidos de los CP asociados con recursos conocidos de nombre similar. Puede realizarse una reordenación adicional. Una vez completada toda la reordenación, el nodo de frontera extendida empieza a buscar el recurso de destino en un CP tras otro.

Tenga en cuenta que, una vez que el nodo de frontera extendida ubique realmente un recurso, recordará el CP de siguiente salto y siempre utilizará este CP de siguiente salto para ese recurso determinado, ignorando las listas de

direccionamiento. Las entradas de esta tabla de recursos ubicados pueden durar bastante. Se desechan si la tabla alcanza el tamaño máximo, si una búsqueda posterior en este CP no puede ubicar el recurso o si una búsqueda desde esta LU procede de un CP diferente.

El parámetro *list dynamics* se establece en uno de los valores siguientes. Es posible volver a especificar este valor para listas de direccionamiento individuales cuando configure, si lo hace, listas de direccionamiento individuales.

**None** El nombre de LU del recurso de destino se compara con los nombres de LU configurados en las listas de direccionamiento. Se selecciona la lista de direccionamiento con la mejor coincidencia de nombres de LU, y los nombres de CP de siguiente salto de esta lista configurada se colocan en la lista creada dinámicamente. Éste es el único origen de nombres de CP de siguiente salto posible cuando *list dynamics* se establece en *none*.

Tenga en cuenta que, si un nombre de LU no aparece en una lista de direccionamiento, la LU no será asequible para el nodo de frontera extendida cuando este parámetro *list dynamics* se establece en *none*.

**Limited** Aumenta la lista de nombres de CP de siguiente salto obtenidos a partir de la lista de direccionamiento configurada de la mejor coincidencia con nombres de CP obtenidos a partir del conocimiento que tiene el nodo de frontera extendida de los recursos y la topología existentes. Estos nombres de CP adicionales se obtienen de la siguiente manera:

- Añadiendo todos los nodos de frontera extendida nativos
- Añadiendo todos los nodos de frontera extendida y nodos de red adyacentes no nativos cuyos NETID coincidan con el NETID del recurso de destino.
- Examinando la tabla de recursos ya conocidos por el nodo de frontera extendida a causa del recibo de una variable GDS de encontrar o encontrado. Estos recursos se colocan en antememoria en la base de datos de servicios de directorio. Para cualquier entrada en que el ID de red de la LU colocada en antememoria sea el mismo que el destino de la búsqueda actual, los NN de la LU en antememoria se añaden a la lista de CP de siguiente salto.

Ninguno de estos nombres de CP de siguiente salto obtenidos dinámicamente se guarda permanentemente con los datos de configuración. La lista se vuelve a crear siempre que hay que ubicar un recurso.

**Full** Funciona igual que *Limited*, con la excepción de que se elimina la restricción de NETID coincidentes cuando se añaden todos los nodos de frontera extendida y nodos de red adyacentes no nativos.

Si se habilita *list optimization*, el proceso de reordenación descrito en la página 32 se repite una segunda vez y los nombres de CP obtenidos a partir de datos configurados también pueden elegirse para la reordenación.

Si se habilita *load balance across parallel inter-subnet boundaries*, el direccionador intentará equilibrar el número de sesiones a través de dos o más puntos de salida intersubredes paralelo. La configuración relevante tiene dos o más direccionadores que sirven de puntos de salida EBN en una subred y el mismo número en la otra subred. Cada direccionador tiene un TG intersubredes con un direccionador dife-

rente de la otra subred, con lo cual se forman dos o más enlaces paralelo. (Tenga en cuenta que éstos no son TG paralelo entre dos direccionadores.)

Para habilitar esta función de equilibrio de carga, debe configurar listas de direccionamiento en cada direccionador EBN de manera que las sesiones para los diferentes nombres de LU de destino tengan diferentes EBN de salida preferentes. También configurará la frontera intersubredes preferente y puede establecer vías de acceso de reserva.

### Add port

Si se habilita el nodo de frontera extendida, se presentan dos solicitudes adicionales cuando invoca el elemento de menú add port. Estos dos nuevos elementos establecen el valor por omisión para los parámetros del nivel de enlace análogos. Los valores de estos parámetros del nivel de enlace determinan el comportamiento de una estación de enlace.

*Subnetwork visit count* es el primero de éstos y describe el mismo concepto definido en el nivel de nodo. La primera vez que se configura un puerto, este parámetro se inicializa con el valor del nodo. Con este parámetro, permite que los puertos individuales se aparten del valor de nivel de nodo.

La otra nueva solicitud de nodo de frontera extendida controla *Adjacent subnetwork affiliation*. Le permite definir si el nodo adyacente está o no en la misma red que el nodo de frontera extendida. El valor especificado aquí se utilizará como valor por omisión para todos los enlaces del puerto. Los valores permitidos son:

**Native** El nodo adyacente está en la misma subred con topología que el nodo de frontera extendida.

### Non-native

El nodo adyacente no forma parte de la subred con topología del nodo de frontera extendida.

### Negotiable

El nodo adyacente puede estar o no en la misma subred con topología según cómo se defina éste. El nodo adyacente está en la subred con topología del nodo de frontera extendida a menos que la definición de enlace correspondiente del nodo adyacente sea una de las siguientes:

- Non-native
- Negotiable y el nodo adyacente tiene un nombre de red diferente
- Negotiable y el nodo adyacente ha definido el enlace como non-native

### Add link

Si se habilita el nodo de frontera extendida, cuando invoca el elemento de menú add link se presentan las dos mismas solicitudes adicionales que se han presentado anteriormente bajo add port.

*Subnetwork visit count* y *adjacent subnetwork affiliation* son el mismo concepto que se ha definido en el nivel de puerto. Se inicializan con el valor de puerto correspondiente la primera vez que se configura un enlace. Cambie el valor aquí si desea que diferentes enlaces tengan diferentes valores aunque estén en el mismo puerto.

## Add Routing Lists

Una lista de direccionamiento configurada le permite definir explícitamente uno o más CP de siguiente salto posible para uno o más recursos de destino (LU). Puede utilizarse el carácter comodín "\*" al definir los nombres de LU para reducir la cantidad de datos configurados. También puede variar algunos de los valores por omisión de nivel de nodo para una lista de direccionamiento determinada.

Puede definir diversas listas de direccionamiento. Normalmente, un grupo de LU con requisitos similares de direccionamiento se configurará en una sola lista de direccionamiento. Los grupos de LU adicionales, cada uno con sus propios requisitos de direccionamiento, se configurarán en listas de direccionamiento adicionales.

Existen límites respecto al número de nombres de LU y número de nombres de CP utilizados en las listas de direccionamiento. Estos límites varían según el modelo de direccionador que tenga. Vea la Tabla 39 en la página 214 para obtener detalles sobre el mandato de configuración. Se han establecido límites para permitir la mayor flexibilidad posible en varios entornos. La capacidad del direccionador para manejar la especificación de muchas listas de direccionamiento, cada una con muchos nombres de LU y nombres de CP, está limitada por la disponibilidad de la memoria de la configuración permanente, la memoria del direccionador y la memoria compartida de APPN. Consulte la sección "Ajuste de nodo APPN" en la página 41 para obtener una descripción de los parámetros de ajuste de APPN que controlan la cantidad de memoria compartida.

Recuerde, a propósito de la descripción de la solicitud *set node*, que las listas de direccionamiento configuradas nunca se modifican por medio del código operativo. Cuando el nodo de frontera extendida utiliza una lista de direccionamiento determinada, copia los nombres de CP de siguiente salto en una lista de direccionamiento temporal. Esta lista de direccionamiento dinámica temporal aumenta con entradas dinámicas de acuerdo con lo que permita el valor de configuración del parámetro *list dynamics*. Esta lista temporal tiene una corta duración y se desecha una vez encontrado el recurso de destino o una vez agotada la lista.

La solicitud *routing list name* es la primera que puede ver cuando añade o modifica una lista de direccionamiento. El código operativo no utiliza este nombre de ninguna manera. Su finalidad es la de permitirle identificar una lista de direccionamiento específica por si desea modificarla o suprimirla más adelante.

*Subnetwork visit count* y *list optimization* son las dos próximas solicitudes y siguen el mismo concepto que los parámetros definidos en el nivel de nodo análogos. Una nueva lista de direccionamiento inicializa estos valores con los valores de nivel de nodo actuales. Cambie estos valores para listas de direccionamiento individuales según lo que determinen sus requisitos.

Sigue(n) la(s) solicitud(es) *Destination LU*. Aquí puede configurar, como mínimo, un recurso de destino y, opcionalmente, más de uno. Cualquiera de los nombres de FQLU puede terminar de forma prematura con el comodín de cola "\*" para identificar a un grupo de LU. No puede incluir un "\*" en medio de un nombre de FQLU.

Una de las listas de direccionamiento puede especificar un "\*" autónomo como una de las LU de destino. Si se hace así, esta lista de direccionamiento se conocerá como la lista de direccionamiento por omisión, y el nodo de frontera extendida utilizará esta lista de direccionamiento por omisión para todas las LU de destino que

no coincidan bien con las LU especificadas en las otras listas de direccionamiento. Esta lista también se utiliza para buscar LU cuando se ha indicado INAUTHENTIC NETID.

Cuando se modifica una lista de direccionamiento existente con muchos nombres de LU, el proceso de pasar por los nombres de LU puede resultar bastante pesado. Existe un número de teclas de atajo definidas para ayudar a agilizar el paso por una lista de nombres existente. Estas teclas de atajo están definidas en la sección de información detallada sobre el mandato de configuración.

Las solicitudes *Routing CP* son la última parte del proceso consistente en entrar una lista de direccionamiento. Aquí se suministran los nombres de uno o más CP que pueden tener conocimiento de cómo alcanzar la lista de LU configurada. Junto con cada nombre de CP puede configurar una cuenta opcional de visitas a subred. Esto le permite especificar otro número máximo de subredes que puede atravesar una sesión para diferentes CP.

Además de configurar nombres de FQCP explícitamente, hay un par de palabras clave definidas equivalentes al nombre de CP del nodo local, a todos los nodos de frontera extendida nativos, etc. Consulte la sección de información detallada sobre el mandato de configuración para saber qué palabras clave son.

Están disponibles las mismas teclas de atajo que en la lista de nombres de LU para agilizar el paso por una lista de nombres de CP existente.

### **Add CoS Mapping Table**

La tabla de correlación de clase de servicio permite la conversión de nombres de CoS no nativos en nombres de CoS nativos y viceversa. Las redes no nativas que utilizan los mismos nombres de CoS que la red nativa del nodo de frontera extendida no necesitan tener definida una tabla de correlación de CoS. Si sólo son algunos nombres de CoS no nativos los que difieren de los nombres de CoS nativos, únicamente deben configurarse en una tabla de correlación de CoS los que difieren.

Una tabla de correlación de CoS determinada puede aplicarse a una sola o diversas redes no nativas. Puede configurar diversas tablas de correlación de CoS si es necesario.

Existen límites respecto al número de nombres de red no nativa utilizados en las tablas de correlación de CoS. Estos límites varían según el modelo de direccionador que tenga. Vea la Tabla 40 en la página 217 para obtener detalles sobre el mandato de configuración. Se han establecido límites para permitir la mayor flexibilidad posible en varios entornos. La capacidad del direccionador para manejar la especificación de muchas tablas de correlación de CoS, cada una con muchos nombres de red no nativa y pares de nombres de CoS, está limitada por la disponibilidad de la memoria de la configuración permanente, la memoria del direccionador y la memoria compartida de APPN. Consulte la sección "Ajuste de nodo APPN" en la página 41 para obtener una descripción de los parámetros de ajuste de APPN que controlan la cantidad de memoria compartida de APPN.

*CoS mapping table name* es la primera solicitud. Como sucede con el nombre análogo para las listas de direccionamiento, el código operativo no utiliza este parámetro. Su finalidad es permitirle referirse a una tabla de correlación de CoS específica para poder modificarla o suprimirla. Las diferentes tablas de correlación

de CoS deben tener nombres diferentes, pero una tabla de correlación de CoS determinada puede tener un nombre idéntico a una lista de direccionamiento.

A continuación, *Non-native CP* solicita uno o más nombres. Éstos se utilizan para especificar las redes no nativas a las que se aplica esta tabla de correlación de CoS.

Como con los nombres de LU de una lista de direccionamiento, puede terminar de forma prematura cualquiera de los nombres de FQCP en cualquier punto con el comodín de cola “\*”. Esto le permite especificar un rango de nombres de FQCP no nativo en una o más redes no nativas. No puede incluir un comodín en medio de un nombre de FQCP.

Una sola tabla de correlación de CoS del nodo de frontera extendida puede tener un comodín “\*” autónomo como uno de los nombres de CP no nativo. Esta tabla se conoce como la *tabla de correlación de CoS por omisión*, y será la tabla utilizada por el nodo de frontera extendida siempre que ninguna otra tabla tenga un nombre de CP que coincida con la red no nativa.

*CoS name pairs* es la parte final del proceso consistente en configurar una tabla de correlación de CoS. Aquí se le solicitan uno o más pares de nombres de CoS. Cada par de nombres de CoS consta de un nombre de CoS nativo seguido del nombre de CoS correspondiente utilizado en la red no nativa.

El nodo de frontera extendida utiliza esta tabla para la conversión de redes nativas en no nativas y viceversa. Si tiene que correlacionar diversos nombres de CoS nativos con un nombre de CoS no nativo común, debe configurar un par de nombres de CoS para cada correlación posible. De manera similar, puede tener que correlacionar diversos nombres de CoS no nativos con un nombre de CoS nativo común, y esto también puede realizarse configurando un par de nombres de CoS para cada correlación posible. Si hay diversas correlaciones posibles en una tabla, el nodo de frontera extendida utilizará la primera correlación exacta que encuentre.

Cada tabla de correlación de CoS puede tener un par de nombres de CoS en que el nombre de CoS no nativo sea el comodín “\*”. Ésta es la entrada de *correlación de CoS por omisión* de esa tabla y se utiliza para convertir todos los nombres de CoS no nativos irreconocidos en un solo nombre de CoS nativo. Cada tabla de correlación de CoS puede tener una de estas entradas de correlación de CoS por omisión. Nunca puede codificar un “\*” como nombre de CoS nativo.

## Direccionamiento de alto rendimiento

Vea la Tabla 3 en la página 25 para obtener la lista de puertos que dan soporte al HPR.

Consulte la sección “Requisitos de la configuración para APPN” en la página 26 para obtener información acerca de cómo configurar los protocolos que dan soporte al direccionamiento de APPN y HPR sobre DLC directos en el direccionador. En el caso de parámetros de HPR como, por ejemplo, los temporizadores de conmutación de la vía de acceso y reintentos, la configuración se realiza en el nivel de nodo y no se especifica para adaptadores individuales.

### DLUR

Vea la Tabla 3 en la página 25 para obtener la lista de puertos que dan soporte al DLUR.

### Configuración de puntos focales

Los puntos focales pueden ser explícitos o implícitos. Los puntos focales explícitos se configuran en el punto focal en sí. No es necesaria ninguna configuración en el direccionador.

Por otra parte, los puntos focales implícitos sí se configuran en el direccionador. Puede configurarlos con el mandato **add focal\_point**. Añada primero el punto focal implícito primario. Si añade otro punto focal, se conocerá como el primer punto focal implícito de reserva. Si añade otro más, se conocerá como el segundo punto focal implícito de reserva. Pueden añadirse hasta ocho puntos focales implícitos de reserva para un total de 9.

Para suprimir un punto focal, utilice el mandato **delete focal\_point**. Se le solicitará el nombre del punto focal a suprimir. Cuando se suprime el nombre, los puntos focales restantes retienen su posición relativa entre sí. Los puntos focales subsiguientes se añadirán al final de la lista.

No es posible insertar un punto focal en medio de la lista. Debe suprimirlos uno por uno y, a continuación, volver a entrar la lista entera.

### Configuración del tamaño de la cola de alertas retenidas

Para configurar el tamaño de la cola de alertas retenidas, entre el mandato **set management** y responda a la pregunta Held Alert Queue Size. La cola toma por omisión el tamaño de 10 alertas y los valores válidos son desde 0 a 255 alertas.

Al aumentar el tamaño de la cola de alertas retenidas, es necesaria memoria adicional. Si lo establece en un valor alto, es posible que desee ajustar el valor de Maximum Shared Memory. Consulte la sección "Ajuste de nodo APPN" en la página 41 para obtener información adicional.

### Definición de características de grupo de transmisión (TG)

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

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

Estas características de TG por omisión también se utilizan para estaciones de enlace dinámicas establecidas cuando un nodo adyacente solicita una conexión con el nodo de red direccionador pero no tiene una definición de estación de enlace predefinida en el nodo de red direccionador. Debe habilitarse el parámetro *Service any node*.



Puede cambiar los siguientes parámetros utilizando la interfaz **talk 6**> así como el Programa de configuración del direccionador:

- el coste por tiempo (de conexión)
- el coste por byte
- las características de TG definidas por el usuario 1 - 3
- la capacidad efectiva
- el retardo de propagación
- la seguridad

## Cómo calcular rutas de APPN utilizando características de TG

La función de cálculo de ruta de APPN utiliza una definición de CoS para TG que es una tabla que contiene filas de rangos de las características de TG. Cada fila define un rango determinado para cada una de las ocho características de TG y el peso del TG correspondiente a esa fila. APPN empieza por el principio de la tabla y desciende por la misma hasta que los ocho valores relacionados con los parámetros de las características de TG encajan en los rangos determinados para esa fila. A continuación, APPN asigna el peso de dicha fila como peso de TG para ese enlace. También hay una definición de CoS para nodos que calcula el peso de un nodo. La función de cálculo de ruta continúa hasta que ha encontrado la vía de acceso con el peso combinado menor entre los TG y nodos. Ésta es la ruta de menor peso.

Como ejemplo de cómo se utilizan las características de TG para influir en la selección de una ruta de un nodo de red APPN, supongamos que una ruta del direccionador nodo de red A al direccionador nodo de red D puede pasar por el direccionador nodo de red B o por el direccionador C. En este ejemplo, el direccionador A define conexiones PPP de puerto serie con el direccionador B y el direccionador C. No obstante, la conexión del direccionador A con el B es un enlace de 64 Kbps, mientras que la conexión del direccionador A con el C es un enlace de velocidad más lenta: 19,2 Kbps.

Para asegurarse de que la conexión de mayor velocidad del direccionador A con el B se vea como la vía de acceso más aconsejable para el tráfico interactivo de APPN de direccionamiento, se modificará la característica de TG de capacidad efectiva para la estación de enlace asociada con esta vía de acceso. En este caso, el valor por omisión de la capacidad efectiva es X'38', que representa con propiedad una velocidad de enlace de unos 19,2 Kbps. No obstante, la capacidad efectiva se cambiará por X'45' para representar adecuadamente el enlace de 64 Kbps. Puesto que la capacidad efectiva para el TG del direccionador A al B es ahora X'45', se asigna a esta vía de acceso un peso menor en el archivo de CoS para el tráfico interactivo. Como consecuencia, la conexión del direccionador A con el direccionador B se representa como conexión más aconsejable que la del direccionador A con el direccionador C.

El usuario también puede cambiar las características de TG si desea favorecer intencionadamente determinados TG para la selección de ruta. Además de las cinco características de TG estructuradas, también hay tres características de TG definidas por el usuario. Puede establecer estas características de TG definidas por el usuario con el fin de predisponer el cálculo de selección de ruta a favor de determinadas vías de acceso.

**Nota:** Respecto a los puertos DLSw, las características de TG que defina sólo tienen efecto en la selección de rutas entre nodos APPN sobre dichos

puertos. Estas características no tienen efecto directo en ningún direccionamiento intermedio realizado por DLSw en nombre de APPN.

## Opciones de CoS

Puede utilizar un modelo con el fin de crear nuevos nombres de CoS definidos por el usuario y definiciones asociadas para TG y nodos que puedan utilizarse con nuevos nombres de modalidad o correlacionarse con nombres de modalidad existentes.

Además, puede crear nuevos nombres de modalidad que puedan correlacionarse con nombres de CoS existentes.

Cada archivo de definición de CoS se identifica mediante un nombre de CoS y contiene una prioridad de transmisión asociada y una tabla de rangos de características de TG y nodo aceptables que APPN compara con las características de TG y nodo reales para determinar los pesos de los TG y nodos con que calcula la ruta de menor peso para la sesión. Utilizando el Programa de configuración, puede:

- Ver un archivo de definición de CoS:
  - Ver la prioridad de transmisión
  - Ver una lista de referencias a fila de nodo junto con sus pesos correspondientes
  - Ver una lista de referencias a fila de TG junto con sus pesos correspondientes
- Seleccionar las tablas de COS estándares o de ATM como modelos para establecer un nuevo archivo de definición de CoS definido por el usuario con un nuevo nombre de CoS:
  - Importar un archivo de definición de CoS definido por IBM para utilizarlo como modelo
  - Importar un archivo de definición de CoS definido por el usuario que se haya exportado anteriormente para utilizarlo como modelo
- Definir los rangos de mínimo y máximo para las características de TG definidas por el usuario en una definición de CoS definida por IBM.

**Nota:** En una definición de COS definida por IBM sólo puede editar los rangos de las características de TG definidas por el usuario.

Utilizando el Programa de configuración o **talk 6**, puede:

- Utilizar las tablas de CoS estándares o las tablas de CoS mejoradas (para ATM).
- Definir un nuevo nombre de modalidad y su correlación con un nombre de CoS.
- Cambiar una correlación de nombre de modalidad con nombre de CoS:
  - Volver a correlacionar un nombre de modalidad definido por IBM con un nombre de CoS diferente.
  - Volver a correlacionar un nombre de modalidad definido por el usuario que se haya especificado anteriormente con un nombre de CoS diferente.

Consulte el tratamiento de los servicios de topología y direccionamiento en el manual *IBM SNA APPN Architecture Reference* para obtener una descripción de las tablas de CoS estándares y de ATM.

## Ajuste de nodo APPN

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

- Estableciendo manualmente los valores de los parámetros de ajuste *maximum shared memory*, *percent of APPN shared memory to be used for buffers* y *maximum cached directory entries* con el Programa de configuración o la opción **talk 6** de la interfaz de línea de mandatos.

Consulte las páginas Web de soporte del direccionador relativas a la herramienta que puede utilizar con el fin de obtener una estimación de la memoria necesaria para APPN y otros componentes del direccionador.

- Seleccionando valores para los parámetros *maximum number of ISR sessions*, *maximum number of adjacent nodes* y otros parámetros que muestra la Tabla 10 en la página 134, y haciendo que el algoritmo de ajuste calcule automáticamente los valores de los parámetros de ajuste *maximum shared memory* y *maximum cached directory entries*.

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

El parámetro *maximum shared memory* afecta a la cantidad de almacenamiento disponible para que el nodo de red APPN realice operaciones de red. Se puede permitir que el direccionador elija un valor por omisión de fines generales para este valor sobre la base de la memoria instalada.

El parámetro *maximum cached directory entries* afecta a la cantidad de información de directorio que se almacenará o colocará en antememoria para reducir el tiempo que tarda la ubicación de un recurso de la red.

En general, el ajuste del nodo de red APPN implica una relación directa entre rendimiento del nodo y utilización de almacenamiento. A mejor rendimiento, más necesidad de almacenamiento.

### Notas para el ajuste

1. Los valores de los parámetros de ajuste deben reflejar un desarrollo previsto de la red.
2. Si define redes de conexiones en la red APPN y cuenta con que la mayoría de los nodos finales inicien sesiones de LU-LU con otros nodos finales en la misma red de conexiones, debe establecer el parámetro *maximum number ISR sessions* en un valor menor (1). La utilización de las redes de conexiones de esta manera reduce los requisitos de memoria compartida para el nodo de red direccionador porque la mayoría de las sesiones de LU-LU no fluirán por el componente de APPN del direccionador.
3. Puesto que el parámetro *maximum shared memory* afecta a la asignación de almacenamiento en el direccionador, debe ir con cuidado cuando defina este parámetro explícitamente. Utilice el valor por omisión auto-configured a menos que realice un análisis más detenido mediante la herramienta para almacenamiento del direccionador.

### Servicio de nodo (rastreos)

La opción Servicio de nodo (rastreos) de APPN le permite iniciar cualquier rastreo de APPN mediante **talk 6** o el Programa de configuración. Los rastreos se activan cuando se aplica el archivo de configuración al direccionador. Los rastreos continuarán activos hasta que se detengan cuando se aplique al direccionador una nueva configuración que los detenga.

**Nota:** La ejecución de rastreos en el direccionador puede afectar a su rendimiento. Sólo deben iniciarse rastreos cuando se necesiten para el servicio del nodo y deben detenerse tan pronto como se reúna la cantidad de información de rastreo necesaria.

Los rastreos de APPN se agrupan en las 5 categorías siguientes:

- Los rastreos de nivel de nodo especifican rastreos relativos al nodo de red APPN global.
- Los rastreos de señales interprocesos especifican rastreos de nivel de componente relativos a las señales entre componentes de APPN.
- Los rastreos de entrada y salida de módulos especifican rastreos de nivel de componente relativos a la entrada y salida de los módulos de APPN.
- Los rastreos generales especifican rastreos de nivel de componente relativos a los componentes de APPN.
- Los rastreos varios especifican información de rastreo sobre las transmisiones y recepciones de DLC.

Ahora puede habilitar/inhabilitar todos los distintivos de rastreo mediante Talk 6 utilizando la pregunta Turn all trace flags off bajo el mandato **set trace** o mediante el Programa de configuración. Vea la página 139 para obtener más información.

Ahora puede filtrar los datos de rastreo de transmisiones y recepciones de control de enlace de datos por medio de cualquier tipo de mensaje o especificando el valor de longitud máxima de los datos por paquete a rastrear. Vea la Tabla 16 en la página 153 para obtener más información.

### Estadísticas de contabilidad y nodos

Las sesiones intermedias son sesiones de LU-LU que pasan por el nodo de red APPN pero cuyos puntos finales (origen y destino) se encuentran fuera del nodo de red. La información sobre las sesiones intermedias se genera mediante el componente ISR del nodo de red y se clasifica en dos categorías:

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

La habilitación del parámetro Collect intermediate session information indica al direccionador que reúna nombres y contadores de sesiones relativos a todas las sesiones intermedias activas. La habilitación del parámetro Save RSCV information for intermediate sessions indica al direccionador que reúna datos de RSCV relativos a las sesiones intermedias activas. Los datos de RSCV son útiles para la supervisión de rutas de sesiones. En ambos casos, puede recuperar los datos de las sesiones activas emitiendo los mandatos de SNMP **get** y **get-next** para las variables de la Base de la información de gestión (MIB) APPN.

La función Collect intermediate session information toma por omisión el valor de estar inhabilitada. Puede habilitarla utilizando el Programa de configuración o utilizando el mandato Talk 6 **set management**. Una vez habilitada, puede controlarla, incluida su inhabilitación y rehabilitación, utilizando los mandatos de SNMP **set** para la MIB APPN de contabilidad.

**Nota:** Esta función puede utilizar una cantidad significativa de memoria de APPN. Debe configurar APPN con la memoria necesaria antes de habilitar la reunión de información del ISR.

Para la contabilidad, puede mantener registros de las sesiones intermedias que pasan por el nodo de red. Los registros de datos pueden crearse y almacenarse en la memoria del direccionador. Debe utilizarse SNMP para recuperar datos de los registros de contabilidad almacenados en la memoria local del direccionador.

**Notas:**

1. Puede habilitar la reunión de datos de las sesiones intermedias activas (características y contadores de sesiones) de las variables de la MIB de SNMP de manera explícita o implícita.

Para habilitar la reunión de manera explícita, establezca el parámetro Collect intermediate session information en yes.

Para habilitar la reunión de manera implícita, establezca Create intermediate session records en yes. Este valor alterará temporalmente el valor de Collect intermediate session information.

2. Los cambios de configuración realizados en los parámetros de contabilidad de APPN utilizando la interfaz Talk 6 no tendrán efecto hasta que se reinicie el direccionador o la función de APPN del direccionador. No obstante, puede efectuar cambios interactivamente emitiendo los mandatos de SNMP **set** para modificar las variables de la MIB APPN asociadas con los parámetros de configuración. Consulte el manual *Guía del usuario de software* para conseguir una lista de estas variables de la MIB.
3. Se obtienen datos de RSCV de las sesiones intermedias examinando la petición BIND utilizada para activar una sesión entre dos LU. No se reúnen datos de RSCV relativos a las sesiones que ya se han establecido porque no está disponible la información de BIND de las mismas.
4. No se reúnen datos de sesiones intermedias para sesiones de HPR porque las sesiones intermedias no forman parte del HPR. Si el direccionador contiene una frontera de ISR/HPR, se reúnen datos de sesiones intermedias al fluir a través de esta frontera.

## Algoritmo de reintentos de DLUR

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

Si Perform retries to restore disrupted pipe es No:

- Si un DLUR recibe un mensaje de fin de no interrupción UNBIND (código de detección de X'08A0 000A'), espera indefinidamente a que un DLUS restablezca el conducto interrumpido.
- Si el conducto falla por cualquier otra razón distinta de un mensaje de fin de no interrupción UNBIND, el DLUR intenta acceder al DLUS primario una vez. Si

esta acción no se realiza satisfactoriamente, el DLUR intenta acceder al DLUS de reserva. Si un DLUR no puede acceder al DLUS de reserva, espera indefinidamente a que un DLUS restablezca el conducto interrumpido.

Si Perform retries to restore disrupted pipe es Yes, un DLUR intentará restablecer el conducto basándose en los parámetros de configuración siguientes:

- Delay before initiating retries
- Perform short retries to restore disrupted pipe
- Short retry timer
- Short retry count
- Perform long retries to restore disrupted pipe
- Long retry timer

Hay dos casos que determinan el algoritmo de reintentos:

- En el caso de recibir un mensaje de fin de no interrupción UNBIND:
  1. Se espera el período de tiempo especificado por el parámetro Delay before initiating retries. Este retardo permite un período para la entrada en función de un SSCP, en que el conducto se restablecería mediante un nuevo DLUS sin ninguna acción por parte del DLUR.
  2. Se intenta acceder al DLUS primario.
  3. Si esta acción no es satisfactoria, se intenta acceder al DLUS de reserva.
  4. Si el intento de acceder al DLUS de reserva no es satisfactorio, el DLUR realizará los reintentos descritos en los pasos del 5 al 7 mientras la DSPU solicite una ACTPU.
  5. Se espera el período de tiempo especificado por el parámetro Long retry timer.

**Nota:** Si Perform long retries to restore disrupted pipe es No, no se realizarán más reintentos.
  6. Se intenta acceder al DLUS primario.
  7. Si el intento de acceder al DLUS primario no es satisfactorio, se intenta acceder al DLUS de reserva.

### Ejemplo:

- Supongamos los siguientes valores de parámetro:
  - Delay before initiating retries = 120 sec
  - Perform short retries to restore disrupted pipe = yes
  - Short retry timer = 60 sec
  - Short retry count = 2
  - Perform long retries to restore disrupted pipe = yes
  - Long retry timer = 300 sec
- Falla la activación de conducto.
- Se espera el período de 120 segundos (el valor de Delay before initiating retries).
- Se realiza un reintento con el DLUS primario y, si falla, con el DLUS de reserva.

- Si falla el reintento, se espera el período de 300 segundos (el valor de Long retry timer), se realiza un reintento con el DLUS primario y, si falla, con el DLUS de reserva.
- Si fallan los reintentos, se continúan realizando reintentos con el DLUS primario y el de reserva, esperando 300 segundos entre las secuencias de reintentos, mientras la DSPU solicite una ACTPU.
- En todos los otros casos de anomalías de conducto, el DLUR realizará de manera inmediata un intento con el DLUS primario y luego con el de reserva. Si esto falla, el DLUR:

1. Esperará el período de tiempo especificado por el valor mínimo de los parámetros Short retry timer y Delay before initiating retries.
2. Intentará acceder al DLUS primario.
3. Si el intento de acceder al DLUS primario no es satisfactorio, intentará acceder al DLUS de reserva.
4. Si la activación del conducto sigue fallando, el DLUR realizará los reintentos descritos en los pasos del 1 al 3 el número de veces especificado en Short retry count.

Si se agota el valor de Short retry count, el DLUR realizará los reintentos definidos en los pasos del 5 al 7 mientras la DSPU solicite una ACTPU.

5. Esperará el período de tiempo especificado por el parámetro Long retry timer.

**Nota:** Si Perform long retries to restore disrupted pipe es No, no se realizarán más reintentos.

6. Intentará acceder al DLUS primario.
7. Si el intento de acceder al DLUS primario no es satisfactorio, intentará acceder al DLUS de reserva.

#### Ejemplo:

- Supongamos los siguientes valores de parámetro:
  - Delay before initiating retries = 120 sec
  - Perform short retries to restore disrupted pipe = yes
  - Short retry timer = 60 sec
  - Short retry count = 2
  - Perform long retries to restore disrupted pipe = yes
  - Long retry timer = 300 sec
- Falla la activación de conducto.
- De inmediato se realizan reintentos con los DLUS primario y de reserva.
- Si falla el reintento, se espera el período de 60 segundos (el valor de Short retry timer).
- Se realiza un reintento con el DLUS primario. Si falla este reintento, se realiza un reintento con el DLUS de reserva. Éste es el intento núm. 1 de Short retry count.
- Si falla, se espera el período de 60 segundos (el valor de Short retry timer).

- Se realiza un reintento con el DLUS primario y luego con el DLUS de reserva. Éste es el intento núm. 2 de Short retry count. En este momento se ha agotado Short retry count.
- Si sigue fallando, se espera el período de 300 segundos (el valor de Long retry timer). Después se realiza un reintento con el DLUS primario. Si falla este reintento, se realiza un reintento con el DLUS de reserva.
- Si falla el reintento, se continúan realizando reintentos con el DLUS primario y el de reserva, esperando 300 segundos entre las secuencias de reintentos, mientras la DSPU solicite una ACTPU.

## Implementación de APPN en el direccionador con DLSw

El direccionador también da soporte a APPN sobre DLSw para la conectividad con nodos mediante un asociado a DLSw remoto. Se muestra un ejemplo de ello en la Figura 2. Este soporte permite que los clientes con redes DLSw accedan a APPN sin necesitar un direccionador de DLSw externo. También permite que los servidores TN3270 remotos accedan al sistema principal mediante los enlaces DLSw de subárea.

**Nota:** Es recomendable utilizar APPN sobre DLC directos cuando estén disponibles en lugar de APPN sobre DLSw. No obstante, únicamente con DLSw local puede utilizar un servidor TN3270 remoto enlaces de subárea SDLC o QLLC X.25 para acceder al sistema principal.

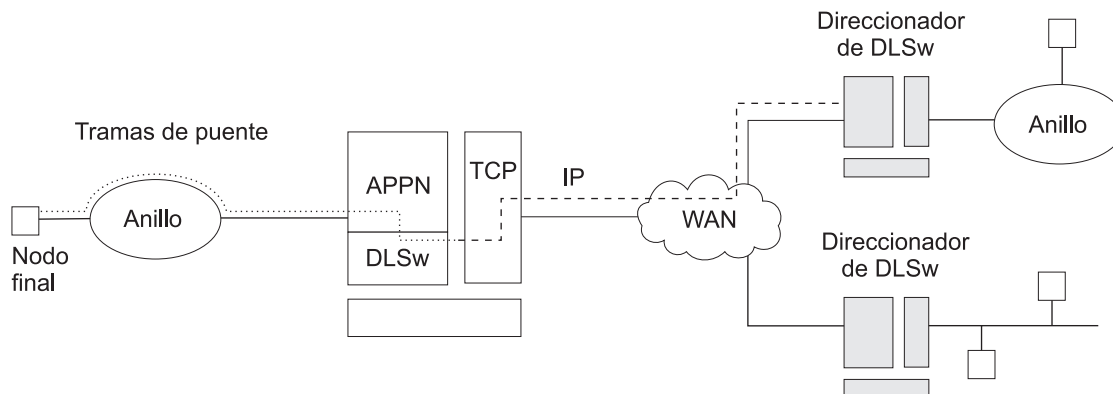


Figura 2. Flujo de datos de una configuración de APPN con puerto DLSw

Restricciones de la configuración de APPN con DLSw:

- Un solo puerto lógico DLSw por direccionador
- Uso de una dirección MAC administrada localmente
- El HPR no está soportado en los puertos DLSw
- Los puertos DLSw no pueden ser miembros de redes de conexiones
- Los TG paralelo no están soportados en los puertos DLSw

Consulte la sección “Configuración del direccionador como nodo de red APPN” en la página 27 para configurar APPN con DLSw.



### Cómo utiliza APPN los puertos DLSw para transportar datos

Cuando se configura APPN en el direccionador de manera que utilice el puerto de conmutación del enlace de datos (DLSw), DLSw proporciona una interfaz orientada a las conexiones (el tipo 2 de LLC de 802.2) entre el componente de APPN del direccionador y los nodos APPN y SNA conectados a un asociado a DLSw remoto.

Al configurar un puerto DLSw para APPN en el direccionador, asigna al nodo de red una o más direcciones de SAP y una dirección MAC de tipo exclusivo que le permiten comunicarse con DLSw. La dirección MAC para el nodo de red se administra localmente y no debe corresponderse con ninguna dirección MAC física de la red DLSw. Sólo son necesarias diversas direcciones de SAP cuando el usuario desea configurar el servidor TN3270 de manera que acceda al sistema principal mediante DLSw y necesita más de una PU dependiente.

### Implementación de una red de conexiones APPN BAN Frame Relay

La implementación de una red de conexiones APPN BAN Frame Relay le permite definir un puerto APPN Frame Relay que dé soporte al formato de puente de Frame Relay (BAN) en una red de conexiones.

Un recurso de transporte de acceso compartido (SATF) es un recurso de transmisión, como, por ejemplo, Red en Anillo o Ethernet, en el que los nodos conectados al SATF pueden conseguir una conectividad de cualquiera con cualquiera. Esta conectividad de cualquiera con cualquiera permite conexiones directas entre dos nodos, lo que elimina el direccionamiento a través de nodos de red intermedios y el paso repetitivo de los datos correspondientes por el SATF. Para conseguir esta conectividad directa, deben definirse TG en cada nodo para todos los otros nodos.

El SATF mostrado en la Figura 3 ilustra que el NN APPN del direccionador debe definir una estación de enlace en cada nodo de la Red en Anillo con el fin de iniciar una conexión con cada nodo de la Red en Anillo. El NN APPN debe tener conocimiento de la dirección DLCI del enlace Frame Relay y de la dirección MAC de cada nodo de la Red en Anillo. Si los nodos de la Red en Anillo desean iniciar una conexión con el NN APPN, deben definir una estación de enlace en el NN APPN del dispositivo y especificar:

- La dirección MAC DLCI de BAN si el dispositivo que conecta la Red en Anillo a la red frame relay realiza la función BAN
- La dirección MAC del identificador de Boundary Node si el dispositivo que conecta la Red en Anillo a la red Frame Relay es un puente

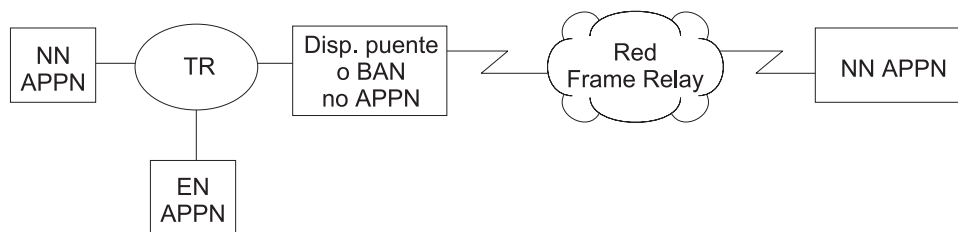


Figura 3. Vista lógica con soporte de red de conexiones BAN/trama de puente de Frame Relay

**Nota:** En este diagrama y en todos los diagramas siguientes sobre BAN Frame Relay, APPN reside en el 2216.

## Utilización de APPN

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

La Figura 4 muestra todos los nodos como miembros de la misma red de conexiones. Los nodos utilizan la red de conexiones para establecer comunicación con todos los otros nodos sin necesidad de crear conexiones con todos los otros nodos del SATF. Para convertirse en un miembro de una red de conexiones, debe conectarse un puerto de un nodo APPN a una red de conexiones mediante la definición de una interfaz de red de conexiones. Cuando se activa el puerto, se crea un TG de red de conexiones mediante el componente de APPN para un Nodo de direccionamiento virtual (VRN). Este TG identifica la conexión directa del puerto a la red de conexiones. El nombre de CP del VRN es el nombre de la red de conexiones.

Puesto que está representada la conectividad mediante un TG de un nodo determinado a un VRN, el servidor de nodos de red puede utilizar los servicios normales de topología y direccionamiento (TRS) para calcular la vía de acceso directa entre dos nodos cualesquiera conectados a la red de conexiones. El nodo de destino devuelve información de señalización de DLC durante el proceso normal de Locate para permitir que el nodo de origen establezca una conexión directamente con el nodo de destino.

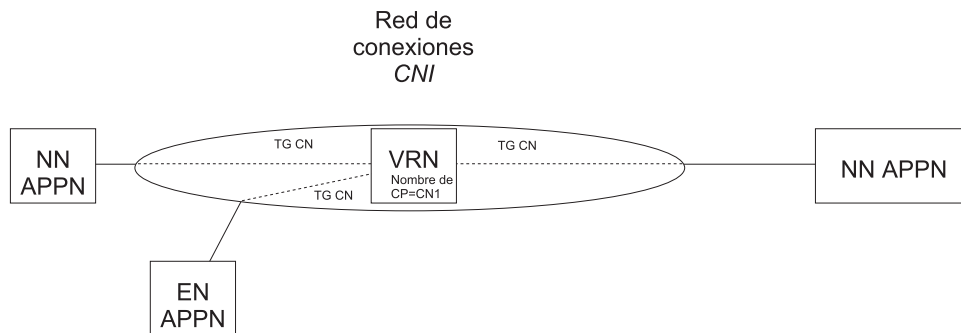


Figura 4. Red de conexiones APPN BAN/trama de puente de Frame Relay

A continuación, se indican las limitaciones que existen al utilizar redes de conexiones APPN BAN Frame Relay:

- Puede definirse la misma red de conexiones en un solo SATF.
- Todos los puertos Frame Relay pertenecientes a la misma red de conexiones del direccionador deben utilizar el mismo número de DLCI para conectarse a la red Frame Relay.
- Cuando se utiliza la función de puente en lugar de BAN, todos los puertos Frame Relay pertenecientes a la misma red de conexiones del direccionador deben tener definido el mismo par de direcciones MAC BNI/SAP.
- No pueden establecerse sesiones de CP-CP sobre los enlaces establecidos en una red de conexiones.

## Definiciones de muestra de red de conexiones APPN BAN Frame Relay

### Ejemplo 1

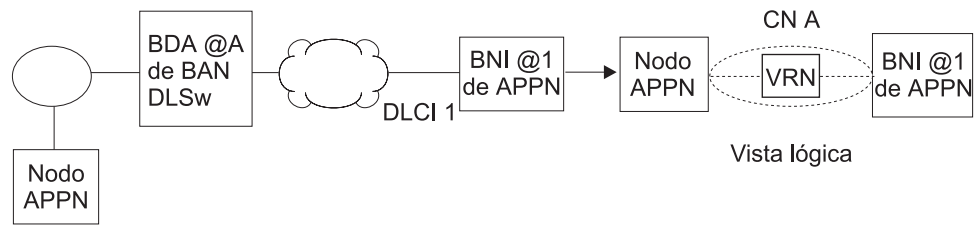


Figura 5. Red de conexiones individual que utiliza BAN con 1 puerto Frame Relay

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

### Ejemplo 2

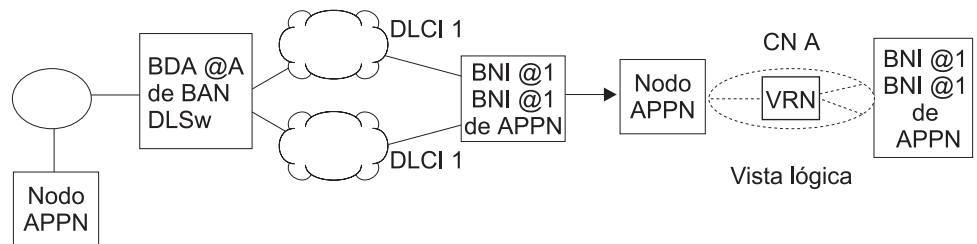


Figura 6. Red de conexiones individual que utiliza BAN con diversos puertos Frame Relay

#### Notas:

1. Debe especificarse el mismo número de DLCI en ambos puertos.
2. Debe definirse la dirección BDA en la definición de la red de conexiones.
3. Los destinatarios BNI de ambos puertos pueden ser el mismo o ser diferentes.
4. Si el nodo APPN inicia la conexión con el dispositivo, el puerto APPN elegido para la conexión depende de qué puerto responda primero a la trama de prueba.

### Ejemplo 3

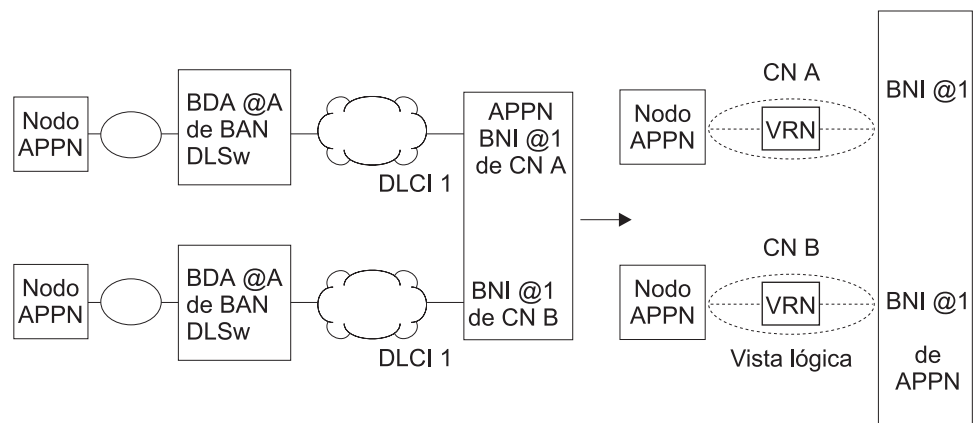


Figura 7. Diversas redes de conexiones que utilizan BAN

## Notas:

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

## Ejemplo 4

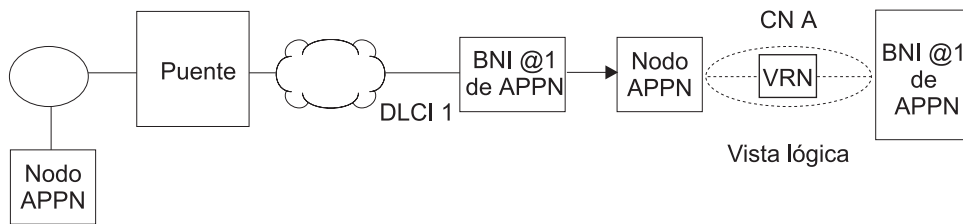


Figura 8. Red de conexiones individual que utiliza la función de puente con un puerto Frame Relay

## Notas:

1. No se define la dirección BDA en la definición de la red de conexiones.

## Ejemplo 5

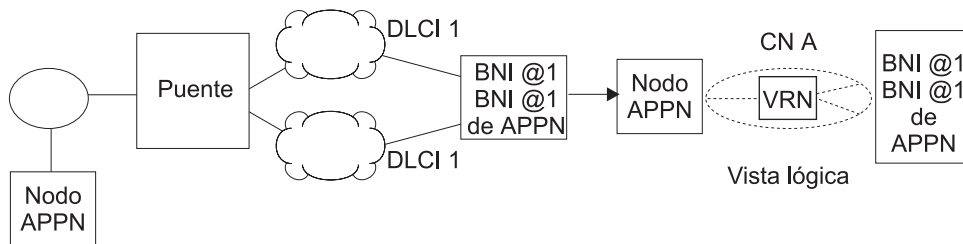


Figura 9. Red de conexiones individual que utiliza la función de puente con diversos puertos Frame Relay

## Notas:

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

## Ejemplo 6

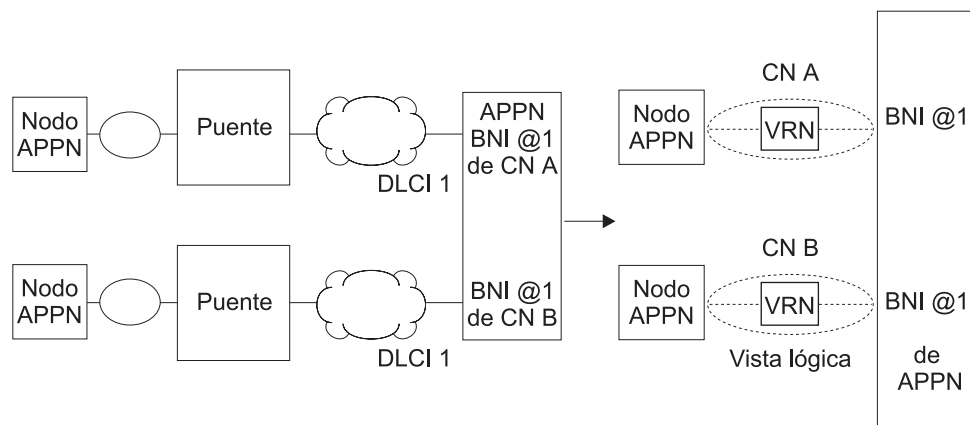


Figura 10. Diversas redes de conexiones que utilizan la función de puente

**Notas:**

1. Esta configuración requiere dos definiciones de red de conexiones porque hay dos SATF.
2. El número de DLCI especificado en los puertos puede ser el mismo o diferente.
3. No se define la dirección MAC BDA en la definición de red de conexiones.
4. El par de direcciones MAC BNI/SAP especificado en los puertos puede ser el mismo o diferente.

**Listas de parámetros de nivel de puerto**

Utilice las tablas siguientes para configurar puertos APPN:

- Configuración de puerto en la página 158
- Definición de puerto en la página 166
- Características de TG de puerto por omisión en la página 170
- Características de LLC de puerto por omisión en la página 175

**Listas de parámetros de nivel de enlace**

Utilice las tablas siguientes para configurar estaciones de enlace APPN:

- Valores por omisión de HPR en la página 178
- Estación de enlace - Información detallada en la página 179
- Modificación de características de TG en la página 193
- Modificación del Servidor de LU dependientes en la página 195
- Modificación de características de LLC en la página 196
- Modificación de valores por omisión de HPR en la página 198

### Lista de parámetros de LU

Utilice la tabla siguiente para configurar una LU:

- Nombre de LU de nodo final LEN en la página 200

### Listas de parámetros de nivel de nodo

Utilice las tablas siguientes para configurar un nodo APPN:

- Características básicas de nodo local en la página 121
- Direccionamiento de alto rendimiento (HPR) en la página 128
- Opciones de temporizadores y reintentos de HPR en la página 128
- Peticionario de LU dependientes en la página 131
- Red de conexiones - Información detallada en la página 201
- Características de TG (Red de conexiones) en la página 206
- COS de APPN - Puerto adicional para CN en la página 210
- Rastros de nivel de nodo en la página 139
- Rastros de señales interprocesos en la página 144
- Rastros de entrada y salida de módulos en la página 147
- Rastros generales de nivel de componente en la página 149
- Gestión de nodo APPN en la página 155
- "TN3270E" en la página 220
- Tabla 39 en la página 214
- Tabla 40 en la página 217

---

## Notas de configuración de APPN

Los ejemplos siguientes muestran parámetros especiales a considerar cuando se configuran diversas funciones para transportar tráfico de APPN.

**Nota:** En estos ejemplos aparece salida de muestra. Puede que la salida que visualice no aparezca exactamente igual que la salida mostrada aquí.

**Nota:** En algunos ejemplos de configuración, los resultados de un mandato **talk 6 list** pueden presentar más configuración de la que se presenta realmente en la muestra. No obstante, en la muestra aparecerá toda la configuración que es exclusiva.

## Configuración de un circuito permanente con RDSI

Este ejemplo es una configuración de un circuito permanente con Frame Relay sobre RDSI del nodo 21 al nodo 1.

**Nota:** Se configura un circuito permanente estableciendo el valor de temporizador desocupado en 0.

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

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

Base net = 3
Destination name = 2216-01
Circuit priority = 8
Destination address: subaddress = 99195551234:

Inbound destination name = 2216-01
Inbound dst address: subaddress = 99195551000:

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

```
FR Config>ex
```

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

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

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

Circuit Name	Circuit Number	Circuit Type	CIR in bps	Burst Size	Excess Burst
2216-21-i6 2	16	Permanent	64000	64000	0

= circuit is required and belongs to a required PVC group

## Utilización de APPN

```
FR Config>ex
Config>p appn
APPN user configuration
APPN config>add p
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (IP) [ ] ? f
Interface number(Default 0): [0] ? 6
Port name (Max 8 characters) [FR006] ?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
Service any node: (Y)es (N)o [Y] ?
Limited resource: (Y)es (N)o [N] ?
High performance routing: (Y)es (N)o [Y] ?
Maximum BTU size (768-2044) [2044] ?
Percent of link stations reserved for incoming calls (0-100) [0] ?
Percent of link stations reserved for outgoing calls (0-100) [0] ?
Local SAP address (04-EC) [4] ?
Support bridged formatted frames: (Y)es (N)o [N] ?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>add li
APPN Station
Port name for the link station [ ] ? fr006
Station name (Max 8 characters) [ ] ? tonn1isdn
Station name (Max 8 characters) [ ] ? tonn1is
Limited resource: (Y)es (N)o [N] ?
Activate link automatically (Y)es (N)o [Y] ?
DLCI number for link (16-1007) [16] ?
Adjacent node type: 0 = APPN network node, 1 = APPN end node
2 = LEN end node, 3 = PU 2.0 node [0]?
High performance routing: (Y)es (N)o [Y] ?
Edit Dependent LU Server: (Y)es (N)o [N]?
Allow CP-CP sessions on this link (Y)es (N)o [Y] ?
CP-CP session level security (Y)es (N)o [N] ?
Configure CP name of adjacent node: (Y)es (N)o [N] ?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>ex
```



```

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

```

**Nota:**

- 1** Idle timer = 0 proporciona un circuito fijo
- 2** Se define un PVC Frame relay
- 3** Es el puerto RDSI
- 4** Es la estación de enlace

## Configuración de APPN sobre circuitos de marcación bajo pedido

Se da soporte a APPN sobre circuitos de marcación bajo pedido para los siguientes tipos de DLC:

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

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

### Consideraciones sobre nodos de PU 2.1

Cuando configure una estación de enlace APPN para los nodos de PU 2.1 sobre un enlace Marcación bajo pedido, debe especificar *yes* en el parámetro de estación de enlace *limited resource*. Esto permite que APPN:

- Considere este enlace un enlace viable a utilizar para el cálculo de ruta aunque el enlace no esté realmente activo. El enlace se activará automáticamente durante la activación de las sesiones de LU-LU para una sesión en que sea necesario utilizarlo.
- Desactive la estación de enlace cuando no haya sesiones activas que utilicen este enlace.

No debe configurar sesiones de CP-CP sobre un enlace marcación bajo pedido. Las sesiones de CP-CP son sesiones de tipo persistente. Es decir, deben permanecer activas mientras el enlace esté activo. Puesto que la cuenta de las sesiones activas no llegará a cero en este caso, el enlace permanecerá activo.

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

### Consideraciones sobre nodos de PU 2.0

Cuando configure una estación de enlace APPN para los nodos de PU 2.0 sobre un enlace Marcación bajo pedido, puede especificar *yes* en el parámetro de estación de enlace *limited resource*. Esto permite que APPN desactive la estación de enlace cuando no haya sesiones activas que lo utilicen.

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

### Consideraciones al utilizar un DLUR para dispositivos T2.0 ó T2.1

En los nodos T2.0 ó T2.1 que utilicen un DLUR para el tráfico de sesiones dependientes, debe estar activa una sesión de SSCP-PU y una sesión de SSCP-LU con el fin de establecer una sesión de LU-LU. Estas sesiones se incluyen en la cuenta de sesiones del enlace con la DSPU. Por lo tanto, si *limited resource* es *yes*, el enlace permanecerá activo mientras la sesión de SSCP-PU o las sesiones de LU-LU estén activas sobre el mismo.

Si especifica *no* en el parámetro *limited resource*, la desactivación del enlace está controlada por el nodo que ha iniciado la conexión.

Si el enlace con la DSPU se ha activado porque la DSPU llamaba al nodo DLUR o porque éste llamaba a la DSPU (es decir, se ha configurado la estación de enlace con la DSPU en el direccionador y *activate link automatically* es *yes*), cuando la cuenta de sesiones activas llegue a cero, el DLUR de APPN sólo desactivará el enlace si la DSPU ha solicitado una DACTPU. En este caso, si el DLUR envía una petición DACTPU al DLUR, el DLUR desactivará la sesión de SSCP-PU. No obstante, no desactivará el enlace con la DSPU. El DLUR intentará restablecer la sesión de SSCP-PU con el DLUR o con el DLUR de reserva hasta obtener un resultado satisfactorio o hasta que la DSPU ya no necesite esta sesión.

Si el enlace con la DSPU se ha activado por medio del DLUS y la cuenta de sesiones llega a cero, el DLUR de APPN sólo desactiva el enlace en el caso de que el DLUS envíe una petición DACTPU al DLUR.

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

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

Ambas partes del enlace de comunicaciones se configuran de la misma manera.

**Nota:** Si permite la realización de sesiones de CP-CP en este enlace, el enlace no se desconectará.

```
*t 6
Gateway user configuration
Config>
*****
**** This is the NN6 configuration for a NN6---NN15 dial on demand link.
**** The NN15 config will look just like this.
**** interface 9 is a Dial On Demand link with destination = NN15
*****
Config>n 9
Circuit configuration
FR Config>li a11

Base net                = 6
Destination name        = 2216-15
Circuit priority        = 8

Inbound destination name = 2216-15

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

FR Config>ex

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

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

## Utilización de APPN

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

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

CONNECTION NETWORK:
  CN NAME          LINK TYPE  PORT INTERFACES
-----
COS:
  COS NAME
-----
  BATCH
  BATCHSC
  CONNECT
  INTER
  INTERSC
  CPSVCMG
  SNASVCMG
  USRBAT
  USRNOT
```

```

MODE:
MODE NAME  COS NAME
-----
          USRBAT      USRBAT
          USRNOT      USRNOT

PORT:
INTF      PORT      LINK      HPR      SERVICE  PORT
NUMBER    NAME      TYPE      ENABLED  ANY      ENABLED
-----
0         TR000    IBMTRNET  YES      YES      YES
1         PPP001    PPP      YES      YES      YES
2         SS      SDLC      NO       YES      YES
3         SDLC      NO       YES      NO
4         PPP      YES      YES      NO
5         TR005    IBMTRNET  YES      YES      YES
254      DLS      NO       YES      NO
17      PPP017    PPP      YES      YES      YES
9       PPP009    PPP      YES      YES      YES  6

STATION:
STATION    PORT      DESTINATION  HPR  ALLOW  ADJ  NODE
NAME      NAME      ADDRESS      ENABLED  CP-CP  TYPE
-----
TONN1     TR000    0004AC4E7505  YES  YES    1
TONN2     TR000    550020004020  YES  YES    1
TONN9     TR000    0004AC4E951D  YES  YES    1
TOPC4     TR000    0004AC9416B4  YES  YES    1
TOVTAM1   TR000    400000003888  YES  YES    1
TONN35    PPP001    000000000000  YES  YES    0
T015D0D  PPP009    000000000000  YES  NO     0  7

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

```

**Nota:**

- 1** Idle timer > 0 significa marcación bajo pedido
- 2** Es un recurso limitado
- 3** Es necesario un número de TG para un recurso limitado
- 4** No permita sesiones de CP-CP en este enlace
- 5** Proporcione un nombre de CP calificado al completo
- 6** Es el puerto
- 7** Es la estación de enlace

## Configuración del redireccionamiento de WAN

El redireccionamiento de WAN le permite configurar una ruta alternativa para que, si falla un enlace primario, el direccionador inicie automáticamente una nueva conexión con el destino mediante la ruta alternativa.

Puede utilizar cualquier tipo de enlace como enlace alternativo y cualquier tipo de enlace como enlace primario. No es necesario que el enlace alternativo esté conectado con el mismo punto final que el enlace primario.

Si se utiliza el HPR en el enlace primario y en el alternativo, cuando falle el enlace primario, la función de conmutación de la vía de acceso de no interrupción del HPR redireccionará el tráfico automáticamente hacia el enlace alternativo sin interrumpir las sesiones de usuario final.

En este ejemplo de configuración, el direccionador que efectúa la función de redireccionamiento de WAN se configura con dos definiciones de estación de enlace APPN; una estación de enlace se define sobre la interfaz primaria y la otra sobre la interfaz alternativa. El direccionador de destino necesita la habilitación de APPN en el puerto. Si el direccionador de destino tiene definida una estación de enlace, ésta no debe intentar activar la conexión para evitar tráfico adicional.

En este ejemplo, Frame Relay es la ruta primaria del NN22 al NN6.

```
*****
**** The configuration is NN22---primary FR
****      ---Alternate WRR to NN6
*****
****
**** This is the NN22 configuration
*****
```

```
Ifc 0 Token Ring           Slot: 1  Port: 1
Ifc 1 V.35/V.36 Frame Relay Slot: 8  Port: 0
Ifc 2 V.35/V.36 Frame Relay Slot: 8  Port: 1
Ifc 3 ISDN Primary T1/J1   Slot: 7  Port: 1
Ifc 4 PPP Dial Circuit
      (Disabled)
Ifc 5 PPP Dial Circuit
      (Disabled)
Ifc 6 Frame Relay Dial Circuit
      (Disabled)
```

```
*****
* Ifc 4 is the ALTERNATE with Ifc 1 configured as PRIMARY.
* Note that interface 4 should be 'Disabled' here.
* Wan Reroute function will 'Enable' it when the
* Primary fails
*
* NN6 (2216-06) is going to be the destination of the Wan Reroute
*****
```

Config>n 4

Circuit configuration

FR Config>li

```
Base net           = 3
Destination name   = 2216-06 3
Circuit priority   = 8
Destination address: subaddress = 99199991201:
```

```

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

Config>ex

\*\*\*\*\*

```

*
**** Configure the Wan Reroute Primary and Alternate circuit
*
    
```

Config>fea wan 4

WAN Restoral user configuration

WRS Config>en wrs

WRS Config>add alt

Alternate interface number [0] ? 4 2

Primary interface number [0] ? 1 1

WRS Config>li all

```

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

[No Primary-Secondary pairs defined ]

Primary Interface	Alt. Alternate Interface	1st Enabled	Subseq TOD	Revert Stab	Back Stab	Start	Stop
1 - WAN Frame Re	4 - PPP Dial Circuit	No		dflt	dflt	Not Set	Not Set

\*\*\*\*\*

```

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

\*\*\*\*\*

WRS Config>set default firs 30

WRS Config>set def stab 10

WRS Config>li all

```

WAN Restoral is enabled.
Default Stabilization Time:      10 seconds
Default First Stabilization Time: 30 seconds
    
```

[No Primary-Secondary pairs defined ]

Primary Interface	Alt. Alternate Interface	1st Enabled	Subseq TOD	Revert Stab	Back Stab	Start	Stop
1 - WAN Frame Re	4 - PPP Dial Circuit	No		dflt	dflt	Not Set	Not Set

WRS Config>en alt

Alternate interface number [0] ? 4

WRS Config>ex

## Utilización de APPN

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



```

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

```

## Utilización de APPN

```
*****
*****
*****
Config>
*****
**** The configuration is NN22---primary FR
****                               ---Alternate WRR to NN6
****
** This is the NN6 configuration which is the destination side for the
* NN22 Wan Reroute
* interface 17 has the ISDN lid for 2216-22 so when NN22 calls into NN6,
* it will map to interface 17
*
*****
11
Config> n 17
Circuit configuration
FR Config>fea li all

Base net                = 6
Destination name        = 2216-22
Circuit priority        = 8

Inbound destination name = 2216-22

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

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

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

```

Port Definition
Service any node: (Y)es (N)o [Y ] ?
Limited resource: (Y)es (N)o [N ] ?
High performance routing: (Y)es (N)o [Y ] ?
Maximum BTU size (768-2044) [2044 ] ?
Local SAP address (04-EC) [4 ] ?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>1i a1
NODE:
  NETWORK ID: STFNET
  CONTROL POINT NAME: NN6
  XID: 00000
  APPN ENABLED: YES
  MAX SHARED MEMORY: 4096
  MAX CACHED: 4000
DLUR:
  DLUR ENABLED: YES
  PRIMARY DLUS NAME: NETB.MVSC
CONNECTION NETWORK:
  CN NAME      LINK TYPE  PORT INTERFACES
-----
COS:
COS NAME
-----
  BATCH
  BATCHSC
  CONNECT
  INTER
  INTERSC
  CPSVCMG
  SNASVCMG
  USRNOT
MODE:
  MODE NAME    COS NAME
-----
  USRBAT       USRBAT
  USRNOT       USRNOT
PORT:
  INTF  PORT  LINK  HPR  SERVICE  PORT
  NUMBER NAME  TYPE  ENABLED ANY  ENABLED
-----
    0   TR000  IBMTRNET  YES  YES  YES
    1   PPP001  PPP  YES  YES  YES
    2           SS  SDLC  NO  YES  YES
    3           SDLC  NO  YES  NO
    4           PPP  YES  YES  NO
    5   TR005  IBMTRNET  YES  YES  YES
   254           DLS  NO  YES  NO
    17   PPP017  PPP  YES  YES  YES
STATION:
  STATION  PORT  DESTINATION  HPR  ALLOW  ADJ
  NAME     NAME  ADDRESS      ENABLED CP-CP  NODE
-----
  TONN1   TR000  0004AC4E7505  YES  YES  1
  TONN2   TR000  550020004020  YES  YES  1
  TONN9   TR000  0004AC4E951D  YES  YES  1
  TOPC4   TR000  0004AC9416B4  YES  YES  1
  TOVTAM1 TR000  400000003888  YES  YES  1
  TONN35  PPP001  000000000000  YES  YES  0
LU NAME:
  LU NAME      STATION NAME      CP NAME
-----
APPN config>

```

**Nota:**

- 1** La ruta primaria es la interfaz 1, Frame Relay

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

## Configuración de la restauración de WAN

El ejemplo siguiente muestra APPN sobre un enlace PPP primario. Para APPN, no son necesarias definiciones exclusivas. Ambas partes del enlace de comunicaciones se habilitan para la restauración de WAN y se configuran de forma similar.

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

```
Circuit configuration  
FR Config>li a1
```

```
Base net                = 6  
Destination name       = 2216-35  
Circuit priority       = 8  
  
Inbound destination name = 2216-35  
  
Inbound calls          = allowed  
Idle timer             = 0 (fixed circuit)  
SelfTest Delay Timer   = 150 ms
```

```
FR Config>ex  
Config>fea wan  
WAN Restoral user configuration  
WRS Config>li a11
```

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

```

Primary Interface      Secondary Interface    Secondary
-----
1 - WAN PPP           8 - PPP Dial Circuit   Yes
[No Primary-Alternate pairs defined ]
WRS Config>ex
Config>p appn
APPN user configuration
APPN config>li a1
NODE:
NETWORK ID: STFNET
CONTROL POINT NAME: NN6
XID: 00000
APPN ENABLED: YES
MAX SHARED MEMORY: 4096
MAX CACHED: 4000
DLUR:
DLUR ENABLED: YES
PRIMARY DLUS NAME: NETB.MVSC
CONNECTION NETWORK:
  CN NAME      LINK TYPE  PORT INTERFACES
-----
COS:
COS NAME
-----
  BATCH
  BATCHSC
  CONNECT
  INTER
  INTERSC
  CPSVCMG
  SNASVCMG
  USRBAT
  USRNOT
MODE:
MODE NAME  COS NAME
-----
  USRBAT    USRBAT
  USRNOT    USRNOT
PORT:
INTF      PORT      LINK      HPR      SERVICE  PORT
NUMBER   NAME      TYPE      ENABLED  ANY      ENABLED
-----
  0        TR000    IBMTRNET  YES      YES      YES
**** < This is the port that will get backed up
  1        PPP001   PPP       YES      YES      YES  2
  2        SS      SDLC      NO       YES      YES
  3        SDLC     SDLC      NO       YES      NO
  4        PPP     PPP       YES      YES      NO
  5        TR005   IBMTRNET  YES      YES      YES
  254     DLS     DLS       NO       YES      NO
  17     PPP017  PPP       YES      YES      YES
  9      PPP009  PPP       YES      YES      YES

STATION:
STATION   PORT      DESTINATION  HPR  ALLOW  ADJ NODE
NAME      NAME      ADDRESS      ENABLED  CP-CP  TYPE
-----
  TONN1   TR000    0004AC4E7505  YES  YES    1
  TONN2   TR000    550020004020  YES  YES    1
  TONN9   TR000    0004AC4E951D  YES  YES    1
  TOPC4   TR000    0004AC9416B4  YES  YES    1
  TOVTAM1 TR000    400000003888  YES  YES    1
**** < this linkstation will get backed up
  TONN35  PPP001   000000000000  YES  YES    0  3
  T015DOD PPP009   000000000000  YES  NO     0

LU NAME:
LU NAME      STATION NAME      CP NAME
-----
APPN config>ex
Config>
*logout
Connection closed.

```

### Nota:

- 1** La restauración de WAN se habilita en ambas partes.
- 2** Puerto del que se obtendrá reserva
- 3** Estación de enlace de la que se obtendrá reserva

## Configuración de V.25 bis

La siguiente es una configuración de V.25 bis de muestra que puede utilizarse cuando el tráfico de APPN utilice PPP sobre V.25 bis:

```
Config> list device
```

```
Ifc 2 WAN V.25bis                CSR 81640, CSR2 80E00, vector 92
Ifc 0 Token Ring                 Slot: 1  Port: 1
Ifc 1 EIA-232E/V.24 PPP         Slot: 8  Port: 0
Ifc 2 EIA-232E/V.24 X.25       Slot: 8  Port: 1
Config>set data v25 2.
Config>list device
```

```
Ifc 0 Token Ring                 Slot: 1  Port: 1
Ifc 1 EIA-232E/V.24 PPP         Slot: 8  Port: 0
Ifc 2 EIA-232E/V.24 V.25bis    Slot: 8  Port: 1
Config>add v25
Assign address name (1-23) chars []? brown
Assign network dial address (1-30 digits) []? 555-1211
Assign address name (1-23) chars []? gray
Assign network dial address (1-30 digits) []? 555-1212
Config>list v25
```

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

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

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

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

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

```

Circuit config: 3>list all

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

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

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

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

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

Cable type = RS-232 DTE

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

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

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

Cable type = RS-232 DTE

Speed (bps) = 9600
V25bis Config>

```

**Nota:**

- 1** Un valor distinto de cero para Idle Timer da como resultado un enlace mar-  
cación bajo pedido
- 2** Un valor de cero da como resultado un enlace alquilado

**Configuración de APPN sobre ATM**

La muestra siguiente configura APPN sobre ATM.

### Notas:

1. Cuando se configuran PVC, debe definirse la estación de enlace en los dos nodos APPN que desean utilizar el PVC. La estación de enlace debe definirse con **Activate link automatically**= yes.
2. Cuando se configuran TG paralelo sobre ATM, deben definirse el nombre de nodo adyacente y el número de TG en ambos nodos para cada estación de enlace.

**Nota:** Cuando defina TG paralelo, si utiliza la asignación dinámica de números de TG, debe definir TODOS los enlaces entre los dos nodos o no definir NINGUNO.

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

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



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

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

```
nada205 APPN config>
```

### Notas:

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

## Configuración de APPN con SDLC

APPN da soporte a las siguientes estaciones SDLC:

- Primarias punto a punto
- Secundarias punto a punto
- Negociables punto a punto
- Primarias multipunto
- Secundarias punto a punto (estaciones de enlace de APPN múltiple)

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

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

Con el fin de activar una conexión APPN con la estación de enlace SDLC remota, debe configurar y activar la estación de enlace APPN SDLC en el direccionador. Esto permite que la estación de enlace APPN del direccionador reciba un XID de activación de la estación de enlace SDLC remota. Es diferente de otros tipos de DLC, como, por ejemplo Red en Anillo o Ethernet, cuyas estaciones de enlace APPN no necesitan definirse explícitamente para APPN en el direccionador porque APPN tiene la posibilidad de definir dinámicamente estos tipos de estaciones de enlace.

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

```

*****
*
* The following examples show how to configure different SDLC stations.
*
*****
*Configuring a Primary Point-To-Point SDLC Station: 1
*****
Config> set data sdlc 1
Config> n 1
SDLC user configuration
SDLC 1 Config> set link role primary
SDLC 1 Config>list link
list link
Link configuration for: LINK_1 (ENABLED)

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

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

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

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

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

```

## Utilización de APPN

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

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

```

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

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

```

## Utilización de APPN

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

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

```

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

```

```

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

```

## Nota:

- 1** Configuración de una estación SDLC primaria punto a punto
- 2** Configuración de una estación SDLC secundaria punto a punto



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

## Configuración de APPN sobre X.25

Este ejemplo muestra una configuración de APPN para un puerto y dos estaciones de enlace X.25. Una estación de enlace es un PVC y la otra es un SVC. El SVC se configura como recurso limitado. El SVC se activará cuando se necesite y se desactivará cuando no se necesite.

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

Boats APPN config>add link
APPN Station
Port name for the link station[ ]? x25002
Station name (Max 8 characters)[ ]? x25svcl
    Limited resource: (Y)es (N)o[N]? Y
    Activate link automatically (Y)es (N)o[N]?
    Link Type (0 = PVC , 1 = SVC)[0]? 1
    DTE Address [0]? 2222
    Adjacent node type: 0 = APPN network node,
    1 = APPN end node or Unknown node type
    2 = LEN end node, 3 = PU 2.0 node[1]?
Edit Dependent LU Server: (Y)es (N)o [N]?
    Allow CP-CP sessions on this link (Y)es (N)o[Y]? N
    CP-CP session level security (Y)es (N)o [N]?
    Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

Boats APPN config>add link
APPN Station
Port name for the link station[ ]? x25002
Station name (Max 8 characters)[ ]? x25pvc1
    Limited resource: (Y)es (N)o[N]?
    Activate link automatically (Y)es (N)o[Y]?
    Link Type (0 = PVC , 1 = SVC)[0]?
    Logical channel number (1-4095)[1]?
    Adjacent node type: 0 = APPN network node,
    1 = APPN end node or Unknown node type
    2 = LEN end node, 3 = PU 2.0 node[1]?
Edit Dependent LU Server: (Y)es (N)o [N]?
    Allow CP-CP sessions on this link (Y)es (N)o [Y]?
    CP-CP session level security (Y)es (N)o [N]?
    Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

## Utilización de APPN

Boats APPN config>**list port x25002**

PORT:  
Interface number(DLSw = 254): 2  
PORT enable: YES  
Service any node: YES  
Link Type: X25  
MAX BTU size: 2048  
MAX number of Link Stations: 239  
Percent of link stations reserved for incoming calls: 0  
Percent of link stations reserved for outgoing calls: 0  
Cost per connect time: 0  
Cost per byte: 0  
Security:(0 = Nonsecure, 1 = Public Switched Network  
2 = Underground Cable, 3 = Secure Conduit,  
4 = Guarded Conduit, 5 = Encrypted, 6 = Guarded Radiation): 0  
Propagation delay:(0 = Minimum, 1 = Lan, 2 = Telephone,  
3 = Packet Switched Network, 4 = Satellite, 5 = Maximum): 3  
Effective capacity: 45  
First user-defined TG characteristic: 128  
Second user-defined TG characteristic: 128  
Third user-defined TG characteristic: 128

Boats APPN config>**list link x25svc1**

STATION:  
Port name: X25002  
Interface number(DLSw = 254): 2  
Link Type: X25  
Link Type (0 = PVC , 1 = SVC): 1  
DTE Address: 2222  
Activate link automatically: YES  
Allow CP-CP sessions on this link: YES  
CP-CP session level security: NO  
Fully-qualified CP name of adjacent node:  
Encryption key: 0000000000000000  
Use enhanced session security only: NO  
Cost per connect time: 0  
Cost per byte: 0  
Security:(0 = Nonsecure, 1 = Public Switched Network  
2 = Underground Cable, 3 = Secure Conduit,  
4 = Guarded Conduit, 5 = Encrypted, 6 = Guarded Radiation): 0  
Propagation delay:(0 = Minimum, 1 = Lan, 2 = Telephone,  
3 = Packet Switched Network, 4 = Satellite, 5 = Maximum): 3  
Effective capacity: 45  
First user-defined TG characteristic: 128  
Second user-defined TG characteristic: 128  
Third user-defined TG characteristic: 128  
Predefined TG number: 0

```

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

```

## Utilización de APPN

```

PORT:
      INTF   PORT   LINK   HPR   SERVICE   PORT
      NUMBER NAME   TYPE   ENABLED ANY   ENABLED
-----
          2   X25002   X25    NO    YES    YES
          5   TR005   IBMTRNET YES    YES    YES
STATION:
      STATION   PORT   DESTINATION   HPR   ALLOW   ADJ NODE
      NAME     NAME   ADDRESS       ENABLED CP-CP   TYPE
-----
      X25SVC1  X25002   2222         NO    NO     1
      X25PVC1  X25002   1            NO    YES    1
LU NAME:
      LU NAME     STATION NAME     CP NAME
-----

```

Boats APPN config>ex

```

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

```

X.25 Configuration Summary

```

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

```

X.25 National Personality Configuration

```

Follow CCITT: on      OSI 1984:  on      OSI 1988:  off
Request Reverse Charges: off  Accept Reverse Charges:  off
Frame Extended seq mode: off  Packet Extended seq mode: off
Incoming Calls Barred:  off  Outgoing Calls Barred:  off
Throughput Negotiation: off  Flow Control Negotiation: off
Suppress Calling Addresses: off
DDN Address Translation: off
Call Request Timer:      20 decaseconds
Clear Request Timer:     18 decaseconds (1 retries)
Reset Request Timer:     18 decaseconds (1 retries)
Restart Request Timer:   18 decaseconds (1 retries)
Min Recall Timer:        10 seconds
Min Connect Timer:       90 seconds
Collision Timer:         10 seconds
T1 Timer: 4.00 seconds   N2 timeouts: 20
T2 Timer: 0.00 seconds   DP Timer: 500 milliseconds
Standard Version:        2      Network Type: CCITT
Disconnect Procedure: passive
Window Size      Frame: 7      Packet: 2
Packet Size      Default: 128    Maximum: 256
    
```

X.25 protocol configuration

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

X.25 PVC configuration

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

X.25 address translation configuration

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

Boats X.25 Config>

## Configuración de APPN sobre Frame Relay

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

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

## Configuración de APPN sobre BAN Frame Relay

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

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

## Configuración de APPN sobre MPC+

El ejemplo siguiente muestra una configuración de APPN sobre MPC+. Consulte el capítulo titulado “Planificación y configuración del Adaptador de Canal Paralelo y ESCON” del manual *Nways Multiprotocol Access Services Guía del usuario de software* para obtener información adicional sobre MPC+ (ESCON/PCA).

```

Config>p appn
APPN config>add port
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (IP) []?m
Interface number(Default 0): [0]?2
Port name (Max 8 characters) [MPC002]?
Enable APPN on this port (Y)es (N)o [Y]?
Config Save: Using bank B and config number 1
    Service any node: (Y)es (N)o [Y]?
    Maximum BTU size (768-32768) [2048]?
Edit MPC+ Sequencing Interval Timer: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>add link
APPN Station
Port name for the link station []? mpc002
Station name (Max 8 characters) []? mpctovt
    Adjacent node type: 0 = APPN network node,
    1 = APPN end node or Unknown node type [0]?
    Allow CP-CP sessions on this link (Y)es (N)o [Y]?
    CP-CP session level security (Y)es (N)o [N]?
    Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>act
APPN config>exit
Config>write
Config Save: Using bank B and config number 1
Config>
    
```



## Configuración del soporte del Enterprise Extender para el HPR sobre IP

```

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

```

## Configuración de redes de conexiones sobre HPR sobre IP

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

## Configuración de un Extended Border Node

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

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

---

## Utilización de TN3270

Este apartado presenta el elemento TN3270 y resume la función de servidor TN3270E implementada en los direccionadores IBM. Incluye los temas siguientes:

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

---

### Visión general

En la actualidad, muchas empresas están consolidando el tráfico de WAN sobre redes troncales de sólo IP. Además, las empresas están en proceso de simplificar sus configuraciones de estación de trabajo e intentan ejecutar solamente la pila de protocolos TCP/IP en el sistema de sobremesa. No obstante, la mayoría de estas empresas todavía necesitan el acceso a sistemas principales de aplicaciones de SNA.

TN3270 cumple estos requisitos al permitir que el usuario ejecute IP desde el sistema de sobremesa sobre la red y se conecte con el sistema principal SNA mediante un servidor TN3270. Los clientes se conectan con el servidor utilizando una conexión TCP. El servidor proporciona una función de pasarela para los clientes TN3270 de sentido directo correlacionando las sesiones de cliente con las sesiones de LU-LU dependientes de SNA que el servidor mantiene con el sistema principal SNA. El servidor TN3270 maneja la conversión entre la corriente de datos de TN3270 y una corriente de datos de SNA 3270.

Para desarrollar una solución de TN3270, instale el software de cliente TN3270 en las estaciones de trabajo de sobremesa<sup>4</sup> y el software de servidor TN3270 en uno de los diversos lugares descritos más abajo. El software de cliente está disponible en IBM y en muchos otros proveedores y se ejecuta en la parte superior de la pila de TCP/IP de la estación de trabajo. Un producto de cliente determinado proporciona uno de los dos niveles posibles de soporte de normas:

- Cliente TN3270 base

Estos clientes se ajustan a RFC 1576 (referente a las prácticas actuales de TN3270) y/o a RFC 1646 (referente a las extensiones de TN3270 para la selección de impresora y nombre de LU).

- Cliente TN3270E

Estos clientes se ajustan a RFC 1647 (referente a mejoras en TN3270) y a RFC 2355 (referente a mejoras en TN3270).

Una implementación de servidor que puede dar soporte a clientes TN3270E es un servidor TN3270E.

---

<sup>4</sup> También puede encontrar productos de cliente TN3270 dedicados de reducidas proporciones que representan impresoras.

### Colocación de la función de servidor TN3270

La función de servidor TN3270 puede colocarse en una variedad de productos y posiciones dentro de una red, lo cual incluye:

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

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

- La capacidad del sistema principal y el efecto en ciclo
- El precio del rendimiento y de la capacidad
- La disponibilidad
- El efecto de una anomalía de servidor
- La escalabilidad

Los direccionadores IBM proporcionan una implementación de servidor TN3270E de alto rendimiento que ofrece una escalabilidad de redes amplias. Combinando esta implementación con la función Network Dispatcher, puede implementar la redundancia de servidor y el compartimiento de carga en las instalaciones grandes de TN3270. También puede colocar un direccionador IBM fuera, en una red SNA o IP alejado del centro de datos, y obtener las mismas ventajas en relación con la escalabilidad, la adición incremental y el efecto reducido de cualquier anomalía de servidor.

### Función de servidor TN3270E

#### Conformidad con las normas

La implementación del servidor TN3270E proporcionada por el direccionador IBM da soporte a estas normas RFC:

- |                 |   |
|-----------------|---|
| <b>RFC 1576</b> | Las prácticas actuales de TN3270                          |
| <b>RFC 1646</b> | Las extensiones de TN3270 para nombres de LU e impresoras |

<b>RFC 1647</b>	Mejoras en TN3270
<b>RFC 2355</b>	Mejoras en TN3270 (con lo que queda obsoleta la norma RFC 1647)

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

### **Conectividad del sistema principal**

La vía de acceso de un cliente TN3270 al sistema principal SNA consta de dos partes:

- Una conexión TCP sobre IP del cliente con el servidor
- Una sesión de LU-LU de SNA del servidor con el sistema principal

El formato de la conexión SNA del servidor con el sistema principal depende de cómo el servidor representa a las PU y a las LU dependientes. Cuando desee utilizar un direccionador IBM como servidor TN3270, puede efectuar una configuración siguiendo una de las dos maneras diferentes que existen de establecer enlaces y representar a PU y LU para VTAM:

- Utilizando enlaces de subárea SNA

Se configura de esta manera cuando no se ejecuta APPN en el sistema principal (aunque el direccionador sigue teniendo la posibilidad de APPN). Se configura un enlace de capa de DLC por separado con el sistema principal para cada PU (con un máximo de 255 LU por PU). Una diversidad de PU requiere diversos enlaces de sistema principal paralelo. Las tramas de SNA que llegan al direccionador en uno de estos enlaces fluyen directamente a la PU interna correspondiente.

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

- Red en Anillo: de tipo físico, emulación de LAN de ATM o canal LSA
- Ethernet: de tipo físico, emulación de LAN de ATM o canal LSA
- FDDI: sólo de tipo físico
- PVC Frame relay: formatos de puente o ruta de RFC 1490/2427
- DLSw (tenga en cuenta que si DLSw es local, puede proporcionar acceso a enlaces de sentido inverso de SDLC y QLLC)
- Utilizando un enlace de Petionario de LU dependientes (DLUR) de APPN

Se configura de esta manera cuando se ejecuta APPN con su función Servidor de LU dependientes (DLUS) en el sistema principal. En el direccionador DLUR, configure uno o más DLUS para dar soporte a las PU dependientes internas de TN3270 (y cualquier PU dependiente externa que pueda existir). Un direccionador que ejecuta el DLUR puede estar directamente conectado con el

sistema principal DLUS o puede estar ubicado remotamente en diversos enlaces APPN. Sólo es necesario un enlace para llevar a cabo el primer salto o el único salto del "conducto" DLUR-DLUS aunque defina diversas PU locales (para tener más de 255 LU en total). Las tramas de SNA que llegan en el conducto DLUR-DLUS fluyen a la función DLUR, que las redirecciona hacia la PU interna o externa correcta.

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

- Red en Anillo: de tipo físico, emulación de LAN de ATM o canal LSA
- Ethernet: de tipo físico, emulación de LAN de ATM o canal LSA
- FDDI: sólo de tipo físico
- PVC Frame relay: formatos de puente o ruta de RFC 1490/2427
- ATM (de tipo nativo, sin emulación de LAN): sólo HPR
- Canal MPC+: sólo HPR
- PPP
- SDLC: sólo ISR
- X.25: sólo ISR
- DLSw: sólo ISR
- IP (Enterprise Extender): sólo HPR

Tenga en cuenta de manera especial que, cuando utiliza el DLUR y el direccionamiento HPR, puede colocar un servidor TN3270E en una red IP desde el sistema principal de aplicaciones de SNA. Enterprise Extender mantiene una prioridad de transmisión y clase de servicio de nivel de sesión en la red IP.

Si existe una sesión de LU-LU cuando el cliente TN3270 se desconecte del servidor TN3270, se enviará una petición UNBIND o TERM-SELF al sistema principal para terminar la sesión de LU-LU. El valor por omisión es el borrado de UNBIND. La estación de enlace o PU local debe estar configurada de forma adecuada para que fluya TERM-SELF. Debe configurar TERM-SELF si desea utilizar una aplicación de gestor de sesiones (componente frontal) para llegar a aplicaciones como, por ejemplo, TSO o CICS.

### Soporte de la gestión de SNA

Desde una consola de operador de VTAM o NetView/390, puede controlar los enlaces, PU y LU que tengan una implicación en TN3270. Respecto a las LU, cuando se conecta un cliente TN3270, el direccionador notifica la dirección IP y el número de puerto TCP del cliente a VTAM en sus flujos de activación de sesión (mediante CV64). Los mandatos de visualización de consola de VTAM, como "/D NET,ID=(nombre de lu),E", tienen la posibilidad de visualizar la información de dirección TCP/IP asociada con LU en particular. Así es posible determinar problemas de los clientes TN3270 desde una consola de operador de VTAM.

El soporte de VTAM a la recepción y visualización de direcciones IP de cliente se encuentra en CS para el código base de OS/390 V2R6. También se le ha aplicado

el PTF en CS para OS/390 V2R5 (APAR de VTAM OW31454, APAR de TCP/IP PQ12574).

Además de habilitar este soporte de consola, APPN genera alertas de SNA en relación con una variedad de configuraciones erróneas y puede reenviar alertas de otros dispositivos SNA. No existen alertas específicas para la función de servidor TN3270, pero las alertas que el propio direccionador genera pueden estar relacionadas con recursos de SNA implicados en TN3270.

### **Soporte de MIB y detección (de condición de excepción) de SNMP**

Los direccionadores IBM dan soporte a una versión de borrador de Internet de estas dos MIB estándares para la función de servidor TN3270:

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

El soporte de direccionador IBM para estas MIB incluye la posibilidad de:

- Visualizar la configuración, el estado y las estadísticas de servidor
- Configurar grupos de clientes para la recogida relativa al tiempo de respuesta
- Visualizar la correlación de nombres de LU, desde el nombre de VTAM hasta el nombre local, con dirección IP de cliente
- Visualizar la correlación de direcciones IP de cliente con nombres de LU de VTAM
- Recoger datos de tiempo de respuesta para los grupos de clientes actuales

Además, la siguiente MIB específica de empresa muestra las razones por las cuales no han podido conectarse clientes de manera satisfactoria con el servidor TN3270:

- IBM TN3270 Connection Rejection

Estas MIB relacionadas con TN3270 sirven de complemento del soporte extensivo de MIB de los direccionadores IBM para los recursos de APPN y SNA.

## **Colocación en antememoria de Host On-Demand Client en TN3270**

Algunos productos de direccionador IBM (actualmente, el 2216 y el 2212) dan soporte a la función "Antememoria del servidor de la Web", según la cual pueden situarse por delante de un servidor HTTP y liberarle de carga colocando en antememoria objetos de la Web y sirviéndolos a los clientes que realizan la petición. Entre los objetos que estos direccionadores pueden colocar en antememoria están los applets de Java que proporcionan la función de cliente TN3270.

La colocación en antememoria de Host On-Demand (HOD) Client permite que uno de estos direccionadores o el programa IBM Network Utility coloque en antememoria los applets de función de cliente TN3270 de un servidor de la Web de sistema principal HOD y los sirva a los navegadores de los clientes a petición. A continuación, los navegadores ejecutan los applets de emulación de terminal TN3270. Estos applets se conectan con un sistema principal SNA mediante la función de servidor TN3270 del direccionador o mediante otro servidor TN3270.

El soporte de Host On-Demand está empaquetado con la función de servidor TN3270, pero debe configurar los dos de forma independiente. El direccionador puede colocar en antememoria clientes HOD y no estar configurado como servidor TN3270. Igualmente, el direccionador puede ser un servidor TN3270 sin tener habilitada la colocación en antememoria de HOD. Las cargas de código de direccionador de la Antememoria del servidor de la Web que no incluyen la función de servidor TN3270 (sólo en el 2216 y el 2212) también pueden colocar en antememoria applets de cliente HOD si la configuración lo permite.

Ya que la función de antememoria de cliente HOD es completamente independiente de la función Servidor, no recibirá más atención en este capítulo. Consulte el capítulo titulado “Configuración y supervisión de la antememoria de IBM eNetwork Host On-Demand Client” en la publicación *Utilización y configuración de las características* para obtener más información sobre esta función.

---

## Configuración general del servidor TN3270E

Este apartado cubre información general sobre la configuración del soporte de servidor TN3270. Si desea configuraciones de ejemplo específicas, consulte el apartado “Configuraciones de ejemplo” en la página 109.

## Carga del código de servidor TN3270

Según el tipo de direccionador y el método de configuración, es posible que tenga que seguir pasos adicionales para cargar el código de APPN y de TN3270 y poder acceder a los indicadores de línea de mandatos de configuración y supervisión:

- Cargue en el disco un paquete de códigos de direccionador que incluya APPN y TN3270. Si arranca el direccionador con una configuración del Programa de configuración, el direccionador cargará APPN y TN3270 desde el disco en el caso de que se hayan configurado estos protocolos. Si arranca el direccionador sin configuración o con una configuración de la línea de mandatos distinta de TN3270, el direccionador no carga estos protocolos en la memoria por omisión. Utilice el mandato **load add** para los paquetes de APPN y TN3270E, guarde la configuración y re arranque con la configuración guardada para configurar estos protocolos.
- Para el programa Network Utility modelo TN1, APPN y TN3270 se cargarán por omisión a menos que utilice el Programa de configuración y no haya configurado los protocolos. No es necesario utilizar el mandato **load add**.

Para obtener información detallada sobre el mandato **load add**, consulte el capítulo titulado “El proceso y los mandatos de CONFIG (CONFIG - Talk 6)” en la publicación *Guía del usuario de software*.

## Cómo configurar TN3270 bajo el protocolo APPN

En la implementación del servidor TN3270 proporcionada por el direccionador IBM, todas las funciones de SNA están en paquetes generales dentro del protocolo APPN. Esto significa que, incluso cuando esté configurando la conexión de sistema principal de subárea SNA y el sistema principal SNA no ejecute APPN, debe utilizar los servicios de configuración y consola del protocolo APPN. En particular:

- Debe pasar por el protocolo APPN, en la línea de mandatos y en el Programa de configuración, para configurar puertos, enlaces y funciones de servidor TN3270



- Debe pasar por el protocolo APPN, en la línea de mandatos, para utilizar los mandatos de supervisión de TN3270
- Debe configurar APPN en el nivel de nodo

Cuando configura el soporte de subárea SNA, el direccionador sigue funcionando como nodo de red APPN en realidad, pero sólo en los enlaces con otros nodos APPN. Si los únicos puertos y enlaces configurados corresponden a la conexión de sistema principal de subárea SNA, entonces no se ejecuta la función APPN en sí.

## Dirección IP de servidor

Para habilitar la función de servidor TN3270, debe configurar la dirección IP a la que se conectarán los clientes TN3270. La implementación de TN3270 proporcionada por el direccionador IBM sólo da soporte a una dirección IP de servidor (pero diversos puertos TCP de destino). La dirección que configure para TN3270 debe coincidir con una de las siguientes direcciones configuradas para IP; de lo contrario, TN3270 no se inicializará.

- Una dirección de interfaz

Puede asignar cualquier número de direcciones a una interfaz. La interfaz puede ser física o una interfaz de "bucle de retorno" virtual. Las direcciones de interfaz física sólo están activas cuando la interfaz está activa, pero las direcciones de interfaz de bucle de retorno siempre están activas.

- La dirección interna

Ésta es una sola dirección que representa a todo el direccionador y está activa independientemente del estado de cualquier interfaz en particular.

Cuando elija la dirección IP para la función TN3270, debe tomar en consideración que los usuarios administrativos también tienen que poder establecer sesiones regulares de Telnet para activar consolas de direccionador de tipo remoto. El puerto de destino por omisión para Telnet y TN3270 es el mismo (23), por lo que, a menos que desee que uno o los otros conjuntos de usuarios utilicen un puerto de destino distinto del valor por omisión, debe dejar de lado direcciones IP diferentes para los usuarios de Telnet y de TN3270.

Si desea utilizar el código de direccionador de la V3.4 o superior, el procedimiento recomendable es el que consiste en definir una interfaz de bucle de retorno y utilizar una de las direcciones IP de esta interfaz como dirección IP de servidor TN3270. Si desea utilizar un código de direccionador anterior a la V3.4, tiene que elegir entre utilizar una dirección de interfaz física para TN3270 y dejar la dirección interna para Telnet, o bien lo contrario. Una consideración importante en esta elección es si tiene diversos servidores TN3270 paralelo, todos los cuales necesitan la misma dirección de servidor pero diferentes direcciones Telnet para el mantenimiento.

## Puertos TCP de servidor

Cuando se configura la dirección IP de servidor, también se especifica el número de puerto TCP de destino al que se conectarán los clientes TN3270. Debe proporcionar, por lo menos, un número de puerto como parte de la configuración general del servidor (mandato `TN3270E config> set; panel TN3270E Server/General` del Programa de configuración). Opcionalmente, puede configurar puertos TCP adicionales en los que vaya a "escuchar" el servidor TN3270 (mandato `TN3270E config> add port; panel TN3270E Server/Ports` del Programa de configuración).

Las siguientes son razones por las cuales es posible que desee configurar más de un puerto TCP de servidor:

- Separación entre clientes "E" y clientes "no E"

El protocolo TN3270 necesita un servidor con posibilidad de E para iniciar ciertas negociaciones con los clientes. Algunos clientes no E antiguos fallan en lugar de ignorar estas negociaciones. Puede configurar el direccionador de manera que dé un tratamiento de clientes no E a los clientes que se conectan a un puerto de destino determinado y no les envíe la petición rechazable. A continuación, puede configurar los clientes no E de manera que se conecten a este puerto.

- Correlación de clientes con recursos de SNA mediante un número de puerto  
Habrán muchos clientes que no puedan solicitar un recurso de SNA por el nombre, pero todos ellos se conectan a un puerto TCP de destino. Cuando configure un puerto de destino, asocie una agrupación de LU con este número de puerto (existe una agrupación por omisión global por si no especifica ninguna en particular). Los clientes que se conecten a este puerto y no especifiquen un nombre de LU tendrán asignada una LU de esta agrupación.
- Inhabilitación de la correlación de direcciones IP para algunos clientes  
Si ha habilitado globalmente la correlación de direcciones IP de cliente con nombres de LU o de agrupación de LU, el direccionador elige la LU utilizando las normas de la correlación de direcciones IP en vez de utilizar la asociación de puerto con agrupación de LU. Es posible que desee tener un conjunto de clientes que estén exentos de esta correlación (tenga en cuenta que los clientes que no coinciden con las correlaciones configuradas no pueden conectarse). Puede configurar un puerto de destino de manera que, cuando un cliente se conecte a este puerto, se ignore la correlación de direcciones IP. Cuando selecciona esta opción, se utiliza en cambio la agrupación de LU asociada con este puerto para elegir la LU.
- Correlación de clientes con recursos de SNA mediante la correlación de direcciones IP específica de puerto  
Si ha habilitado globalmente la correlación de direcciones IP de cliente con nombres de LU o de agrupación de LU, es posible que desee aplicar diferentes normas de correlación de IP a los diferentes conjuntos de clientes. Cuando configura una entrada de tabla de correlaciones de IP, puede especificar un número de puerto TCP de destino (el valor por omisión hace referencia a todos los puertos). Cuando hace esto, sólo se comprueban con esta entrada de correlación los clientes que se conectan a este número de puerto.

## Definición de PU

Siempre debe definir PU dependientes en el direccionador, que contendrán las LU que el direccionador asocie con conexiones TCP de cliente TN3270 de entrada. Cada PU que defina debe tener una definición de PU correspondiente en VTAM.

Si decide utilizar el DLUR para la conexión de sistema principal, cada PU interna definida presentará el aspecto de tener un enlace lógico "de dentro del sistema" con la función DLUR. Este enlace lógico siempre está activo cuando APPN y TN3270 están activos. Es posible que, al mismo tiempo, el DLUR sirva a otras PU dependientes que sean externas respecto al direccionador.

Sólo tiene que definir el número de PU que necesite para que contengan las LU, siendo posible que cada PU abarque 255 LU. Si define más de una PU local, debe distinguirlas especificando diferentes ID de nodo local. Si desea configurar una PU local para el DLUR mediante la línea de mandatos, utilice el mandato **add local-pu**. Desde el Programa de configuración, seleccione Local PUs bajo el protocolo de servidor TN3270E en la ventana Navigation.

Si decide utilizar enlaces de subárea para la conexión de sistema principal, cada enlace se enlaza lógicamente con la PU interna asociada. El direccionador crea esta PU interna automáticamente cuando se configura un enlace de subárea; el usuario no configura explícitamente PU internas como en el DLUR. El enlace asociado con cada PU es un enlace externo real que se puede activar o desactivar. Algunos usuarios distribuyen las LU de una sola agrupación entre diversas PU de subárea para que, si un enlace falla, pueda haber otro disponible con el fin de dar servicio a los intentos de los clientes para volver a conectarse.

Si desea configurar un enlace de subárea mediante la línea de mandatos, utilice el mandato **add link**. Responda **yes** a la pregunta "Solicit SSCP session?", y **no** a la pregunta "Does link support APPN function?". Desde el Programa de configuración, seleccione Interfaces bajo el protocolo APPN en la ventana Navigation y, a continuación, efectúe una pulsación sobre la cabecera de la columna de estaciones de enlace. Si configura más de un enlace de subárea bajo el mismo puerto físico, debe habilitar este puerto para el soporte de diversas PU. Las PU se distinguen por el ID de nodo local así como por la información de sistema de dirección local, como, por ejemplo, la dirección de SAP.

## Definición de LU

Cuando un cliente TN3270 se conecta completamente, su conexión TCP queda emparejada con la representación de LU de SNA del servidor. VTAM también tiene una representación para la misma LU. Cada una de estas representaciones de LU tiene un nombre, y es posible, pero no necesario, que el nombre de LU del servidor coincida con el nombre de LU de VTAM. Puesto que una configuración normal de TN3270 implica miles de LU para satisfacer a otros tantos clientes potenciales, se han desarrollado diversos esquemas para aliviar la carga de configurar LU y para posibilitar la coincidencia entre nombres del servidor y nombres de VTAM.

Actualmente, la implementación del servidor TN3270 proporcionada por el direccionador IBM da soporte a los métodos de definición de LU que aparecerán a continuación. Consulte las secciones que siguen para obtener una descripción detallada de cada método. Todos estos métodos están disponibles tanto si la conexión del enlace de sistema principal es de DLUR como si es de subárea.

- Estático en el direccionador, estático en el sistema principal

Utilizando este método configura LU en el direccionador individualmente, por el nombre, o bien en grupos, mediante gérmes de nombre. El usuario define las LU correspondientes en VTAM manualmente utilizando los mismos nombres de LU o diferentes. El ID de PU y las direcciones de NAU de LU son los elementos que relacionan las LU del direccionador con las LU de VTAM.

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

Con este método también configura LU en el direccionador individualmente, por el nombre, o bien en grupos, mediante gérmes de nombre. En VTAM,

codifica definiciones de LU modelo y las asocia con las PU dependientes definidas en el direccionador. Cuando un cliente TN3270 se conecta con el direccionador, éste selecciona una LU y envía la información configurada del mismo sobre esta LU a VTAM (dirección de NAU y nombre). La acción de pasar el nombre de LU del direccionador de esta manera se denomina "empuje de nombre". VTAM crea la definición de LU dinámicamente utilizando su propio germen de nombre o el nombre de LU que ha "pasado" el direccionador.

Cuando un cliente TN3270 se desconecta, el direccionador envía una notificación de este suceso. Los niveles más recientes de VTAM tienen la posibilidad de destruir la LU dinámica. Las versiones anteriores no destruyen la LU, sino que simplemente la desactivan hasta que la utilice otro cliente. La creación y supresión dinámicas hacen posible que la misma LU definida esté servida por cualquiera de los servidores TN3270 con equilibrio de carga paralelo.

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

Con este método, no tiene que configurar LU en el direccionador. Sólo se realiza una configuración basada en que una PU dé soporte a LU dinámicas iniciadas por sistema principal. En VTAM, se definen PU y LU manualmente de la manera normal. Cuando activa las LU en VTAM, los ACTLU causan que el direccionador cree dinámicamente las LU correspondientes utilizando el nombre de LU de VTAM. Las LU dinámicas reciben el tratamiento de LU explícitas o se colocan en agrupaciones de LU implícitas dependiendo de si se ha configurado un nombre de agrupación para la PU con posibilidad de HIDLU.

Puede elegir cualquiera de estos métodos de definición de LU basándose en el tamaño de la configuración de la red, el nivel del direccionador y código de VTAM, los requisitos de denominación de LU y los requisitos de equilibrio de carga de servidor. Puede combinar el método HIDLU con los otros métodos configurando algunas LU en el direccionador y permitiendo que las restantes se creen dinámicamente, incluso dentro de la misma PU.

## LU configuradas

Es necesario configurar LU en el direccionador a menos que utilice LU dinámicas iniciadas por sistema principal. Puede configurar LU individuales o grupos de LU. Normalmente, deberá configurar LU individuales cuando desee especificar completamente el nombre de LU y fijarlo en una dirección de NAU determinada. Deberá configurar grupos de LU cuando tenga un elevado número de LU similares para definir y desee que el direccionador genere los nombres de LU.

Para configurar una LU individual desde la línea de mandatos, utilice el mandato **add lu**. Especifique el nombre de la PU (o del enlace de subárea) para la LU, así como el nombre, tipo y dirección de NAU de la LU. Para configurar una LU individual desde el Programa de configuración, seleccione LUs bajo el protocolo de servidor TN3270E en la ventana Navigation y después efectúe una pulsación sobre la cabecera de la columna de LU.

Para configurar un grupo de LU desde la línea de mandatos, utilice el mandato **add implicit-pool**. Este mandato define un grupo de LU bajo una sola PU y las coloca en una agrupación. Puede utilizar este mandato diversas veces para colocar diferentes grupos de LU en la misma agrupación, como, por ejemplo, LU de diferentes PU.

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

En lugar de un solo nombre de LU, para un grupo se especifica una máscara de nombre de LU. Cuando el direccionador se inicializa, asigna los nombres de LU añadiendo a esta máscara como sufijo la dirección de NAU de LU en decimal (sin rellenos de ceros iniciales). Por ejemplo, la máscara "@LU1A" puede dar como resultado los nombres de LU @LU1A1, @LU1A2, y así sucesivamente.

Si se especifica un rango de direcciones de NAU, el direccionador genera los nombres añadiendo la dirección de NAU a partir del final del rango hasta arriba, como se acaba de mostrar con @LU1A. Si se especifica el número de LU en lugar de un rango de direcciones de NAU, el direccionador genera los nombres a partir de la NAU 2 y va aumentando, hasta llegar al 255 y finalizar con 1. Por ejemplo, la máscara @LU2A para 10 LU generará los nombres @LU2A2, @LU2A3, ..., @LU2A11. El código de servidor empieza por el 2 para mantener una coherencia de migración con los releases de código anteriores que no daban soporte al valor 1 de NAU. Si desea ver los nombres exactos generados por el direccionador para las LU de una PU en particular, utilice el mandato de Talk 5 de TN3270 **list pu nombre**.

Para configurar un grupo de LU desde el Programa de configuración, primero debe dar nombre a la agrupación de destino seleccionando Pools bajo el protocolo de servidor TN3270E en la ventana Navigation. A continuación, seleccione LUs en la ventana Navigation y efectúe una pulsación sobre la cabecera de la columna de agrupaciones implícitas.

## Definición dinámica de LU dependientes (DDDLU)

Tal como se ha resumido en la sección Definición de LU, puede utilizar la DDDLU para evitar la definición duplicada de LU en VTAM y en el direccionador. La DDDLU le permite configurar LU en un solo sitio, el direccionador. En VTAM, sólo tiene que definir una o más PU según el número de LU que necesite. La implementación de la DDDLU también elimina el esfuerzo que suponen las definiciones de VTAM y el mantenimiento para los requisitos futuros de definición de LU.

### Creación de LU en VTAM

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

- La dirección de NAU local de la LU
- El nombre del direccionador para la LU
- El indicador de encendido/apagado
- El tipo de dispositivo y número de modelo del dispositivo
- Otra información que es opcional y depende de cada dispositivo

Al recibir este NMVT, VTAM ve en la definición de PU que no existe definición para la LU en cuestión. Entonces VTAM utiliza la definición de PU y la información del NMVT para elegir una sentencia de LU modelo y crear una definición de LU.

El nombre que VTAM elige para la LU dinámica viene determinado por una rutina de salida relativa a la Selección de definiciones para LU dependientes (SDDL). Si se utiliza la rutina de salida de usuario suministrada por IBM estándar, VTAM crea un nombre utilizando el valor de LUSEED de la sentencia de PU, cuyo sufijo es la dirección de NAU. El usuario también debe codificar el operando LUGROUP para especificar un nodo principal modelo. Estas operaciones están descritas en la publicación *VTAM Network Implementation Guide*, SC31-8370, bajo la sección titulada "Defining Dependent LUs Dynamically".

Si desea que VTAM utilice el nombre de LU que el direccionador envía en el mandato Reply PSID NMVT, debe sustituir la salida de usuario estándar de la SDDL por una disponible en las páginas Web de bajada de soporte de direccionador IBM. Esta rutina ignora el operando LUSEED y simplemente utiliza el nombre empujado desde el direccionador. Para bajar esta rutina desde las páginas Web sobre el 2216, por ejemplo, vaya a <http://www.networking.ibm.com/support/downloads/2216>, seleccione el enlace con los archivos de APPN/TN3270 y seleccione el paquete de la salida de usuario. El paquete es común a todos los direccionadores IBM.

### Supresión de LU de VTAM

Cuando un cliente TN3270 se desconecta del direccionador, éste envía a VTAM otro Reply PSID NMVT para indicar que el dispositivo está desactivado. Entonces VTAM puede suprimir la LU creada dinámicamente. Así se libera almacenamiento y el nombre está disponible para que se vuelva a utilizar.

El soporte de VTAM a la supresión de LU dinámicas después de desconexión de cliente se encuentra en el código base de CS para OS/390 V2R6, y se le ha aplicado el PTF en CS para OS/390 V1R3 y anteriores con el APAR OW29773.

### LU dinámicas y Network Dispatcher

El asignador de tareas Network Dispatcher (ND) de IBM puede proporcionar una función de equilibrio de carga de TCP cuando se instala entre los clientes y dos o más servidores TN3270. La versión de direccionador IBM del asignador ND y el Servidor TN3270 funcionan conjuntamente para que ND envíe nuevas conexiones de cliente al servidor TN3270 menos ocupado. Anteriormente, cuando se utilizaba ND para equilibrar la carga entre los servidores TN3270 en relación con el mismo VTAM, no se podían tener LU que necesitaran un nombre de LU de VTAM fijo. Esto es porque ND podía direccionar la conexión TCP de cliente hacia cualquiera de los servidores pero no se podían tener nombres de LU duplicados activos en VTAM al mismo tiempo.

Con el empuje y la supresión de nombres de LU, puede configurar el nombre de LU que desee en todos los servidores TN3270 potenciales. Cuando el cliente se conecta, el servidor seleccionado por ND envía el nombre a VTAM para la creación dinámica. Cuando el cliente se desconecta, VTAM puede suprimirlo. Esto hace que esté disponible para que vuelva a crearse por medio de cualquier servidor TN3270 que ND seleccione la próxima vez que el cliente se conecte.

## Detalles adicionales

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

### Ejemplo:

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

**1** En esta definición de muestra, se ha solicitado que esté la LU 'SALE01' en LOCADDR=98 por requisitos específicos. Como consecuencia, se ha definido esta LU específica bajo esta 'DDDPV' para cumplir los requisitos.

**2** En esta definición, la impresora también debe estar en una dirección específica. Esto sucede especialmente en el caso de algunas aplicaciones de SNA (p.e. CICS). La aplicación del departamento de ventas necesita una impresora en la dirección 99, con LOGMODE=SAL3287, y tiene que conectarse a la aplicación CICSA cuando se active.

Para los usuarios que deseen escribir sus propias rutinas de salida o modificar una de las rutinas de salida de la SDDL de VTAM, el direccionador envía información de LU en el Reply PSID NMVT de la manera siguiente:

- SV10, el subcampo 11 contiene uno de los valores de tipo de dispositivo y modelo listados en la Tabla 4 en la página 102.
- SV86, el subcampo 00 contiene IBMTN3270LUNAME para indicar que se empuja un nombre de LU.
- SV86, el subcampo 10 contiene el nombre de LU real en EBCDIC.

A continuación, se muestra un ejemplo de estos subvectores:

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

<i>Tabla 4. Valores de tipo de dispositivo/modelo</i>	
<b>Dispositivo/Modelo</b>	<b>Vector de NMVT</b>
Pantalla 3270 mod 2	3270002
Pantalla 3270 mod 3	3270003
Pantalla 3270 mod 4	3270004
Pantalla 3270 mod 5	3270005
Impresora 3270	3270P
Impresora SCS	SCSP

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

Tal como se ha resumido en la sección “Definición de LU” en la página 97, la HIDLU elimina la carga de configurar LU en el direccionador al permitir que éste cree LU dinámicamente cuando se activan las mismas en VTAM. En realidad, se trata del opuesto de la DDDL, según la cual las LU se configuran en el direccionador y se crean dinámicamente en VTAM. La HIDLU permite que las LU se definan en VTAM únicamente. En el direccionador defina sólo una PU, o las que necesite, pero no LU para estas PU.

Cuando VTAM activa las PU y sus LU, los nombres de LU de VTAM se transportan al direccionador en mandatos ACTLU dentro del vector de control 0E. Las LU definidas de esta manera tienen el mismo nombre en VTAM y en el direccionador.

Para configurar la HIDLU en el direccionador, debe definir PU dependientes locales en éste para el DLUR o para enlaces de subárea tal como se describen en la sección “Definición de PU” en la página 96. Cuando configure la PU de DLUR o el enlace de subárea, indique que para esta PU deben permitirse LU dinámicas iniciadas por sistema principal. Indique también si estas LU dinámicas se van a colocar en una agrupación o no; para ello, especifique opcionalmente un nombre de agrupación. Si no especifica ningún nombre de agrupación, las LU sólo recibirán el tratamiento de LU de estación de trabajo. Si especifica un nombre de agrupación, puede indicar si son LU de estación de trabajo o de impresora. Todas las LU con HIDLU agrupadas de una PU determinada deben estar en la misma agrupación y tener el mismo tipo. Puede utilizar el mismo nombre de agrupación para diversas PU si desea que haya más de 255 LU en la agrupación o si desea que la agrupación abarque diversos enlaces de subárea.

Si coloca las HIDLU en una agrupación, no es necesario que configure clientes que soliciten explícitamente una LU en particular. Los clientes pueden solicitar una LU por el nombre de agrupación mediante una correlación de dirección IP con agrupación o mediante una correlación de puerto TCP con agrupación. También puede mezclar LU explícitas con LU agrupadas de HIDLU configurando una LU individual bajo una PU que esté configurada con una agrupación iniciada por sistema principal. Cuando llegue el ACTLU para la LU individual configurada, el direccionador no creará una LU dinámica.

Para configurar la HIDLU en VTAM, debe definir las LU dependientes en el nodo principal y especificar INCLUD0E=YES en la sentencia de PU. La palabra clave



INCLUD0E está soportada por VTAM V4R4 con los APAR OW31805 y OW31436. En las conexiones de subárea de tipo remoto a través de NCP, es necesaria la V7R6 para el soporte de la palabra clave INCLUD0E.

Si el sistema principal es un DLUS y un DLUR sirve a la PU en otro nodo, sucede que el CV0E de la petición ACTLU no puede remitirse a la PU desde el DLUR. En este caso, las LU no se crearán dinámicamente. Una vez que se hayan creado LU dinámicamente, sólo pueden eliminarse rearrancando o con la supresión manual por medio de la configuración. Si se cambian los nombres de LU en el archivo de nodo principal del sistema principal después de que se hayan creado las LU dinámicamente, los nombres locales del direccionador no cambiarán.

## Correlación de cliente con LU

Cuando un cliente TN3270 se conecta con un servidor, el servidor debe elegir una LU para asociarla con este cliente o bien rechazar la conexión. Existen varias maneras de configurar los clientes y el servidor para controlar qué LU se elegirán y qué clientes se rechazarán. La implementación del servidor TN3270 proporcionada por el direccionador IBM da soporte a los métodos siguientes:

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

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

### Conceptos

**LU individuales y agrupaciones de LU:** Tal como se ha descrito anteriormente en la sección "LU configuradas" en la página 98, puede configurar LU individuales o grupos de LU en el direccionador. Asimismo, las LU dinámicas iniciadas por sistema principal pueden tratarse individualmente o en grupos. Una agrupación de LU es un grupo de LU con un nombre. Por ejemplo, una agrupación puede denominarse MYPOOLA.

Las LU de una agrupación pueden proceder de una o muchas PU diferentes. A excepción de las LU dinámicas iniciadas por sistema principal, las LU de una PU pueden colocarse en diversas agrupaciones. Normalmente, las LU que coloque en una agrupación específica tendrán definiciones de VTAM y características similares, como, por ejemplo, la utilización del mismo USSMSG10. La utilización de agrupaciones es el método primario para agrupar LU similares y, al final, se efectuará la correlación de un conjunto de usuarios finales de cliente TN3270 con agrupaciones específicas.

**La agrupación por omisión global:** Siempre hay, como mínimo, una agrupación definida en el Servidor TN3270E: se trata de la agrupación por omisión global. Esta agrupación recibe nombre cuando se configura inicialmente el Servidor TN3270E, y por omisión se denomina PUBLIC. Sea cual sea el nombre que dé a la agrupación por omisión, puede hacer referencia a este nombre en otras partes de la configuración de servidor utilizando la serie de caracteres especial <DEFAULT >. Ello le permite cambiar más adelante el nombre de agrupación en un solo sitio sin tener

que cambiar todas las referencias al nombre. No obstante, tenga en cuenta que la serie <DEFLT> tiene un significado especial cuando se utiliza en una entrada de tabla de correlaciones de dirección IP, por lo que debe ir con cuidado para comprender este significado al definir tales correlaciones.

Es posible que no sea necesario tener una agrupación por omisión, pero ésta existirá de todas formas. No obstante, no tiene que poner ninguna LU en esta agrupación.

**LU explícitas y LU implícitas:** Es posible dividir las LU del servidor TN3270 en dos categorías, que dependen de cómo pueden acceder a ellas los clientes. Las LU implícitas siempre son miembros de una agrupación y los clientes pueden acceder a ellas por el nombre individual de las mismas o mediante cualquiera de los métodos que utilizan nombres de agrupación. Configuraré LU implícitas añadiendo un grupo de LU a una agrupación o añadiendo LU individuales a una agrupación. Las LU explícitas nunca son miembros de una agrupación (ni de la agrupación por omisión global), por lo que sólo permiten el acceso a los clientes que soliciten el nombre individual de las mismas o mediante correlaciones de dirección IP con este nombre. La función de servidor nunca asignará una LU explícita a un cliente que solicite un nombre de agrupación o que esté correlacionado con un nombre de agrupación.

### Clientes peticionarios de nombres de LU

Las implementaciones de cliente que dan soporte a las normas RFC 1646 ó 2355 pueden solicitar un nombre de recurso cuando se conectan con un servidor TN3270. En el servidor de direccionador IBM, este nombre recibe el tratamiento de nombre de LU individual o de nombre de agrupación. En la configuración de cliente puede ser un nombre de LU aunque el mismo nombre esté configurado en el direccionador como nombre de agrupación.

Si el método de definición de LU elegido implica diferentes nombres de LU en el direccionador y en VTAM, el nombre que pase el cliente debe coincidir con el nombre de LU del direccionador y no con el nombre de LU de VTAM.

En ausencia de correlación de dirección IP y de puerto TCP, el servidor intenta satisfacer la petición del cliente del modo que sigue:

- Si el cliente solicita un nombre de LU individual válido y ésta se encuentra disponible, se asigna la LU. Si no está disponible, el servidor rechaza la conexión.
- Si el cliente solicita un nombre de agrupación válido y está disponible una LU en esta agrupación, se asigna la LU. Si no hay LU disponibles, el servidor rechaza la conexión.
- Si el nombre solicitado no es válido, el servidor rechaza la conexión.

Consulte las secciones que siguen para saber qué sucede cuando un cliente solicita un nombre y también es aplicable uno de los métodos de correlación.

## Correlación de dirección IP de cliente con LU/agrupación

Puede configurar la función de servidor TN3270 del direccionador de manera que correlacione direcciones IP de cliente con nombres de LU individual o con nombres de agrupación de LU. Es posible que desee elegir este método si los clientes no tienen la posibilidad de solicitar nombres de recurso o no desea configurar los clientes de manera individual. Asimismo, puede que desee utilizar esta función

como mecanismo de seguridad, para rechazar las conexiones con cualquier cliente que no esté en la lista de acceso de correlaciones de IP.

Para configurar esta función de correlación, primero debe habilitarla globalmente como parte de la configuración de servidor TN3270 general. Si desea que los clientes que se conecten a determinados puertos TCP de servidor estén exentos de la correlación de dirección IP, puede inhabilitar esta función según el puerto cuando configure los puertos. A continuación, cree una tabla de entradas de correlación de dirección IP, cada una de las cuales correlacionará un conjunto de direcciones IP con un nombre de LU individual o agrupación. Por omisión, una entrada determinada se aplica a todos los puertos TCP de servidor, pero el usuario puede especificar que una entrada sólo se utilice para las conexiones a un puerto TCP de destino determinado. Esto le permite hacer que clientes de diferentes redes IP utilicen el mismo conjunto de números de puerto pero se correlacionen con diferentes agrupaciones de LU sobre la base de la red y del número de puerto de servidor de destino.

Los campos clave de cada entrada de correlación son: una dirección IP, una máscara de dirección IP y un nombre de LU o de agrupación de LU. La máscara de dirección IP indica qué bits de la dirección IP configurada deben compararse con los bits correspondientes de la dirección IP de origen de cliente de entrada. Así puede correlacionar clientes individuales o subredes enteras.

Por ejemplo, si la entrada de correlación está definida de la siguiente manera:

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

Si un cliente TN3270 se conecta utilizando la dirección IP 1.2.3.4, el Servidor TN3270E asignará MYLU a este cliente. Aquí se correlaciona una dirección IP individual con una LU individual. También pueden correlacionarse clientes específicos con una agrupación.

Si la entrada de correlación está definida de la siguiente manera:

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

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

Suponga que define las dos entradas de correlación anteriores. Tenga en cuenta que el cliente 1.2.3.4 coincide con ambas entradas de correlación. El Servidor TN3270E siempre utilizará primero la coincidencia más específica. En este ejemplo, el cliente se correlacionará con la LU denominada MYLU.

Suponga de nuevo que ha definido las dos entradas de correlación anteriores y que el cliente 1.2.3.4 se conecta. TN3270 elegirá la entrada de correlación más específica e intentará conectarse con la LU denominada MYLU. No obstante, por alguna razón el servidor no puede establecer la sesión con MYLU de manera satisfactoria; puede que MYLU ya se utilice o que VTAM no la haya activado. Después

de intentar conectarse con MYLU sin resultados satisfactorios, normalmente el servidor explorará la tabla de correlaciones de dirección IP para ver si hay otra coincidencia menos específica en relación con este cliente. En el ejemplo anterior existe otra coincidencia y el Servidor TN3270E conectará el cliente con una LU de YOURPOOL.

Hay casos en que es posible que el usuario no desee que el direccionador utilice una coincidencia menos específica después de que falle una coincidencia más específica. Para controlar este comportamiento, puede configurar opcionalmente una entrada como "final LU mapping connection attempt". Si se establece este distintivo de yes/no, la función de servidor no busca coincidencias menos específicas después de una coincidencia fallida con esta entrada.

El servidor TN3270 efectúa las comprobaciones siguientes cuando un cliente se conecta con el direccionador y no pasa la petición de un nombre específico:

1. En el caso de que esté habilitada globalmente la correlación, la pregunta es si lo está en el puerto de destino. Si no lo está, las peticiones de entrada se tratan sin utilizar la correlación de dirección IP.
2. Si lo está, se intenta comparar la dirección IP de cliente de entrada con las entradas de correlación siguiendo este orden:
  - a. entradas para el puerto de destino específico, primero la dirección IP más específica
  - b. entradas para todos los puertos de destino, primero la dirección IP más específica
3. Si hay una coincidencia, se intenta emparejar la conexión con la LU indicada o una LU de la agrupación indicada, respetando el tipo de LU (estación de trabajo o impresora) solicitado por el cliente.
4. Si hay algún problema y ésta no es la entrada de correlación "final", se repite la acción de buscar por si hay coincidencias menos específicas. Antes de rechazar la conexión, se continúa hasta que se han agotado todas las coincidencias o hasta que la conexión es satisfactoria.
5. Si no hay ninguna coincidencia, se rechaza la conexión.

Cuando un cliente se conecta y realiza la petición de un nombre específico, la lógica de la comparación es diferente. Para una conexión satisfactoria, debe existir una entrada de correlación en que la dirección IP y máscara coincidan con el cliente y cuyo nombre de recurso sea exactamente igual que el nombre pasado por el cliente. Si el cliente solicita un nombre de LU individual, debe estar este nombre en la tabla de correlaciones, no tan sólo el nombre de una agrupación que contenga esta LU. El servidor no busca en la tabla de correlaciones la coincidencia de dirección IP y máscara más específica. Si no puede satisfacerse la conexión con la LU/agrupación del nombre solicitado, el servidor no explora de nuevo la tabla de correlaciones para buscar otras entradas coincidentes.

Puede utilizar el mandato de Talk 5 de TN3270 list mapping para ver el orden por el cual se buscarán las entradas de correlación. Puede poner en este mandato una dirección IP específica como parámetro para ver solamente las entradas de correlación que son aplicables a esta dirección IP.

A continuación, se describen varias consideraciones adicionales importantes respecto a la creación de entradas de correlación de dirección IP:

- Si tiene diversas entradas que son igualmente específicas, se utilizan primero las definidas más recientemente.
- Si la agrupación por omisión global tiene el nombre PUBLIC y el usuario configura una entrada de correlación con el nombre PUBLIC, el servidor conecta los clientes de entrada con las LU de esta agrupación. Si, en lugar de ello, el usuario configura una entrada de correlación con el nombre <DEFLT>, el servidor no conecta los clientes con la agrupación PUBLIC. Lo que hace es pasar a las normas de asociación de puerto TCP y conectar el cliente con la agrupación asociada con el puerto de servidor de destino al que el cliente se ha conectado.
- Inicialmente, el servidor TN3270E crea la tabla de correlaciones de dirección IP con una entrada por omisión que contiene la dirección IP 0.0.0.0, la máscara de subred 0.0.0.0 y el nombre de agrupación <DEFLT>. Esta entrada coincidirá con todas las direcciones de cliente de entrada. Como se ha mencionado antes, causará que el servidor correlacione los clientes con LU de la agrupación asociada con el(los) puerto(s) TCP de destino. Si prefiere no tener esta entrada por omisión en la tabla de correlaciones de nombre de LU, puede crear una entrada similar por encima que se correlacione con una agrupación definida e indicar que sea la última de la búsqueda. Si la agrupación definida es la agrupación por omisión global, se puede elegir no configurar ninguna LU en esta agrupación.
- Los nombres de LU y agrupación que configure en las entradas de correlación de IP deben configurarse en el direccionador para que se activen. Por ejemplo, no puede configurar nombres de LU individual dinámica iniciada por sistema principal en las entradas de correlación de IP porque estos nombres no son conocidos para el direccionador cuando se inicializa. No obstante, puede configurar nombres de agrupación de HIDLU porque éstos se configuran en el direccionador.
- En el caso de las LU de estación de trabajo individuales con impresoras asociadas, tanto la LU de estación de trabajo como la LU de impresora han de tener una entrada de tabla de correlaciones de IP con la misma dirección IP de cliente.
- La especificación de un número de puerto en una entrada de tabla de correlaciones de dirección IP no causa que el servidor TN3270 defina el puerto y escuche en él para las conexiones de cliente. Debe configurar el puerto de manera explícita (utilizando **add port**) para que una referencia al mismo en esta tabla tenga sentido.

## Asociación de puerto TCP de servidor con agrupación

Puede configurar la función de servidor TN3270 del direccionador de manera que correlacione conexiones de cliente de entrada con agrupaciones de LU basándose en el número de puerto TCP al que se conecten los clientes. Es posible que desee elegir este método si los clientes no tienen la posibilidad de solicitar nombres de recurso o no desea configurar los clientes de manera individual. Asimismo, puede que desee realizar una migración relativa a una red existente en la que los clientes ya se conecten a diferentes números de puerto TCP según las necesidades de la aplicación.

Para configurar la asociación de puerto TCP con agrupación, especifique un nombre de agrupación con el puerto cuando configure el puerto (consulte la sección "Puertos TCP de servidor" en la página 95). Obviamente, cada cliente

tiene que conectarse mediante uno de los puertos definidos y la función de servidor asigna una LU basándose en qué agrupación está asociada con el puerto. Si no especifica un nombre de agrupación para un puerto o bien proporciona el valor especial <DEFLT>, se asociará con este puerto la agrupación por omisión global. Ésta es la misma agrupación que asocia con el puerto de servidor definido globalmente la primera vez que configura el servidor TN3270.

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

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

- Si el puerto está asociado con un nombre de LU o agrupación que es exactamente igual que el nombre pasado por el cliente, el cliente se conectará con la LU o con una LU de la agrupación (si está disponible).
- Si el puerto está definido con un nombre de agrupación nulo o con el nombre <DEFLT>, el cliente se conectará con la LU específica o una LU de la agrupación que ha pasado, siempre y cuando este nombre de LU o agrupación exacto esté configurado en alguna parte del servidor TN3270E. Una LU individual puede ser explícita o implícita. El tipo de LU o agrupación (estación de trabajo, impresora SCS o impresora 3270) debe coincidir con la petición. Si el nombre es de LU, no importa la agrupación, si la hay, en que esté agrupada la LU.
- Si no es aplicable ninguna de las dos condiciones anteriores o no está(n) disponible(s) la(s) LU(s) especificada(s), se rechaza la conexión.

En la descripción anterior se da por supuesto que la correlación de IP está inhabilitada. Si está habilitada la correlación de dirección IP, por omisión se aplicará esta función a todos los puertos y alterará temporalmente la correlación de puerto TCP con agrupación. Puede cambiar este comportamiento por omisión si inhabilita la correlación de dirección IP según el puerto TCP, tal como se ha descrito más arriba. Tenga en cuenta también el caso especial en que una entrada de correlación de dirección IP con la agrupación <DEFLT> puede causar la asignación de una LU de la agrupación asociada con el puerto TCP.

## Combinación de correlación de puerto y correlación de dirección IP

Es posible servirse de una combinación entre la correlación de dirección IP y la asociación de puerto TCP con agrupación. El ejemplo siguiente muestra cómo un usuario ha combinado estos métodos para satisfacer las necesidades de correlación.

- El usuario había habilitado la correlación de dirección IP y había definido entradas de correlación para correlacionar subredes IP de cliente específicas con agrupaciones específicas.
- Los mismos clientes del usuario final tienen que conectarse de vez en cuando con un grupo de LU que presenta una pantalla de inicio de sesión de USSMSG10 diferente.
- Puesto que éste es el mismo conjunto de clientes, utilizarían las mismas direcciones IP, por lo que la adición de entradas de correlación adicionales a la tabla de correlaciones de dirección IP no resolverá sus necesidades.

- El usuario ha definido una nueva agrupación de LU, ha definido un nuevo puerto y lo ha asociado con la nueva agrupación. Además, se ha definido este nuevo puerto de manera que no utilice la tabla de correlaciones de dirección IP porque esto significaría utilizar las agrupaciones originales.
- A continuación, se han configurado los clientes de las estaciones de trabajo de usuario final de manera que se conecten con el nuevo puerto.

## Equilibrio de carga entre diversas PU

Es normal definir una gran agrupación de LU que residen en diversas PU. Cualquier agrupación con más de 255 LU debe incluir más de una PU. El que las LU de una agrupación estén diseminadas entre diversas PU puede disminuir el número de clientes afectados por cualquier anomalía de una PU o un enlace determinado. La manera en que el servidor asigna LU procedentes de esta diversidad de PU también determina cuántos clientes quedarán afectados por una anomalía de PU o enlace. Por ejemplo, si el servidor asigna todas las LU de una PU antes de asignar cualquier LU de la segunda PU, la anomalía de la primera puede afectar a un número de 255 clientes sin necesidad.

En general, la implementación de TN3270 proporcionada por el direccionador IBM realiza una asignación rotatoria de LU de entre diversas PU de una agrupación. En igualdad de condiciones, asignará la LU1 de la PU1, la LU1 de la PU2, y así sucesivamente. Al mismo tiempo, el algoritmo de asignación actúa en favor de las PU que están actualmente activas (evita el retardo de un intento de activación) y en favor de las LU que coinciden exactamente con el tipo de modelo solicitado por el cliente.

Las normas de la selección de LU son las siguientes:

- Siempre se devuelve una coincidencia exacta con el tipo de modelo si se encuentra en una PU activa.
- Si no puede encontrarse una coincidencia exacta en una PU activa, se devolverá una LU aceptable de una PU activa antes que una coincidencia exacta de una PU inactiva.
- Para que sea una coincidencia “aceptable”, el tipo de LU (estación de trabajo, impresora SCS o impresora 3270) debe coincidir con la petición del cliente. El tipo de modelo de una LU de estación de trabajo debe tener el mismo tamaño de pantalla o menor que el solicitado por el cliente. Por ejemplo, si un cliente ha solicitado un modelo 4, una LU de modelo 4 será una coincidencia exacta, y las LU de modelo 3 ó 2 serán coincidencias aceptables.

Basándose en si se encuentra una coincidencia exacta o aceptable, las PU se trasladan dentro una lista para proporcionar la asignación rotatoria general a la vez que se impide que se busquen primero las PU menos convenientes en todo momento.

---

## Configuraciones de ejemplo

Este apartado contiene configuraciones de muestra de línea de mandatos de VTAM y direccionador respecto a situaciones básicas de servidor TN3270. Para obtener información sobre situaciones más avanzadas y sobre el Programa de configuración, consulte la sección “Otras configuraciones de ejemplo” en la página 116.

## Configuración de TN3270 con DLUR

Si va a utilizar el DLUR para comunicarse con el sistema principal, las PU locales utilizadas por el Servidor TN3270E tienen que configurarse en el sistema principal como PU internas de DLUR. El código siguiente es un ejemplo de la configuración de VTAM del sistema principal:

```

PUJ0E7      PU      ADDR=12,
              IDBLK=077, IDNUM=EEEE7, 1
              MAXPATH=8,
              ISTATUS=ACTIVE,
              MODETAB=LMT3270,
              USSTAB=STFTSNA2,
              ANS=CONT,
              MAXDATA=521,
              IRETRY=YES,
              MAXOUT=7,
              DLOGMOD=G22NNE,
              NETID=STFNET,
              PASSLIM=5,
              PUTYPE=2
JCPATH7     PATH    PID=1,
              DLURNAME=VLNN01,
              DLCADDR=(1,C,INTPU),
              DLCADDR=(2,X,07711111)
JC7LU2      LU      LOCADDR=2
JC7LU3      LU      LOCADDR=3
JC7LU4      LU      LOCADDR=4
JC7LU5      LU      LOCADDR=5
JC7LU6      LU      LOCADDR=6
    
```

**Nota:** 1 077111111 representa el bloque de ID/número de ID de la PU local. La parte 077 de este valor no puede configurarse en el direccionador.

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



```

APPN config>
APPN config>set node
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [STFNET]?
Control point name (Max 8 characters) [VLNN2]?
Enable branch extender (Y)es (N)o [N]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y ] ?
The record has been written.
APPN config>
APPN config>
APPN config>set dlur
Enable DLUR (Y)es (N)o [Y]?
Fully-qualified CP name of primary DLUS [STFNET.MVS8]?
Fully-qualified CP name of backup DLUS []?
Perform retries to restore disrupted pipe [Y]?
Delay before initiating retries(0-2756000 seconds) [120]?
Perform short retries to restore disrupted pipe [Y]?
Short retry timer(0-2756000 seconds)[120]?
Short retry count(0-65535) [5]?
Perform long retry to restore disrupted pipe [Y]?
Long retry timer(0-2756000 seconds) [300]?
Write this record? [Y ] ?
The record has been written.
APPN config>
APPN config>tn3270e
TN3270E config>set
TN3270E Server Parameters
Enable TN3270E Server (Y/N) [Y]?
TN3270E Server IP Address[4.3.2.1]?
Port Number[23]?
Enable Client IP Address to LU Name Mapping (Y/N) [N]
Default Pool Name[PUBLIC]?
NetDisp Advisor Port Number[10008]?
  Kealive type:
    0 = none,
    1 = Timing Mark,
    2 = NOP[2]?
  Frequency ( 1 - 65535 seconds)[60]?
  Automatic Logoff (Y/N)[N]?
Write this record?[Y]?
The record has been written.
TN3270E config>exit
APPN config>
APPN config>add loc
Local PU information
  Station name (Max 8 characters) []? link1
  Fully-qualified CP name of primary DLUS[STFNET.MVS8] ?
  Fully-qualified CP name of a backup DLUS[]?
  Local Node ID (5 hex digits)[11111]?
  Autoactivate (y/n)[Y]?
Write this record?[Y]?
The record has been written.

```

## Utilización de TN3270

```
APPN config>tn3270
TN3270E config>add im
TN3270E Server Implicit definitions
  Pool name (Max 8 characters)[<DEFLT>]?
  Station name (Max 8 characters)[]? link1
  LU Name Mask (Max 5 characters) [001LU]?
  LU Type      ( 1 - 3270 mod 2 display
                2 - 3270 mod 3 display
                3 - 3270 mod 4 display
                4 - 3270 mod 5 display) [1]?
  Specify LU Address Range(s) (y/n) [n]
  Number of Implicit LUs in Pool(1-255) [50]?
Write this record?[Y]?
The record has been written.
TN3270E config>
TN3270E config>add lu
TN3270E Server LU Definitions
  LU name(Max 8 characters) []? printer1
  NAU Address (1-255) [0] 2
  Station name (Max 8 characters) []? link1
  Class:
    1 = Explicit Workstation,
    2 = Implicit Workstation,
    3 = Explicit Printer,
    4 = Implicit Printer[3]?
  LU Type ( 5 - 3270 printer
            6 - SCS printer) [5]?
Write this record[Y]?
The record has been written.
TN3270E config>
TN3270E config>list all
TN3270E Server Definitions
TN3270E enabled: YES
TN3270E IP Address: 4.3.2.1
TN3270E Port Number: 23
Keepalive type: NOP           Frequency: 60
Automatic Logoff: N           Timeout: 30
  Enable IP Precedence: N
Link Station: link1
  Local Node ID: 11111
  Auto activate : YES
  Implicit Pool Informationø
    Number of LUs: 50
    LU Mask: 001LU
  LU Name   NAU addr   Class           Assoc LU Name   Assoc NAU addr
-----
printer1   2           Explicit Printer

TN3270E config>exit
APPN Config>exit
```

```

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

Routing

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

IP config>
*
```

## Configuración de TN3270E con conexión de subárea

El ejemplo siguiente muestra cómo configurar el direccionador de manera que utilice una conexión de sistema principal de sentido inverso de subárea SNA (sin APPN) para TN3270 mediante la línea de mandatos. En este ejemplo, el direccionador toma el aspecto de diversas PU de sentido directo ante VTAM.

```

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

```

APPN config>add port
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P [ ]?fr
Interface number(Default 0): [0]? 2
Port name (Max 8 characters) [F00002]?
Enable APPN on this port (Y)es (N)o [Y ] ?
Port Definition
  Support multiple subarea (Y)es (N)o [N]? y
  All active port names will be of the form <port name sap>
  Service any node: (Y)es (N)o [Y]?
  High performance routing: (Y)es (N)o [Y]? n
  Maximum BTU size (768-8136) [2048]?
  Percent of link stations reserved for incoming calls (0-100) [0]?
  Percent of link stations reserved for outgoing calls (0-100) [0]?
  Local SAP address (04-EC) [4]?
  Support bridged formatted frames: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.
APPN config>add link
APPN Station
Port name for the link station [ ]? f00002
Station name (Max 8 characters) [ ]? suba1
  Activate link automatically (Y)es (N)o [Y]?
  DLCI number for link (16-1007) [16]? 23
  Adjacent node type: 0 = APPN network node,
  1 = APPN end node or Unknown node type,
  2 = LEN end node [0]?
  Solicit SSCP Session: (Y)es (N)o [N]? y
    Local Node ID (5 hex digits) [00000]? 12345
  Local SAP address (04-EC) [4]? c
  Allow CP-CP sessions on this link (Y)es (N)o [Y]? n
  Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.
APPN config>act

```

```
APPN config>
APPN config>tn3270e
TN3270E config>set
TN3270E Server Parameters
  Enable TN3270E Server (Y/N) [Y]?
  TN3270E Server IP Address[4.3.2.1]?
  Port Number[23]?
  Enable Client IP Address to LU Name Mapping (Y/N) [N]
  Default Pool Name[PUBLIC]?
  NetDisp Advisor Port Number[10008]?
  Keepalive type:
    0 = none,
    1 = Timing Mark,
    2 = NOP[2]?
  Frequency ( 1 - 65535 seconds)[60]?
  Automatic Logoff (Y/N)[N]?
  Write this record? [Y ] ?
  The record has been written.
TN3270E config>exit
APPN config>
Write this record? [Y ] ?
  The record has been written.
```

## Utilización de TN3270

```
APPN config>tn3270
TN3270E config>add im
TN3270E Server Implicit definitions
Pool name (Max 8 characters)[<DEFLT>]?
  Station name (Max 8 characters) []? suba1
  LU Name Mask (Max 5 characters) [001LU]?
  Specify LU Address Range(s) (y/n) [N]
  Number of Implicit LUs in Pool(1-255) [50]?
Write this record? [Y ] ?
The record has been written.
TN3270E config>
TN3270E config>add lu
TN3270E Server LU Definitions
LU name(Max 8 characters) []? printer1
  NAU Address (1-255) [2]
  Station name (Max 8 characters) []? suba1
  Class:
    1 = Explicit Workstation,
    2 = Implicit Workstation,
    3 = Explicit Printer,
    4 = Implicit Printer[3]?
  LU Type ( 5 - 3270 printer
    6 - SCS printer) [5]?
Write this record[Y]?
The record has been written.
TN3270E config>
TN3270E config>list all
TN3270E Server Definitions
TN3270E enabled: YES
TN3270E IP Address: 4.3.2.1
TN3270E Port Number: 23
Keepalive type: NOP          Frequency: 60
Automatic Logoff: N         Timeout: 30
  Enable IP Precedence: N
Link Station: suba1
  Local Node ID: 12345
  Auto activate : YES
  Implicit Pool Information
    Number of LUs: 50
    LU Mask: 001LU
  LU Name   NAU addr   Class           Assoc LU Name   Assoc   NAU addr
-----
printer1   2           Explicit Printer
```

```
TN3270E config>exit
APPN Config>exit

APPN config>act
```

## Otras configuraciones de ejemplo

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

La publicación *Network Utility: Installation, Getting Started, and User's Guide*, GA27-4167-02, presenta documentación sobre la configuración del direccionador

(normalmente, de la línea de mandatos y del Programa de configuración) y configuraciones de VTAM de muestra para las configuraciones de red siguientes:

- Conexión de sistema principal de subárea mediante Red en Anillo a NCP (lo mismo para la pasarela de canal u OSA)
- Equilibrio de carga de servidores TN3270 de subárea paralelo por medio de dos direccionadores Network Dispatcher
- Conexión de sistema principal de DLUR mediante Red en Anillo con un nodo de red
- Conexión de sistema principal de DLUR mediante Enterprise Extender con una pasarela o direccionador IBM
- Definición dinámica de LU dependientes (DDDLU)
- Definición dinámica iniciada por sistema principal de LU (HIDLU)
- Antememoria de Host On-Demand (HOD) Client
- Conexión de sistema principal de subárea sobre DLSw
- Conexión de sistema principal de subárea sobre canal mediante bucle de retorno LSA

Algunas de las configuraciones anteriores están complementadas en la Web mediante archivos binarios de configuración de formato de direccionador y formato de Programa de configuración. Utilice el navegador para llegar a éstos de la manera siguiente:

1. Abra la página de bajadas de Network Utility en:  
**<http://www.networking.ibm.com/support/downloads/networkutility>**
2. Siga el enlace con los archivos "Configuration Program"
3. Busque el release de código que utilice (el contenido de los archivos ya está actualizado para cada release)
4. Abra el paquete denominado "Example Configuration Files"

Algunas de las tablas de la documentación son específicas de Network Utility porque este producto preestablece determinados parámetros de ajuste configurables. Para saber cómo correlacionar la documentación con un IBM 2216 de capacidad de memoria similar, lea las instrucciones de los paquetes de la Web "Example Configuration File" mencionados anteriormente. Los archivos de formato de Programa de configuración sólo pueden utilizarse en Network Utility, excepto un ejemplo que puede examinar utilizando el Programa de configuración.





## Configuración y supervisión de APPN

Este capítulo describe los mandatos de configuración y supervisión de APPN. Incluye los apartados siguientes:

- “Resumen de los mandatos de configuración de APPN”
- “Información detallada sobre los mandatos de configuración de APPN” en la página 121
- “Soporte de la reconfiguración dinámica de APPN” en la página 288

### Acceso al proceso de configuración de APPN

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

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

### Resumen de los mandatos de configuración de APPN

Tabla 5 (Página 1 de 2). Resumen de los mandatos de configuración de APPN

Mandato	Función	Vea la página:
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi.	
Enable/Disable	Habilita/inhabilita lo siguiente: APPN Dependent LU Requestor Port <i>nombre de puerto</i>	121
Set	Establece lo siguiente: Node Traces HPR DLUR Management Tuning	121 139 128 131 155 134
Add	Añade o actualiza lo siguiente: Port <i>nombre de puerto</i> Link-station <i>nombre de estación de enlace</i>	158 179

## Mandatos de configuración de APPN (Talk 6)

Tabla 5 (Página 2 de 2). Resumen de los mandatos de configuración de APPN		
Mandato	Función	Vea la página:
	LU-Name <i>nombre de LU</i>	200
	Connection-network <i>nombre de red de conexiones</i>	201
	Additional-port-to-connection-network	210
	Mode	209
	Focal_point	211
	local-pu	211
	Routing_list	214
	COS_mapping_table	217
Delete	Suprime lo siguiente: <ul style="list-style-type: none"> <li>• Port <i>nombre de puerto</i></li> <li>• Link-station <i>nombre de estación de enlace</i></li> <li>• LU-Name <i>nombre de LU</i></li> <li>• Connection-network <i>nombre de red de conexiones</i></li> <li>• Connection networks port interface (CN PORTIF) <i>nombre de CN</i></li> <li>• Mode <i>nombre de modalidad</i></li> <li>• Focal_point</li> <li>• local-pu</li> <li>• Routing_list</li> <li>• COS_mapping_table</li> </ul>	219
List	Lista lo siguiente de la memoria de la configuración: <ul style="list-style-type: none"> <li>• All</li> <li>• Node</li> <li>• Traces</li> <li>• Management</li> <li>• HPR</li> <li>• DLUR</li> <li>• Port <i>nombre de puerto</i></li> <li>• Link-station <i>nombre de enlace</i></li> <li>• LU-Name <i>nombre de LU</i></li> <li>• Mode <i>nombre de modalidad</i></li> <li>• Connection-network <i>nombre de red de conexiones</i></li> <li>• Focal_point</li> <li>• Routing_list</li> <li>• COS_mapping_table</li> </ul>	219
Activate_new_config	Lee la configuración en la memoria de la configuración permanente.	219
TN3270	Accede al indicador de mandatos TN320E config>	220
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.	

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

## Información detallada sobre los mandatos de configuración de APPN

### Enable/Disable

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

**Sintaxis:**

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

### Set

Utilice el mandato **set** para establecer:

**Sintaxis:**

```
set            node
```

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

*Tabla 6 (Página 1 de 7). Lista de parámetros de configuración - Direccionamiento de APPN*

Información de parámetros	
<b>Parámetro</b>	Enable APPN
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	<p>Este parámetro habilita o inhabilita al direccionador como nodo de red APPN.</p> <p>Este parámetro permite la posibilidad de direccionamiento de APPN y HPR para este nodo de red realizable al definir el ID de red y el nombre de CP del mismo. No obstante, debe habilitarse APPN en los puertos determinados en los que desee dar soporte al direccionamiento de APPN. Además, debe estar habilitado soporte para el HPR en los puertos APPN determinados que elija y debe estar soportado por las estaciones de enlace determinadas de estos puertos.</p> <p><b>Nota:</b> Sólo se da soporte al HPR en los puertos DLC directos LAN, Frame Relay y PPP.</p>

<i>Tabla 6 (Página 2 de 7). Lista de parámetros de configuración - Direccionamiento de APPN</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Network ID (necesario)
<b>Valores válidos</b>	<p>Una serie de 1 a 8 caracteres:</p> <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul> <p><b>Nota:</b> Un identificador de red de una red existente, a la que este nodo de red direccionador vaya a pertenecer, con los caracteres especiales @, \$ y # del juego de caracteres A también está soportado; no obstante, estos caracteres no deben utilizarse para nuevos ID de red.</p>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre de la red APPN a la que pertenece este nodo de red. El ID de red debe ser el mismo para todos los nodos de red en la red APPN. Los nodos finales LEN y APPN conectados pueden tener ID de red diferentes.
<b>Parámetro</b>	Control point name (necesario)
<b>Valores válidos</b>	<p>Una serie de 1 a 8 caracteres:</p> <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul> <p><b>Nota:</b> Un nombre de CP existente que este nodo vaya a obtener con los caracteres especiales @, \$ y # del juego de caracteres A también está soportado; no obstante, estos caracteres no deben utilizarse para nuevos nombres de CP.</p>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre del CP de este nodo de red APPN. El CP tiene la responsabilidad de gestionar el nodo de red APPN y sus recursos. El nombre de CP es el nombre lógico del nodo de red APPN en la red. El nombre de CP debe ser exclusivo en la red APPN identificada por el parámetro Network ID.
<b>Parámetro</b>	Enable branch extender or border node
<b>Valores válidos</b>	<p>0 (enable neither)</p> <p>1 (enable branch extender)</p> <p>2 (enable border node)</p>
<b>Valor por omisión</b>	0
<b>Descripción</b>	Este parámetro especifica si en este nodo se habilitará la función de extensor de rama, la función de nodo de frontera o ninguna de las dos. Si se habilita una de estas funciones, aparecerán las preguntas adicionales correspondientes.

Tabla 6 (Página 3 de 7). Lista de parámetros de configuración - Direccionamiento de APPN	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Enable Branch Awareness Support
<b>Valores válidos</b>	0 (Full), 1 (Partial), 2 (None)
<b>Valor por omisión</b>	0 (Full)
<b>Descripción</b>	<p>Este parámetro especifica si el usuario desea limitar el flujo de información topológica referente a la topología de Branch Extender.</p> <p><i>Full</i> significa que el nodo difundirá todos los TG de Branch Extender a la red cuando se aprendan.</p> <p><i>Partial</i> significa que el nodo no difundirá la topología de Branch Extender local, pero almacenará y difundirá la topología de Branch Extender no local.</p> <p><i>None</i> significa que el nodo no difundirá la topología de Branch Extender local, que ignorará cualquier topología de Branch Extender recibida de la red y que no almacenará ni difundirá la topología de Branch Extender no local.</p>
<b>Parámetro</b>	Permit search for unregistered LUs
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	<p>Este parámetro especifica si se pueden buscar LU en este nodo (cuando actúe como Nodo final) aunque las LU no se hayan registrado con el servidor de nodos de red del Branch Extender. Si se especifica <i>yes</i>, pueden buscarse LU en este nodo.</p> <p><b>Nota:</b> Esta pregunta sólo aparece si el parámetro <b>Enable Branch Extender or Border Node</b> se ha establecido en <i>branch extender</i>.</p>
<b>Parámetro</b>	Subnet visit count
<b>Valores válidos</b>	1 — 255
<b>Valor por omisión</b>	3
<b>Descripción</b>	<p>Especifica el valor por omisión de nivel de nodo para el número máximo de subredes que una sesión de diversas subredes puede atravesar. El valor por omisión puede alterarse temporalmente en la parte de la configuración de puertos, enlaces o listas de direccionamiento.</p> <p><b>Nota:</b> Ésta es la primera de las preguntas que sólo aparecen si se ha habilitado el nodo de frontera.</p>
<b>Parámetro</b>	Cache searches for (0-255) minutes
<b>Valores válidos</b>	0 - 255
<b>Valor por omisión</b>	8
<b>Descripción</b>	<p>Especifica los minutos durante los cuales el BN retendrá información en la antememoria de búsquedas en diversas subredes una vez terminada la búsqueda.</p>

<p>Tabla 6 (Página 4 de 7). Lista de parámetros de configuración - Direccionamiento de APPN</p>	
<p><b>Información de parámetros</b></p>	
<p><b>Parámetro</b> Maximum number of searches in cache</p> <p><b>Valores válidos</b> 0 - 32765 (0=unlimited)</p> <p><b>Valor por omisión</b> 0</p> <p><b>Descripción</b> Especifica el número máximo de entradas de la antememoria de búsquedas en diversas redes. Una vez alcanzado este límite, se desechan las entradas de mayor antigüedad.</p> <p><b>Nota:</b> El mecanismo primario para la supresión de estas entradas es el valor de tiempo de la antememoria de búsquedas especificado en <b>cache searches for (0–255) minutes</b>.</p>	
<p><b>Parámetro</b> Dynamic routing list updates</p> <p><b>Valores válidos</b> 0 (none) - No se añaden entradas dinámicas.</p> <p>1 (full) - Se añaden todos los nodos de frontera nativos, todos los nodos de frontera y de red no nativos adyacentes y nodos que tienen conocimiento de LU de destino de nombre similar.</p> <p>2 (limited) - Se añaden todos los nodos de frontera nativos, todos los nodos de frontera y de red no nativos adyacentes <b>con el mismo NETID</b> y nodos que tienen conocimiento de LU de destino de nombre similar.</p> <p><b>Valor por omisión</b> 2</p> <p><b>Descripción</b> Indica hasta qué grado, si lo hay, un BN puede complementar los datos de una lista de direccionamiento configurada con datos de topología aprendidos por el código operativo. Estos datos adicionales no se guardan en la SRAM.</p>	
<p><b>Parámetro</b> Enable routing list optimization</p> <p><b>Valores válidos</b> Yes o No</p> <p><b>Valor por omisión</b> Yes</p> <p><b>Descripción</b> Indica si un BN puede reordenar o no la copia temporal del código operativo de una lista de direccionamiento de subredes de manera que las entradas con más probabilidades de obtener un resultado satisfactorio se encuentren en primer lugar.</p>	

Tabla 6 (Página 5 de 7). Lista de parámetros de configuración - Direccionamiento de APPN

Información de parámetros	
<b>Parámetro</b>	Load balance across parallel inter-subnet boundaries
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	<p>Este parámetro especifica si el direccionador debe intentar equilibrar el número de sesiones a través de dos o más puntos de salida intersubredes paralelo cuando funciona como EBN. La configuración relevante tiene dos o más direccionadores de IBM que sirven de puntos de salida EBN en una subred y el mismo número en la otra subred. Cada direccionador tiene un TG intersubredes con un direccionador diferente de la otra subred, con lo cual se forman dos o más enlaces paralelo. (Tenga en cuenta que éstos no son TG paralelo entre dos direccionadores.)</p> <p>Para configurar el equilibrio de carga de sesiones entre los puntos de salida paralelo:</p> <ol style="list-style-type: none"> <li>1. Establezca este parámetro en <i>yes</i>.</li> <li>2. Configure listas de direccionamiento (vea la página 213) en cada direccionador EBN de manera que las sesiones para los diferentes nombres de LU de destino tengan diferentes EBN de salida preferentes. También configurará la frontera intersubredes preferente y puede establecer vías de acceso de reserva.</li> <li>3. Configure las listas de direccionamiento con <b>dynamic routing list updates</b> establecido en <i>none</i> y <b>Enable routing list optimization</b> establecido en <i>no</i>.</li> </ol> <p><b>Nota:</b> Ésta es la última de las preguntas que sólo aparecen si se ha habilitado el nodo de frontera.</p>
<b>Parámetro</b>	Route addition resistance
<b>Valores válidos</b>	Del 0 al 255
<b>Valor por omisión</b>	128
<b>Descripción</b>	Este parámetro indica la conveniencia del direccionamiento a través de este nodo. Este parámetro se utiliza en el cálculo de ruta basado en clase de servicio. Los valores menores indican niveles mayores de conveniencia.

<i>Tabla 6 (Página 6 de 7). Lista de parámetros de configuración - Direccionamiento de APPN</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	XID number for subarea connection (vea las notas de la tabla)
<b>Valores válidos</b>	Una serie de 5 dígitos hexadecimales
<b>Valor por omisión</b>	X'00000'
<b>Descripción</b>	<p>Este parámetro especifica un número de ID (identificador) exclusivo para el nodo de red. El número de XID se combina con un número de bloque de ID (que identifica a un producto específico) para formar una identificación de nodo XID. Se intercambian identificaciones de nodo entre nodos adyacentes cuando los nodos van a establecer una conexión. El nodo de red direccionador añade automáticamente un número de bloque de ID a este parámetro durante el intercambio de XID para crear una identificación de nodo XID.</p> <p>El número de ID que asigne a este nodo debe ser exclusivo en la red APPN identificada por el parámetro Network ID. Póngase en contacto con el administrador de la red para verificar si el número de ID es exclusivo.</p>
<b>Nota:</b>	<p>Normalmente, se intercambian identificaciones de nodo entre nodos T2.1 durante el establecimiento de una sesión de CP-CP. Si el nodo de red va a comunicarse con el producto IBM Virtual Telecommunications Access Method (VTAM) mediante un nodo LEN T2.1 y el nodo LEN tiene definido un nombre de CP para éste, no es necesario el parámetro de número de XID. Si el nodo LEN adyacente no es un nodo T2.1 o no tiene definido explícitamente un nombre de CP, debe especificarse el parámetro de número de XID para establecer una conexión con el nodo LEN. Las versiones de VTAM anteriores a la Versión 3 Release 2 no permiten la definición de nombres de CP para los nodos LEN.</p>
<b>Parámetro</b>	Use enhanced BATCH COS
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	<p>Este parámetro especifica si se utilizarán las tablas de COS mejoradas. Las tablas mejoradas asignan pesos razonables a TG ATM basándose en el coste, la velocidad y el retardo. Para ATM, el orden de preferencia es:</p> <ul style="list-style-type: none"> <li>• SVC o PVC Campus Mayor Eficacia/PVC Reservado (WAN o Campus)</li> <li>• SVC Campus Reservado</li> <li>• SVC o PVC WAN Mayor Eficacia</li> <li>• SVC WAN Reservado</li> </ul>



Tabla 6 (Página 7 de 7). Lista de parámetros de configuración - Direccionamiento de APPN

Información de parámetros	
<b>Parámetro</b>	Use enhanced BATCHSC COS
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	<p>Este parámetro especifica si se utilizarán las tablas de COS mejoradas. Las tablas mejoradas asignan pesos razonables a TG ATM basándose en el coste, la velocidad y el retardo. Para ATM, el orden de preferencia es:</p> <ul style="list-style-type: none"> <li>• SVC o PVC Campus Mayor Eficacia/PVC Reservado (WAN o Campus)</li> <li>• SVC Campus Reservado</li> <li>• SVC o PVC WAN Mayor Eficacia</li> <li>• SVC WAN Reservado</li> </ul>
<b>Parámetro</b>	Use enhanced INTER COS
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	<p>Este parámetro especifica si se utilizarán las tablas de COS mejoradas. Las tablas mejoradas asignan pesos razonables a TG ATM basándose en el coste, la velocidad y el retardo. Para ATM, el orden de preferencia es:</p> <ul style="list-style-type: none"> <li>• SVC o PVC Campus Reservado</li> <li>• SVC o PVC Campus Mayor Eficacia/PVC WAN reservado</li> <li>• SVC WAN Reservado</li> <li>• SVC o PVC WAN Mayor Eficacia</li> </ul>
<b>Parámetro</b>	Use enhanced INTERSC COS
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	<p>Este parámetro especifica si se utilizarán las tablas de COS mejoradas. Las tablas mejoradas asignan pesos razonables a TG ATM basándose en el coste, la velocidad y el retardo. Para ATM, el orden de preferencia es:</p> <ul style="list-style-type: none"> <li>• SVC o PVC Campus Reservado</li> <li>• SVC o PVC Campus Mayor Eficacia/PVC WAN reservado</li> <li>• SVC WAN Reservado</li> <li>• SVC o PVC WAN Mayor Eficacia</li> </ul>

**Sintaxis:**

set high-performance routing

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

## Mandatos de configuración de APPN

<i>Tabla 7. Lista de parámetros de configuración - Direccionamiento de alto rendimiento (HPR)</i>	
<b>Información del parámetro</b>	
<b>Parámetro</b>	Maximum sessions for HPR connections
<b>Valores válidos</b>	Del 1 al 65535
<b>Valor por omisión</b>	100
<b>Descripción</b>	<p>Este parámetro especifica el número máximo de sesiones permitidas en una conexión de HPR. Una conexión de HPR se define mediante la clase de servicio (COS), la vía de acceso física (TG) y los puntos finales de conexión de red.</p> <p>Este parámetro sólo es aplicable cuando el direccionador es el iniciador de la BIND. Si el número de sesiones sobrepasa el valor especificado para este parámetro, el HPR asignará otra conexión de HPR (RTP).</p>

<i>Tabla 8 (Página 1 de 3). Lista de parámetros de configuración - Opciones de temporizadores y reintentos de HPR</i>	
<b>Información de parámetros</b>	
<i>Tráfico de prioridad de transmisión de tipo bajo</i>	
<b>Parámetro</b>	RTP inactivity timer
<b>Valores válidos</b>	De 1 a 3600 segundos
<b>Valor por omisión</b>	180 segundos
<b>Descripción</b>	<p>Este parámetro especifica el intervalo de inactividad de RTP para conexiones de HPR que transportan tráfico con una prioridad de transmisión <i>baja</i>. Ésta es una versión de final a final del temporizador de inactividad de LLC, Ti. Si no se producen recepciones durante este intervalo, RTP transmite un sondeo. Los períodos de inactividad se supervisan para asegurar la integridad de la conexión.</p>
<b>Parámetro</b>	Maximum RTP retries
<b>Valores válidos</b>	Del 0 al 10
<b>Valor por omisión</b>	6
<b>Descripción</b>	<p>Este parámetro especifica el número máximo de reintentos antes de que RTP inicie una conmutación de la vía de acceso en una conexión de HPR que transporta tráfico con una prioridad de transmisión baja.</p>
<b>Parámetro</b>	Path switch timer
<b>Valores válidos</b>	De 0 a 7200 segundos
<b>Valor por omisión</b>	180 segundos
<b>Descripción</b>	<p>Este parámetro especifica el período de tiempo máximo durante el cual puede intentarse una conmutación de la vía de acceso en una conexión de HPR que transporta tráfico con una prioridad de transmisión baja. Un valor de cero indica que debe inhabilitarse la función de conmutación de la vía de acceso y que no se realizará una conmutación de la vía de acceso.</p>
<i>Tráfico de prioridad de transmisión de tipo medio</i>	

<i>Tabla 8 (Página 2 de 3). Lista de parámetros de configuración - Opciones de temporizadores y reintentos de HPR</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	RTP inactivity timer
<b>Valores válidos</b>	De 1 a 3600 segundos
<b>Valor por omisión</b>	180 segundos
<b>Descripción</b>	Este parámetro especifica el intervalo de inactividad de RTP para conexiones de HPR que transportan tráfico con una prioridad de transmisión <i>media</i> . Ésta es una versión de final a final del temporizador de inactividad de LLC, Ti. Si no se producen recepciones durante este intervalo, RTP transmite un sondeo. Los períodos de inactividad se supervisan para asegurar la integridad de la conexión.
<b>Parámetro</b>	Maximum RTP retries
<b>Valores válidos</b>	Del 0 al 10
<b>Valor por omisión</b>	6
<b>Descripción</b>	Este parámetro especifica el número máximo de reintentos antes de que RTP inicie una conmutación de la vía de acceso en una conexión de HPR que transporta tráfico con una prioridad de transmisión media.
<b>Parámetro</b>	Path switch timer
<b>Valores válidos</b>	De 0 a 7200 segundos
<b>Valor por omisión</b>	180 segundos
<b>Descripción</b>	Este parámetro especifica el período de tiempo máximo durante el cual puede intentarse una conmutación de la vía de acceso en una conexión de HPR que transporta tráfico con una prioridad de transmisión media. Un valor de cero indica que debe inhabilitarse la función de conmutación de la vía de acceso y que no se realizará una conmutación de la vía de acceso.
<i>Tráfico de prioridad de transmisión de tipo alto</i>	
<b>Parámetro</b>	RTP inactivity timer
<b>Valores válidos</b>	De 1 a 3600 segundos
<b>Valor por omisión</b>	180 segundos
<b>Descripción</b>	Este parámetro especifica el intervalo de inactividad de RTP para conexiones de HPR que transportan tráfico con una prioridad de transmisión <i>alta</i> . Ésta es una versión de final a final del temporizador de inactividad de LLC, Ti. Si no se producen recepciones durante este intervalo, RTP transmite un sondeo. Los períodos de inactividad se supervisan para asegurar la integridad de la conexión.
<b>Parámetro</b>	Maximum RTP retries
<b>Valores válidos</b>	Del 0 al 10
<b>Valor por omisión</b>	6
<b>Descripción</b>	Este parámetro especifica el número máximo de reintentos antes de que RTP inicie una conmutación de la vía de acceso en una conexión de HPR que transporta tráfico con una prioridad de transmisión alta.

<i>Tabla 8 (Página 3 de 3). Lista de parámetros de configuración - Opciones de temporizadores y reintentos de HPR</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Path switch timer
<b>Valores válidos</b>	De 0 a 7200 segundos
<b>Valor por omisión</b>	180 segundos
<b>Descripción</b>	Este parámetro especifica el período de tiempo máximo durante el cual puede intentarse una conmutación de la vía de acceso en una conexión de HPR que transporta tráfico con una prioridad de transmisión alta. Un valor de cero indica que debe inhabilitarse la función de conmutación de la vía de acceso y que no se realizará una conmutación de la vía de acceso.
<i>Tráfico de prioridad de transmisión de red</i>	
<b>Parámetro</b>	RTP inactivity timer
<b>Valores válidos</b>	De 1 a 3600 segundos
<b>Valor por omisión</b>	180 segundos
<b>Descripción</b>	Este parámetro especifica el intervalo de inactividad de RTP para conexiones de HPR que transportan tráfico con una prioridad de transmisión <i>de red</i> . Ésta es una versión de final a final del temporizador de inactividad de LLC, Ti. Si no se producen recepciones durante este intervalo, RTP transmite un sondeo. Los períodos de inactividad se supervisan para asegurar la integridad de la conexión.
<b>Parámetro</b>	Maximum RTP retries
<b>Valores válidos</b>	Del 0 al 10
<b>Valor por omisión</b>	6
<b>Descripción</b>	Este parámetro especifica el número máximo de reintentos antes de que RTP inicie una conmutación de la vía de acceso en una conexión de HPR que transporta tráfico con una prioridad de transmisión de red.
<b>Parámetro</b>	Path switch timer
<b>Valores válidos</b>	De 0 a 7200 segundos
<b>Valor por omisión</b>	180 segundos
<b>Descripción</b>	Este parámetro especifica el período de tiempo máximo durante el cual puede intentarse una conmutación de la vía de acceso en una conexión de HPR que transporta tráfico con una prioridad de transmisión de red. Un valor de cero indica que debe inhabilitarse la función de conmutación de la vía de acceso y que no se realizará una conmutación de la vía de acceso.

### Sintaxis:

set

dlur

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

Tabla 9 (Página 1 de 4). Lista de parámetros de configuración - Peticionario de LU dependientes	
Información de parámetros	
<b>Parámetro</b>	Enable dependent LU requester (DLUR) on this network node
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si va a habilitarse funcionalmente un peticionario de LU dependientes en este nodo.
<b>Parámetro</b>	Default fully-qualified CP name of primary DLUS (necesario cuando se habilita DLUR)
<b>Valores válidos</b>	Una serie de un máximo de 17 caracteres con el formato de <i>IDred.nombCP</i> , donde: <ul style="list-style-type: none"> <li>• <i>IDred</i> es un ID de red de 1 a 8 caracteres</li> <li>• <i>nombCP</i> es un nombre de CP de 1 a 8 caracteres</li> </ul> Cada nombre debe ajustarse a las normas siguientes: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul> <b>Nota:</b> Un nombre de CP calificado al completo existente con los caracteres especiales @, \$ y # del juego de caracteres A también está soportado; no obstante, estos caracteres no deben utilizarse para nuevos nombres de CP.
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre de punto de control (CP) calificado al completo del servidor de LU dependientes (DLUS) que se utilice por omisión. Puede alterarse temporalmente el servidor primario por omisión según la estación de enlace. Se utiliza el servidor por omisión para peticiones de entrada de PU de sentido directo cuando no se ha especificado un DLUS primario para la estación de enlace asociada.
<b>Parámetro</b>	Default fully-qualified CP name of backup dependent LU server (DLUS)
<b>Valores válidos</b>	Una serie de un máximo de 17 caracteres con el formato de <i>IDred.nombCP</i> , donde: <ul style="list-style-type: none"> <li>• <i>IDred</i> es un ID de red de 1 a 8 caracteres</li> <li>• <i>nombCP</i> es un nombre de CP de 1 a 8 caracteres</li> </ul> Cada nombre debe ajustarse a las normas siguientes: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul> <b>Nota:</b> Un nombre de CP calificado al completo existente con los caracteres especiales @, \$ y # del juego de caracteres A también está soportado; no obstante, estos caracteres no deben utilizarse para nuevos nombres de CP.
<b>Valor por omisión</b>	Valor nulo
<b>Descripción</b>	Este parámetro especifica el nombre de CP calificado al completo del servidor de LU dependientes (DLUS) que se utilice como reserva por omisión. No es necesario un servidor de reserva, y el valor nulo (para representar que no hay entrada) indica la ausencia de un servidor de reserva por omisión. Puede alterarse temporalmente el servidor de reserva por omisión según la estación de enlace.

<p>Tabla 9 (Página 2 de 4). Lista de parámetros de configuración - Peticionario de LU dependientes</p>	
<p><b>Información de parámetros</b></p>	
<p><b>Parámetro</b> Perform retries to restore disrupted pipe</p> <p><b>Valores válidos</b> Yes, No</p> <p><b>Valor por omisión</b> No</p> <p><b>Descripción</b> Este parámetro especifica si un DLUR intentará restablecer el conducto con un DLUS después de una anomalía del conducto. Si un DLUR recibe un mensaje de fin de no interrupción UNBIND y este parámetro es No, el DLUR espera indefinidamente a que un DLUS restablezca el conducto interrumpido. Si el conducto falla por cualquier otra razón distinta y este parámetro es No, el DLUR intenta acceder al DLUS primario una vez. Si esta acción no se realiza satisfactoriamente, el DLUR intenta acceder al DLUS de reserva. Si este intento también falla, el DLUR espera indefinidamente a que un DLUS restablezca el conducto.</p> <p>Consulte la sección "Algoritmo de reintentos de DLUR" en la página 43 para obtener una descripción del algoritmo de reintentos.</p>	
<p><b>Parámetro</b> Delay before initiating retries</p> <p><b>Valores válidos</b> De 0 a 2756000 segundos</p> <p><b>Valor por omisión</b> 120 segundos</p> <p><b>Descripción</b> Este parámetro especifica un período de tiempo para dos casos diferentes cuando se interrumpe el conducto entre el DLUR y su DLUS.</p> <ul style="list-style-type: none"> <li>• En el caso de recibir un mensaje de fin de no interrupción UNBIND: <p style="margin-left: 40px;">Este parámetro especifica el período de tiempo durante el cual el DLUR debe esperar antes de intentar acceder al DLUS primario.</p> <p style="margin-left: 40px;">Un valor de 0 indica un reintento inmediato por parte del DLUR.</p> </li> <li>• En todos los otros casos de anomalía de conducto: <p style="margin-left: 40px;">El DLUR realizará de manera inmediata un intento con el DLUS primario y luego con el DLUS de reserva. Si falla, el DLUR esperará el período de tiempo especificado por el valor mínimo existente en <i>short retry timer</i> y este parámetro antes de intentar acceder al DLUS primario.</p> </li> </ul> <p>Consulte la sección "Algoritmo de reintentos de DLUR" en la página 43 para obtener una descripción completa del algoritmo de reintentos.</p>	
<p><b>Parámetro</b> Perform short retries to restore disrupted pipe</p> <p><b>Valores válidos</b> Yes, No</p> <p><b>Valor por omisión</b> Si <i>Perform retries to restore disrupted pipes</i> es Yes, el valor por omisión es Yes. De lo contrario, el valor por omisión es No.</p> <p><b>Descripción</b> Consulte la sección "Algoritmo de reintentos de DLUR" en la página 43 para obtener una descripción completa del algoritmo de reintentos.</p>	

Tabla 9 (Página 3 de 4). Lista de parámetros de configuración - Peticionario de LU dependientes	
Información de parámetros	
<b>Parámetro</b>	Short retry timer
<b>Valores válidos</b>	De 0 a 2756000 segundos
<b>Valor por omisión</b>	120 segundos
<b>Descripción</b>	<p>En todos los casos en que la anomalía del conducto sea distinta del mensaje de fin de no interrupción UNBIND, el valor mínimo existente en <i>Delay before initiating retries</i> y este parámetro especifica el período de tiempo durante el cual el DLUR esperará antes de intentar acceder al DLUS primario después de que haya fallado un intento de establecer esta conexión.</p> <p>Consulte la sección “Algoritmo de reintentos de DLUR” en la página 43 para obtener una descripción completa del algoritmo de reintentos.</p>
<b>Parámetro</b>	Short retry count
<b>Valores válidos</b>	Del 0 al 65535
<b>Valor por omisión</b>	5
<b>Descripción</b>	<p>En todos los casos en que la anomalía del conducto sea distinta del mensaje de fin de no interrupción UNBIND, este parámetro especifica el número de veces que el DLUR realizará reintentos cortos para acceder al DLUS después de que haya fallado un intento de establecer esta conexión.</p> <p>Consulte la sección “Algoritmo de reintentos de DLUR” en la página 43 para obtener una descripción completa del algoritmo de reintentos.</p>
<b>Parámetro</b>	Perform long retries to restore disrupted pipe
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	Si <i>Perform retries to restore disrupted pipes</i> es Yes, el valor por omisión es Yes. De lo contrario, el valor por omisión es No.
<b>Descripción</b>	Consulte la sección “Algoritmo de reintentos de DLUR” en la página 43 para obtener una descripción completa del algoritmo de reintentos.
<b>Parámetro</b>	Long retry timer
<b>Valores válidos</b>	De 0 a 2756000 segundos
<b>Valor por omisión</b>	300 segundos
<b>Descripción</b>	<p>Este parámetro especifica el tiempo que el DLUR esperará cuando realice reintentos largos.</p> <p>Consulte la sección “Algoritmo de reintentos de DLUR” en la página 43 para obtener una descripción completa del algoritmo de reintentos.</p>

## Mandatos de configuración de APPN

Tabla 9 (Página 4 de 4). Lista de parámetros de configuración - Peticionario de LU dependientes

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

### Sintaxis:

set                      tuning

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

**Nota:** Tendrá que reentrar para que tengan lugar los cambios que especifique.

Tabla 10 (Página 1 de 6). Lista de parámetros de configuración - Ajuste de nodo APPN

Información de parámetros	
<b>Parámetro</b>	Maximum number of adjacent nodes
<b>Valores válidos</b>	Del 1 al 8000
<b>Valor por omisión</b>	100
<b>Descripción</b>	<p>Este parámetro es una estimación del número máximo de nodos que espera que sean adyacentes lógicamente respecto a este nodo de red direccionador en cualquier momento.</p> <p>El algoritmo de ajuste automático utiliza este parámetro junto con el parámetro <i>Número máximo de sesiones de ISR</i> (Maximum number of ISR sessions) para calcular los valores de los parámetros de ajuste <i>Máximo de memoria compartida</i> (Maximum shared memory) y <i>Número máximo de entradas de directorio en antememoria</i> (Maximum cached directory entries).</p> <p>Este parámetro sólo puede configurarse con el Programa de configuración.</p>



Tabla 10 (Página 2 de 6). Lista de parámetros de configuración - Ajuste de nodo APPN	
Información de parámetros	
<b>Parámetro</b>	Maximum number of network nodes sharing the same APPN network id
<b>Valores válidos</b>	Del 10 al 8000
<b>Valor por omisión</b>	50
<b>Descripción</b>	Este parámetro es una estimación del número máximo de nodos que espera en la subred (es decir, en la topología que este nodo conoce).  Este parámetro sólo puede configurarse con el Programa de configuración.
<b>Parámetro</b>	Maximum number of TGs connecting network nodes with the same APPN network id
<b>Valores válidos</b>	Del 9 al 64000
<b>Valor por omisión</b>	3 veces el valor de <i>número máximo de nodos de red en la subred</i> (maximum number of network nodes in the subnetwork).
<b>Descripción</b>	Este parámetro es una estimación del número máximo de TG para conectar nodos de red de la subred (es decir, de la topología que conoce este nodo).  Este parámetro sólo puede configurarse con el Programa de configuración.
<b>Parámetro</b>	Maximum number of ISR sessions
<b>Valores válidos</b>	Del 10 al 60000
<b>Valor por omisión</b>	200
<b>Descripción</b>	Este parámetro especifica una estimación del número máximo de sesiones de direccionamiento de sesiones intermedias (ISR) a las que se espera que dé soporte este nodo de red direccionador en cualquier momento.  El algoritmo de ajuste automático utiliza este parámetro junto con el parámetro Maximum number of adjacent nodes para calcular los valores de los parámetros de ajuste Maximum shared memory y Maximum cached directory entries.  Este parámetro sólo puede configurarse con el Programa de configuración.
<b>Parámetro</b>	Percent of adjacent nodes with CP-CP sessions using HPR
<b>Valores válidos</b>	De un 0 a un 100%
<b>Valor por omisión</b>	0 (ninguno)
<b>Descripción</b>	Este parámetro especifica una estimación del número máximo de EN y NN con sesiones de CP-CP en que se utilice el conjunto de opciones 1402 (Control de los flujos sobre el conjunto de opciones RTP).  Este parámetro sólo puede configurarse con el Programa de configuración.

## Mandatos de configuración de APPN

<i>Tabla 10 (Página 3 de 6). Lista de parámetros de configuración - Ajuste de nodo APPN</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Maximum percent of ISR sessions using HPR data connections
<b>Valores válidos</b>	Porcentaje de 0 a 100
<b>Valor por omisión</b>	Porcentaje de 0
<b>Descripción</b>	Este parámetro especifica el porcentaje mayor de sesiones de ISR que utilicen correlaciones de ISR con HPR.  Este parámetro sólo puede configurarse con el Programa de configuración.
<b>Parámetro</b>	Percent adjacent nodes that function as DLUR PU nodes
<b>Valores válidos</b>	Porcentaje de 0 a 100
<b>Valor por omisión</b>	Porcentaje de 0
<b>Descripción</b>	Este parámetro especifica el porcentaje mayor de nodos adyacentes a los que se permite funcionar como nodos de PU DLUR adyacentes.  Este parámetro sólo puede configurarse con el Programa de configuración.
<b>Parámetro</b>	Maximum percent ISR sessions used by DLUR LUs
<b>Valores válidos</b>	Porcentaje de 0 a 100
<b>Valor por omisión</b>	Porcentaje de 0
<b>Descripción</b>	Este parámetro especifica el porcentaje mayor de sesiones de ISR utilizadas por LU de DLUR.  Este parámetro sólo puede configurarse con el Programa de configuración.
<b>Parámetro</b>	Maximum number of ISR accounting memory buffers
<b>Valores válidos</b>	0 ó 1
<b>Valor por omisión</b>	0 (el valor por omisión es 1 si se habilita la contabilidad de sesiones de ISR)
<b>Descripción</b>	Este parámetro especifica el número máximo de almacenamientos intermedios a reservar para la contabilidad de sesiones de ISR.  Este parámetro sólo puede configurarse con el Programa de configuración.
<b>Parámetro</b>	Maximum memory records per ISR accounting buffer
<b>Valores válidos</b>	Del 0 al 2000
<b>Valor por omisión</b>	100
<b>Descripción</b>	Este parámetro especifica el número máximo de registros de memoria por almacenamiento intermedio de contabilidad de ISR.  Este parámetro sólo puede configurarse con el Programa de configuración.

Tabla 10 (Página 4 de 6). Lista de parámetros de configuración - Ajuste de nodo APPN

Información de parámetros	
<b>Parámetro</b>	Override tuning algorithm
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	<p>Cuando se habilita, este parámetro altera temporalmente los cálculos de ajuste generados por los parámetros de entrada de ajuste y le permite especificar valores explícitos para el parámetro Maximum shared memory, el parámetro relativo al porcentaje de memoria de los almacenamientos intermedios y el parámetro Maximum cached directory entries.</p> <p>Este parámetro sólo puede configurarse con el Programa de configuración.</p>
<b>Parámetro</b>	Number of local-pus for TN3270E support
<b>Valores válidos</b>	
<b>Valor por omisión</b>	
<b>Descripción</b>	<p>Este parámetro especifica el número de PU locales que estén disponibles para el soporte de TN3270.</p> <p>Este parámetro sólo puede configurarse con el Programa de configuración.</p>
<b>Parámetro</b>	Total number of LUs for TN3270E
<b>Valores válidos</b>	
<b>Valor por omisión</b>	
<b>Descripción</b>	<p>Este parámetro especifica el número total de LU disponibles para el soporte de TN3270E.</p> <p>Este parámetro sólo puede configurarse con el Programa de configuración.</p>

Tabla 10 (Página 5 de 6). Lista de parámetros de configuración - Ajuste de nodo APPN	
Información de parámetros	
<p><b>Parámetro</b> Maximum shared memory</p> <p><b>Valores válidos</b> 0 - 16777215 KB</p> <p><b>Valor por omisión</b> Auto-configured (configuración basada en la memoria instalada)</p> <p><b>Descripción</b> Este parámetro especifica la cantidad de memoria compartida del direccionador que se asigna al nodo de red APPN. APPN utiliza esta asignación de memoria compartida para realizar operaciones de red y para mantener las tablas y los directorios necesarios.</p> <p>Puede entrar un valor en Kilobytes o seleccionar que el direccionador elija un valor por omisión de fines generales razonable en el momento del arranque basándose en la memoria instalada. Tenga en cuenta que el valor por omisión que el direccionador elige no está basado en el tamaño de la configuración de APPN. Los valores por omisión suponen que se va a ejecutar una red APPN o TN3270 de medianas proporciones y alguna otra función de direccionamiento importante. Es posible que el valor por omisión no sea el adecuado si además se configura otra función de direccionador con un uso muy intensivo de la memoria.</p> <p>Cuando seleccione el valor de <i>autoconfigurado</i> (auto-configured) en el indicador de línea de mandatos, podrá ver qué será si arranca la configuración en el direccionador que utilice. Si selecciona este valor en el Programa de configuración, debe bajar y activar la configuración para poder ver el resultado.</p> <p>Este parámetro puede configurarse con el Programa de configuración y desde la línea de mandatos.</p>	
<p><b>Parámetro</b> Percent of APPN shared memory to be used for buffers</p> <p><b>Valores válidos</b> Del 5 al 50</p> <p><b>Valor por omisión</b> Un 11% ó 512 Kilobytes, el valor que sea mayor.</p> <p><b>Descripción</b> Este parámetro especifica la cantidad de memoria compartida que APPN utilizará para los almacenamientos intermedios.</p> <p>Puede permitir que APPN tenga un tamaño de RU de 4 KB estableciendo el <i>máximo de memoria compartida</i> (maximum shared memory) en 1 MB como mínimo y estableciendo el <i>porcentaje de memoria compartida de APPN a utilizar para los almacenamientos intermedios</i> (percent of APPN shared memory used for buffers) en un valor lo suficientemente grande como para permitir que esté disponible un mínimo de 1 MB de memoria para el gestor de almacenamientos intermedios.</p> <p>Este parámetro puede configurarse con el Programa de configuración y desde la línea de mandatos.</p>	

Tabla 10 (Página 6 de 6). Lista de parámetros de configuración - Ajuste de nodo APPN

Información de parámetros	
<b>Parámetro</b>	Maximum cached directory entries
<b>Valores válidos</b>	Del 0 al 65535
<b>Valor por omisión</b>	4000
<b>Descripción</b>	<p>Este parámetro especifica el número de entradas de directorio que el nodo de red direccionador almacenará o colocará en antememoria. Si se coloca en antememoria una entrada de directorio para un nodo, el direccionador no tiene que difundir una petición de búsqueda para localizar el nodo. Reduce el tiempo que tarda el inicio de sesiones con el nodo.</p> <p>Este parámetro puede configurarse con el Programa de configuración y desde la línea de mandatos.</p>

**Sintaxis:**

set                      traces

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

Tabla 11 (Página 1 de 2). Lista de parámetros de configuración - Opciones de configuración de rastreo

Información de parámetros	
<b>Parámetro</b>	Turn all trace flags off
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita los distintivos de rastreo.
<b>Parámetro</b>	Edit Node-Level Traces
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Consulte la Tabla 12 en la página 140 para saber el conjunto de preguntas que aparecerán si se habilita esta opción.
<b>Parámetro</b>	Edit Interprocess Signals
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Consulte la Tabla 13 en la página 144 para saber el conjunto de preguntas que aparecerán si se habilita esta opción.

## Mandatos de configuración de APPN

*Tabla 11 (Página 2 de 2). Lista de parámetros de configuración - Opciones de configuración de rastreo*

<b>Información de parámetros</b>	
<b>Parámetro</b>	Edit Module Entry and Exit
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Consulte la Tabla 14 en la página 147 para saber el conjunto de preguntas que aparecerán si se habilita esta opción.
<b>Parámetro</b>	Edit General
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Consulte la Tabla 15 en la página 149 para saber el conjunto de preguntas que aparecerán si se habilita esta opción.

*Tabla 12 (Página 1 de 4). Lista de parámetros de configuración - Rastros de nivel de nodo*

<b>Información de parámetros</b>	
<b>Parámetro</b>	Process management
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos sobre la gestión de procesos del nodo de red APPN, lo que incluye la creación y terminación de procesos, procesos que entran en un estado de espera y el envío de procesos.
<b>Parámetro</b>	Process to process communication
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos sobre mensajes intercambiados entre procesos del nodo de red APPN, lo que incluye la puesta en cola y la recepción de estos mensajes.
<b>Parámetro</b>	Locking
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos sobre bloqueos que se han obtenido y liberado en procesos del nodo de red APPN.

Tabla 12 (Página 2 de 4). Lista de parámetros de configuración - Rastros de nivel de nodo

Información de parámetros	
<b>Parámetro</b>	Miscellaneous tower activities
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos sobre actividades varias del nodo de red APPN.
<b>Parámetro</b>	I/O to and from the system
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos sobre el flujo de mensajes que entran en el nodo de red APPN y salen del mismo.
<b>Parámetro</b>	Storage management
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos sobre toda memoria compartida que el nodo de red APPN ha obtenido y liberado.
<b>Parámetro</b>	Queue data type management
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos sobre todas las llamadas del nodo de red APPN que gestionan colas con fines generales.
<b>Parámetro</b>	Table data type management
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos sobre todas las llamadas del nodo de red APPN que gestionan tablas con fines generales, lo que incluye llamadas para añadir entradas de tabla y llamadas para consultar entradas específicas en tablas.

## Mandatos de configuración de APPN

<i>Tabla 12 (Página 3 de 4). Lista de parámetros de configuración - Rastros de nivel de nodo</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Buffer management
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos sobre almacenamientos intermedios del nodo de red APPN que se han obtenido y liberado.
<b>Parámetro</b>	Configuration control
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos sobre las actividades del componente de control de la configuración del nodo de red APPN. El componente de control de la configuración gestiona la información sobre los recursos del nodo.
<b>Parámetro</b>	Timer service
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos sobre peticiones de servicio de temporizador del nodo de red APPN.
<b>Parámetro</b>	Service provider management
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos sobre la definición y habilitación o inhabilitación de servicios del nodo de red APPN.
<b>Parámetro</b>	Inter-process message segmenting
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos sobre la transferencia de los almacenamientos intermedios y la liberación de mensajes encadenados del nodo de red APPN.



Tabla 12 (Página 4 de 4). Lista de parámetros de configuración - Rastros de nivel de nodo

Información de parámetros	
<b>Parámetro</b>	Control of processes outside scope of this tower
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos sobre la definición y activación de procesos externos a este nodo de red APPN, como, por ejemplo, cuando el recurso de operador del nodo (NOF) define el control de la configuración de los procesos externos.
<b>Parámetro</b>	Monitoring existence of processes, services, towers
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos sobre las peticiones que inician o detienen la supervisión de procesos o servicios del nodo de red APPN.
<b>Parámetro</b>	Distributed environment control
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos sobre las peticiones del nodo de red APPN que definen subsistemas y crean entornos.
<b>Parámetro</b>	Process to service dialogs
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos sobre todas las llamadas del nodo de red APPN que abren diálogos, los cierran o envían datos de los mismos.
<b>Parámetro</b>	AVL Tree Support
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos sobre todas las llamadas que gestionan árboles AVL.

## Mandatos de configuración de APPN

<i>Tabla 13 (Página 1 de 4). Lista de parámetros de configuración - Rastros de señales interprocesos</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Address space manager
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre señales interprocesos del componente gestor de espacios de direcciones.
<b>Parámetro</b>	Attach manager
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre señales interprocesos del componente gestor de conexiones.
<b>Parámetro</b>	Configuration services
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre señales interprocesos del componente servicios de configuración.
<b>Parámetro</b>	Dependent LU requester
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre señales interprocesos del componente peticionario de LU dependiente.
<b>Parámetro</b>	Directory services
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre señales interprocesos del componente servicios de directorio.

Tabla 13 (Página 2 de 4). Lista de parámetros de configuración - Rastreo de señales interprocesos

Información de parámetros	
<b>Parámetro</b>	Half Session
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre señales interprocesos del componente media sesión.
<b>Parámetro</b>	HPR Path Control
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre señales interprocesos del componente control de la vía de acceso de HPR.
<b>Parámetro</b>	LUA RUI
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre señales interprocesos del componente LUA RUI.
<b>Parámetro</b>	Management Services
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre señales interprocesos del componente servicios de gestión.
<b>Parámetro</b>	Node Operator Facility
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre señales interprocesos del componente recurso de operador del nodo.

## Mandatos de configuración de APPN

<i>Tabla 13 (Página 3 de 4). Lista de parámetros de configuración - Rastreo de señales interprocesos</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Path Control
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre señales interprocesos del componente control de la vía de acceso.
<b>Parámetro</b>	Presentation Services
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre señales interprocesos del componente servicios de presentación.
<b>Parámetro</b>	Resource manager
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre señales interprocesos del componente gestor de recursos.
<b>Parámetro</b>	Session connector manager
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre señales interprocesos del componente gestor de conectores de sesión.
<b>Parámetro</b>	Session connector
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre señales interprocesos del componente conector de sesión.

<i>Tabla 13 (Página 4 de 4). Lista de parámetros de configuración - Rastros de señales interprocesos</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Session manager
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre señales interprocesos del componente gestor de sesiones.
<b>Parámetro</b>	Session services
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre señales interprocesos del componente servicios de sesión.
<b>Parámetro</b>	Topology and routing services
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre señales interprocesos del componente servicios de topología y direccionamiento.

<i>Tabla 14 (Página 1 de 3). Lista de parámetros de configuración - Rastros de entrada y salida de módulos</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Attach manager
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información de entrada y salida de módulos del componente gestor de conexiones.
<b>Parámetro</b>	Half session
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información de entrada y salida de módulos del componente media sesión.

## Mandatos de configuración de APPN

<i>Tabla 14 (Página 2 de 3). Lista de parámetros de configuración - Rastros de entrada y salida de módulos</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	LUA RUI
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información de entrada y salida de módulos del componente LUA RUI.
<b>Parámetro</b>	Node operator facility
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información de entrada y salida de módulos del componente recurso de operador del nodo.
<b>Parámetro</b>	Presentation services
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información de entrada y salida de módulos del componente servicios de presentación.
<b>Parámetro</b>	Rapid transport protocol
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información de entrada y salida de módulos del componente control del transporte rápido.
<b>Parámetro</b>	Resource manager
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información de entrada y salida de módulos del componente gestor de recursos.

Tabla 14 (Página 3 de 3). Lista de parámetros de configuración - Rastros de entrada y salida de módulos

Información de parámetros	
<b>Parámetro</b>	Session manager
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información de entrada y salida de módulos del componente gestor de sesiones.

Tabla 15 (Página 1 de 4). Lista de parámetros de configuración - Rastros generales de nivel de componente

Información de parámetros	
<b>Parámetro</b>	Accounting services
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información general del componente servicios de contabilidad.
<b>Parámetro</b>	Address space manager
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información general del componente gestor de espacios de direcciones.
<b>Parámetro</b>	Architected transaction programs
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información general del componente programas de transacción estructurados.
<b>Parámetro</b>	Configuration services
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información general del componente servicios de configuración.

## Mandatos de configuración de APPN

<i>Tabla 15 (Página 2 de 4). Lista de parámetros de configuración - Rastros generales de nivel de componente</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Dependent LU requester
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información general del componente peticionario de LU dependiente.
<b>Parámetro</b>	Directory services
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información general del componente servicios de directorio.
<b>Parámetro</b>	HPR path control
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información general del componente control de la vía de acceso de HPR.
<b>Parámetro</b>	LUA RUI
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información general del componente LUA RUI.
<b>Parámetro</b>	Management services
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información general del componente servicios de gestión.



Tabla 15 (Página 3 de 4). Lista de parámetros de configuración - Rastros generales de nivel de componente

Información de parámetros	
<b>Parámetro</b>	Node operator facility
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información general del componente recurso de operador del nodo.
<b>Parámetro</b>	Path control
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información general del componente control de la vía de acceso.
<b>Parámetro</b>	Problem determination services
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información general del componente determinación de problemas.
<b>Parámetro</b>	Rapid transport protocol
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información general del componente control del transporte rápido.
<b>Parámetro</b>	Session connector manager
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información general del componente gestor de conectores de sesión.

## Mandatos de configuración de APPN

<i>Tabla 15 (Página 4 de 4). Lista de parámetros de configuración - Rastros generales de nivel de componente</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Session connector
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información general del componente conector de sesión.
<b>Parámetro</b>	Session services
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información general del componente servicios de sesión.
<b>Parámetro</b>	SNMP subagent
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información general del componente subagente de SNMP.
<b>Parámetro</b>	TN3270E Server
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información general del componente Servidor TN3270E.
<b>Parámetro</b>	Topology and routing services
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo sobre información general del componente servicios de topología y direccionamiento.

Tabla 16 (Página 1 de 2). Lista de parámetros de configuración - Rastreo varios	
Información de parámetros	
<b>Parámetro</b>	Data link control transmissions and receptions
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Si se habilita este parámetro, el recurso de rastreo de APPN rastreará todas las XID y las PIU que transmita y reciba el nodo APPN.
<b>Parámetro</b>	Trace RTP Headers
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Si se habilita este parámetro, el recurso de rastreo de APPN rastreará todas las cabeceras de los flujos de RTP. Esta opción sólo está disponible si <b>Data link control transmissions and receptions</b> es yes.
<b>Parámetro</b>	Include payload in RTP trace
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Si se habilita este parámetro, el recurso de rastreo de APPN rastreará los datos de carga útil de los flujos de RTP. Esta opción sólo está disponible si <b>trace RTP headers</b> es yes.
<b>Parámetro</b>	Filter the Data
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Si se habilita este parámetro, el recurso de rastreo de APPN filtrará datos de rastreo según cómo el usuario responda a las siguientes preguntas.
<b>Parámetro</b>	Truncate the data
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Si se habilita este parámetro, el recurso de rastreo de APPN truncará los datos de rastreo. Se le solicitará que especifique la <i>longitud a rastrear</i> (length to trace)
<b>Parámetro</b>	Length to trace
<b>Valores válidos</b>	1 - 3600
<b>Valor por omisión</b>	100
<b>Descripción</b>	Este parámetro especifica el número de bytes de datos de rastreo a acumular.
<b>Parámetro</b>	Trace Locates
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Si se habilita este parámetro, el recurso de rastreo de APPN rastreará peticiones Locate.

## Mandatos de configuración de APPN

<i>Tabla 16 (Página 2 de 2). Lista de parámetros de configuración - Rastreo varios</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Trace TDUs
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Si se habilita este parámetro, el recurso de rastreo de APPN rastreará actualizaciones de datos de topología.
<b>Parámetro</b>	Trace route setups
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Si se habilita este parámetro, el recurso de rastreo de APPN rastreará configuraciones de ruta.
<b>Parámetro</b>	Trace CP Capabilities
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Si se habilita este parámetro, el recurso de rastreo de APPN rastreará posibilidades de CP.
<b>Parámetro</b>	Trace Session Control
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Si se habilita este parámetro, el recurso de rastreo de APPN rastreará tráfico de control de sesión.
<b>Parámetro</b>	Trace XIDs
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Si se habilita este parámetro, el recurso de rastreo de APPN rastreará XID.

### Sintaxis:

set                      management

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

Tabla 17 (Página 1 de 2). Lista de parámetros de configuración - Gestión de nodo APPN	
Información de parámetros	
<b>Parámetro</b>	Collect intermediate session information
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si el nodo APPN debe reunir datos de las sesiones intermedias que pasan por este nodo (características y contadores de sesiones). Los datos se capturan en las variables de la MIB de SNMP para APPN.
<b>Parámetro</b>	Save RSCV information for intermediate sessions
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si el nodo APPN debe guardar el vector de control de selección de ruta (RSCV) para una sesión intermedia. Los datos se capturan en una variable de MIB de SNMP para APPN asociada.  El RSCV de una sesión está contenido en la petición BIND utilizada para activar una sesión entre dos LU. Describe la ruta óptima por una red APPN para una sesión de LU-LU determinada. El RSCV de una sesión contiene los nombres de CP y los TG asociados con cada par de nodos adyacentes a lo largo de una ruta de un nodo de origen a un nodo de destino.
<b>Parámetro</b>	Create intermediate session records
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita la creación de registros de datos relativos a las sesiones intermedias que pasan por este nodo. Los registros contienen información sobre características y contadores de sesiones. También se incluye información de RSCV en los registros de datos si se habilita el parámetro Save RSCV information for intermediate sessions.  Si este parámetro se establece en yes, se altera temporalmente el valor de <i>collect intermediate session information</i> .
<b>Parámetro</b>	Record creation threshold
<b>Valores válidos</b>	Del 0 al 4 294 967, en incrementos de 1 KB
<b>Valor por omisión</b>	0
<b>Descripción</b>	Este parámetro especifica un umbral de bytes para la creación de registros de las sesiones intermedias. Cuando datos de las sesiones sobrepasan el valor de este contador de bytes en un múltiplo par, se crea un registro.

## Mandatos de configuración de APPN

<i>Tabla 17 (Página 2 de 2). Lista de parámetros de configuración - Gestión de nodo APPN</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Held alert queue size
<b>Valores válidos</b>	0 — 255
<b>Valor por omisión</b>	10
<b>Descripción</b>	Este parámetro establece el tamaño de la cola de alertas retenidas configurable. Esta cola se utiliza para guardar alertas de APPN antes de enviarlas a un punto focal. Si se desborda la cola, se desechan las alertas de mayor antigüedad.

<i>Tabla 18 (Página 1 de 2). Lista de parámetros de configuración - Soporte para el registro del ISR de APPN</i>	
<b>Información de parámetros</b>	
<i>Parámetros de memoria</i>	
<b>Parámetro</b>	Memory (vea las notas de la tabla)
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro habilita o inhabilita la reunión de datos de las sesiones intermedias en la memoria local del direccionador.
<b>Parámetro</b>	Maximum memory buffers
<b>Valores válidos</b>	Del 0 al 1
<b>Valor por omisión</b>	1
<b>Descripción</b>	Este parámetro especifica el número de almacenamientos intermedios a asignar en la memoria local del direccionador para almacenar registros de las sesiones intermedias.
<b>Parámetro</b>	Maximum memory records per buffer
<b>Valores válidos</b>	Del 0 al 2000
<b>Valor por omisión</b>	100
<b>Descripción</b>	Este parámetro especifica el número máximo de registros de las sesiones intermedias que pueden almacenarse en el almacenamiento intermedio de la memoria del direccionador.
<b>Parámetro</b>	Memory buffers full
<b>Valores válidos</b>	Stop recording (0), Wrap (1)
<b>Valor por omisión</b>	Stop recording (0)
<b>Descripción</b>	Este parámetro especifica la acción a emprender cuando se llena el almacenamiento intermedio de la memoria asignado para almacenar registros de las sesiones intermedias. Seleccione <b>Stop recording</b> para indicar al direccionador que deseche cualquier nuevo registro de sesión intermedia. Seleccione <b>Wrap</b> para permitir que los nuevos registros se graben encima de registros existentes del almacenamiento intermedio. Se sobregaban primero los registros de mayor antigüedad del almacenamiento intermedio.

Tabla 18 (Página 2 de 2). Lista de parámetros de configuración - Soporte para el registro del ISR de APPN

Información de parámetros	
<b>Parámetro</b>	Memory record format
<b>Valores válidos</b>	ASCII (0), Binary (1)
<b>Valor por omisión</b>	ASCII (0)
<b>Descripción</b>	Este parámetro especifica el formato con el que van a almacenarse los registros de las sesiones intermedias en la memoria local del direccionador.
<b>Parámetro</b>	Topology safe store
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si la base de datos de topología va a guardarse en el disco fijo.
<b>Parámetro</b>	Time between database updates
<b>Valores válidos</b>	60 — 1440 minutos
<b>Valor por omisión</b>	60
<b>Descripción</b>	Este parámetro establece el tiempo en minutos entre las actualizaciones de la base de datos de topología.
<b>Nota:</b>	
<ul style="list-style-type: none"> <li>• Cuando habilita la reunión de registros de las sesiones intermedias, los datos asociados con los registros también se reúnen, por omisión, en SNMP.</li> <li>• Variables de la MIB para APPN. Las variables de la MIB se actualizan, en este caso, tanto si se ha habilitado el parámetro Collect intermediate session information (en la Tabla 17 en la página 155) como si no.</li> <li>• Los datos de las sesiones intermedias pueden almacenarse en la memoria del direccionador.</li> </ul>	

## Add

Utilice el mandato **add** para añadir o actualizar:

### Sintaxis:

add                      port

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

## Mandatos de configuración de APPN

<i>Tabla 19 (Página 1 de 4). Lista de parámetros de configuración - Configuración de puerto</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Link type
<b>Valores válidos</b>	Ethernet (E) Token ring (T) ATM (A) DLSw (D) PPP (P) Frame relay (F) SDLC (S) X.25 (X) MPC+ (M) FDDI IP
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el tipo de enlace asociado con este puerto.
<b>Parámetro</b>	Interface number
<b>Valores válidos</b>	Del 0 al 65533
<b>Valor por omisión</b>	0
<b>Descripción</b>	Este parámetro define el número de interfaz física de la interfaz de hardware a la que está conectado este dispositivo.
<b>Parámetro</b>	Port name
<b>Valores válidos</b>	Una serie de 1 a 8 caracteres, donde el primero es alfabético y los caracteres 2 a 8 son alfanuméricos.
<b>Valor por omisión</b>	Un nombre sin calificar exclusivo que se genera automáticamente.  El nombre estará compuesto por: <ul style="list-style-type: none"> <li>• TR (token-ring, que es la Red en Anillo)</li> <li>• EN (Ethernet)</li> <li>• DLS (DLSw)</li> <li>• IP255</li> <li>• ATM</li> <li>• FR (Frame Relay)</li> <li>• X25 (X.25)</li> <li>• SDLC (SDLC)</li> <li>• PPP (point-to-point, que significa punto a punto)</li> <li>• MPC</li> <li>• FDD (FDDI)</li> <li>• IP</li> </ul> y, a continuación, el número de interfaz.
<b>Descripción</b>	Puede cambiar el nombre del puerto por un nombre de su elección. Este parámetro especifica el nombre que representa a este puerto.
<b>Parámetro</b>	Enable APPN routing on this port
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	Este parámetro especifica si se va a habilitar el direccionamiento de APPN en este puerto.



Tabla 19 (Página 2 de 4). Lista de parámetros de configuración - Configuración de puerto	
Información de parámetros	
<b>Parámetro</b>	Support multiple PU
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si el puerto dará soporte a la multiplicidad de las subáreas.
<b>Parámetro</b>	Service any node
<b>Valores válidos</b>	Yes No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	<p>Este parámetro especifica cómo responde el nodo de red direccionador a una petición de otro nodo para establecer una conexión sobre este puerto. Cuando se habilita este parámetro, el nodo de red acepta cualquier petición que reciba de otro nodo para establecer una conexión. Cuando se inhabilita este parámetro, el nodo de red sólo acepta peticiones de conexión de los nodos que el usuario defina explícitamente (mediante definiciones de estación de enlace). Esta opción proporciona un nivel de seguridad añadido para el nodo de red direccionador.</p> <p><b>Nota:</b> Cuando inhabilite este parámetro, sólo se aceptará una petición de conexión de un nodo adyacente si se ha configurado el parámetro de nombre de CP calificado al completo del nodo para una estación de enlace definida en este puerto.</p> <p>Cuando se habilita este parámetro (el valor por omisión), es posible que desee que este nodo de red pueda iniciar conexiones con nodos específicos sobre este puerto.</p>
<b>Parámetro</b>	Treat non-configured callers as LEN nodes
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	<p>Este parámetro especifica si APPN debe tratar como nodos LEN a los llamantes de nodo de red dinámicos que no solicitan sesiones de CP-CP. Sólo es aplicable si <b>service any node</b> es yes.</p> <p>Si este parámetro es yes:</p> <ul style="list-style-type: none"> <li>• el direccionador trata de nodo LEN al nodo adyacente sin tener en cuenta el tipo de nodo de la XID3 recibida</li> <li>• el direccionador envía XID3 que indican que el direccionador es un nodo LEN (un EN sin sesiones de CP-CP ni soporte del HPR)</li> </ul>
<b>Parámetro</b>	High-performance routing (HPR) supported
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	Yes para puertos Red en Anillo, Ethernet, Frame Relay, FDDI y PPP.
<b>Descripción</b>	Este parámetro indica si las estaciones de enlace de este puerto darán soporte al HPR. Este valor puede alterarse temporalmente en la definición de estación de enlace.

## Mandatos de configuración de APPN

Tabla 19 (Página 3 de 4). Lista de parámetros de configuración - Configuración de puerto	
<b>Información de parámetros</b>	
<b>Parámetro</b>	IPv4 Precedence
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro establece el valor de prioridad de IPv4, que permite la filtración de paquetes encapsulados de IPv4 con prioridad de BRS.
<b>Parámetro</b>	Limited Resource (sólo PPP y FR sobre circuitos de marcación)
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	Si el circuito de marcación es de <i>marcación bajo pedido</i> , el valor por omisión es Yes. De lo contrario, el valor por omisión es No.
<b>Descripción</b>	Este parámetro especifica si las estaciones de enlace de este puerto son un recurso limitado. Este valor puede alterarse temporalmente en la definición de estación de enlace.
<b>Parámetro</b>	Support bridged formatted frames (sólo Frame relay)
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si el puerto Frame Relay dará soporte a tramas de formato de puente.  Si desea configurar Frame Relay de manera que dé soporte al formato de puente, también tendrá que configurar un identificador de nodo de frontera.
<b>Parámetro</b>	Boundary node identifier (sólo Frame Relay)
<b>Valores válidos</b>	Del X'0000 0000 0001' al X'7FFF FFFF FFFF'
<b>Valor por omisión</b>	X'4FFF 0000 0000'
<b>Descripción</b>	Este parámetro especifica la dirección MAC del identificador de nodo de frontera. El direccionador utiliza esta dirección MAC para reconocer que la trama es una trama de puente de Frame Relay destinada a APPN.
<b>Parámetro</b>	Subnet visit count
<b>Valores válidos</b>	1 - 255
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro de nivel de nodo equivalente
<b>Descripción</b>	Este parámetro especifica el valor por omisión de este puerto para el número máximo de subredes que una sesión de diversas subredes puede atravesar.  <b>Nota:</b> Esta pregunta sólo aparece si se ha habilitado la función de nodo de frontera en este nodo.

<i>Tabla 19 (Página 4 de 4). Lista de parámetros de configuración - Configuración de puerto</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Adjacent node subnet affiliation
<b>Valores válidos</b>	<ul style="list-style-type: none"> <li>• 0 (native)</li> <li>• 1 (non-native)</li> <li>• 2 (negotiable)</li> </ul>
<b>Valor por omisión</b>	2
<b>Descripción</b>	Este parámetro especifica el valor por omisión para todos los enlaces a través de este puerto respecto a si el nodo adyacente está en la subred APPN nativa de este nodo o en una subred APPN no nativa. Un valor de 2 indica al nodo que negocie durante la activación del enlace para determinar si la estación de enlace adyacente es nativa o no nativa.
	<b>Nota:</b> Esta pregunta sólo aparece si se ha habilitado la función de nodo de frontera en este nodo.

<i>Tabla 20 (Página 1 de 5). Lista de parámetros de configuración - Configuración de puerto para ATM</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Local ATM Address
<b>Valores válidos</b>	Cualquier serie de 14 caracteres hexadecimales
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica la serie de 7 bytes que comprende la parte del usuario de la dirección ATM local. La parte del usuario es el ESI de 6 bytes y el campo de selector de 1 byte. Esta parte del usuario debe ser exclusiva con respecto a la parte de red de la dirección ATM, que se recupera del adaptador de ATM. El selector debe ser exclusivo para cada tipo de protocolo.
<b>Parámetro</b>	Enable incoming calls
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	Este parámetro determina si se rechazarán llamadas en el nivel de ATM.
<b>Parámetro</b>	ATM Network Type
<b>Valores válidos</b>	Campus o Widearea
<b>Valor por omisión</b>	Campus
<b>Descripción</b>	Este parámetro especifica el tipo de red utilizado para los valores por omisión de las redes de conexiones y otras estaciones de enlace definidas en este puerto.

## Mandatos de configuración de APPN

<i>Tabla 20 (Página 2 de 5). Lista de parámetros de configuración - Configuración de puerto para ATM</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Shareable connection network traffic
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si puede direccionarse tráfico de red de conexiones en el VC ATM configurado para una estación de enlace de este puerto.
<b>Parámetro</b>	Shareable other protocol traffic
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si puede direccionarse tráfico de otros protocolos de nivel superior en el VC ATM configurado para una estación de enlace de este puerto.
<b>Parámetro</b>	Broadband Bearer Class
<b>Valores válidos</b>	Class_A, Class_C, Class_X
<b>Valor por omisión</b>	Class_X
<b>Descripción</b>	Este parámetro especifica la clase portadora solicitada de la red ATM. Las clases se definen:  <b>Class A</b> Velocidad en bits constante (CBR) con requisitos de temporización de final a final  <b>Class C</b> Velocidad en bits variable (VBR) sin requisitos de temporización de final a final  <b>Class X</b> Servicio que permite unos requisitos de temporización y tipo de tráfico definidos por el usuario
<b>Parámetro</b>	Best Effort Indicator
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro indica si es necesaria una garantía de productividad en este SVC. Si el valor de este parámetro es <i>yes</i> , se asignarán las VCC asociadas con esta interfaz sobre la base del ancho de banda disponible.
<b>Nota:</b> Los parámetros siguientes son parámetros del tráfico hacia adelante.	
<b>Parámetro</b>	Forward Traffic Peak Cell Rate
<b>Valores válidos</b>	De un 1 a un 85% de la velocidad de línea
<b>Valor por omisión</b>	Capacidad efectiva por omisión del puerto/48
<b>Descripción</b>	Este parámetro indica un límite superior para la velocidad de transmisión de las células.

<i>Tabla 20 (Página 3 de 5). Lista de parámetros de configuración - Configuración de puerto para ATM</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Forward Traffic Sustained Cell Rate
<b>Valores válidos</b>	De un 1 a un 85% de la velocidad de línea
<b>Valor por omisión</b>	Capacidad efectiva por omisión del puerto/48
<b>Descripción</b>	Este parámetro indica un límite superior para la velocidad media de transmisión de las células. No puede especificar este parámetro si desea utilizar una conexión Mayor Eficacia.
<b>Parámetro</b>	Forward Traffic Tagging
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	Este parámetro indica que las células que no se ajustan a la especificación de tráfico de prioridad de pérdida de célula 0 pero se ajustan a la especificación de tráfico de prioridad de pérdida de célula 1 se marcan y se permiten en la red ATM. No puede especificar este parámetro si desea utilizar una conexión Mayor Eficacia.
<b>Parámetro</b>	Forward QoS
<b>Valores válidos</b>	CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, donde
	<b>CLASS_0</b> La clase sin especificar. La red no especifica ninguna QoS.
	<b>CLASS_1</b> El rendimiento es comparable al de una línea privada digital actual.
	<b>CLASS_2</b> Pensada para los paquetes de vídeo y audio de aplicaciones de teleconferencia y multimedia.
	<b>CLASS_3</b> Pensada para la interoperación de los protocolos orientados a las conexiones, como, por ejemplo, Frame Relay.
	<b>CLASS_4</b> Pensada para la interoperación de los protocolos sin conexiones, como, por ejemplo, IP.
<b>Valor por omisión</b>	CLASS_0
<b>Descripción</b>	Este parámetro indica qué clase de servicio se proporciona a una conexión virtual ATM. Este parámetro siempre es CLASS_0 para una conexión Mayor Eficacia.
<b>Nota:</b> Los parámetros siguientes son parámetros del tráfico hacia atrás.	
<b>Parámetro</b>	Backward Traffic Peak Cell Rate
<b>Valores válidos</b>	De un 1 a un 85% de la velocidad de línea
<b>Valor por omisión</b>	Capacidad efectiva por omisión del puerto/48
<b>Descripción</b>	Este parámetro indica un límite superior para la velocidad de transmisión de las células.

<i>Tabla 20 (Página 4 de 5). Lista de parámetros de configuración - Configuración de puerto para ATM</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Backward Traffic Sustained Cell Rate
<b>Valores válidos</b>	De un 1 a un 85% de la velocidad de línea
<b>Valor por omisión</b>	Capacidad efectiva por omisión del puerto/48
<b>Descripción</b>	Este parámetro indica un límite superior para la velocidad media de transmisión de las células. No puede especificar este parámetro para una conexión Mayor Eficacia.
<b>Parámetro</b>	Backward Traffic Tagging
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	Yes, a menos que se trate de una conexión Mayor Eficacia
<b>Descripción</b>	Este parámetro indica que las células que no se ajustan a la especificación de tráfico de prioridad de pérdida de célula 0 pero se ajustan a la especificación de tráfico de prioridad de pérdida de célula 1 se marcan y se permiten en la red ATM. No puede especificar este parámetro para una conexión Mayor Eficacia.
<b>Parámetro</b>	Backward QoS
<b>Valores válidos</b>	CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, donde
	<b>CLASS_0</b> La clase sin especificar. La red no especifica ninguna QoS.
	<b>CLASS_1</b> El rendimiento es comparable al de una línea privada digital actual.
	<b>CLASS_2</b> Pensada para los paquetes de vídeo y audio de aplicaciones de teleconferencia y multimedia.
	<b>CLASS_3</b> Pensada para la interoperación de los protocolos orientados a las conexiones, como, por ejemplo, Frame Relay.
	<b>CLASS_4</b> Pensada para la interoperación de los protocolos sin conexiones, como, por ejemplo, IP.
<b>Valor por omisión</b>	CLASS_0
<b>Descripción</b>	Este parámetro indica qué clase de servicio se proporciona a una conexión virtual ATM. No puede especificar este parámetro para una conexión Mayor Eficacia.
<b>Parámetro</b>	Callout Anonymously
<b>Valores válidos</b>	Yes, no
<b>Valor por omisión</b>	no
<b>Descripción</b>	Este parámetro indica si APPN pasará la dirección de origen al efectuar la llamada.

Tabla 20 (Página 5 de 5). Lista de parámetros de configuración - Configuración de puerto para ATM

Información de parámetros	
<b>Parámetro</b>	LDLC retry count
<b>Valores válidos</b>	1 — 255
<b>Valor por omisión</b>	3
<b>Descripción</b>	Este parámetro se utiliza junto con el período del temporizador de LDLC para proporcionar una entrega de XID fiable. La cuenta de reintentos se inicializa la primera vez que se transmite un mandato o una petición sobre el enlace. Si el período del temporizador de LDLC caduca antes de que se reciba una respuesta, se retransmite el mandato o respuesta, disminuye la cuenta de reintentos y se reinicia el período del temporizador de LDLC. Si el temporizador caduca con la cuenta de reintentos de 0, se supone que el enlace no es operativo.
<b>Parámetro</b>	LDLC Timer Period
<b>Valores válidos</b>	1 — 255 segundos
<b>Valor por omisión</b>	Para ATM: 1 segundo Para IP: 15 segundos
<b>Descripción</b>	Este parámetro especifica el período del temporizador que se utiliza con <b>LDLC retry count</b> .

Tabla 21 (Página 1 de 4). Lista de parámetros de configuración - Definición de puerto	
Información de parámetros	
<b>Parámetro</b>	Maximum BTU size
<b>Valores válidos</b>	De 768 a 1496 bytes para Ethernet De 768 a 17745 bytes para Red en Anillo De 768 a 17745 bytes para FDDI De 768 a 4096 bytes para ATM De 768 a 4096 bytes para IP De 768 a 8136 bytes para Frame Relay De 768 a 8132 bytes para Frame Relay sobre RDSI y V.25bis De 768 a 4086 bytes para PPP De 768 a 4082 bytes para PPP sobre RDSI y V.25bis X.25 tomará el valor del nivel de red De 768 a 32768 bytes para MPC+ De 768 a 2048 bytes para todos los otros puertos
<b>Valor por omisión</b>	1289 bytes para Ethernet 2048 bytes para Red en Anillo 2048 bytes para FDDI 2048 para ATM 1469 bytes para IP 2048 bytes para Frame Relay o PPP 2044 bytes para Frame Relay o PPP sobre RDSI y V.25bis 2048 bytes para SDLC X.25 tomará el valor del nivel de red 2048 bytes para MPC+
<b>Descripción</b>	Este parámetro especifica el número de bytes de la unidad básica de transmisión (BTU) mayor que puede procesar (transmitir o recibir) una estación de enlace definida en este puerto.  <b>Nota:</b> Si se recibe una BIND negociable con un tamaño de RU superior a 2048, el dispositivo elegirá un tamaño máximo de RU de 2048 normalmente. Si se recibe una BIND no negociable con un tamaño de RU superior a 2048, el dispositivo dará soporte al tamaño de RU mayor hasta un tamaño máximo de 4096.
<b>Parámetro</b>	MPC+ Sequencing Interval Timer
<b>Valores válidos</b>	1 — 300 (décimas de segundo)
<b>Valor por omisión</b>	0
<b>Descripción</b>	Este parámetro especifica el temporizador utilizado al definir la interfaz MPC+.
<b>Parámetro</b>	Maximum number of link stations
<b>Valores válidos</b>	Del 1 al 127 para puertos SDLC  Del 1 al 65535 para los otros puertos
<b>Valor por omisión</b>	
<b>Descripción</b>	Si se configura SDLC como multipunto y primario, este parámetro toma por omisión el valor de 127. Este parámetro especifica el número máximo de estaciones de enlace que podrán utilizar este puerto. Este parámetro permite limitar los recursos para el nodo APPN y este puerto.



<i>Tabla 21 (Página 2 de 4). Lista de parámetros de configuración - Definición de puerto</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Percent of link stations reserved for incoming calls (sólo Ethernet, Red en Anillo, FR, X.25)
<b>Valores válidos</b>	Del 0 al 100
	La suma del porcentaje de estaciones de enlace reservadas para llamadas de entrada con el porcentaje de estaciones de enlace reservadas para llamadas de salida no puede sobrepasar el 100%.
<b>Valor por omisión</b>	0
<b>Descripción</b>	Este parámetro especifica el porcentaje del número máximo de estaciones de enlace que se reservarán para llamadas de entrada. Las estaciones de enlace que no se reservan para llamadas de entrada ni de salida están disponibles para cualquier fin a petición.
<b>Parámetro</b>	Percent of link stations reserved for outgoing calls
<b>Valores válidos</b>	Del 0 al 100
	La suma del porcentaje de estaciones de enlace reservadas para llamadas de entrada con el porcentaje de estaciones de enlace reservadas para llamadas de salida no puede sobrepasar el 100%. Si SDLC es primario y multipunto, el valor válido es 100.
<b>Valor por omisión</b>	0 Si SDLC es primario y multipunto, el valor por omisión es 100.
<b>Descripción</b>	Este parámetro especifica el porcentaje del número máximo de estaciones de enlace que se reservarán para llamadas de salida. Las fracciones resultantes del cálculo se truncan. Las estaciones de enlace que no se reservan para llamadas de entrada ni de salida están disponibles para cualquier fin a petición.
<b>Parámetro</b>	UDP port number for XID exchange
<b>Valores válidos</b>	Del 1024 al 65535
<b>Valor por omisión</b>	11000
<b>Descripción</b>	Este parámetro especifica el número de puerto UDP a utilizar para el intercambio de XID y se utiliza durante la definición de un puerto IP. Este número de puerto debe ser el mismo que el definido en los otros dispositivos de la red.
<b>Parámetro</b>	UDP port number for network priority traffic
<b>Valores válidos</b>	Del 1024 al 65535
<b>Valor por omisión</b>	11001
<b>Descripción</b>	Este parámetro especifica el número de puerto UDP a utilizar para el tráfico de prioridad de red.
<b>Parámetro</b>	UDP port number for high priority traffic
<b>Valores válidos</b>	Del 1024 al 65535
<b>Valor por omisión</b>	11002
<b>Descripción</b>	Este parámetro especifica el número de puerto UDP a utilizar para el tráfico de prioridad alta.

## Mandatos de configuración de APPN

<i>Tabla 21 (Página 3 de 4). Lista de parámetros de configuración - Definición de puerto</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	UDP port number for medium priority traffic
<b>Valores válidos</b>	Del 1024 al 65535
<b>Valor por omisión</b>	11003
<b>Descripción</b>	Este parámetro especifica el número de puerto UDP a utilizar para el tráfico de prioridad media.
<b>Parámetro</b>	UDP port number for low priority traffic
<b>Valores válidos</b>	Del 1024 al 65535
<b>Valor por omisión</b>	11004
<b>Descripción</b>	Este parámetro especifica el número de puerto UDP a utilizar para el tráfico de prioridad baja.
<b>Parámetro</b>	IP network type
<b>Valores válidos</b>	Campus o Widearea
<b>Valor por omisión</b>	Widearea
<b>Descripción</b>	Este parámetro especifica el tipo de red IP.
<b>Parámetro</b>	Local APPN SAP address
<b>Valores válidos</b>	Múltiplos de cuatro en el rango hexadecimal del X'04' al X'EC'
<b>Valor por omisión</b>	X'04'
<b>Descripción</b>	Este parámetro especifica la dirección de SAP local a utilizar para la comunicación con las estaciones de enlace APPN definidas en este puerto.
<b>Parámetro</b>	Local HPR SAP address (sólo Ethernet y Red en Anillo)
<b>Valores válidos</b>	Múltiplos de cuatro en el rango hexadecimal del X'04' al X'EC'
<b>Valor por omisión</b>	X'C8'
<b>Descripción</b>	Este parámetro indica el punto de acceso a servicios local a utilizar para la comunicación con las estaciones de enlace de HPR definidas en este puerto.

Tabla 21 (Página 4 de 4). Lista de parámetros de configuración - Definición de puerto

Información de parámetros	
<b>Parámetro</b>	Branch uplink
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	<p>Este parámetro indica si el valor por omisión para las estaciones de enlace que utilicen este puerto será de enlace superior o inferior. Si se especifica <i>yes</i>, las estaciones de enlace que utilicen este puerto establecerán por omisión <b>Branch uplink</b> en <i>yes</i>.</p> <p><b>Notas:</b></p> <ol style="list-style-type: none"> <li>1. Esta pregunta sólo aparece si el parámetro de nivel de nodo <b>Enabled Branch Extender</b> es <i>yes</i>.</li> <li>2. Si <b>Branch uplink</b> es <i>yes</i>, el Branch Extender presentará un aspecto de nodo final ante esta estación de enlace. De lo contrario, el Branch Extender presentará un aspecto de nodo de red.</li> <li>3. Normalmente, <b>Branch uplink</b> es <i>yes</i> para los nodos de red conectados a una WAN y es <i>no</i> para los nodos finales conectados a una LAN.</li> </ol>

Tabla 22 (Página 1 de 6). Lista de parámetros de configuración - Características de TG de puerto por omisión	
Información de parámetros	
<b>Parámetro</b>	Cost per connect time
<b>Valores válidos</b>	Del 0 al 255
<b>Valor por omisión</b>	0
	Para los SVC ATM:
	<b>Campus ATM de mayor eficacia</b> 0
	<b>Campus ATM reservado</b> 64
	<b>WAN ATM de mayor eficacia</b> 0
	<b>WAN ATM reservada</b> 128
	Para los PVC ATM:
	<b>Campus ATM de mayor eficacia</b> 0
	<b>Campus ATM reservado</b> 0
	<b>WAN ATM de mayor eficacia</b> 0
	<b>WAN ATM reservada</b> 0
	Para IP: 0 para Campus y WAN
	Para los otros: 0
<b>Descripción</b>	Este parámetro especifica la característica de TG de coste por tiempo de conexión para todas las estaciones de enlace de este puerto.  La característica de TG de coste por tiempo de conexión expresa el coste relativo del mantenimiento de una conexión sobre el TG asociado. Las unidades están definidas por el usuario y, normalmente, se basan en las tarifas aplicables del recurso de transmisión que se utiliza. Los valores asignados deben reflejar el gasto real del mantenimiento de una conexión sobre el TG en relación con todos los otros TG de la red. Un valor de cero significa que las conexiones sobre el TG pueden realizarse sin coste adicional (como es el caso de muchos recursos no conmutados). Los valores más elevados representan costes más elevados.

Tabla 22 (Página 2 de 6). Lista de parámetros de configuración - Características de TG de puerto por omisión

Información de parámetros	
<b>Parámetro</b>	Cost per byte
<b>Valores válidos</b>	Del 0 al 255
<b>Valor por omisión</b>	
	Para los SVC ATM y los PVC ATM:
	<b>Campus ATM de mayor eficacia</b> 0
	<b>Campus ATM reservado</b> 0
	<b>WAN ATM de mayor eficacia</b> 128
	<b>WAN ATM reservada</b> 0
	Para IP: 0 para Campus y WAN
	Para los otros: 0
<b>Descripción</b>	<p>Este parámetro especifica la característica de TG de coste por byte para todas las estaciones de enlace definidas en este puerto.</p> <p>La característica de TG de coste por byte expresa el coste relativo de la transmisión de un byte sobre el TG asociado. Las unidades están definidas por el usuario y el valor asignado debe reflejar los gastos reales en los que se incurra para la transmisión sobre el TG en relación con todos los otros TG de la red. Un valor de cero significa que los bytes pueden transmitirse sobre el TG sin coste adicional. Los valores más elevados representan costes más elevados.</p>

Tabla 22 (Página 3 de 6). Lista de parámetros de configuración - Características de TG de puerto por omisión

Información de parámetros	
<b>Parámetro</b>	Security
<b>Valores válidos</b>	<p><b>Nonsecure</b> todo lo demás (por ejemplo, conectado a satélite o ubicado en una zona no segura).</p> <p><b>Public switched network</b> seguridad en el sentido de que la ruta no está predeterminada</p> <p><b>Underground cable</b> ubicado en una zona segura (según lo que determina el administrador de la red)</p> <p><b>Secure conduit</b> no protegido (por ejemplo, un conducto presurizado)</p> <p><b>Guarded conduit</b> protegido contra infiltraciones físicas</p> <p><b>Encrypted</b> se proporciona cifrado de nivel de enlace</p> <p><b>Guarded radiation</b> conducto protegido que contiene el medio de transmisión; protegido contra infiltraciones físicas e infiltraciones de la radiación</p>
<b>Valor por omisión</b>	<p>Para los SVC ATM y los PVC ATM:</p> <p><b>Campus ATM de mayor eficacia</b> Nonsecure</p> <p><b>Campus ATM reservado</b> Nonsecure</p> <p><b>WAN ATM de mayor eficacia</b> Public switched network</p> <p><b>WAN ATM reservada</b> Public switched network</p> <p>Para IP:</p> <p><b>Campus</b> Nonsecure</p> <p><b>WAN</b> Public switched network</p>
<b>Descripción</b>	<p>Para los otros: Nonsecure</p> <p>Este parámetro especifica la característica de TG de seguridad para todas las estaciones de enlace definidas en este puerto. La característica de TG de seguridad indica el nivel de protección de seguridad asociado con el TG. Si son necesarios unos atributos de seguridad diferentes de los definidos estructuralmente, puede utilizarse una de las características de TG definidas por el usuario para especificar valores adicionales.</p>

Tabla 22 (Página 4 de 6). Lista de parámetros de configuración - Características de TG de puerto por omisión

<b>Información de parámetros</b>	
<b>Parámetro</b>	Propagation delay
<b>Valores válidos</b>	
	<p><b>Minimum LAN</b> menos de 480 microsegundos</p> <p><b>Telephone</b> entre 0,48 y 49,152 milisegundos</p> <p><b>Packet switched</b> entre 49,152 y 245,76 milisegundos</p> <p><b>Satellite</b> superior al máximo de 245,76 milisegundos</p>
<b>Valor por omisión</b>	
	<p>Para los SVC ATM y los PVC ATM:</p> <p><b>Campus ATM de mayor eficacia</b> Telephone</p> <p><b>Campus ATM reservado</b> Minimum LAN</p> <p><b>WAN ATM de mayor eficacia</b> Packet switched</p> <p><b>WAN ATM reservada</b> Telephone</p> <p>Para IP:</p> <p><b>Campus</b> Telephone</p> <p><b>WAN</b> Packet switched</p>
<b>Descripción</b>	<p>Este parámetro especifica la característica de TG de retardo de propagación para todas las estaciones de enlace definidas en este puerto. La característica de TG de retardo de propagación especifica el rango aproximado para el período de tiempo que tarda una señal en propagarse de un extremo a otro del TG.</p>

Tabla 22 (Página 5 de 6). Lista de parámetros de configuración - Características de TG de puerto por omisión	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Effective capacity
<b>Valores válidos</b>	2 dígitos hexadecimales en el rango del X'00' al X'FF'
<b>Valor por omisión</b>	<p>FR=X'45' (64 kbps)                      PPP=X'45' (64 kbps)                      DLSw=X'75' (4 Mbps)                      SDLC=X'45' (64 kbps)                      X.25=X'45' (64 kbps)                      Red en Anillo: X'75' cuando la velocidad mínima es de 4 Mbps                      Red en Anillo: X'85' cuando la velocidad mínima es de 16 Mbps                      Puertos Ethernet/802.3: X'80' para 10 Mbps                      FDDI: X'9A'                      TR a 100 Mbps: X'9A'                      Ethernet a 100 Mbps: X'9A'                      MPC+: X'9F'</p> <p>Para los SVC ATM (155 Mbps) y SVC ATM (155 Mbps):</p> <p>Campus ATM de mayor eficacia: X'9F'                      Campus ATM reservado: X'9F'                      WAN ATM de mayor eficacia: X'9F'                      WAN ATM reservada: X'9F'</p> <p>Para IP:</p> <p>Campus: X'75'                      WAN: X'43'</p>
<b>Descripción</b>	<p>Este parámetro especifica la característica de TG de capacidad efectiva para todas las conexiones (TG) asociadas de este puerto.</p> <p>Este parámetro especifica la velocidad máxima de transmisión de los bits para los enlaces físicos y los enlaces lógicos. Tenga en cuenta que la capacidad efectiva de un enlace lógico puede ser inferior a la velocidad del enlace físico. La velocidad se representa en los archivos de COS como un número de coma flotante codificado en un solo byte con unidades de 300 bps. La capacidad efectiva se codifica como una representación de un solo byte. Los valores X'00' y X'FF' son casos especiales que se utilizan para denotar la capacidad mínima y la máxima. El rango de la codificación es muy grande; no obstante, sólo pueden especificarse 256 valores del mismo.</p> <p>Este parámetro proporciona el valor por omisión para el parámetro Effective capacity de la opción de la línea de mandatos correspondiente a la modificación de características de TG. La opción de la línea de mandatos correspondiente a la modificación de características de TG le permite alterar temporalmente los valores por omisión .* asignados a las características de TG en las estaciones de enlace individuales que defina.</p>



<i>Tabla 22 (Página 6 de 6). Lista de parámetros de configuración - Características de TG de puerto por omisión</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	First user-defined TG characteristic
<b>Valores válidos</b>	Del 0 al 255
<b>Valor por omisión</b>	128
<b>Descripción</b>	<p>Este parámetro especifica la primera característica de TG definida por el usuario para todas las estaciones de enlace definidas en este puerto.</p> <p>La primera característica de TG definida por el usuario especifica la primera de las tres características adicionales que los usuarios pueden definir para describir los TG en una red. El valor por omisión de 128 permite que se defina un subconjunto de TG como más o menos conveniente que el resto sin definir valores para todos los TG.</p>
<b>Parámetro</b>	Second user-defined TG characteristic
<b>Valores válidos</b>	Del 0 al 255
<b>Valor por omisión</b>	128
<b>Descripción</b>	<p>Este parámetro especifica la segunda característica de TG definida por el usuario para todas las estaciones de enlace definidas en este puerto.</p> <p>La segunda característica de TG definida por el usuario especifica la segunda de las tres características adicionales que los usuarios pueden definir para describir los TG en una red.</p>
<b>Parámetro</b>	Third user-defined TG characteristic
<b>Valores válidos</b>	Del 0 al 255
<b>Valor por omisión</b>	128
<b>Descripción</b>	<p>Este parámetro especifica la tercera característica de TG definida por el usuario para todas las estaciones de enlace definidas en este puerto.</p> <p>La tercera característica de TG definida por el usuario especifica la tercera de las tres características adicionales que los usuarios pueden definir para describir los TG en una red.</p>

<i>Tabla 23 (Página 1 de 3). Lista de parámetros de configuración - Características de LLC de puerto por omisión</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Remote APPN SAP
<b>Valores válidos</b>	Múltiplos de cuatro en el rango hexadecimal del X'04' al X'EC'
<b>Valor por omisión</b>	X'04'
<b>Descripción</b>	Este parámetro especifica el SAP asociado con la estación de enlace APPN de un nodo adyacente.

<i>Tabla 23 (Página 2 de 3). Lista de parámetros de configuración - Características de LLC de puerto por omisión</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Maximum number of outstanding I-format LPDUs (TW)
<b>Valores válidos</b>	Del 1 al 127
<b>Valor por omisión</b>	26
<b>Descripción</b>	<p>Este parámetro especifica el valor TW, número máximo de LPDU de formato I pendientes de LLC para todas las estaciones de enlace de este puerto.</p> <p>El número máximo de LPDU de formato I pendientes define la opción de transmisión de la línea de mandatos (TW) que consiste en el número máximo de LPDU de formato I numeradas secuencialmente que la estación de enlace puede no haber reconocido en un momento determinado.</p>
<b>Parámetro</b>	Receive window size
<b>Valores válidos</b>	Del 1 al 127
<b>Valor por omisión</b>	26
<b>Descripción</b>	<p>Este parámetro especifica el tamaño de RW, opción de recepción de la línea de mandatos de LLC para todas las estaciones de enlace de este puerto.</p> <p>El parámetro RW especifica el número máximo de LPDU de formato I numeradas secuencialmente sin acuse de recibo que la estación de enlace puede recibir de la estación de enlace remota. El RW se anuncia en las tramas de XID de SNA y las tramas de XID de IEEE 802.2. El receptor de XID debe establecer su TW efectivo en un valor inferior o igual al valor del RW recibido para evitar desbordamientos.</p>
<b>Parámetro</b>	Inactivity timer (Ti)
<b>Valores válidos</b>	De 1 a 254 segundos
<b>Valor por omisión</b>	30 segundos
<b>Descripción</b>	<p>Este parámetro especifica el Ti, temporizador de inactividad de LLC para todas las estaciones de enlace de este puerto.</p> <p>Una estación de enlace LLC utiliza el Ti para detectar una condición no operativa en la estación de enlace remota o en el medio de transmisión. Si no se recibe una LPDU en el intervalo de tiempo especificado por el Ti, se transmite una LPDU de mandato de formato S con el conjunto de bits de sondeo para solicitar el estado de la estación de enlace remota. La recuperación está basada en el temporizador de respuesta (T1).</p>

Tabla 23 (Página 3 de 3). Lista de parámetros de configuración - Características de LLC de puerto por omisión

Información de parámetros	
<b>Parámetro</b>	Reply timer (T1)
<b>Valores válidos</b>	De 1 a 254 segundos
<b>Valor por omisión</b>	2 segundos
<b>Descripción</b>	<p>Este parámetro especifica el T1, temporizador de respuesta de LLC para todas las estaciones de enlace de este puerto.</p> <p>Una estación de enlace LLC utiliza el T1 para detectar una anomalía en la recepción de un acuse de recibo o respuesta necesaria de la estación de enlace remota. Cuando caduca el T1, la estación de enlace envía una unidad de datos de protocolo de capa (LPDU) de enlace de mandato en formato S con el conjunto de bits de sondeo para solicitar el estado de la estación de enlace remota o cualquier LPDU de mandato en formato U a la que no se haya respondido. La duración del T1 debe tener en cuenta los retardos aportados por las capas subyacentes.</p>
<b>Parámetro</b>	Maximum number of retransmissions (N2)
<b>Valores válidos</b>	Del 1 al 254
<b>Valor por omisión</b>	8
<b>Descripción</b>	<p>Este parámetro especifica el N2, número máximo de retransmisiones para todas las estaciones de enlace de este puerto.</p> <p>El parámetro N2 especifica el número máximo de veces que puede retransmitirse una LPDU después de que caduque el temporizador de respuesta (T1).</p>
<b>Parámetro</b>	Receive acknowledgment timer (T2)
<b>Valores válidos</b>	Del 1 al 254, medido en décimas de segundo
<b>Valor por omisión</b>	1
<b>Descripción</b>	<p>Este parámetro especifica el T2, temporizador de acuse de recibo del receptor de LLC para todas las estaciones de enlace de este puerto.</p> <p>El parámetro T2 puede utilizarse con el contador N3 para reducir el tráfico de acuses de recibo. Una estación de enlace utiliza el T2 para retardar el envío de un acuse de recibo para una LPDU de formato I recibida. El T2 se inicia cuando se recibe una LPDU de formato I y se restablece cuando se envía un acuse de recibo en una LPDU de formato I o S. Si el T2 caduca, la estación de enlace debe enviar un acuse de recibo lo más pronto posible. El valor del T2 debe ser menor que el del T1 para asegurarse de que la estación de enlace remota reciba el acuse de recibo retardado antes de que caduque su T1.</p>
<b>Parámetro</b>	Acknowledgments needed to increment working window
<b>Valores válidos</b>	Del 0 al 127
<b>Valor por omisión</b>	1
<b>Descripción</b>	<p>Cuando la ventana de trabajo (Ww) no es igual al tamaño máximo de la ventana de transmisión (Tw), este parámetro es el número de LPDU de formato I transmitidas que deben reconocerse para que pueda aumentar la ventana de trabajo (en 1). Cuando se detecta una congestión, por la pérdida de LPDU de formato I, la Ww se establece en 1.</p>

## Mandatos de configuración de APPN

<i>Tabla 24. Lista de parámetros de configuración - Valores por omisión de alteración temporal de HPR</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Inactivity timer override for HPR (HPR Ti)
<b>Valores válidos</b>	De 1 a 254 segundos
<b>Valor por omisión</b>	2 segundos
<b>Descripción</b>	Este parámetro especifica el HPR Ti, temporizador de inactividad de LLC a utilizar para todas las estaciones de enlace de este puerto que den soporte al HPR cuando se habilite el parámetro de HPR soportado en este puerto. Este valor por omisión altera temporalmente el valor del parámetro de temporizador de inactividad de LLC por omisión, Ti, especificado en el parámetro de características de LLC por omisión.
<b>Parámetro</b>	Reply timer override for HPR (HPR T1)
<b>Valores válidos</b>	De 1 a 254 segundos
<b>Valor por omisión</b>	2 segundos
<b>Descripción</b>	Este parámetro especifica el HPR T1, temporizador de respuesta de LLC a utilizar para todas las estaciones de enlace de este puerto que den soporte al HPR cuando se habilite el parámetro de HPR soportado en este puerto. Este valor por omisión altera temporalmente el valor del parámetro de temporizador de respuesta de LLC por omisión, T1, especificado en el parámetro de características de LLC por omisión.
<b>Parámetro</b>	Maximum number of retransmissions for HPR (HPR N2)
<b>Valores válidos</b>	Del 1 al 254
<b>Valor por omisión</b>	3
<b>Descripción</b>	Este parámetro especifica el HPR N2, número máximo de retransmisiones de LLC a utilizar para todas las estaciones de enlace de este puerto que den soporte al HPR cuando se habilite el parámetro de HPR soportado en este puerto. Este valor por omisión altera temporalmente el valor del parámetro de número máximo de retransmisiones de LLC por omisión, N2, especificado en el parámetro de características de LLC por omisión.

### Sintaxis:

add link-station

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

Tabla 25 (Página 1 de 10). Lista de parámetros de configuración - Estación de enlace - Información detallada

Información de parámetros	
<b>Parámetro</b>	Does link support APPN function
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	<p>Este parámetro especifica si la estación de enlace dará soporte a la función de APPN.</p> <p>Si la respuesta es <i>no</i>, no aparecerán preguntas relativas a las sesiones de CP-CP, seguridad, cifrado, nombre de CP, tipo de nodo adyacente, extensor de rama y nodo de frontera extendida, y todas estas funciones estarán inhabilitadas. Además, estará inhabilitado el HPR y no aparecerán preguntas sobre este tipo de direccionamiento.</p>
<b>Parámetro</b>	Link station name (necesario)
<b>Valores válidos</b>	<p>Una serie de 1 a 8 caracteres:</p> <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	<p>Este parámetro especifica el nombre de una estación de enlace que representa al TG (enlace) entre el nodo de red direccionador y el nodo adyacente. El nombre de estación de enlace debe ser exclusivo en este nodo de red.</p>
<b>Parámetro</b>	Port name
<b>Valores válidos</b>	<p>Un nombre sin calificar exclusivo que se genera automáticamente.</p> <p>El nombre estará compuesto por:</p> <ul style="list-style-type: none"> <li>• TR (token-ring, que es la Red en Anillo)</li> <li>• EN (Ethernet)</li> <li>• DLS (DLSw)</li> <li>• FR (Frame Relay)</li> <li>• X25 (X.25)</li> <li>• SDLC (SDLC)</li> <li>• PPP (point-to-point, que significa punto a punto)</li> <li>• IP</li> <li>• FDD (FDDI)</li> </ul> <p>y, a continuación, el número de interfaz.</p>
<b>Valor por omisión</b>	El nombre del puerto en que se define esta estación de enlace.
<b>Descripción</b>	<p>Este parámetro especifica el nombre que representa al puerto en que se define esta estación de enlace. Ya debe haberse configurado el puerto para APPN.</p>

Tabla 25 (Página 2 de 10). Lista de parámetros de configuración - Estación de enlace - Información detallada	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Link type (sólo X.25 y ATM)
	Si se configura <i>limited resource</i> = yes para la estación de enlace, el parámetro de tipo de enlace toma por omisión un valor de 1 (SVC) y no puede configurarse.
<b>Valores válidos</b>	Si es un PVC, especifique un número de canal lógico en el rango del 1 al 4095 Si es un SVC, especifique una dirección de DTE de longitud variable hasta 15 dígitos
<b>Valor por omisión</b>	0, a menos que se trate de un recurso limitado.
<b>Descripción</b>	Este parámetro especifica si el enlace X.25 es un PVC o un SVC.
<b>Parámetro</b>	MAC address of adjacent node (necesario) (sólo Ethernet, Red en Anillo, DLSw, formato de puente de FR)
<b>Valores válidos</b>	Puertos Red en Anillo y DLSw: <ul style="list-style-type: none"> <li>12 dígitos hexadecimales en el rango del X'000000000001' al X'7FFFFFFFFFFFF'</li> </ul> Puertos Ethernet/802.3: <ul style="list-style-type: none"> <li>12 dígitos hexadecimales con el formato X'xyxxxxxxxxx', donde: x es cualquier dígito hexadecimal y es un dígito hexadecimal del conjunto {0, 2, 4, 6, 8, A, C, E}</li> </ul>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica la dirección de capa del control del acceso al medio (MAC) del nodo adyacente. Se utilizan formatos diferentes para Red en Anillo y Ethernet/802.3.  Puertos Red en Anillo y DLSw: La dirección MAC se especifica con formato no canónico. En el formato no canónico de dirección, el bit de cada octeto que debe transmitirse en primer lugar se representa como el bit más significativo.  Puertos Ethernet/802.3: La dirección MAC se especifica con formato canónico. En el formato canónico de dirección, el bit de cada octeto que debe transmitirse en primer lugar se representa como el bit menos significativo.
<b>Parámetro</b>	IP address of adjacent node (sólo Enterprise Extender)
<b>Valores válidos</b>	Cualquier dirección IP válida
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Cada enlace del puerto HPR/IP debe tener una dirección IP de destino exclusiva.

Tabla 25 (Página 3 de 10). Lista de parámetros de configuración - Estación de enlace - Información detallada

Información de parámetros	
<b>Parámetro</b>	Adjacent node type
<b>Valores válidos</b>	APPN network node, APPN end node, LEN end node
<b>Valor por omisión</b>	APPN network node
<b>Descripción</b>	<p>Este parámetro identifica si el nodo adyacente es un nodo APPN o un nodo final de red de entrada baja (LEN).</p> <p>Cuando se seleccione <i>APPN end node</i> y <i>Limited resource</i> sea No, APPN cambiará el tipo de nodo adyacente internamente por <i>learn</i> y funcionará con cualquier tipo de nodo.</p> <p>Cuando se seleccione <i>APPN end node</i> y <i>Limited resource</i> sea Yes, el tipo de nodo adyacente no se cambiará.</p> <p>Cuando seleccione <i>LEN end node</i>, será necesario el parámetro de nombre de punto de control calificado al completo. Si este nodo de red va a comunicarse con el producto IBM Virtual Telecommunications Access Method (VTAM) mediante el nodo LEN y éste no es un nodo T2.1 o no tiene definido explícitamente un nombre de punto de control (CP), también debe especificarse el número de XID del nodo de red direccionador en el parámetro de conexión de subárea con el fin de establecer una conexión.</p> <p><b>Nota:</b> <i>LEN end node</i> no es un tipo de nodo válido para la interfaz HPR/IP.</p>
<b>Parámetro</b>	XID node identification
<b>Valores válidos</b>	Una serie de 8 dígitos hexadecimales (0-F)
<b>Valor por omisión</b>	X'00000000'
<b>Descripción</b>	<p>Este parámetro especifica los campos de bloque de ID y número de ID que identifican al nodo adyacente. Sólo es aplicable cuando el campo <b>Adjacent node type</b> está establecido en <i>LEN end node</i>. Si elige <i>yes</i> para <b>replace inbound XID3 CP name and XID with configured values</b>, el valor de este campo sustituye a los parámetros correspondientes de la XID recibida.</p>

Tabla 25 (Página 4 de 10). Lista de parámetros de configuración - Estación de enlace - Información detallada

Información de parámetros	
<b>Parámetro</b>	fully-qualified CP name of adjacent node
<b>Valores válidos</b>	<p>Una serie de un máximo de 17 caracteres con el formato de <i>IDred.nombCP</i>, donde:</p> <ul style="list-style-type: none"> <li>• <i>IDred</i> es un ID de red de 1 a 8 caracteres</li> <li>• <i>nombCP</i> es un nombre de punto de control de 1 a 8 caracteres</li> </ul> <p>Cada nombre debe ajustarse a las normas siguientes:</p> <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul> <p><b>Nota:</b> Un nombre de CP calificado al completo existente con los caracteres especiales @ y \$ del juego de caracteres A también está soportado; no obstante, estos caracteres no deben utilizarse para nuevos nombres de CP.</p>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	<p>Este parámetro especifica el nombre de CP del nodo adyacente calificado al completo. En los casos en que no sea necesario este parámetro, el nombre de CP del nodo adyacente puede aprenderse dinámicamente durante el intercambio de XID; no obstante, si se especifica un nombre de CP, debe coincidir con la definición del nodo adyacente para que el enlace se active satisfactoriamente.</p> <p><b>Nota:</b> Este parámetro es necesario en cualquiera de las situaciones siguientes:</p> <ul style="list-style-type: none"> <li>• El parámetro <i>Service any node</i> está inhabilitado.</li> <li>• El parámetro <i>Adjacent node type</i> está establecido en <i>LEN end node</i>.</li> <li>• El parámetro <i>CP-CP session level security</i> está habilitado.</li> <li>• El enlace es un recurso limitado.</li> </ul>
<b>Parámetro</b>	Replace inbound XID3 CP name and XID with configured values
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	<p>Este parámetro especifica si el direccionador debe alterar temporalmente o no los parámetros de identificador de nodo y nombre de CP recibidos de las XID de un nodo LEN configurado. Sólo es aplicable cuando el campo <b>adjacent node type</b> está establecido en <i>LEN end node</i>.</p> <p>Si tiene un número elevado de nodos LEN que no están configurados de manera adecuada para participar en una red APPN al completo, puede configurar la identidad de los mismos en el direccionador y hacer que éste altere temporalmente los valores de las XID de los mismos antes de reenviarlas.</p>



Tabla 25 (Página 5 de 10). Lista de parámetros de configuración - Estación de enlace - Información detallada

Información de parámetros	
<b>Parámetro</b>	Activate link automatically
	Si es un recurso limitado, este parámetro se establece en No, y no puede configurarse.
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	Cuando se habilita este parámetro, el nodo de red direccionador activa automáticamente el enlace con el nodo adyacente e inicia una conexión.
<b>Parámetro</b>	Retry link activation unconditionally
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	<p>Este parámetro especifica si el direccionador siempre debe intentar reactivar el enlace, sea cual sea la causa de la anomalía del enlace. Sólo es aplicable a los enlaces con posibilidad de marcación de salida en que <b>activate link automatically</b> es yes.</p> <p>Normalmente, si un enlace no puede iniciarse o se desactiva debido a algún suceso distinto de un mandato del operador, el direccionador elige de manera selectiva si lo reactivará o no. Si es probable que la causa de la anomalía requiera la reconfiguración de uno de los dos nodos, el direccionador no reinicia el enlace automáticamente. De este modo, se evita una repetición periódica (con anotación cronológica, alertas, etc.) del intento de conexión no satisfactorio. Si desea alterar temporalmente este comportamiento y hacer que los enlaces siempre intenten volver a conectarse, seleccione <b>yes</b> para este parámetro.</p>
<b>Parámetro</b>	Allow CP-CP sessions on this link
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	Yes, si el tipo de nodo adyacente es un nodo de red APPN o un nodo final APPN. Para cualquier otro tipo de nodo adyacente, el valor es No
<b>Descripción</b>	<p>Este parámetro especifica si van a activarse sesiones entre puntos de control sobre esta estación de enlace.</p> <p>Este parámetro permite el control del establecimiento de sesiones de CP-CP entre nodos de red adyacentes para que pueda limitarse la actividad general asociada con actualizaciones de base de datos de topología (TDU).</p> <p><b>Nota:</b> Cada nodo de red APPN debe tener establecida al menos una sesión de CP-CP con otro nodo de red APPN para mantener la conectividad mínima que necesitan las actualizaciones de la base de datos de topología. Además, puede ser conveniente una conectividad superior a la mínima para eliminar puntos individuales de anomalías y para mejorar la dinámica de la red.</p>

## Mandatos de configuración de APPN

<i>Tabla 25 (Página 6 de 10). Lista de parámetros de configuración - Estación de enlace - Información detallada</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	CP-CP session level security
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si debe aplicarse la seguridad de nivel de sesión a las sesiones de CP-CP establecidas sobre la estación de enlace. Cuando se habilita la seguridad de nivel de sesión, se intercambian y se comparan datos cifrados durante los flujos de BIND (incluidas la BIND, la respuesta a BIND y una RU de seguridad FMH-12). Para establecer satisfactoriamente una sesión de CP-CP habiendo habilitado la seguridad de nivel de sesión, ambos asociados deben estar configurados con la misma clave de cifrado. Actualmente, el soporte de seguridad de nivel de sesión se limita al protocolo básico de verificación de LU-LU.
<b>Parámetro</b>	Encryption key
<b>Valores válidos</b>	Un máximo de 16 dígitos hexadecimales. Si se especifican menos, el valor se rellena hacia la derecha con ceros.
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro se utiliza para cifrar los datos intercambiados durante los flujos de BIND. Ambos asociados deben estar configurados con la misma clave para establecer una sesión de CP-CP.
<b>Parámetro</b>	Use enhanced session security (si se ha habilitado la seguridad)
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Parámetro</b>	High-performance routing (HPR) supported
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	Si es un nodo de red APPN, un nodo final APPN o un nodo final LEN, el valor especificado en el parámetro por omisión de este puerto de HPR soportado. Cualquier otro tipo de nodo adyacente No
<b>Descripción</b>	Este parámetro indica si la estación de enlace da soporte al HPR. El usuario debe inhabilitar el soporte de HPR si el enlace subyacente no es fiable. No se establecerá una conexión de HPR a menos que ambas estaciones de enlace anuncien el soporte de HPR durante el intercambio de XID.
<b>Parámetro</b>	DLCI number for link (sólo Frame Relay)
<b>Valores válidos</b>	Del 16 al 1007
<b>Valor por omisión</b>	16
<b>Descripción</b>	El parámetro DLCI identifica la conexión del enlace de datos lógico frame-relay con el nodo adyacente.

Tabla 25 (Página 7 de 10). Lista de parámetros de configuración - Estación de enlace - Información detallada	
Información de parámetros	
<b>Parámetro</b>	Station address of adjacent node (sólo SDLC)
<b>Valores válidos</b>	Una dirección en el rango del 1 al FE
<b>Valor por omisión</b>	C1
<b>Descripción</b>	Este parámetro especifica la dirección del nodo adyacente.
<b>Parámetro</b>	Limited Resource (PPP, X.25, FR sobre circuitos de marcación, ATM)
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Si el <i>tipo de enlace</i> (link type) es PPP o FR, el valor por omisión se tomará del parámetro <i>recurso limitado</i> (limited resource) para el puerto asociado. Este parámetro especifica si el TG para la estación de enlace es un recurso limitado. Si responde <i>yes</i> , <b>Virtual Channel Type</b> es <i>SVC</i> .
<b>Parámetro</b>	Branch Uplink
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	El valor especificado para <b>Branch Uplink</b> en el puerto.
<b>Descripción</b>	Este parámetro indica si este enlace será un enlace superior de rama (para WAN) o un enlace inferior de rama (para LAN).  Esta pregunta sólo aparece si <b>Enabled Branch Extender</b> se ha establecido en <i>yes</i> y si esta estación de enlace no es un nodo de red. Si <b>Enabled Branch Extender</b> se ha establecido en <i>yes</i> y la estación de enlace es un nodo de red, <b>Branch Uplink</b> toma por omisión el valor de <i>yes</i> .
<b>Parámetro</b>	Is uplink to another Branch Extender node
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro indica si el nodo adyacente tiene habilitada o no la función Branch Extender.  Esta pregunta sólo aparece si se ha habilitado <b>Branch Extender</b> en este nodo, es un enlace superior y el enlace superior es un recurso limitado.

Tabla 25 (Página 8 de 10). Lista de parámetros de configuración - Estación de enlace - Información detallada	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Preferred Network Node Server
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	<p>Este parámetro indica si este enlace superior es para un servidor de nodos de red que va a utilizarse como el servidor de nodos de red del nodo que da soporte a la función Branch Extender y actúa como nodo final. Si se especifica <i>yes</i>, este enlace superior se utilizará como el servidor de nodos de red de este nodo.</p> <p>Esta pregunta sólo aparecerá si:</p> <ul style="list-style-type: none"> <li>• <b>Enabled Branch Extender</b> es <i>yes</i>,</li> <li>• Esta estación es un nodo de red,</li> <li>• <b>Branch Uplink</b> es <i>yes</i></li> <li>• Y se da soporte a sesiones de CP-CP en este enlace.</li> </ul>
<b>Parámetro</b>	TG Number
<b>Valores válidos</b>	<p>Si el <i>recurso limitado</i> (limited resource) es Yes, los valores válidos son 1 - 20. Si el <i>recurso limitado</i> (limited resource) es No y el <i>tipo de enlace</i> (link type) es un SVC X.25, los valores válidos son 0 - 20.</p> <p>De lo contrario, los valores válidos son 0 - 20.</p>
<b>Valor por omisión</b>	<p>Si el <i>recurso limitado</i> (limited resource) es Yes, el valor por omisión es 1. Si el <i>recurso limitado</i> (limited resource) es No, el valor por omisión es 0.</p> <p>De lo contrario, el valor por omisión es 0.</p>
<b>Descripción</b>	Este parámetro identifica de manera exclusiva a un TG entre nodos adyacentes.
<b>Parámetro</b>	Solicit SSCP session
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
	Si <b>link station name</b> es igual que <b>CP name</b> , el valor por omisión es <i>yes</i> .
<b>Descripción</b>	Este parámetro indica si este enlace va a solicitar sesiones de SSCP.
<b>Parámetro</b>	Local Node ID
<b>Valores válidos</b>	5 dígitos hexadecimales
<b>Valor por omisión</b>	X'00000'
<b>Descripción</b>	Este parámetro especifica el identificador de nodo local que representa la PU dependiente local para VTAM. Esta pregunta sólo aparece si el valor para la solicitud de sesión de SSCP es <i>yes</i> . El ID de nodo local debe ser exclusivo.

Tabla 25 (Página 9 de 10). Lista de parámetros de configuración - Estación de enlace - Información detallada

Información de parámetros	
<b>Parámetro</b>	Enable Host Initiated Dynamic LU Definition
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	<p>Este parámetro indica si se crearán o no LU dependientes de manera dinámica (en contraposición a que tengan que configurarse). Si se especifica <i>yes</i>, se definirán LU para esta PU al recibirse peticiones ACTLU (con CV0E). Con esta función, no tienen que configurarse LU para el Servidor TN3270E.</p> <p><b>Nota:</b> Esta pregunta sólo aparece si el valor para la solicitud de sesión de SSCP es <i>yes</i>.</p>
<b>Parámetro</b>	Pool Name for Host-initiated Dynamic LUs
<b>Valores válidos</b>	<p>Una serie de 1 a 8 caracteres:</p> <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z, \$, #, @ o &lt;</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9, \$, #, @, &gt; o &lt;</li> </ul>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	<p>Este parámetro especifica el nombre de una agrupación a crear para que contenga LU activadas por el sistema principal en este enlace de subárea. Este parámetro sólo es aplicable si <b>Solicit SSCP session</b> es <i>yes</i> y <b>Enable Host Initiated Dynamic LU Definition</b> es <i>yes</i>.</p> <p>No es necesario utilizar el mandato <b>add implicit-pool</b> para definir esta agrupación; basta con especificar el nombre y otros parámetros aquí para que se cree la agrupación. Si entra un nombre de agrupación, se le solicitará que entre valores para los parámetros siguientes:</p> <ul style="list-style-type: none"> <li>• Pool class (vea la Tabla 43 en la página 223)</li> <li>• LU type (vea la Tabla 43 en la página 223)</li> </ul> <p>Puede proporcionar el mismo nombre de agrupación para diversos enlaces de subárea si lo desea.</p> <p>Si especifica información de agrupación, causa que las LU iniciadas por sistema principal que todavía no se han configurado en el direccionador se coloquen en la agrupación especificada. Después se les pueden asignar clientes TN3270 solicitando el nombre de agrupación o correlacionando puertos de destino o direcciones IP de cliente con esta agrupación.</p> <p>Si no especifica información de agrupación, estas LU iniciadas por sistema principal reciben el tratamiento de LU explícitas y sólo se pueden asignar a clientes que las soliciten por el nombre de LU individual.</p>

Tabla 25 (Página 10 de 10). Lista de parámetros de configuración - Estación de enlace - Información detallada	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Local SAP address
<b>Valores válidos</b>	Cualquier dirección de SAP válida entre el X'04' y el X'EC'.
<b>Valor por omisión</b>	El valor se toma del puerto
<b>Descripción</b>	Este parámetro especifica la dirección de SAP local.
	<b>Notas:</b>
	<ol style="list-style-type: none"> <li>1. Esta pregunta sólo se visualiza si hay definidas diversas PU en el puerto.</li> <li>2. Si la dirección de SAP local no es la dirección de SAP local principal del puerto,</li> <li>3. el nombre de puerto y el nombre de SAP se visualizarán en la salida de supervisión y pantalla de SNMP.</li> </ol>
<b>Parámetro</b>	Send Terminate-Self when TN3270 Client Disconnects
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro indica si se enviará o no una petición terminate_self al SSCP cuando se desconecte el cliente TN3270. Si se especifica yes, se enviará terminate_self y el sistema principal será el responsable de terminar la sesión de LU-LU (es decir, la SLU NO enviará una petición UNBIND).
<b>Parámetro</b>	Subnet visit count
<b>Valores válidos</b>	1 - 255
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro de nivel de puerto equivalente
<b>Descripción</b>	Este parámetro especifica el valor por omisión para el número máximo de subredes que una sesión de diversas subredes puede atravesar.
	<b>Nota:</b> Esta pregunta sólo aparece si se ha habilitado la función de nodo de frontera en este nodo.
<b>Parámetro</b>	Adjacent node subnet affiliation
<b>Valores válidos</b>	<ul style="list-style-type: none"> <li>• 0 (native)</li> <li>• 1 (non-native)</li> <li>• 2 (negotiable)</li> </ul>
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro de nivel de puerto equivalente
<b>Descripción</b>	Este parámetro especifica si el nodo adyacente está en la subred APPN nativa de este nodo o en una subred APPN no nativa. Un valor de 2 indica al nodo que negocie durante la activación del enlace para determinar si la estación de enlace adyacente es nativa o no nativa.
	<b>Nota:</b> Esta pregunta sólo aparece si se ha habilitado la función de nodo de frontera en este nodo.

<i>Tabla 26 (Página 1 de 5). Lista de parámetros de configuración - Configuración de estación para ATM</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Virtual Channel Type
<b>Valores válidos</b>	SVC, PVC
<b>Valor por omisión</b>	SVC
<b>Descripción</b>	Este parámetro identifica el tipo de canal de ATM como circuito virtual conmutado (SVC) o circuito virtual permanente (PVC).
<b>Nota:</b> Los parámetros siguientes son comunes para los SVC y los PVC.	
<b>Parámetro</b>	Destination ATM Address
<b>Valores válidos</b>	Una serie hexadecimal de 40 caracteres
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica la serie de 20 bytes que comprende toda la dirección ATM de destino.
<b>Parámetro</b>	ATM network type
<b>Valores válidos</b>	Campus, Widearea
<b>Valor por omisión</b>	Campus
<b>Descripción</b>	Este parámetro especifica el tipo de red ATM.
<b>Parámetro</b>	Shareable connection network traffic
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si puede direccionarse tráfico de red de conexiones en el VC ATM configurado para este TG.
<b>Parámetro</b>	Shareable other protocol traffic
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si puede direccionarse tráfico de otros protocolos de nivel superior en el VC ATM configurado para este TG.
<b>Parámetro</b>	LDLC retry count
<b>Valores válidos</b>	1 — 255
<b>Valor por omisión</b>	3
<b>Descripción</b>	Este parámetro se utiliza junto con el período del temporizador de LDLC para proporcionar una entrega de XID fiable. La cuenta de reintentos se inicializa la primera vez que se transmite un mandato o una petición sobre el enlace. Si el período del temporizador de LDLC caduca antes de que se reciba una respuesta, se retransmite el mandato o respuesta, disminuye la cuenta de reintentos y se reinicia el período del temporizador de LDLC. Si el temporizador caduca con la cuenta de reintentos de 0, se supone que el enlace no es operativo.

## Mandatos de configuración de APPN

<i>Tabla 26 (Página 2 de 5). Lista de parámetros de configuración - Configuración de estación para ATM</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	LDLC Timer Period
<b>Valores válidos</b>	1 — 255 segundos
<b>Valor por omisión</b>	Para ATM: 1 segundo Para IP: 15 segundos
<b>Descripción</b>	Este parámetro especifica el período del temporizador que se utiliza con <b>LDLC retry count</b> .
<b>Parámetro</b>	VPI
<b>Valores válidos</b>	0 — 255
<b>Valor por omisión</b>	0
<b>Descripción</b>	Este parámetro identifica el valor de VPI del PVC en la interfaz.
<b>Parámetro</b>	VCI
<b>Valores válidos</b>	Del 0 al 65535
<b>Valor por omisión</b>	0
<b>Descripción</b>	Este parámetro identifica el valor de VCI del PVC en la interfaz.
<b>Parámetro</b>	Broadband Bearer Class
<b>Valores válidos</b>	Class_A, Class_C, Class_X
<b>Valor por omisión</b>	Class_X
<b>Descripción</b>	Este parámetro especifica la clase portadora solicitada de la red ATM. Las clases se definen:  <b>Class A</b> Velocidad en bits constante (CBR) con requisitos de temporización de final a final  <b>Class C</b> Velocidad en bits variable (VBR) sin requisitos de temporización de final a final  <b>Class X</b> Servicio que permite unos requisitos de temporización y tipo de tráfico definidos por el usuario
<b>Parámetro</b>	Best Effort Indicator
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro indica si es necesaria una garantía de productividad en este SVC. Si el valor de este parámetro es <i>yes</i> , se asignarán las VCC asociadas con esta interfaz sobre la base del ancho de banda disponible.
<b>Nota:</b> Los parámetros siguientes son parámetros del tráfico hacia adelante.	



<i>Tabla 26 (Página 3 de 5). Lista de parámetros de configuración - Configuración de estación para ATM</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Forward Peak Cell Rate
<b>Valores válidos</b>	Un 85% de la velocidad de línea
<b>Valor por omisión</b>	Capacidad efectiva por omisión del puerto/48
<b>Descripción</b>	Este parámetro indica un límite superior para la velocidad de transmisión de las células.
<b>Parámetro</b>	Forward Sustained Cell Rate
<b>Valores válidos</b>	De un 1 a un 85% de la velocidad de línea
<b>Valor por omisión</b>	Capacidad efectiva por omisión del puerto/48
<b>Descripción</b>	Este parámetro indica un límite superior para la velocidad media de transmisión de las células. No puede especificar este parámetro para las conexiones Mayor Eficacia.
<b>Parámetro</b>	Forward Tagging
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	Este parámetro indica que las células que no se ajustan a la especificación de tráfico de prioridad de pérdida de célula 0 pero se ajustan a la especificación de tráfico de prioridad de pérdida de célula 1 se marcan y se permiten en la red ATM. No puede especificar este parámetro para las conexiones Mayor Eficacia.
<b>Parámetro</b>	QoS
<b>Valores válidos</b>	CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, donde
	<b>CLASS_0</b> La clase sin especificar. La red no especifica ninguna QoS.
	<b>CLASS_1</b> El rendimiento es comparable al de una línea privada digital actual.
	<b>CLASS_2</b> Pensada para los paquetes de vídeo y audio de aplicaciones de teleconferencia y multimedia.
	<b>CLASS_3</b> Pensada para la interoperación de los protocolos orientados a las conexiones, como, por ejemplo, Frame Relay.
	<b>CLASS_4</b> Pensada para la interoperación de los protocolos sin conexiones, como, por ejemplo, IP.
<b>Valor por omisión</b>	CLASS_0
<b>Descripción</b>	Este parámetro indica qué clase de servicio se proporciona a una conexión virtual ATM. No puede especificar este parámetro para las conexiones Mayor Eficacia.
<b>Nota:</b> Los parámetros siguientes son parámetros del tráfico hacia atrás.	

## Mandatos de configuración de APPN

<i>Tabla 26 (Página 4 de 5). Lista de parámetros de configuración - Configuración de estación para ATM</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Backward Peak Cell Rate
<b>Valores válidos</b>	De un 1 a un 85% de la velocidad de línea
<b>Valor por omisión</b>	Se toma de la definición de puerto
<b>Descripción</b>	Este parámetro indica un límite superior para la velocidad de transmisión de las células.
<b>Parámetro</b>	Backward Sustained Cell Rate
<b>Valores válidos</b>	De un 1 a un 85% de la velocidad de línea
<b>Valor por omisión</b>	Se toma de la definición de puerto
<b>Descripción</b>	Este parámetro indica un límite superior para la velocidad media de transmisión de las células. No puede especificar este parámetro para las conexiones Mayor Eficacia.
<b>Parámetro</b>	Backward Tagging
<b>Valores válidos</b>	Yes, No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	Este parámetro indica que las células que no se ajustan a la especificación de tráfico de prioridad de pérdida de célula 0 pero se ajustan a la especificación de tráfico de prioridad de pérdida de célula 1 se marcan y se permiten en la red ATM. No puede especificar este parámetro para las conexiones Mayor Eficacia.
<b>Parámetro</b>	QoS
<b>Valores válidos</b>	CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, donde
	<b>CLASS_0</b> La clase sin especificar. La red no especifica ninguna QoS.
	<b>CLASS_1</b> El rendimiento es comparable al de una línea privada digital actual.
	<b>CLASS_2</b> Pensada para los paquetes de vídeo y audio de aplicaciones de teleconferencia y multimedia.
	<b>CLASS_3</b> Pensada para la interoperación de los protocolos orientados a las conexiones, como, por ejemplo, Frame Relay.
	<b>CLASS_4</b> Pensada para la interoperación de los protocolos sin conexiones, como, por ejemplo, IP.
<b>Valor por omisión</b>	CLASS_0
<b>Descripción</b>	Este parámetro indica qué clase de servicio se proporciona a una conexión virtual ATM. No puede especificar este parámetro para las conexiones Mayor Eficacia.

Tabla 26 (Página 5 de 5). Lista de parámetros de configuración - Configuración de estación para ATM

Información de parámetros	
<b>Parámetro</b>	Callout Anonymously
<b>Valores válidos</b>	Yes, no
<b>Valor por omisión</b>	no
<b>Descripción</b>	Este parámetro indica si APPN pasará la dirección de origen al efectuar la llamada.

Tabla 27 (Página 1 de 3). Lista de parámetros de configuración - Modificación de características de TG

Información de parámetros	
<b>Parámetro</b>	Cost per connect time
<b>Valores válidos</b>	Del 0 al 255
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	Este parámetro expresa el coste relativo del mantenimiento de una conexión sobre el TG asociado. Las unidades están definidas por el usuario y, normalmente, se basan en las tarifas aplicables del recurso de transmisión que se utiliza. Los valores asignados deben reflejar el gasto real del mantenimiento de una conexión sobre el TG en relación con todos los otros TG de la red. Un valor de cero significa que las conexiones sobre el TG pueden realizarse sin coste adicional (como es el caso de muchos recursos no conmutados). Los valores más elevados representan costes más elevados.
<b>Parámetro</b>	Cost per byte
<b>Valores válidos</b>	Del 0 al 255
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	Este parámetro expresa el coste relativo de la transmisión de un byte sobre el TG asociado. Las unidades están definidas por el usuario y el valor asignado debe reflejar los gastos reales en los que se incurra para la transmisión sobre el TG en relación con todos los otros TG de la red. Un valor de cero significa que los bytes pueden transmitirse sobre el TG sin coste adicional. Los valores más elevados representan costes más elevados.

<i>Tabla 27 (Página 2 de 3). Lista de parámetros de configuración - Modificación de características de TG</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Security
<b>Valores válidos</b>	<ul style="list-style-type: none"> <li>• Nonsecure - todo lo demás (por ejemplo, conectado a satélite o ubicado en una zona no segura).</li> <li>• Public switched network - seguridad en el sentido de que la ruta no está predeterminada.</li> <li>• Underground cable - ubicado en una zona segura (según lo que determina el administrador de la red).</li> <li>• Secure conduit - no protegido (por ejemplo, un conducto presurizado).</li> <li>• Guarded conduit - protegido contra infiltraciones físicas.</li> <li>• Encrypted - se proporciona cifrado de nivel de enlace.</li> <li>• Guarded radiation - conducto protegido que contiene el medio de transmisión; protegido contra infiltraciones físicas e infiltraciones de la radiación.</li> </ul>
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	Este parámetro indica el nivel de protección de seguridad asociado con el TG. Si son necesarios unos atributos de seguridad diferentes de los definidos estructuralmente, puede utilizarse una de las características de TG definidas por el usuario para especificar valores adicionales.
<b>Parámetro</b>	Propagation delay
<b>Valores válidos</b>	<p>Minimum LAN – menos de 480 microsegundos                      Telephone – entre 0,48 y 49,152 milisegundos                      Packet switched - entre 49,152 y 245,76 milisegundos                      Satellite - superior al máximo de 245,76 milisegundos</p>
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	Este parámetro especifica el rango aproximado para el período de tiempo que tarda una señal en propagarse de un extremo a otro del TG.
<b>Parámetro</b>	Effective capacity
<b>Valores válidos</b>	2 dígitos hexadecimales en el rango del X'00' al X'FF'
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	<p>Este parámetro especifica la velocidad máxima de transmisión de los bits para los enlaces físicos y los enlaces lógicos. Tenga en cuenta que la capacidad efectiva de un enlace lógico puede ser inferior a la velocidad del enlace físico.</p> <p>La capacidad efectiva se codifica como una representación de un solo byte. Los valores X'00' y X'FF' son casos especiales que se utilizan para denotar la capacidad mínima y la máxima. El rango de la codificación es muy grande; no obstante, sólo pueden especificarse 256 valores del mismo.</p>

<i>Tabla 27 (Página 3 de 3). Lista de parámetros de configuración - Modificación de características de TG</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	First user-defined TG characteristic
<b>Valores válidos</b>	Del 0 al 255
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	Este parámetro especifica la primera de las tres características adicionales que los usuarios pueden definir para describir los TG en una red.
<b>Parámetro</b>	Second user-defined TG characteristic
<b>Valores válidos</b>	Del 0 al 255
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	Este parámetro especifica la segunda de las tres características adicionales que los usuarios pueden definir para describir los TG en una red.
<b>Parámetro</b>	Third user-defined TG characteristic
<b>Valores válidos</b>	Del 0 al 255
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	Este parámetro especifica la tercera de las tres características adicionales que los usuarios pueden definir para describir los TG en una red.

<i>Tabla 28 (Página 1 de 2). Lista de parámetros de configuración - Modificación del Servidor de LU dependientes</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	fully-qualified CP name of primary DLUS
<b>Valores válidos</b>	Una serie de un máximo de 17 caracteres con el formato de <i>IDred.nombCP</i> , donde: <ul style="list-style-type: none"> <li>• <i>IDred</i> es un ID de red de 1 a 8 caracteres</li> <li>• <i>nombCP</i> es un nombre de punto de control de 1 a 8 caracteres</li> </ul> Cada nombre debe ajustarse a las normas siguientes: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul> <b>Nota:</b> Un nombre de CP calificado al completo existente con los caracteres especiales @, \$ y # del juego de caracteres A también está soportado; no obstante, estos caracteres no deben utilizarse para nuevos nombres de CP.
<b>Valor por omisión</b>	El valor especificado en el parámetro de nombre de CP calificado al completo por omisión del servidor de LU dependientes primario.
<b>Descripción</b>	Este parámetro especifica el nombre de CP calificado al completo del servidor de LU dependientes (DLUS) que va a utilizarse para las peticiones de entrada de la PU de sentido directo asociada con la estación de enlace.

<i>Tabla 28 (Página 2 de 2). Lista de parámetros de configuración - Modificación del Servidor de LU dependientes</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	fully-qualified CP name for backup DLUS
<b>Valores válidos</b>	Una serie de un máximo de 17 caracteres con el formato de <i>IDred.nombCP</i> , donde: <ul style="list-style-type: none"> <li>• <i>IDred</i> es un ID de red de 1 a 8 caracteres</li> <li>• <i>nombCP</i> es un nombre de punto de control de 1 a 8 caracteres</li> </ul> Cada nombre debe ajustarse a las normas siguientes: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul> <b>Nota:</b> Un nombre de CP calificado al completo existente con los caracteres especiales @, \$ y # del juego de caracteres A también está soportado; no obstante, estos caracteres no deben utilizarse para nuevos nombres de CP.
<b>Valor por omisión</b>	El valor especificado en el parámetro de nombre de CP calificado al completo por omisión del servidor de LU dependientes de reserva.
<b>Descripción</b>	Este parámetro especifica el nombre de CP calificado al completo del servidor de LU dependientes (DLUS) que va a utilizarse como reserva para la PU de sentido directo asociada con la estación de enlace. Este parámetro permite alterar temporalmente el servidor de reserva por omisión. No es necesario un servidor de reserva, y el valor nulo indica la ausencia de un servidor de reserva. Tenga en cuenta que puede especificarse el valor nulo incluso cuando se ha definido un servidor de reserva por omisión (borrando el valor por omisión que aparece para este parámetro).

<i>Tabla 29 (Página 1 de 3). Lista de parámetros de configuración - Modificación de características de LLC</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Remote APPN SAP
<b>Valores válidos</b>	Múltiplos de cuatro en el rango hexadecimal del X'04' al X'EC'.
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	Este parámetro especifica la dirección de SAP de destino (DSAP) del nodo de destino al que se enviarán datos. Este valor de dirección de DSAP aparecerá en la trama de LLC para identificar a la dirección de punto de acceso a servicios (SAP) asociada con la estación de enlace APPN del nodo adyacente.
<b>Parámetro</b>	Maximum number of outstanding I-format LPDUs (TW)
<b>Valores válidos</b>	Del 1 al 127
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	Este parámetro especifica la opción de transmisión de la línea de mandatos que consiste en el número máximo de LPDU de formato I numeradas secuencialmente que la estación de enlace puede no haber reconocido en un momento determinado.

Tabla 29 (Página 2 de 3). Lista de parámetros de configuración - Modificación de características de LLC

Información de parámetros	
<b>Parámetro</b>	Receive window size
<b>Valores válidos</b>	Del 1 al 127
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	Este parámetro especifica el número máximo de LPDU de formato I numeradas secuencialmente sin acuse de recibo que la estación de enlace LLC puede recibir de la estación de enlace remota. El RW se anuncia en las tramas de XID de SNA y las tramas de XID de IEEE 802.2. El receptor de XID debe establecer su TW efectivo en un valor inferior o igual al valor del RW recibido para evitar desbordamientos.
<b>Parámetro</b>	Inactivity timer (Ti)
<b>Valores válidos</b>	De 1 a 254 segundos
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	Una estación de enlace utiliza el Ti para detectar una condición no operativa en la estación de enlace remota o en el medio de transmisión. Si no se recibe una LPDU en el intervalo de tiempo especificado por el Ti, se transmite una LPDU de mandato de formato S con el conjunto de bits de sondeo para solicitar el estado de la estación de enlace remota. La recuperación está basada en el temporizador de respuesta (T1).
<b>Parámetro</b>	Reply timer (T1)
<b>Valores válidos</b>	De 1 a 254 segundos
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	Una estación de enlace utiliza el T1 para detectar una anomalía en la recepción de un acuse de recibo o respuesta necesaria de la estación de enlace remota. Cuando caduca el T1, la estación de enlace envía una unidad de datos de protocolo de capa (LPDU) de enlace de mandato en formato S con el conjunto de bits de sondeo para solicitar el estado de la estación de enlace remota o cualquier LPDU de mandato en formato U a la que no se haya respondido. La duración del T1 debe tener en cuenta los retardos aportados por las capas subyacentes.
<b>Parámetro</b>	Maximum number of retransmissions (N2)
<b>Valores válidos</b>	Del 1 al 254
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	Este parámetro especifica el número máximo de veces que se retransmitirá una LPDU después de que caduque el temporizador de respuesta (T1).

<i>Tabla 29 (Página 3 de 3). Lista de parámetros de configuración - Modificación de características de LLC</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Receive acknowledgment timer (T2)
<b>Valores válidos</b>	Del 1 al 254, medido en décimas de segundo
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	Este parámetro puede utilizarse junto con el contador N3 para reducir el tráfico de acuses de recibo. Una estación de enlace utiliza el T2 para retardar el envío de un acuse de recibo para una LPDU de formato I recibida. El T2 se inicia cuando se recibe una LPDU de formato I y se restablece cuando se envía un acuse de recibo en una LPDU de formato I o S. Si el T2 caduca, la estación de enlace debe enviar un acuse de recibo lo más pronto posible. El valor del T2 debe ser menor que el del T1 para asegurarse de que la estación de enlace remota reciba el acuse de recibo retardado antes de que caduque su T1.
<b>Parámetro</b>	Acknowledgment needed to increment working window
<b>Valores válidos</b>	De 0 a 127 acuses de recibo
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	Cuando la ventana de trabajo (Ww) no es igual al tamaño máximo de la ventana de transmisión (Tw), este parámetro es el número de LPDU de formato I transmitidas que deben reconocerse para que pueda aumentar la ventana de trabajo (en 1). Cuando se detecta una congestión, por la pérdida de LPDU de formato I, la Ww se establece en 1.

<i>Tabla 30 (Página 1 de 2). Lista de parámetros de configuración - Modificación de valores por omisión de HPR</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Inactivity timer override for HPR (HPR Ti)
<b>Valores válidos</b>	De 1 a 254 segundos
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	Este parámetro especifica el HPR Ti, alteración temporal para el HPR que es el temporizador de inactividad de LLC a utilizar cuando la estación de enlace dé soporte al HPR. Este parámetro altera temporalmente el valor tomado de la alteración temporal del temporizador de inactividad por omisión para el parámetro de HPR.  Este parámetro suplanta el valor del parámetro de temporizador de inactividad de LLC, Ti, especificado en el parámetro de modificación de características de control de enlace lógico (LLC) cuando se da soporte al HPR.



Tabla 30 (Página 2 de 2). Lista de parámetros de configuración - Modificación de valores por omisión de HPR

Información de parámetros	
<b>Parámetro</b>	Reply timer override for HPR (HPR T1)
<b>Valores válidos</b>	De 1 a 254 segundos
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	<p>Este parámetro especifica el HPR T1, alteración temporal para el HPR que es el temporizador de respuesta de LLC a utilizar cuando la estación de enlace dé soporte al HPR. Este parámetro altera temporalmente el valor tomado de la alteración temporal del temporizador de respuesta por omisión para el parámetro de HPR especificado en Valores por omisión de HPR.</p> <p>Este parámetro suplanta el valor del parámetro de temporizador de respuesta de LLC, T1, especificado en el parámetro de modificación de características de control de enlace lógico (LLC) cuando se da soporte al HPR.</p>
<b>Parámetro</b>	Maximum number retransmission (HPR N2)
<b>Valores válidos</b>	Del 1 al 216 000
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	<p>Este parámetro especifica el HPR N2, alteración temporal para el HPR que es el número máximo de retransmisiones a utilizar cuando la estación de enlace dé soporte al HPR. Este parámetro altera temporalmente el valor tomado del número máximo de retransmisiones por omisión del parámetro de HPR especificado en Valores por omisión de alteración temporal de LLC de HPR.</p> <p>Este parámetro suplanta el valor del parámetro de número máximo de retransmisiones de LLC, N2, especificado en el parámetro de modificación de características de control de enlace lógico (LLC) cuando se da soporte al HPR.</p>
<b>Parámetro</b>	Limited Resource Timer
<b>Valores válidos</b>	De 1 a 216 000 segundos
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro del puerto asociado.
<b>Descripción</b>	Este parámetro especifica el valor de temporizador asociado con el recurso limitado.

**Sintaxis:**addlu-name

Se le solicitará que entre un nombre de estación con el que asociar esta LU.

Se le solicitará que entre un valor para el parámetro siguiente. El rango del parámetro se mostrará entre paréntesis ( ). El valor por omisión del parámetro se mostrará entre corchetes [ ].

Tabla 31. Lista de parámetros de configuración - Nombre de LU de nodo final LEN	
Información del parámetro	
<b>Parámetro</b>	fully-qualified LU name
<b>Valores válidos</b>	<p>Un nombre de LU calificado al completo (explícito), un nombre de LU genérico (parcialmente explícito) o una entrada con comodín</p> <p>Una serie de un máximo de 17 caracteres con el formato de <i>IDred.nombLU</i>, donde:</p> <ul style="list-style-type: none"> <li>• <i>IDred</i> es un ID de red de 1 a 8 caracteres</li> <li>• <i>nombLU</i> es un nombre de punto de control de 1 a 8 caracteres</li> </ul> <p>Cada nombre debe ajustarse a las normas siguientes:</p> <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul> <p><b>Nota:</b> Un nombre de LU calificado al completo existente con los caracteres especiales @, \$ y # del juego de caracteres A también está soportado; no obstante, estos caracteres no deben utilizarse para nuevos nombres de LU.</p> <p>Si desea reducir el número de nombres de LU calificados al completo que tenga que especificar, puede definir un nombre de LU genérico utilizando el carácter comodín (*) para representar una parte del nombre de LU (<i>nombLU</i>). También puede definir una entrada con comodín utilizando el carácter comodín para todo el nombre de LU.</p>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	<p>Este parámetro especifica los nombres calificados al completo de LU asociadas con un nodo final LEN. Los nombres de LU especificados se registran en la base de datos de servicios de directorio del nodo de red. Si no se registra un nombre, el nodo de red no puede ubicar la LU (a menos que el nombre de LU sea igual que el nombre de CP del nodo final LEN).</p> <p>Tiene que especificar un nombre de LU calificado al completo, que está compuesto por un ID de red y el nombre de LU. El ID de red es el nombre de la red que contiene el nodo final LEN adyacente. El nombre de LU es el nombre de una unidad lógica a la que puede accederse mediante el nodo final LEN adyacente.</p>

**Sintaxis:**

add connection-network

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

Tabla 32 (Página 1 de 3). Lista de parámetros de configuración - Red de conexiones - Información detallada

Información de parámetros	
<b>Parámetro</b>	Fully-qualified Connection network name (necesario para cada red de conexiones definida)
<b>Valores válidos</b>	<p>Una serie de 1 a 8 caracteres:</p> <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul> <p><b>Nota:</b> El nombre de una red de conexiones existente, a la que este nodo vaya a pertenecer, con los caracteres especiales @, \$ y # del juego de caracteres A también está soportado; no obstante, estos caracteres no deben utilizarse para nuevos nombres de red de conexiones.</p>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	<p>Este parámetro especifica el nombre calificado al completo de la red de conexiones que se está definiendo en este nodo de red direccionador. Puesto que este nombre se convierte en el nombre de CP del nodo de direccionamiento virtual (VRN), el nombre debe ser exclusivo entre todos los nombres de CP y de LU de la red APPN (como en el nombre de punto de control local).</p> <p>Todos los nodos que son miembros de una red de conexiones determinada deben utilizar el mismo nombre de VRN.</p> <p>El nombre de VRN calificado al completo (nombre de CP del VRN) tiene el formato:</p> <p style="padding-left: 40px;"><i>IDRed.NombRedConexiones</i>, donde <i>IDRed</i> es el identificador de red de este nodo de red direccionador.</p>
<b>Parámetro</b>	Port type (necesario)
<b>Valores válidos</b>	<p>Token-ring, Ethernet, Frame Relay BAN, IP, ATM</p> <p><b>Nota:</b> Si <b>port type</b> es IP, no se le especificará <b>port name</b> porque sólo hay un puerto IP.</p>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	<p>Este parámetro especifica el tipo de puerto que proporciona conectividad al SATF para la red de conexiones que se está definiendo. Una red de conexiones determinada sólo da soporte a un tipo de puerto con un conjunto de características.</p>

Tabla 32 (Página 2 de 3). Lista de parámetros de configuración - Red de conexiones - Información detallada

Información de parámetros	
<b>Parámetro</b>	Port name (necesario)
<b>Valores válidos</b>	El nombre de un puerto en el que se haya habilitado el direccionamiento de APPN.  <b>Nota:</b> Si <b>port type</b> es IP, no se le especificará <b>port name</b> porque sólo hay un puerto IP.
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre de un puerto que proporciona conectividad al recurso de transporte de acceso compartido (SATF) para la red de conexiones que se está definiendo.  Todos los puertos definidos para una red de conexiones determinada deben ser del mismo tipo y tener las mismas características.  <b>Nota:</b> Si <b>port type</b> es IP, los puertos adicionales añadidos a una red de conexiones IP pueden ser cualquier puerto que IP utilice por definición.  Como mínimo, debe añadirse un puerto adicional además del puerto IP para utilizar la red de conexiones.  Puesto que el puerto IP es un pseudopuerto que siempre se activa cuando se inicializa el nodo, deben añadirse los puertos reales en que esté definido IP (TR, ATM,FR, ...) a la CN. Cuando está activo uno de estos puertos reales como mínimo, se supone que el enlace de red de conexiones está activo. Cuando están inactivos todos estos puertos reales, se supone que el enlace de red de conexiones está inactivo.
<b>Parámetro</b>	Limited Resource Timer
<b>Valores válidos</b>	De 1 a 216000 segundos
<b>Valor por omisión</b>	180
<b>Descripción</b>	Este parámetro especifica el valor de temporizador asociado con un recurso limitado.
<b>Parámetro</b>	DLCI number
<b>Valores válidos</b>	Del 16 al 1007
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el número de DLCI utilizado por el direccionador para conectarse a la red Frame Relay. Cuando el direccionador inicie una conexión con una estación de enlace en la LAN mediante la red de conexiones, utilizará este número de DLCI para conectarse a la red Frame Relay.

Tabla 32 (Página 3 de 3). Lista de parámetros de configuración - Red de conexiones - Información detallada

Información de parámetros	
<b>Parámetro</b>	BAN destination address (BDA)
<b>Valores válidos</b>	Del X'0000 0000 0000' al X'7FFF FFFF FFFF'
<b>Valor por omisión</b>	X'0000 0000 0000'
<b>Descripción</b>	Este parámetro especifica la dirección de destino de BAN configurada en el nodo que realice la función BAN. Si desea utilizar la función de puente para conectar la red LAN a la red Frame Relay, especifique X'0000 0000 0000' como valor de este parámetro. En este caso, la dirección MAC notificada a la topología de APPN para el TG de red de conexiones es la dirección MAC BNI codificada en el puerto APPN asociado con esta definición de red de conexiones.

Tabla 33 (Página 1 de 4). Lista de parámetros de configuración - Configuración de red de conexiones para ATM

Información de parámetros	
<b>Parámetro</b>	Port name (necesario)
<b>Valores válidos</b>	El nombre de un puerto en el que se haya habilitado el direccionamiento de APPN.
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre de un puerto que proporciona conectividad al recurso de transporte de acceso compartido (SATF) para la red de conexiones que se está definiendo.  Todos los puertos definidos para una red de conexiones determinada deben ser del mismo tipo y tener las mismas características.
<b>Parámetro</b>	fully-qualified connection network name
<b>Valores válidos</b>	Una serie de 3 a 17 caracteres con el formato de <i>IDred.nombCN</i> , donde: <ul style="list-style-type: none"> <li>• <i>IDred</i> es un ID de red de 1 a 8 caracteres</li> <li>• <i>nombCN</i> es un nombre de red de conexiones de 1 a 8 caracteres</li> </ul> Cada nombre debe ajustarse a las normas siguientes: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre de CN calificado al completo para el que se define este TG.
<b>Parámetro</b>	Connection network TG number
<b>Valores válidos</b>	Del 1 al 239
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el número de TG que identifica de manera exclusiva a esta conexión del puerto local a la CN. El par formado por nombre de CN y número de TG debe ser exclusivo.

## Mandatos de configuración de APPN

<i>Tabla 33 (Página 2 de 4). Lista de parámetros de configuración - Configuración de red de conexiones para ATM</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Limited Resource
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	Este parámetro indica si debe desactivarse este TG cuando no esté en uso para el tráfico de sesiones.
<b>Parámetro</b>	Limited Resource Timer
<b>Valores válidos</b>	De 1 a 2 160 000 segundos
<b>Valor por omisión</b>	180 segundos
<b>Descripción</b>	Este parámetro indica el límite de tiempo después del cual deberá desactivarse este TG de CN cuando no esté en uso para el tráfico de sesiones.
<b>Parámetro</b>	LDLC retry count
<b>Valores válidos</b>	Del 1 al 255
<b>Valor por omisión</b>	3
<b>Descripción</b>	Este parámetro se utiliza junto con el período del temporizador de LDLC para proporcionar una entrega de XID fiable. La cuenta de reintentos se inicializa la primera vez que se transmite un mandato o una petición sobre el enlace. Si el período del temporizador de LDLC caduca antes de que se reciba una respuesta, se retransmite el mandato o respuesta, disminuye la cuenta de reintentos y se reinicia el período del temporizador de LDLC. Si el temporizador caduca con la cuenta de reintentos de 0, se supone que el enlace no es operativo.
<b>Parámetro</b>	LDLC Timer Period
<b>Valores válidos</b>	De 1 a 255 segundos
<b>Valor por omisión</b>	Para ATM: 1 segundo Para IP: 15 segundos
<b>Descripción</b>	Este parámetro especifica el período del temporizador que se utiliza con <b>LDLC retry count</b> .

Tabla 33 (Página 3 de 4). Lista de parámetros de configuración - Configuración de red de conexiones para ATM

Información de parámetros	
<b>Parámetro</b>	Broadband Bearer Class
<b>Valores válidos</b>	Class_A, Class_C o Class_X
<b>Valor por omisión</b>	Class_X
<b>Descripción</b>	Este parámetro especifica la clase portadora solicitada de la red ATM. Las clases se definen:  <b>Class A</b> Velocidad en bits constante (CBR) con requisitos de temporización de final a final  <b>Class C</b> Velocidad en bits variable (VBR) sin requisitos de temporización de final a final  <b>Class X</b> Servicio que permite unos requisitos de temporización y tipo de tráfico definidos por el usuario
<b>Parámetro</b>	Shareable Regular Network traffic
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	Si es una CN Mayor Eficacia, Yes. De lo contrario, No.
<b>Descripción</b>	Este parámetro especifica si puede direccionarse tráfico de este TG de red de conexiones en un VC ATM configurado para un TG normal u otro TG de CN.
<b>Parámetro</b>	Shareable other protocol traffic
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si el VC ATM establecido para este TG de CN puede compartirse con otros protocolos de nivel superior en el direccionador.
<b>Nota:</b> Los parámetros siguientes son parámetros del tráfico hacia adelante.	
<b>Parámetro</b>	Forward Peak Cell Rate
<b>Valores válidos</b>	De un 1 a un 85% de la velocidad de línea
<b>Valor por omisión</b>	Se toma de la definición de puerto
<b>Descripción</b>	Este parámetro indica un límite superior para la velocidad de transmisión de las células.
<b>Parámetro</b>	Forward Sustained Cell Rate
<b>Valores válidos</b>	De un 1 a un 85% de la velocidad de línea
<b>Valor por omisión</b>	Se toma de la definición de puerto
<b>Descripción</b>	Este parámetro indica un límite superior para la velocidad media de transmisión de las células.

## Mandatos de configuración de APPN

<i>Tabla 33 (Página 4 de 4). Lista de parámetros de configuración - Configuración de red de conexiones para ATM</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Forward Tagging
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	Este parámetro indica que las células que no se ajustan a la especificación de tráfico de prioridad de pérdida de célula 0 pero se ajustan a la especificación de tráfico de prioridad de pérdida de célula 1 se marcan y se permiten en la red ATM.
<b>Parámetro</b>	QoS
<b>Valores válidos</b>	CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, donde
	<b>CLASS_0</b> La clase sin especificar. La red no especifica ninguna QoS.
	<b>CLASS_1</b> El rendimiento es comparable al de una línea privada digital actual.
	<b>CLASS_2</b> Pensada para los paquetes de vídeo y audio de aplicaciones de teleconferencia y multimedia.
	<b>CLASS_3</b> Pensada para la interoperación de los protocolos orientados a las conexiones, como, por ejemplo, Frame Relay.
	<b>CLASS_4</b> Pensada para la interoperación de los protocolos sin conexiones, como, por ejemplo, IP.
<b>Valor por omisión</b>	CLASS_3
<b>Descripción</b>	Este parámetro indica qué clase de servicio se proporciona a una conexión virtual ATM.

<i>Tabla 34 (Página 1 de 3). Lista de parámetros de configuración - Características de TG (Red de conexiones)</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Cost per connect time
<b>Valores válidos</b>	Del 0 al 255
<b>Valor por omisión</b>	0
<b>Descripción</b>	Este parámetro expresa el coste relativo del mantenimiento de una conexión sobre el TG asociado. Las unidades están definidas por el usuario y, normalmente, se basan en las tarifas aplicables del recurso de transmisión que se utiliza. Los valores asignados deben reflejar el gasto real del mantenimiento de una conexión sobre el TG en relación con todos los otros TG de la red. Un valor de cero significa que las conexiones sobre el TG pueden realizarse sin coste adicional (como es el caso de muchos recursos no conmutados). Los valores más elevados representan costes más elevados.



Tabla 34 (Página 2 de 3). Lista de parámetros de configuración - Características de TG (Red de conexiones)

Información de parámetros	
<b>Parámetro</b>	Cost per byte
<b>Valores válidos</b>	Del 0 al 255
<b>Valor por omisión</b>	0
<b>Descripción</b>	Este parámetro expresa el coste relativo de la transmisión de un byte sobre el TG asociado. Las unidades están definidas por el usuario y el valor asignado debe reflejar los gastos reales en los que se incurra para la transmisión sobre el TG en relación con todos los otros TG de la red. Un valor de cero significa que los bytes pueden transmitirse sobre el TG sin coste adicional. Los valores más elevados representan costes más elevados.
<b>Parámetro</b>	Security
<b>Valores válidos</b>	<p>Nonsecure – todo lo demás (por ejemplo, conectado a satélite o ubicado en una zona no segura).</p> <p>Public switched network – seguridad en el sentido de que la ruta no está predeterminada.</p> <p>Underground cable – ubicado en una zona segura (según lo que determina el administrador de la red).</p> <p>Secure conduit – no protegido (por ejemplo, un conducto presurizado).</p> <p>Guarded conduit – protegido contra infiltraciones físicas.</p> <p>Encrypted – se proporciona cifrado de nivel de enlace.</p> <p>Guarded radiation – conducto protegido que contiene el medio de transmisión; protegido contra infiltraciones físicas e infiltraciones de la radiación.</p>
<b>Valor por omisión</b>	Nonsecure
<b>Descripción</b>	Este parámetro indica el nivel de protección de seguridad asociado con el TG. Si son necesarios unos atributos de seguridad diferentes de los definidos estructuralmente, puede utilizarse una de las características de TG definidas por el usuario para especificar valores adicionales.
<b>Parámetro</b>	Propagation delay
<b>Valores válidos</b>	<ul style="list-style-type: none"> <li>• Minimum LAN – menos de 480 microsegundos</li> <li>• Telephone – entre 0,48 y 49,152 milisegundos</li> <li>• Packet switched – entre 49,152 y 245,76 milisegundos</li> <li>• Satellite – superior al máximo de 245,76 milisegundos</li> </ul>
<b>Valor por omisión</b>	LAN
<b>Descripción</b>	Este parámetro especifica el rango aproximado para el período de tiempo que tarda una señal en propagarse de un extremo a otro del TG.

<i>Tabla 34 (Página 3 de 3). Lista de parámetros de configuración - Características de TG (Red de conexiones)</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Effective capacity
<b>Valores válidos</b>	2 dígitos hexadecimales en el rango del X'00' al X'FF'
<b>Valor por omisión</b>	X'75'
<b>Descripción</b>	<p>Este parámetro especifica la velocidad máxima efectiva de transmisión de los bits para este TG de red de conexiones. La capacidad efectiva especifica la velocidad máxima efectiva para los enlaces físicos y los enlaces lógicos.</p> <p>La capacidad efectiva se codifica como una representación de un solo byte. Los valores X'00' y X'FF' son casos especiales que se utilizan para denotar la capacidad mínima y la máxima. El rango de la codificación es muy grande; no obstante, sólo pueden especificarse 256 valores del mismo.</p>
<b>Parámetro</b>	First user-defined characteristic
<b>Valores válidos</b>	Del 0 al 255
<b>Valor por omisión</b>	128
<b>Descripción</b>	Este parámetro especifica la primera de las tres características adicionales que los usuarios pueden definir para describir los TG en la red. El valor por omisión de 128 permite que se defina un subconjunto de TG como más o menos conveniente que el resto sin definir valores para todos los TG.
<b>Parámetro</b>	Second user-defined characteristic
<b>Valores válidos</b>	Del 0 al 255
<b>Valor por omisión</b>	128
<b>Descripción</b>	Este parámetro especifica la segunda de las tres características adicionales que los usuarios pueden definir para describir los TG en la red. El valor por omisión de 128 permite que se defina un subconjunto de TG como más o menos conveniente que el resto sin definir valores para todos los TG.
<b>Parámetro</b>	Third user-defined characteristic
<b>Valores válidos</b>	Del 0 al 255
<b>Valor por omisión</b>	128
<b>Descripción</b>	Este parámetro especifica la tercera de las tres características adicionales que los usuarios pueden definir para describir los TG en la red. El valor por omisión de 128 permite que se defina un subconjunto de TG como más o menos conveniente que el resto sin definir valores para todos los TG.

### Sintaxis:

add                      mode

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

Tabla 35. Lista de parámetros de configuración - COS de APPN - Correlación de nombre de modalidad con nombre de COS - Información detallada

Información de parámetros	
<b>Parámetro</b>	Mode name (necesario)
<b>Valores válidos</b>	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul>
<b>Nota:</b>	Un nombre de modalidad existente de una red existente, a la que este nodo de red direccionador vaya a pertenecer, con los caracteres especiales @, \$ y # del juego de caracteres A también está soportado; no obstante, estos caracteres no deben utilizarse para nuevos nombres de modalidad.
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre de modalidad para la correlación de nombre de modalidad con nombre de COS que se está definiendo. Consulte la sección "Opciones de CoS" en la página 40 para obtener información adicional sobre la correlación de nombre de modalidad con COS.
<b>Parámetro</b>	COS name (necesario)
<b>Valores válidos</b>	El nombre de una definición de COS establecida anteriormente, que se selecciona de la lista de nombres de COS definidos para este nodo de red direccionador.
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre de COS a asociar con el nombre de modalidad definido para esta correlación de nombre de modalidad con nombre de COS.
<b>Parámetro</b>	Session-level pacing Command Line option size
<b>Valores válidos</b>	Del 1 al 63
<b>Valor por omisión</b>	7
<b>Descripción</b>	Este parámetro especifica el tamaño de la opción de ritmo de nivel de sesión de la línea de mandatos. Este parámetro tiene definiciones diferentes según el tipo de ritmo utilizado: <ul style="list-style-type: none"> <li>• Para el ritmo de nivel de sesión fijo: <ul style="list-style-type: none"> <li>– El parámetro Session-level pacing Command Line option size especifica la opción de ritmo de recepción de la línea de mandatos para este nodo.</li> <li>– El valor de este parámetro es la opción de ritmo de recepción de la línea de mandatos que se sugiere para el nodo adyacente.</li> </ul> </li> <li>• Para el ritmo de nivel de sesión adaptable: <ul style="list-style-type: none"> <li>– El parámetro Session-level pacing Command Line option size especifica un parámetro de ajuste a utilizar como el tamaño mínimo para los mensajes de ritmo aislados que envíen los nodos adyacentes.</li> </ul> </li> </ul>

#### Sintaxis:

## Mandatos de configuración de APPN

add

additional-port-to-connection-network

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

**Nota:** Puede tener un máximo de 5 puertos por definición de red de conexiones.

Tabla 36. Lista de parámetros de configuración - Puerto adicional APPN para red de conexiones

Información de parámetros	
<b>Parámetro</b>	Connection network name (fully-qualified) (necesario para cada red de conexiones definida)
<b>Valores válidos</b>	<p>Una serie de 1 a 8 caracteres:</p> <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul> <p><b>Nota:</b> El nombre de una red de conexiones existente, a la que este nodo vaya a pertenecer, con los caracteres especiales @, \$ y # del juego de caracteres A también está soportado; no obstante, estos caracteres no deben utilizarse para nuevos nombres de red de conexiones.</p>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	<p>Este parámetro especifica el nombre de la red de conexiones que se está definiendo en este nodo de red direccionador. Puesto que este nombre se convierte en el nombre de CP del nodo de direccionamiento virtual (VRN), el nombre debe ser exclusivo entre todos los nombres de CP y de LU de la red APPN (como en el nombre de punto de control local).</p> <p>Todos los nodos que son miembros de una red de conexiones determinada deben utilizar el mismo nombre de VRN.</p> <p>El nombre de VRN calificado al completo (nombre de CP del VRN) tiene el formato:</p> <p style="padding-left: 40px;"><i>IDRed.NombRedConexiones</i>, donde <i>IDRed</i> es el identificador de red de este nodo de red direccionador.</p>
<b>Parámetro</b>	Port name
<b>Valores válidos</b>	<p>Un nombre sin calificar exclusivo que genera automáticamente la línea de mandatos.</p> <p>El nombre estará compuesto por:</p> <ul style="list-style-type: none"> <li>• TR (token-ring, que es la Red en Anillo)</li> <li>• EN (Ethernet)</li> </ul>
<b>Valor por omisión</b>	Un nombre sin calificar generado por la línea de mandatos.
<b>Descripción</b>	<p>Este parámetro especifica el nombre que representa a este puerto.</p> <p>Cuando la red de conexiones a la que se añade el puerto es IP, sólo podrán añadirse a la CN IP los puertos en los que IP tenga una interfaz por definición. Debe añadirse a la CN IP un mínimo de un puerto real que tenga definido IP para activar y utilizar la CN.</p>

**Sintaxis:**

add

focal\_point

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

Tabla 37. Lista de parámetros de configuración - Punto focal implícito APPN

Información del parámetro	
<b>Parámetro</b>	focal point
<b>Valores válidos</b>	Un nombre de CP calificado al completo
<b>Valor por omisión</b>	Blancos
<b>Descripción</b>	Este parámetro especifica el nombre de CP calificado al completo que representa a este punto focal.  El primer punto focal que se añade es el punto focal implícito primario. Puede añadirse un máximo de 8 puntos focales implícitos de reserva adicionales invocando <b>Add focal_point</b> diversas veces. Si se elimina el punto focal implícito primario de la lista de puntos focales con <b>Delete focal_point</b> , el primer punto focal implícito de reserva, si lo hay, se convierte en el punto focal implícito primario.

**Sintaxis:**

add

local-pu

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

Tabla 38 (Página 1 de 3). Lista de parámetros de configuración - PU local de APPN

Información de parámetros	
<b>Parámetro</b>	Station name
<b>Valores válidos</b>	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre que representa al enlace entre el DLUR y la PU.
<b>Parámetro</b>	Primary DLUS name
<b>Valores válidos</b>	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre a utilizar para alterar temporalmente el DLUS primario configurado para este nodo.

<i>Tabla 38 (Página 2 de 3). Lista de parámetros de configuración - PU local de APPN</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Secondary DLUS name
<b>Valores válidos</b>	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre a utilizar para alterar temporalmente el DLUS secundario configurado para este nodo.
<b>Parámetro</b>	Autoactivate
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	Este parámetro especifica si se va a activar este enlace en el arranque. <p><b>Nota:</b> Si el enlace local se utilizará para una PU de DDDLU, debe especificar <i>yes</i> para esta pregunta.</p> <p>Si el enlace local no se establece en Autoactivate, fallará el primer intento de utilizar la PU local (es decir, el primer intento de establecer una sesión de TN3270) porque el enlace todavía no está activo. Aunque falle este intento, hace que se active el enlace, el cual se encontrará disponible para el siguiente intento. Puesto que el enlace se activa cuando se establece la sesión de SSCP-PU, que es cuando el enlace se identifica como enlace de DDDLU, no puede establecerse ninguna sesión de DDDLU hasta que el enlace se identifique como enlace de DDDLU.</p>
<b>Parámetro</b>	Enable Host Initiated Dynamic LU Definition
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro indica si se crearán o no LU dependientes de manera dinámica (en contraposición a que tengan que configurarse). Si se especifica <i>yes</i> , se definirán LU para esta PU al recibirse peticiones ACTLU (con CV0E). No es necesario configurar LU para el Servidor TN3270E.

Tabla 38 (Página 3 de 3). Lista de parámetros de configuración - PU local de APPN

Información de parámetros	
<b>Parámetro</b>	Pool Name for Host-initiated Dynamic LUs
<b>Valores válidos</b>	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z, \$, #, @ o &lt;</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9, \$, #, @, &gt; o &lt;</li> </ul>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	<p>Este parámetro especifica el nombre de una agrupación a crear para que contenga LU activadas por el sistema principal en esta PU local. Este parámetro sólo es aplicable si <b>Enable Host Initiated Dynamic LU Definition</b> es <i>yes</i>.</p> <p>No es necesario utilizar el mandato <b>add implicit-pool</b> para definir esta agrupación; basta con especificar el nombre y otros parámetros aquí para que se cree la agrupación.</p> <p>Si entra un nombre de agrupación, se le solicitará que entre valores para los parámetros siguientes:</p> <ul style="list-style-type: none"> <li>• Pool class (vea la Tabla 43 en la página 223)</li> <li>• LU type (vea la Tabla 43 en la página 223)</li> </ul> <p>Puede proporcionar el mismo nombre de agrupación para diversas PU locales si lo desea.</p> <p>Si especifica información de agrupación, causa que las LU iniciadas por sistema principal que todavía no se han configurado en el direccionador se coloquen en la agrupación especificada. Después se les pueden asignar clientes TN3270 solicitando el nombre de agrupación o correlacionando puertos de destino o direcciones IP de cliente con esta agrupación.</p> <p>Si no especifica información de agrupación, estas LU iniciadas por sistema principal reciben el tratamiento de LU explícitas y sólo se pueden asignar a clientes que las soliciten por el nombre de LU individual.</p>
<b>Parámetro</b>	Send Terminate-Self when TN3270 Client Disconnects
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro indica si se enviará o no una petición terminate_self al SSCP cuando se desconecte el cliente TN3270. Si se especifica <i>yes</i> , se enviará terminate_self y el sistema principal será el responsable de terminar la sesión de LU-LU (es decir, la SLU NO enviará una petición UNBIND).

**Sintaxis:**

add                      routing\_list

**Nota:** Estas preguntas sólo aparecen si ha configurado el nodo como nodo de frontera.

Hay una serie de teclas de atajo de edición disponibles para agilizar la modificación de los datos existentes en una lista de

## Mandatos de configuración de APPN

direccionamiento configurada anteriormente. Pueden utilizarse estas teclas de atajo cuando aparezcan las solicitudes Destination LU y Routing CP.

- Pulsando sólo **Intro** retendrá el nombre visualizado actualmente.
- La **barra espaciadora** seguida de **Intro** suprimirá el nombre visualizado actualmente.
- Si entra una serie de datos de caracteres y después pulsa **Intro**, sustituirá el nombre visualizado actualmente por los nuevos datos de caracteres.
- El número **9** seguido de **Intro** hará saltar hasta el final de la lista, donde pueden añadirse nuevos nombres.
- Al final de la lista, pulsando sólo **Intro** completará la lista.

<i>Tabla 39 (Página 1 de 3). Lista de parámetros de configuración - Configuración de lista de direccionamiento</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Routing list name
<b>Valores válidos</b>	Una serie de caracteres de un máximo de 20 caracteres de longitud sin incluir blancos. Están permitidos caracteres especiales y la mezcla de mayúsculas y minúsculas.
<b>Valor por omisión</b>	Blanco
<b>Descripción</b>	Este parámetro identifica a una lista de direccionamiento específica para la modificación, listado o supresión por medio del código de configuración. El código operativo no lo utiliza. Pueden configurarse hasta 255 listas de direccionamiento de acuerdo con la disponibilidad de la memoria de la configuración. Se respetan las mayúsculas y minúsculas.
<b>Parámetro</b>	Subnet visit count
<b>Valores válidos</b>	Del 1 al 255
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro de nivel de nodo correspondiente
<b>Descripción</b>	Este parámetro especifica cuántas redes puede atravesar el procedimiento de búsqueda Locate.
<b>Parámetro</b>	Dynamic routing list updates
<b>Valores válidos</b>	0 (none) 1 (full) 2 (limited)
<b>Valor por omisión</b>	El valor por omisión se toma del parámetro de nivel de nodo correspondiente
<b>Descripción</b>	Este parámetro controla si pueden añadirse entradas automáticamente a la lista de direccionamiento de subred temporal del nodo. Puede establecerse en los mismos valores que el parámetro de nivel de nodo análogo. Si se habilita esta función, las entradas añadidas automáticamente sólo se añaden a la copia temporal de la lista de direccionamiento.



Tabla 39 (Página 2 de 3). Lista de parámetros de configuración - Configuración de lista de direccionamiento

Información de parámetros	
<b>Parámetro</b>	Enable routing list optimization
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	Indica si se permite que el nodo reordene la lista de direccionamiento de subredes de manera que vayan en primer lugar las entradas con más probabilidades de obtener un resultado satisfactorio. Esta reordenación se produce en la copia temporal interna de la lista de direccionamiento.
<b>Parámetro</b>	Destination LU found via this list
<b>Valores válidos</b>	<p>Un nombre de LU calificado al completo con comodín de cola opcional. Los caracteres permitidos para el nombre de LU son: A-Z, @, \$, #, 0-9.</p> <p>El primer carácter de la parte del NETID y el primero de la parte del nombre de LU no deben ser numéricos.</p> <p>Cualquiera de los nombres de LU de FQ puede terminar con el carácter comodín "*" para designar el rango de LU. Por ejemplo,</p> <ul style="list-style-type: none"> <li>• *</li> <li>• NETI*</li> <li>• NETI.LUA*</li> </ul>
<b>Valor por omisión</b>	Blanco
<b>Descripción</b>	<p>Este parámetro especifica la lista de las LU de destino que pueden encontrarse mediante esta lista de direccionamiento.</p> <p>Esta pregunta se repetirá hasta que se termine con una entrada de valor nulo.</p> <p><b>Notas:</b></p> <ol style="list-style-type: none"> <li>1. Sólo una entrada entre todas las listas de direccionamiento puede tener un "*" autónomo. Éste coincidirá con todas las LU, y la lista de direccionamiento que lo contenga se conocerá como la lista de direccionamiento por omisión.</li> <li>2. Todas las teclas de atajo de edición descritas al principio de esta tabla están disponibles para agilizar la modificación de una lista de CP de direccionamiento configurada anteriormente.</li> <li>3. No puede duplicarse ningún nombre de LU determinado en otra lista de direccionamiento.</li> <li>4. El número máximo de nombres de LU que puede especificar: <ul style="list-style-type: none"> <li>• 2216 - 126</li> </ul> </li> </ol>

Tabla 39 (Página 3 de 3). Lista de parámetros de configuración - Configuración de lista de direccionamiento

Información de parámetros	
<b>Parámetro</b>	Routing CP and optional subnet visit count
<b>Valores válidos</b>	<p>Un nombre de CP calificado al completo que consta de 1 a 17 caracteres seguido de una cuenta opcional de visitas a subred numérica. Los caracteres permitidos para el nombre de CP son: A-Z, @, \$, #, 0-9</p> <p>El primer carácter de la parte del NETID y el primero de la parte del nombre de CP no deben ser numéricos. El rango de la cuenta opcional de visitas a subred va del 1 al 255 y debe estar separado del nombre de CP calificado al completo por uno o más espacios.</p>
<b>Valor por omisión</b>	Un blanco para el nombre de CP calificado al completo y el valor de nivel de nodo para la cuenta de visitas a subred.
<b>Descripción</b>	<p>Este parámetro especifica una lista de uno o más nombres de CP calificados al completo para CP que pueden tener conocimiento de cómo acceder a una, o más, de las LU de destino configuradas anteriormente.</p> <p>Cada una de las siguientes palabras clave especiales puede utilizarse una vez en cualquier lista de direccionamiento dada:</p> <ul style="list-style-type: none"> <li>• "*" - equivale a especificar todos los BN nativos, todos los BN no nativos adyacentes y todos los NN no nativos adyacentes</li> <li>• "**SELF" - equivale a especificar el nombre de CP calificado al completo del nodo local</li> <li>• "**EBNS" - equivale a especificar todos los BN nativos</li> </ul> <p>Esta pregunta se repetirá hasta que se termine con una entrada de valor nulo.</p> <p><b>Notas:</b></p> <ol style="list-style-type: none"> <li>1. Todas las teclas de atajo de edición descritas al principio de esta tabla están disponibles para agilizar la modificación de una lista de CP de direccionamiento configurada anteriormente.</li> <li>2. Si configura "**SELF" como nombre de CP, no puede configurar el nombre de CP del nodo local.</li> <li>3. Cualquier lista de direccionamiento dada puede tener el siguiente número máximo de nombres de CP y palabras clave: <ul style="list-style-type: none"> <li>• 2216 - 144</li> </ul> </li> <li>4. Entre todas las listas de direccionamiento, no puede utilizar más nombres de CP y palabras clave diferentes de los que indique el número siguiente: <ul style="list-style-type: none"> <li>• 2216 - 144</li> </ul> </li> <li>5. Ningún nombre de CP o palabra clave en particular puede aparecer en más de 255 listas de direccionamiento.</li> </ol>

**Sintaxis:**

add                      cos\_mapping\_table

**Nota:** Estas preguntas sólo aparecen si ha configurado el nodo como nodo de frontera.

Las teclas de atajo de edición especificadas al principio de la tabla sobre las listas de direccionamiento también son válidas aquí. Utilícelas para agilizar la modificación de los nombres de CP no nativos y pares de nombres de COS.

Tabla 40 (Página 1 de 2). Lista de parámetros de configuración - Configuración de tabla de correlación de COS

Información de parámetros	
<b>Parámetro</b>	COS mapping table name
<b>Valores válidos</b>	Una serie de caracteres de un máximo de 20 caracteres de longitud sin incluir blancos. Están permitidos caracteres especiales y la mezcla de mayúsculas y minúsculas.
<b>Valor por omisión</b>	Blanco
<b>Descripción</b>	Este parámetro identifica a una tabla de correlación de COS específica. Le permite identificar la tabla para la modificación, listado o supresión por medio del software de configuración. El software operativo no lo utiliza. Pueden configurarse hasta 255 tablas de correlación de COS de acuerdo con la disponibilidad de la memoria de la configuración. Se respetan las mayúsculas y minúsculas.
<b>Parámetro</b>	Non-native NETID or CP name
<b>Valores válidos</b>	Un nombre de CP calificado al completo con comodín de cola opcional. Los caracteres permitidos para el nombre de CP son: A-Z, @, \$, #, 0-9  El primer carácter de la parte del NETID y el primero de la parte del nombre de CP no deben ser numéricos. Cualquiera de los nombres de CP calificados al completo puede terminar con el carácter comodín "*" para designar un rango de CP. Por ejemplo: <ul style="list-style-type: none"> <li>• *</li> <li>• NET1*</li> <li>• NET1.LUA*</li> </ul>
<b>Valor por omisión</b>	Blanco
<b>Descripción</b>	Este parámetro especifica una lista de una o más redes no nativas a las que se aplica esta tabla de correlación. Esta pregunta se repite hasta que se termina con una entrada de valor nulo.
	<b>Notas:</b>
	<ol style="list-style-type: none"> <li>1. Sólo una entrada entre todas las listas de direccionamiento puede tener un "*" autónomo. Éste coincidirá con todas las redes no nativas, y se conocerá como la lista de direccionamiento por omisión.</li> <li>2. No puede duplicarse ningún nombre de CP determinado en otra tabla de correlación de COS.</li> <li>3. El número máximo de nombres de CP que puede especificar: <ul style="list-style-type: none"> <li>• 2216 - 126</li> </ul> </li> </ol>

Tabla 40 (Página 2 de 2). Lista de parámetros de configuración - Configuración de tabla de correlación de COS

Información de parámetros	
<b>Parámetro</b>	Native and non-native COS-name pair
<b>Valores válidos</b>	<p>Un par de nombres de COS separados por un blanco. Los caracteres permitidos son: A-Z, @, \$, #, 0-9</p> <p>El primer carácter de cada nombre no debe ser numérico.</p>
<b>Valor por omisión</b>	Blanco
<b>Descripción</b>	<p>Este parámetro identifica a un par de nombres de COS. Un nombre de COS nativo va seguido del nombre de COS no nativo correspondiente.</p> <p>Para cualquier tabla de correlación de COS dada, en uno de los pares de nombres de COS puede especificarse el nombre de COS no nativo como “*”. Éste designa la entrada por omisión a utilizar para todos los nombres de COS no nativos que no coincidan explícitamente con otra entrada de la tabla.</p> <p>Un par de nombres de COS no puede coincidir exactamente con otro par de nombres de COS en una tabla determinada. No obstante, un nombre de COS nativo determinado puede utilizarse en diversas entradas, y también es posible que un nombre de COS no nativo determinado se utilice en diversas entradas. El software operativo utilizará la primera entrada que encuentre.</p> <p>Esta pregunta se repetirá hasta que se termine con una entrada de valor nulo.</p> <p><b>Notas:</b></p> <ol style="list-style-type: none"> <li>1. Los nombres nativos y los no nativos no pueden ser idénticos. Sólo deben especificarse nombres de COS que deban cambiarse.</li> <li>2. Un nombre de COS nativo o no nativo determinado puede aparecer en diversas entradas, pero no puede tener dos pares de nombres de COS idénticos.</li> <li>3. Si tiene diversos nombres de COS nativos en correlación con el mismo nombre de COS no nativo, el nodo de frontera utilizará la primera de estas correlaciones cuando tenga que correlacionar de no nativo a nativo. De manera similar, si tiene diversos nombres de COS no nativos en correlación con un nombre de COS nativo común, el nodo de frontera utilizará la primera de estas correlaciones cuando tenga que correlacionar de nativo a no nativo.</li> <li>4. Cualquier tabla de correlación de COS dada puede tener el siguiente número máximo de pares de nombres de COS: <ul style="list-style-type: none"> <li>• 2216 - 46</li> </ul> </li> <li>5. Entre todas las tablas de correlación de COS, no puede utilizar más nombres de COS nativos de los que indique el número siguiente: <ul style="list-style-type: none"> <li>• 2216 - 144</li> </ul> <p>No existe un límite análogo para los nombres de COS no nativos.</p> </li> <li>6. Ningún nombre de COS nativo determinado puede aparecer más de 255 veces entre todas las listas de direccionamiento.</li> </ol>

## Delete

Utilice el mandato **delete** para suprimir:

### Sintaxis:

delete                    port *nombre-puerto*  
link *nombre-estación-enlace*  
lu-name *nombre-lu*  
connection-network *nombre-red-conexiones*  
additional-port-to-connection-network *nombre-puerto-cn*  
mode *nombre*  
focal\_point *nombre-punto-focal*  
local-pu  
routing\_list *nombre de lista de direccionamiento*  
cos\_mapping\_table *nombre de tabla de correlación*

## List

Utilice el mandato **list** para listar:

### Sintaxis:

list                    all  
node  
traces  
management  
hpr  
dlur  
port (*nombre de puerto*)  
link station (*nombre de estación de enlace*)  
lu name *nombre de lu*  
mode name *nombre de modalidad*  
connection network *nombre de red de conexiones*  
focal\_point  
routing\_list *nombre de lista de direccionamiento*  
cos\_mapping\_table *nombre de tabla de correlación*

## Activate\_new\_config

Utilice el mandato **activate\_new\_config** para leer la configuración en la memoria permanente.

### Sintaxis:

activate\_new\_config

TN3270E

*Tabla 41. Resumen de los mandatos de configuración de TN3270E*

Mandato	Función	Vea la página:
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxxi.	
Set	tn3270e	220
Add	Añade o actualiza lo siguiente:	
	implicit-pool	223
	lu	225
	mapping	226
	port	228
Delete	Suprime lo siguiente:	229
	<ul style="list-style-type: none"> <li>• implicit-pool</li> <li>• lu</li> <li>• mapping</li> <li>• port</li> </ul>	
List all	Lista la memoria de la configuración	231
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxi.	

**Sintaxis:**

set

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

*Tabla 42 (Página 1 de 3). Lista de parámetros de configuración - Establecimiento de TN3270E*

Información de parámetros	
<b>Parámetro</b>	Enable TN3270E Server
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	Este parámetro especifica si se habilitará el soporte del Servidor TN3270E.

Tabla 42 (Página 2 de 3). Lista de parámetros de configuración - Establecimiento de TN3270E	
<b>Información de parámetros</b>	
<b>Parámetro</b>	TN3270E Server IP Address
<b>Valores válidos</b>	Se acepta cualquier dirección IP como entrada válida. No obstante, la dirección también debe estar configurada en IP como dirección de interfaz o como dirección IP interna del direccionador.
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro es la dirección IP asociada con el Servidor TN3270E.
<b>Parámetro</b>	Port number
<b>Valores válidos</b>	Del 1 al 65535
<b>Valor por omisión</b>	23
<b>Descripción</b>	Este parámetro especifica el número de puerto asociado con el Servidor TN3270E.
<b>Parámetro</b>	Enable Client IP address to LU name mapping?
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si se producirá la correlación de dirección IP de cliente con nombre de LU.
<b>Parámetro</b>	Default pool name
<b>Valores válidos</b>	Cualquier serie alfanumérica de 1 a 8 caracteres
<b>Valor por omisión</b>	PUBLIC
<b>Descripción</b>	Este parámetro especifica el nombre de la agrupación por omisión. Esta agrupación se utiliza cuando se conectan clientes TN3270 y no especifican un nombre de LU/agrupación.
<b>Parámetro</b>	NetDisp Advisor Port Number
<b>Valores válidos</b>	Del 1 al 65535
<b>Valor por omisión</b>	10008
<b>Descripción</b>	Este parámetro establece el número de puerto para el Network Dispatcher Advisor.
<b>Parámetro</b>	Keepalive type
<b>Valores válidos</b>	<ul style="list-style-type: none"> <li>0 None</li> <li>1 Timing mark</li> <li>2 NOP</li> </ul>
<b>Valor por omisión</b>	0
<b>Descripción</b>	<p>Este parámetro especifica el tipo de Keepalive.</p> <p>Un tipo de Keepalive de <i>Timing mark</i> requiere respuestas del cliente dentro del período de tiempo especificado en el parámetro <b>Timer</b>.</p> <p>Un tipo de Keepalive de <i>NOP</i> especifica que el cliente no devolverá una respuesta al mensaje Keepalive. Vendrá una notificación procedente de TCP de que el cliente ya no está.</p>

## Mandatos de configuración de APPN

<i>Tabla 42 (Página 3 de 3). Lista de parámetros de configuración - Establecimiento de TN3270E</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Frequency
<b>Valores válidos</b>	De 1 a 65535 segundos
<b>Valor por omisión</b>	60
<b>Descripción</b>	Este parámetro especifica la frecuencia con que se envía al cliente el mensaje Keepalive.
<b>Parámetro</b>	Timer
<b>Valores válidos</b>	De 1 a 65535 segundos
<b>Valor por omisión</b>	10
<b>Descripción</b>	Este parámetro establece el valor de temporizador a utilizar con la función Keepalive.
<b>Parámetro</b>	Automatic logoff
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si se habilitará la desconexión automática.
<b>Parámetro</b>	Time
<b>Valores válidos</b>	De 1 a 65535 minutos
<b>Valor por omisión</b>	30
<b>Descripción</b>	Este parámetro establece el período durante el cual el enlace TN3270E puede estar desocupado antes de que se desconecte automáticamente.
<b>Parámetro</b>	IPv4 Precedence
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro establece el valor de prioridad de IPv4, que permite la puesta en cola de los paquetes encapsulados de IPv4 con prioridad.
<b>Parámetro</b>	Enable LU Capping?
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro le permite determinar cuántas sesiones de TN3270 puede iniciar cada dirección IP. Si la respuesta a esta pregunta es <i>yes</i> , aparecerá la pregunta siguiente.
<b>Parámetro</b>	Max number of LUs per IP address
<b>Valores válidos</b>	0 - 65535
<b>Valor por omisión</b>	0
<b>Descripción</b>	Este parámetro establece el número máximo de sesiones de TN3270 que puede iniciar cada dirección IP de cliente.

### Sintaxis:



addimplicit-pool

Este mandato define una agrupación de LU en contraposición al mandato **add lu**, que añade una sola LU. Se le solicitará que entre valores para los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis ( ). El valor por omisión del parámetro se mostrará entre corchetes [ ].

<i>Tabla 43 (Página 1 de 2). Lista de parámetros de configuración - Adición de agrupación implícita de TN3270E</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Pool name
<b>Valores válidos</b>	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z, \$, #, @ o &lt;</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9, \$, #, @, &gt; o &lt;</li> </ul>
<b>Valor por omisión</b>	PUBLIC
<b>Descripción</b>	Este parámetro especifica el nombre de la agrupación de LU a utilizar cuando se conecten clientes TN3270.
<b>Parámetro</b>	Pool class
<b>Valores válidos</b>	1 ó 2, donde: <ol style="list-style-type: none"> <li>1. Implicit workstation</li> <li>2. Implicit printer</li> </ol>
<b>Valor por omisión</b>	1
<b>Descripción</b>	Este parámetro especifica el tipo de agrupación de LU.
<b>Parámetro</b>	Station name
<b>Valores válidos</b>	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre que representa al enlace entre el DLUR y la PU o al enlace de subárea por el que fluirán datos de SNA.
<b>Parámetro</b>	LU Name Mask
<b>Valores válidos</b>	Una serie de 1 a 5 caracteres: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z, @, \$ y #</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul>
<b>Valor por omisión</b>	@01LU
<b>Descripción</b>	Este parámetro especifica la máscara a utilizar para asegurarse de que los nombres de LU no sean duplicados de otros nombres en la red. <p>Los nombres de LU se generan añadiendo la dirección de NAU al final de la máscara de nombre de LU. Cuando no se especifique un rango de direcciones, se comprobarán las direcciones de NAU de la 2 a la 253 para ver si la dirección no se utiliza. Si la dirección está disponible, se utilizará. De lo contrario, se realizará un intento con la siguiente dirección de NAU.</p> <p>Por ejemplo, si la máscara de nombre de LU es FRED, los nombres de LU posibles son [FRED2, FRED3, ..., FRED253].</p>

## Mandatos de configuración de APPN

<i>Tabla 43 (Página 2 de 2). Lista de parámetros de configuración - Adición de agrupación implícita de TN3270E</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	LU type
<b>Valores válidos</b>	<ul style="list-style-type: none"> <li>• 1 - 3270 Mod 2 display</li> <li>• 2 - 3270 Mod 3 display</li> <li>• 3 - 3270 Mod 4 display</li> <li>• 4 - 3270 Mod 5 display</li> <li>• 5 - 3270 printer</li> <li>• 6 - SCS printer</li> </ul>
<b>Valor por omisión</b>	1
<b>Descripción</b>	Este parámetro especifica el tipo de LU dependiente para la LU que se añade.
<b>Parámetro</b>	Specify LU address range?
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si desea definir un rango de direcciones de LU.
<b>Parámetro</b>	LU address range
<b>Valores válidos</b>	Cualquier rango de valores del 1 al 255
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	<p>Este parámetro especifica el rango de direcciones de LU.</p> <p>El rango de direcciones de LU puede especificarse utilizando el formato siguiente:</p> <p style="text-align: center;">límite_inferior_dirección-límite_superior_dirección</p> <p>Si el primer valor no va seguido de un guión, se supone que este valor es una sola dirección de LU. Pueden entrarse diversos rangos, que estarán separados por comas. Por ejemplo, la serie siguiente especifica 2 rangos de direcciones y 2 direcciones de LU específicas:</p> <p style="text-align: center;">2-40,56,58,100-250</p>
<b>Parámetro</b>	Number of implicit workstation definitions
<b>Valores válidos</b>	Del 1 al 255
<b>Valor por omisión</b>	1
<b>Descripción</b>	Este parámetro especifica el número de LU dependientes a añadir a la agrupación implícita.

add

lu

Este mandato añade una LU específica. Se le solicitará que entre valores para los parámetros siguientes. El rango del parámetro se

mostrará entre paréntesis ( ). El valor por omisión del parámetro se mostrará entre corchetes [ ].

Información de parámetros	
<b>Parámetro</b>	LU name
<b>Valores válidos</b>	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z, @, \$ y #</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre de LU de la LU dependiente que se está definiendo.
<b>Parámetro</b>	NAU address
<b>Valores válidos</b>	Del 1 al 255
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica la dirección de NAU de la LU que se está definiendo.
<b>Parámetro</b>	Station name
<b>Valores válidos</b>	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre que representa al enlace entre el DLUR y la PU definida con el mandato <b>add local-pu</b> o al enlace de subárea por el que fluirán datos de SNA.
<b>Parámetro</b>	Class
<b>Valores válidos</b>	<ul style="list-style-type: none"> <li>1 Explicit Workstation</li> <li>2 Implicit Workstation</li> <li>3 Explicit Printer</li> <li>4 Implicit Printer</li> </ul>
<b>Valor por omisión</b>	1
<b>Descripción</b>	Este parámetro especifica la clase de LU.

## Mandatos de configuración de APPN

Tabla 44 (Página 2 de 2). Lista de parámetros de configuración - Adición de LU de TN3270E	
<b>Información de parámetros</b>	
<b>Parámetro</b>	LU type
<b>Valores válidos</b>	<ul style="list-style-type: none"> <li>• 1 — 3270 Mod 2 display</li> <li>• 2— 3270 Mod 3 display</li> <li>• 3 — 3270 Mod 4 display</li> <li>• 4 — 3270 Mod 5 display</li> <li>• 5 — 3270 printer</li> <li>• 6 — SCS printer</li> </ul>
<b>Valor por omisión</b>	1
<b>Descripción</b>	Este parámetro especifica el tipo de LU dependiente para la LU que se añade.
<b>Parámetro</b>	Implicit pool name
<b>Valores válidos</b>	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z, &lt;</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul>
<b>Valor por omisión</b>	<DEFLT>
<b>Descripción</b>	Este parámetro especifica el nombre de la agrupación implícita a utilizar en la definición de LU. Esta pregunta sólo aparece si <i>class</i> es una estación de trabajo implícita o una impresora implícita.
<b>Parámetro</b>	Define an associated printer
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si desea definir una impresora asociada.
<b>Parámetro</b>	Associated printer name
<b>Valores válidos</b>	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z, @, \$ y #</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre de la impresora asociada.
<b>Parámetro</b>	Associated printer NAU address
<b>Valores válidos</b>	Del 1 al 255
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica la dirección de NAU de la definición de LU de la impresora asociada.

### Sintaxis:

add                    map

Este mandato añade una correlación de dirección IP de cliente con nombre de LU. Se le solicitará que entre valores para los paráme-

tros siguientes. El rango del parámetro se mostrará entre paréntesis ( ). El valor por omisión del parámetro se mostrará entre corchetes [ ].

Se aplican las normas de correlación siguientes:

- Si una definición de correlación contiene una máscara de subred completa (255.255.255.255), lo que indicará que la entrada es para un cliente específico, y el cliente no solicita una LU/agrupación específica, puede hacerse un intento con cualquier LU/agrupación de la definición de correlación que coincida con el tipo de conexión.
- Si una definición de correlación no contiene una máscara de subred completa y no se solicita una LU/agrupación específica, sólo se realizarán intentos con entradas de agrupación en la definición de correlación. No puede crear una definición que correlacione una subred con una LU específica. Debe correlacionar la subred con una agrupación.
- Si se recibe una petición de conexión de un cliente y no hay ninguna entrada de correlación que coincida, se rechazará la petición.
- Puede añadirse una mezcla de tipos de agrupación y de LU a una correlación en particular. La selección del recurso se basará en el tipo de petición de conexión. El orden en que estén definidos los recursos en la correlación será el orden en que se elija para una petición de conexión en particular.
- Si una definición de correlación contiene un número de puerto de destino distinto de cero, sólo se comprobarán con esta correlación los clientes que se conecten a este puerto.

**Nota:** Cuando un cliente se conecte mientras esté habilitada la correlación, el servidor empezará por comparar la dirección IP del cliente con la máscara de subred de cada correlación secuencial. La coincidencia más larga entre la dirección IP de cliente de entrada y la definición de correlación determina con qué definición de correlación se hace el primer intento. Si todos los recursos elegibles de la definición de correlación están en uso y **final LU mapping connection attempt** es *no*, se busca de nuevo en las definiciones de correlación para hallar la siguiente coincidencia más específica.

<i>Tabla 45. Lista de parámetros de configuración - Adición de correlación de TN3270E</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Pool name/LU name
<b>Valores válidos</b>	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica un nombre de LU o un nombre de agrupación a correlacionar con la dirección IP. El nombre de LU sólo puede correlacionarse con una dirección de sistema principal. Si la máscara es una máscara de red, el nombre especificado debe ser un nombre de agrupación.
<b>Parámetro</b>	Client IP address or Network address
<b>Valores válidos</b>	Cualquier dirección IP válida
<b>Valor por omisión</b>	0.0.0.0
<b>Descripción</b>	Este parámetro especifica la dirección IP de la definición de correlación de red o cliente a añadir.
<b>Parámetro</b>	Address Mask
<b>Valores válidos</b>	Cualquier máscara de dirección IP válida
<b>Valor por omisión</b>	0.0.0.0
<b>Descripción</b>	Este parámetro especifica la máscara de dirección IP que el direccionador aplica a las direcciones IP de cliente de entrada y a las direcciones de red o IP de cliente configuradas para determinar si coinciden.
<b>Parámetro</b>	Port number
<b>Valores válidos</b>	Del 1 al 65535
	Si desea especificar un puerto en particular, debe seleccionar el valor de puerto de servidor TN3270 global definido con el mandato <b>set</b> o bien uno de los valores de puerto definidos con el mandato <b>add port</b> .
<b>Valor por omisión</b>	0
<b>Descripción</b>	Este parámetro especifica el número de puerto TCP de destino con el que un cliente TN3270 debe conectarse para que se compruebe esta entrada de correlación. Si el valor es cero, la entrada de correlación se aplica a las conexiones de cliente con cualquier número de puerto TCP definido.
<b>Parámetro</b>	Final LU mapping connection attempt
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si el direccionador debe continuar realizando intentos con entradas de correlación menos específicas en el caso de que una coincidencia de un cliente con esta entrada no haya podido dar como resultado una LU disponible válida.

### Sintaxis:

addport

Este mandato especifica un puerto adicional en el que pueda escuchar el Servidor TN3270E. Se le solicitará que entre valores para los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis ( ). El valor por omisión del parámetro se mostrará entre corchetes [ ].

Tabla 46. Lista de parámetros de configuración - Adición de puerto TN3270E

Información de parámetros	
<b>Parámetro</b>	Port number
<b>Valores válidos</b>	Del 1 al 65535
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el número de puerto a añadir.
<b>Parámetro</b>	Support TN3270E?
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	Yes
<b>Descripción</b>	Este parámetro especifica si el puerto añadido negociará para ser un servidor TN3270E. Si no es un Servidor "E", no dará soporte a peticiones de impresión ni del sistema.
<b>Parámetro</b>	Pool name
<b>Valores válidos</b>	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre de la agrupación asociada con este puerto. Los clientes que se conecten a este puerto y no especifiquen un nombre de LU ni un nombre de agrupación tendrán asignada una LU de esta agrupación.
<b>Parámetro</b>	Disable Client Filtering for this port?
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si las conexiones de entrada con este puerto deben utilizar la amplia función Correlación de dirección IP de cliente con nombre de LU si está habilitada.

**Sintaxis:**deletelu

Este mandato elimina una LU de TN3270E. Se le solicitará que entre valores para los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis ( ). El valor por omisión del parámetro se mostrará entre corchetes [ ].

## Mandatos de configuración de APPN

<i>Tabla 47. Lista de parámetros de configuración - Supresión de LU de TN3270E</i>	
<b>Información del parámetro</b>	
<b>Parámetro</b>	LU name
<b>Valores válidos</b>	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z, @, \$ y #</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre de LU de la LU dependiente a eliminar.

### Sintaxis:

delete            implicit-pool

Este mandato elimina una agrupación implícita de TN3270E. Se le solicitará que entre valores para los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis ( ). El valor por omisión del parámetro se mostrará entre corchetes [ ].

<i>Tabla 48. Lista de parámetros de configuración - Supresión de agrupación implícita de TN3270E</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Pool name
<b>Valores válidos</b>	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre de la agrupación de LU a suprimir.
<b>Parámetro</b>	Delete entire pool
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si se va a suprimir toda la agrupación o una entrada específica.
<b>Parámetro</b>	Station name
<b>Valores válidos</b>	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre de la estación a suprimir.

### Sintaxis:

delete            map

Este mandato elimina una correlación de dirección IP de cliente con nombre de LU. Se le solicitará que entre valores para los parámetros siguientes. El rango del parámetro se mostrará entre parén-



tesis ( ). El valor por omisión del parámetro se mostrará entre corchetes [ ].

<i>Tabla 49. Lista de parámetros de configuración - Supresión de correlación de TN3270E</i>	
<b>Información de parámetros</b>	
<b>Parámetro</b>	Client IP address or Network address
<b>Valores válidos</b>	Cualquier dirección IP válida
<b>Valor por omisión</b>	0.0.0.0
<b>Descripción</b>	Este parámetro especifica la dirección IP de la definición de correlación de red o cliente a suprimir.
<b>Parámetro</b>	Client IP address or Network address Mask
<b>Valores válidos</b>	Cualquier máscara de dirección IP válida
<b>Valor por omisión</b>	0.0.0.0
<b>Descripción</b>	Este parámetro especifica la máscara de dirección IP de la definición de correlación de red o cliente a suprimir.
<b>Parámetro</b>	Delete all entries for this client?
<b>Valores válidos</b>	Yes o No
<b>Valor por omisión</b>	No
<b>Descripción</b>	Este parámetro especifica si se va a suprimir toda la agrupación o un nombre específico.
<b>Parámetro</b>	Pool name
<b>Valores válidos</b>	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> <li>• Primer carácter: de la A a la Z</li> <li>• Caracteres segundo a octavo: de la A a la Z, del 0 al 9</li> </ul>
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el nombre de LU o el nombre de agrupación a suprimir.

**Sintaxis:**

delete            port

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

<i>Tabla 50. Lista de parámetros de configuración - Supresión de puerto TN3270E</i>	
<b>Información del parámetro</b>	
<b>Parámetro</b>	Port number
<b>Valores válidos</b>	Del 1 al 65536
<b>Valor por omisión</b>	Ninguno
<b>Descripción</b>	Este parámetro especifica el número de puerto a añadir.

**Sintaxis:**

## Mandatos de supervisión de APPN

list

all

Este mandato lista una configuración de TN3270E.

---

## Supervisión de APPN

Este apartado describe cómo supervisar APPN. Incluye los apartados siguientes:

- “Acceso a los mandatos de supervisión de APPN”
- “Mandatos de supervisión de APPN”

---

## Acceso a los mandatos de supervisión de APPN

Utilice el procedimiento siguiente para acceder a los mandatos de supervisión de APPN. Este proceso le proporciona acceso a un proceso de *supervisión* de APPN.

En el indicador de OPCON, entre **talk 5**.

Después de que se entre el mandato **talk 5**, se visualizará el indicador de GWCON (+) en el terminal. Si no aparece el indicador la primera vez que entre la configuración, pulse **Intro** de nuevo.

Entre **protocol APPN**. Por ejemplo:

```
* talk 5
+
+ protocol APPN
APPN>
```

Si después de que escriba **p appn** aparece el mensaje “Protocol APPN is available but not configured”, probablemente existe uno de los errores siguientes:

- No ha habilitado globalmente APPN en la configuración activa (aunque pueda haber configurado parámetros de APPN). Compruebe la configuración actual y, si éste es el caso, habilite APPN y reinicie o vuelva a cargar el direccionador.
- En el direccionador no hay disponible la cantidad de memoria que se necesita para que APPN se inicialice correctamente. Utilice **talk 2** con el fin de ver si se ha anotado cronológicamente un mensaje de error para tal efecto. Si es así, reconfigure APPN de manera que utilice menos memoria y reinicie o vuelva a cargar el direccionador.

Una vez que haya accedido al indicador de supervisión de APPN, entre **tn3270** para acceder al indicador de supervisión TN3270E >.

---

## Mandatos de supervisión de APPN

Este apartado describe los mandatos de supervisión de APPN para supervisar interfaces APPN. Entre los mandatos en el indicador APPN>, y los mandatos de servidor TN3270 en el indicador TN3270E>.

Tabla 51 (Página 1 de 4). Resumen de los mandatos de supervisión de APPN

Mandato	Función	Vea los detalles en la página:
---------	---------	--------------------------------

<i>Tabla 51 (Página 2 de 4). Resumen de los mandatos de supervisión de APPN</i>		
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de palabra clave para mandatos específicos.	--
activate link	Activa un enlace configurado.	“Activate” en la página 237
aping	Comprueba la conectividad de SNA/APPN con una LU de destino.	“Aping” en la página 237
deactivate link	Desactiva un enlace configurado o dinámico.	“Deactivate link” en la página 238
dump	Graba un vuelco de APPN en el disco o en la red.	“Dump” en la página 238
list cp-cp_sessions	Visualiza una lista de todos los CP adyacentes que pueden tener sesiones de CP-CP con este direccionador.	página 240
list dlur dlus	Visualiza una lista de los DLUS activos y el estado de cada sesión del conducto DLUS-DLUR.	página 241
list dlur lu	Visualiza una lista de PU internas o de sentido directo con estadísticas de LU para cada PU.	página 242
list dlur pu	Visualiza una lista de PU internas o de sentido directo con el estado de la conexión.	página 243
list dlur status	Visualiza un resumen de la información de configuración de DLUR global que actualmente está activa.	página 245
list ds incomplete_locates	Visualiza una lista de las búsquedas de APPN que se encuentran actualmente en proceso.	página 245
list ds resource	Visualiza una lista completa o parcial de nombres de LU del directorio de APPN de este direccionador.	página 246
list ds status	Visualiza estadísticas de resumen relativas a los Servicios de directorio de APPN.	página 247
list dumps	Visualiza una lista de los vuelcos en disco.	página 247
list focal	Visualiza una lista de puntos focales de gestión de red con el estado de los mismos.	página 248
list isr_sessions	Visualiza, siguiendo los enlaces, el número de sesiones activas de LU-LU de ISR que pasan por este direccionador.	página 249
list link	Visualiza una lista de enlaces configurados y dinámicos de este direccionador.	página 250

## Mandatos de supervisión de APPN

<i>Tabla 51 (Página 3 de 4). Resumen de los mandatos de supervisión de APPN</i>		
list link <i>nombre-enlace</i>	Visualiza la configuración y el estado en detalle de un enlace determinado.	página 251
list local_link	Visualiza una lista de los enlaces lógicos de DLUR con PU2.0 locales (que se utilizan para contener LU de TN3270) de este direccionador.	página 253
list log	Sustituido ahora por "log view" y "log status".	página 265
list port	Visualiza una lista de los puertos configurados de direccionador APPN lógicos y físicos con el estado de los mismos.	página 254
list port <i>nombre-puerto</i>	Visualiza la configuración y el estado en detalle de un puerto determinado.	página 255
list rtp	Visualiza una lista de los nodos de la Tabla de asociados a RTP e información de resumen sobre todas las conexiones RTP activas.	página 256
list rtp <i>tcid</i>	Visualiza información detallada sobre una o todas las conexiones RTP.	página 258
list session	Visualiza una lista de las sesiones de ISR que fluyen por el direccionador.	página 260
list status	Visualiza un resumen de la configuración general de APPN e información sobre su estado.	página 261
list topo node	Visualiza información de la base de datos de topología de este direccionador sobre un nodo determinado de una subred de esta topología.	página 262
list topo status	Visualiza un resumen de las estadísticas de base de datos de topología.	página 263
list topo tg	Visualiza una lista completa o parcial de TG activos de una subred de esta topología.	página 264
log status	Visualiza información de resumen sobre la anotación cronológica de sucesos de APPN.	página 265
log view	Entra en un submenú para navegar y ver las entradas de anotación cronológica de sucesos de APPN.	página 266

<i>Tabla 51 (Página 4 de 4). Resumen de los mandatos de supervisión de APPN</i>		
memory	Visualiza información detallada y de resumen sobre el uso de la memoria en APPN dentro del direccionador.	"Memory" en la página 270
restart	Detiene y reactiva APPN y TN3270 de manera disruptiva.	"Restart" en la página 275
rtp status	Visualiza información sobre la configuración global de RTP que actualmente se utiliza.	"Rtp status" en la página 273
rtp switchpath	Hace que una conexión RTP realice una conmutación de la vía de acceso para elegir la mejor vía de acceso que actualmente está disponible.	"Rtp switchpath" en la página 273
rtp test	Efectúa una prueba de ruta de HPR y visualiza los resultados.	"Rtp test" en la página 274
stop	Detiene APPN y TN3270 de manera disruptiva.	"Stop" en la página 275
test rtp	Efectúa una prueba de ruta de HPR y visualiza los resultados (es el formato antiguo de "rtp test").	"Rtp test" en la página 274
tn3270e	Accede al menú de mandatos de supervisión de TN3270.	"Mandatos de supervisión de TN3270E" en la página 276
transmit dump	Transmite un vuelco de APPN del disco duro del direccionador (2216, Network Utility, 2212) a una estación de trabajo en la red con TFTP.	"Transmit" en la página 276
exit	Le devuelve al menú de supervisión principal de Talk 5.	--

## Mandatos de supervisión de APPN

<i>Tabla 52. Resumen de los mandatos de supervisión del Servidor TN3270E</i>		
<b>Mandato</b>	<b>Función</b>	<b>Vea los detalles en la página:</b>
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de palabra clave para mandatos específicos.	--
deactivate lu	Desactiva de manera forzada a una LU utilizada por un cliente TN3270 y desconecta la conexión TCP correspondiente a este cliente.	"Deactivate LU" en la página 276
list connections	Visualiza una lista completa o parcial de conexiones de cliente activas.	277
list lu <i>nombre-lu</i>	Visualiza información detallada sobre la configuración y el estado de una sola LU interna.	278
list mapping	Visualiza una lista de las correlaciones configuradas de dirección IP de cliente con nombre de LU/agrupación.	279
list pools	Visualiza una lista de las agrupaciones de LU implícitas configuradas.	280
list pools <i>nombre-agrupación</i>	Visualiza información detallada sobre una sola agrupación de LU.	281
list ports	Visualiza una lista de los puertos TCP de destino de servidor TN3270 configurados.	282
list pu	Visualiza una lista de todas las PU internas (tanto de DLUR como de subárea) con información de resumen sobre el estado y la configuración.	283
list pu <i>nombre-pu</i>	Visualiza una lista de todas las LU internas bajo la PU especificada, con información de resumen sobre el estado y la configuración para cada LU.	284
list rejections	Visualiza una lista de las conexiones de cliente rechazadas más recientemente.	285
list status	Visualiza la configuración de servidor TN3270 global y un resumen estadístico.	286
exit	Le devuelve al menú de supervisión de APPN.	--

## Información detallada sobre los mandatos de supervisión de APPN

Esta sección describe la sintaxis detallada de los mandatos de supervisión de APPN. Estos mandatos se entran en el indicador de mandatos APPN>.

### Activate

Utilice el mandato **activate link** para activar un enlace configurado. Utilice el mandato **list link** para buscar el nombre del enlace que desee activar y para ver el estado del enlace después de activarlo.

#### Sintaxis:

**activate link** *nombre\_enlace*

### Aping

#### Sintaxis:

**aping** *pares-distintivo-valor nombre\_lu*

donde

#### **pares-distintivo-valor**

Especifica un distintivo (o más) de los que siguen y, a continuación, un valor. Especifique estos valores de distintivo únicamente si desea alterar temporalmente los valores por omisión.

<i>Tabla 53. Distintivos</i>		
<b>Distintivo</b>	<b>Significado</b>	<b>Valor por omisión</b>
-m	Nombre de modalidad para la sesión de LU6.2	#INTER
-t	Nombre de TP (programa de transacción) de destino	APING
-i	Cuenta de envíos y recepciones a emitir	1
-x	Cuenta de conversaciones de LU6.2 a ejecutar (en serie)	1
-y	Cuenta de TP a ejecutar (en serie)	1
-s	Tamaño de paquete	100 bytes
-q	Silencioso	Mensajes de estado
-b	Paso de la pantalla de salida a talk 2 (en segundo plano)	Pantalla para Talk 5

#### **nombre\_lu**

Especifica el nombre de LU calificado al completo del destino del APING.

**Valores válidos:** Cualquier nombre de LU calificado al completo válido

#### **Ejemplo:**

## Mandatos de supervisión de APPN

```

APPN >aping stfnet.mvs8
Allocate duration: 536 msec
Iteration Duration Data Sent Data Rate
number (msec) (bytes) (Kb/s) LU name
-----
0 458 100 1 STFNET.MVS8
-----
Avg. 458 100 1
  
```

Tabla 54. Descripción de la salida de APING

Elemento	Descripción	Valores clave
Allocate duration	El tiempo necesario para definir la sesión y la conversación de LU6.2 en el mandato aping.	--
Iteration duration	El tiempo de ida y vuelta necesario para que se envíe y reciba un acuse de recibo del paquete de datos.	--
Iteration data rate	La velocidad de datos calculada (como mínimo, 1 Kb/s), que se basa en la duración y en los bytes enviados.	--

### Deactivate link

Utilice el mandato **deactivate link** para desactivar un enlace configurado. Utilice el mandato **list link** para ver los nombres de los enlaces y para ver el estado del enlace después de utilizar tal mandato. Los enlaces configurados deben tener un estado inactivo y los enlaces dinámicos deben desaparecer.

#### Sintaxis:

deactivate link *nombre\_enlace*

### Dump

Utilice el mandato **Dump** para crear un vuelco de APPN.

#### Sintaxis:

dump

Dado que este vuelco no significa ninguna interrupción para las funciones de APPN, se puede mejorar su integridad minimizando el tráfico y los mandatos de control de APPN mientras el vuelco está en proceso.

### List

Utilice el mandato **List** para visualizar información sobre la configuración de APPN. El mandato lista lo siguiente:

#### Sintaxis:

list  
appc\_sessions



cp-cp\_sessions  
 dlur dlus  
 dlur lu  
 dlur pu  
 dlur status  
 ds incomplete\_locates  
 ds resource  
 ds status  
 dumps  
 focal  
 isr\_sessions  
 link  
 link *nombre-enlace*  
 local\_link  
 log  
 port  
 port *nombre-puerto*  
 rtp  
 rtp *tcid*  
 session  
 status  
 topo node  
 topo status  
 topo tg

**Mandato****Función****list appc\_sessions**

Utilice el mandato **list appc** para visualizar una lista de todas las sesiones de LU6.2 que tienen un punto final en este direccionador. Ejemplos de tales sesiones son: sesiones de CP-CP, sesiones de DLUR a DLUS, sesiones con un punto focal de gestión de red y sesiones iniciadas debido al mandato "aping". Este mandato lista todas las sesiones activas. Si un conducto consta de dos sesiones de un sola dirección, se visualizan ambas sesiones del par.

**Ejemplo:**

## Mandatos de supervisión de APPN

```

APPN >1i appc
LU Name           Mode Type FSM FID PCID
=====
STFNET.CP3174BC  CPSVCMG Pri ACT FID2 C4 9B 1F 3B 03 54 83 3D
STFNET.CP3174BC  CPSVCMG Sec ACT FID2 CB 13 AF 4A 23 AC E5 06
STFNET.VL14      CPSVCMG Pri ACT FID5 C4 9B 1F 3B 03 54 83 40
STFNET.VL14      CPSVCMG Sec ACT FID5 CB 67 9F CA F8 27 B5 9F
STFNET.VLNN045  CPSVCMG Sec ACT FID5 C8 8B 1F 3B 04 42 34 FA
STFNET.VLNN045  CPSVCMG Pri ACT FID5 C4 9B 1F 3B 03 54 83 41
STFNET.MVS8      CPSVRMGR Pri ACT FID2 C4 9B 1F 3B 03 54 83 42
STFNET.MVS8      CPSVRMGR Sec ACT FID2 D3 B7 7C D5 57 35 0B C8
  
```

Tabla 55. Descripción de la salida de List appc\_sessions

Elemento	Descripción	Valores clave
LU name	El nombre de LU de asociado calificado al completo	--
Mode	El nombre de modalidad para la sesión	<ul style="list-style-type: none"> <li>• #CONNECT = prioridad media estándar</li> <li>• #INTER = prioridad alta estándar</li> <li>• CPSVCMG = sesión de CP-CP</li> <li>• CPSVRMGR = sesión de DLUR-DLUS</li> <li>• SNASVCMG = sesión de punto focal</li> <li>• están estructurados otros nombres de modalidad y también pueden estar definidos por el usuario</li> </ul>
Type	La función de activación de la sesión del direccionador	<ul style="list-style-type: none"> <li>• Pri = Primaria</li> <li>• Sec = Secundaria</li> </ul>
FSM	El estado actual de la sesión (valor de Máquina de estado finito)	<ul style="list-style-type: none"> <li>• ACT = activo</li> <li>• PBIR = petición BIND pendiente</li> <li>• PCIN = CINIT pendiente (los servicios de sesión consisten en encontrar y activar el TG de salida)</li> <li>• RES = restablecido (inicial)</li> </ul>
FID	El tipo de ID de formato	<ul style="list-style-type: none"> <li>• FID2 = ISR</li> <li>• FID5 = HPR</li> </ul>
PCID	El ID correlacionador de procedimiento: el identificador de la sesión	--

### list cp-cp\_sessions

Utilice el mandato **list cp** para visualizar una lista de todos los nodos adyacentes que pueden tener sesiones de CP-CP con este direccionador. La lista de la salida incluye todos los CP que tienen un enlace activo que da soporte a sesiones de CP-CP, así como los CP que ya no están conectados pero han tenido un enlace activo con posibilidad de CP-CP anteriormente (desde el último reinicio de APPN). A diferencia del

mandato **list appc**, en una sola línea de salida se representan un par de sesiones: la sesión ganadora de la contención y la sesión perdedora de la contención.

Si el direccionador está configurado como nodo Branch Extender, la lista indicará solamente un par de sesiones de CP-CP activas con un NN adyacente. Éste es el servidor de NN del nodo BEX.

**Ejemplo:**

```
APPN >li cp
      CP Name Type      Status      ConWinner ConLoser ConWinner ConLoser
      ID       Sense      Sense      ID
=====
      STFNET.NN12 NN      Active    BAF92A69  BAF92A84 080F6051 00000000
      STFNET.CP3174BC NN      Active    BAF927E3  BAF927E5 00000000 00000000
```

Tabla 56. Descripción de la salida		
Elemento	Descripción	Valores clave
CP name	El nombre calificado al completo del CP adyacente	--
Type	El tipo de nodo del CP adyacente	NN = nodo de red EN = nodo final Virt = nodo virtual
Status	El estado del par de sesiones de CP-CP	Active Inactive Pending
ConWinner/Loser ID	El ID de sesión interno del direccionador para la sesión ganadora/perdedora de la contención del par de sesiones de CP-CP, 0 si la sesión no está conectada	--
ConWinner/Loser sense	El código de detección de SNA que indica la razón de la última desconexión de la sesión ganadora/perdedora de la contención	--

**list dlur dlus**

Utilice el mandato **list dlur dlus** para visualizar una lista de los DLUS activos y el estado de cada sesión del conducto DLUR-DLUS. Los DLUS listados pueden proceder de uno de estos orígenes:

- Configuración en el direccionador como DLUS primario o de reserva global
- Configuración en el direccionador como DLUS primario o de reserva para un enlace de sentido directo en particular
- DLUS dinámico (no configurado) que se conecta con el direccionador y dirige llamadas a las PU dependientes

**Ejemplo:**

## Mandatos de supervisión de APPN

```

APPN >1i dlur dlus
DLUS  NAME          CONWINNER  CONLOSER
      STATE          STATE
-----
STFNET.MVS8        UP          UP
  
```

Tabla 57. Descripción de la salida de List dlur-dlus

Elemento	Descripción	Valores clave
DLUS name	El nombre de CP calificado al completo del DLUS	--
ConWinner/Loser state	El estado de la sesión ganadora/perdedora de la contención del par de sesiones de DLUR-DLUS	UP DOWN PENDING_UP PENDING_DOWN BLOCKED = en espera de la sustitución del SSCP

### list dlur lu

Utilice el mandato **list dlur lu** para visualizar una lista de PU de sentido directo (o internas, en el caso de TN3270) activas con estadísticas de LU para cada PU. Las PU dependientes de esta lista tienen un enlace activo con el direccionador o bien éste intenta establecer un enlace actualmente.

### Ejemplo:

```

APPN >1i dlur lu
CP NAME          LINK  TOTAL  ---NO SSCP LU STATE---  NO OF LUs
                  NAME  LUs    DOWN  PENDING  ACTIVE  LU_LU SESS
-----
STFNET.VLNN105   PUSUD1  253    0     0     253    0
STFNET.VLNN105   PUSUD21  10     0     0     10     0
STFNET.VLNN105   PUSU02   9      0     0     9      0
STFNET.VLNN105   PUSU01  10     0     0     10     0
  
```

*Tabla 58. Descripción de la salida de List dlur lu*

Elemento	Descripción	Valores clave
CP name	El nombre del CP en el que reside la LU. En el caso de las LU internas de TN3270, el nombre de CP del direccionador.	--
Link name	El nombre de estación de enlace configurado o creado dinámicamente para el enlace con la PU dependiente. Este enlace puede ser interno o externo respecto al direccionador.	--
Total LUs	La suma del número de LU en todos los estados de SSCP-LU. No es necesario que estas LU estén definidas en el direccionador, pero lo están en el sistema principal.	--
SSCP-LU state: down	El número de LU que no tienen SSCP propietario pero sí sesiones de LU-LU (pérdida de enlace con SSCP, pero ANS=CONT).	--
SSCP-LU state: pending	El número de LU que están en espera de la respuesta a ACTLU.	--
SSCP-LU state: active	El número de LU que han recibido la respuesta a ACTLU. Este número no disminuye cuando una LU se enlaza lógicamente y entra en el estado de LU-LU.	--
LU-LU session	El número de LU que tienen sesiones de LU-LU activas actualmente.	--

**list dlur pu**

Utilice el mandato **list dlur pu** para visualizar una lista de PU de sentido directo (o internas, en el caso de TN3270) con el estado de la conexión. Las PU dependientes de esta lista tienen un enlace activo con el direccionador o bien éste intenta establecer un enlace actualmente.

**Ejemplo:**

```

APPN >li dlur pu
CP NAME          STATUS      LOC LINK      SESS  ANS SSCP      ACT DLUS
                   NAME          NAME          STAT
; PUNAME  NAME
-----
STFNET.VLNN105  active      INT PUSUD1    act   CON PUSUD12  STFNET.MVS8
STFNET.VLNN105  active      INT PUSUD21   act   CON PUSUD1   STFNET.MVS8
STFNET.VLNN105  active      INT PUSU02    act   CON PUSU02   STFNET.MVS8
STFNET.VLNN105  active      INT PUSU01    act   CON PUSU01   STFNET.MVS8

```

## Mandatos de supervisión de APPN

<i>Tabla 59. Descripción de la salida</i>		
<b>Elemento</b>	<b>Descripción</b>	<b>Valores clave</b>
CP name	El nombre de CP de la PU dependiente. En el caso de las PU externas, éste es el nombre de CP que envían en las XID o, si no envían ninguno, es un nombre que el direccionador crea utilizando el formato DLUR..@nnn. En el caso de las PU internas, es el nombre de CP del direccionador.	--
Status	El estado de sesión de SSCP-PU, desde la perspectiva del direccionador DLUR. Puede decodificar los valores de estado de la manera siguiente: <ul style="list-style-type: none"> <li>• pe = pendiente</li> <li>• Re = petición</li> <li>• Rs = respuesta</li> <li>• Actp, Actpu = ACTPU Dactpu = DACTPU</li> <li>• LnkAct = activación de enlace</li> <li>• Inop = inoperativo</li> </ul>	active peReActpRs (p.e., el conducto está inactivo) reset (inactivo) peActpu peActpuRs peLnkAct peDactpuRs peInop peInopActpu
Loc	La ubicación de la PU en relación con el direccionador DLUR.	INT = interna DON = sentido directo
Link name	El nombre de estación de enlace configurado o creado dinámicamente para el enlace con la PU dependiente. Este enlace puede ser interno o externo respecto al direccionador.	--
Sess stat	El estado del conducto DLUR-DLUS que contiene flujos de control para esta PU dependiente.	act = activo res = restablecido (inactivo) pAct = activación pendiente plnac = desactivación pendiente
ANS	El valor definido en el sistema principal para la Conclusión automática de la red: si las sesiones de LU-LU deben continuar o deben detenerse cuando se pierde la conectividad con el SSCP.	CON = continuar STP = detener
SSCP PU name	El nombre de VTAM para esta PU dependiente, que se recibe en la ACTPU.	--
Act DLUS name	El nombre de CP del DLUS que posee esta PU actualmente (el "DLUS activo").	--

**list dlur status**

Utilice el mandato **list dlur status** para visualizar un resumen de la información de configuración de DLUR global que actualmente está activa. Tenga en cuenta que algunos de estos valores tienen alteraciones temporales de nivel de enlace opcionales.

**Ejemplo:**

```
APPN >li dlur st
Primary DLUS Name           = STFNET.MVS8
Backup DLUS Name            =
Retry Time Limit             = 15
Short Retry Timer            = 15
Short Retry Count            = 20
Long Retry Timer             = 30
Drop Link when there are no sessions = NO
```

Todos ellos son elementos de datos configurados. Vea la página 130.

**list ds incompletes**

Utilice el mandato **list ds inc** para visualizar una lista de las peticiones de búsqueda de APPN (peticiones "locate") que se encuentran actualmente en proceso. Este direccionador está esperando respuestas de otros nodos de la red.

El mandato solicita diversos filtros de datos posibles. Para obtener una descripción de cada uno, consulte la tabla de descripción de la salida que se mostrará a continuación.

**Ejemplo:**

```
APPN >li ds inc
PCID (0 if unknown) [00000000 00000000]?
Locate origin CP      (NetID.CPname or *) [*]?
Locate origin LU      (NetID.LUname or *) [*]?
Locate destination LU (NetID.LUname or *) [*]?

PCID & Incomplete
Child CP Name(s)      Origin CP      Origin LU      Destination LU
-----
c49b1f3b 03310d51 STFNET.VLNN105  STFNET.VLNN105  STFNET.VL12
STFNET.VL15

c49b1f3b 03310d50 STFNET.VLNN105  STFNET.VLNN105  STFNET.MVS8
STFNET.VL15
```

## Mandatos de supervisión de APPN

*Tabla 60. Descripción de la salida*

Elemento	Descripción	Valores clave
PCID	El ID correlacionador de procedimiento: el correlacionador de nivel de red para este procedimiento de búsqueda en particular.	--
Incomplete child CP names	Los nombres de CP de los nodos a los que este direccionador ha enviado peticiones locate y de los que todavía está esperando respuestas.	--
Origin CP	El nombre del CP que ha iniciado la búsqueda originalmente.	--
Origin LU	El nombre de la LU que ha iniciado la búsqueda originalmente.	--
Destination LU	El nombre de la LU que se está buscando.	--

### list ds resource par distintivo-valor

Utilice este mandato para visualizar una lista de nombres de recursos (LU) del directorio de APPN de este direccionador.

Para limitar los datos visualizados, puede especificar uno de los distintivos de filtro siguientes y el valor correspondiente:

*Tabla 61. Descripción de la salida*

Distintivo de filtro	Valor
-c	El nombre de CP del propietario de LU, que puede estar calificado con ID de red o no
-n	El ID de red del propietario de LU
-l	El nombre de LU calificado al completo
-s	El nombre de servidor calificado al completo

### Ejemplo:

APPN >1i ds res

```

LU NAME          SERVER NAME      OWNER NAME      LOCATION TYPE
-----
*                STFNET.VLNN105  STFNET.TEMP     WILDCARD HOME
STFNET.MVS8      STFNET.MVS8     STFNET.MVS8     X-DOMAIN CACHE
STFNET.CNM08     STFNET.MVS8     STFNET.MVS8     X-DOMAIN CACHE
STFNET.SD1L02   STFNET.VLNN105  STFNET.VLNN105  LOCAL HOME
STFNET.SD1L03   STFNET.VLNN105  STFNET.VLNN105  LOCAL HOME
STFNET.SD1L04   STFNET.VLNN105  STFNET.VLNN105  LOCAL HOME

```



<i>Tabla 62. Descripción de la salida</i>		
Elemento	Descripción	Valores clave
LU name	El nombre de la LU o "*" para representar un comodín completo.	--
Server name	El nombre de CP del servidor de NN para esta LU.	--
Owner name	El nombre de CP del propietario de la LU. Por ejemplo, un EN puede poseer una LU que resida en el EN.	--
Location	La ubicación de la LU.	REGISTER = registrada por un EN servido X-DOMAIN = dentro o servida por otro NN LOCAL = en el direccionador, incluidas las LU servidas por DLUR DOMAIN = servida por el direccionador como NN, pero no registrada WILDCARD = el propietario tiene una definición de comodín completo (no explícita)
Type	La categoría de la entrada en el directorio, que refleja cómo debe manejarse la entrada.	HOME = definición de sistema en el direccionador CACHE = aprendida dinámicamente por el direccionador; tendrá una duración REGISTER = registrada por un EN servido; él mismo puede desregistrarla

**list ds status**

Utilice este mandato para visualizar estadísticas de resumen sobre el directorio de APPN de este direccionador.

**Ejemplo:**

```
APPN >li ds s
Maximum Directory Entries = 4000
Current Cache Entries = 3
Current Home Entries = 284
Registered Entries = 0
Directed Locates Received = 0
Broadcast Locates Received = 1
Directed Locates Sent = 2
Broadcast Locates Sent = 2
Directed Locates Not Found = 0
Broadcast Locates Not Found = 0
Outstanding Locates = 0
```

**list dumps**

Utilice este mandato para listar todos los archivos de vuelco de APPN del disco duro del direccionador. Este mandato no está disponible para los direccionadores que no tienen disco duro.

## Mandatos de supervisión de APPN

### Ejemplo:

```
APPN >li du
1      168084      Thu Jul 01 15:11:18 1999
```

<i>Tabla 63. Descripción de la salida</i>		
Elemento	Descripción	Valores clave
Un número	El número de vuelco a utilizar con el mandato <b>transmit dump</b> .	--
Un tamaño	El tamaño del archivo de vuelco, en bytes. Mientras el vuelco está en proceso, este número aumenta.	--
Una fecha/hora	La fecha y la hora del último cambio del archivo. Mientras el vuelco está en proceso, la hora cambia.	--

### list focal

Utilice este mandato para visualizar una lista de los puntos focales de gestión de red configurados y dinámicos activos con el estado de los mismos.

### Ejemplo:

```
APPN >li foc
CATEGORY      STATUS  TYPE    FOCAL POINT
-----
ALERT         NOTACT  IMP_PRI STFNET.CNM08
```

Tabla 64. Descripción de la salida		
Elemento	Descripción	Valores clave
Category	La categoría de la función realizada por el punto focal.	ALERT MS_CAPS ACCTNG OTH = otras
Status	El estado de las sesiones de LU6.2 con este punto focal.	NOTACT = no activo ACT = activo PENDING NEVERACT = nunca ha estado activo
Type	La naturaleza del punto focal, que se describe en términos centrados en el sistema principal: Explícito = El FP no se configura en el direccionador; se conecta con el direccionador Implícito = El FP se configura en el direccionador; éste se conecta con el FP  Los valores de la derecha aparecen listados por orden de prioridad, de la alta a la baja, donde un FP de prioridad superior puede realizar funciones de sustitución dinámicamente como FP.	EXP_PRI = explícito primario IMP_PRI = implícito primario BKUP_FP = punto focal de reserva DEF_PRI = primario por omisión DEF_BKP = reserva por omisión DOMAIN HOST
Focal point	El nombre de CP del nodo que proporciona la función de punto focal.	--

**list jsr\_sessions** Utilice este mandato para visualizar, siguiendo los enlaces, el número de sesiones activas de LU-LU de ISR que pasan por este direccionador. Las cuentas incluyen:

- Sesiones que entran y salen del sistema mediante ISR (estas sesiones se cuentan una vez en cada uno de los TG de entrada y salida)
- Sesiones que entran en el sistema mediante ISR pero salen sobre una conexión RTP (estas sesiones sólo se cuentan una vez en el TG que no es de HPR)
- Sesiones de LU de TN3270 direccionadas por DLUR que salen del sistema mediante ISR (estas sesiones sólo se cuentan en el TG de ISR externo real y no en los enlaces internos entre el DLUR y las PU locales)

Utilice el mandato **list session** para visualizar más información sobre las sesiones de ISR contadas.

#### Ejemplo:

```
APPN >li isr
Adjacent CP Name  TG Number  ISR Sessions
-----
STFNET.CP3174BC  21         3
```

## Mandatos de supervisión de APPN

Tabla 65. Descripción de la salida		
Elemento	Descripción	Valores clave
Adjacent CP name	El nombre de CP del nodo adyacente al direccionador en este TG, configurado o recibido en una XID.	--
TG number	El número de TG negociado para este enlace.	--
ISR sessions	El número de sesiones de ISR activas de este enlace.	--

### list link\_information

Utilice este mandato para visualizar una lista de todos los enlaces configurados y todos los dinámicos activos.

#### Ejemplo:

```
APPN > li 1
Name Port Name Intf Adj CP Name Type HPR State
-----
T03174 TR005 5 STFNET.CP3174BC NN INACTIVE ACT_LS
TOLEN TR00 0 STFNET.TEMP LEN ENABLED RESET_LS
TOLEN1 TR00 0 STFNET.ABCD LEN ENABLED RESET_LS
@@@ TR005 5 STFNET.NN12 NN ACTIVE ACT_LS
```

Tabla 66 (Página 1 de 2). Descripción de la salida		
Elemento	Descripción	Valores clave
Name	En el caso de los enlaces configurados, el nombre de estación de enlace que ha configurado. En el caso de los enlaces dinámicos, el direccionador crea un nombre con el formato "@@nnnn", donde nnnn empieza en el cero y sigue aumentando hasta el reinicio.	--
Port name	El nombre de APPN configurado para el puerto mediante el cual se ha conectado este enlace.	--
Intf	El número de interfaz lógica del direccionador para el puerto mediante el cual se ha conectado este enlace.	--
Adj CP name	El nombre de CP del nodo adyacente al direccionador en este enlace, configurado o recibido en una XID.	--
Type	El tipo de nodo configurado o real (si el enlace está activo) del nodo adyacente.	LEN EN NN LEARN (sólo los configurados)

Tabla 66 (Página 2 de 2). Descripción de la salida		
HPR	El estado configurado o real (si el enlace está activo) del HPR en el enlace.	ACTIVE INACTIVE ENABLED (sólo los configurados) DISABLED (sólo los configurados)
State	<p>El estado actual de la conexión del enlace lógico.</p> <p>Algunas definiciones de estado de tipo intermedio: SENT_REQ_OPNSTN = el puerto subyacente está activo; se ha solicitado al DLC que se ponga en contacto con la estación de enlace remota</p> <p>PEND_XID_EXCH = estación remota en contacto; intercambio de XID</p>	<p><b>Estados de fijación</b></p> <p>RESET_LS = restablecido (inactivo)</p> <p>ACT_LS = activo</p> <p><b>Estados de activación</b></p> <p>SENT_REQ_OPNSTN PEND_XID_EXCH SENT_ACT_AS SENT_SET_MODE SENT_CREATE_TG SENT_CONN_REQ PEND_RCV_CONN_IND PEND_SEND_CONN_RSP SENT_CONN_RSP</p> <p><b>Estados de desactivación</b></p> <p>SENT_DEACT_AS_ORD SENT_DISC_ORD SENT_DESTROY_TG PEND_DEACT PEND_CLOSE_STN</p>

**list link\_information nombre-enlace**

Utilice este mandato para obtener información detallada sobre la configuración y el estado de un solo enlace lógico con un nodo adyacente.

**Ejemplo:**

## Mandatos de supervisión de APPN

```
APPN > li link vm30pu1
```

```
Link Station Information
```

```
=====
```

```
ls_name = VM30PU1
type = DEFINED
act_at_startup = TRUE
auto_act_supported = FALSE
pan_uplink = FALSE
replace_inbound_CP_name/node_id = FALSE
retry_link_act_unconditionally = FALSE
adjacent_node_subnet_affiliation = NEGOTIABLE
subnet_visit_count = 3
remote_mac_addr = 402222222222
remote_sap_value = 04
hpr_sap_value = C8
real_adj_cp_name = USIBMNR.NRMVM30
node_id = 00000000
cp_cp_sessions_supported = FALSE
hpr_supp = FALSE
hpr_link = FALSE
link_station_state = ACT_LS
direction = OUTBOUND
actual_max_send_btu_size = 2006
partner_node_type (actual) = EN
partner_node_type (defined) = LEARN
tg_isr_type = ENDPOINT_TG
tg_num (defined) = 0
tg_num (actual) = 0
Received CV22 Sense code = 0
```

Tabla 67 (Página 1 de 2). Descripción de la salida

Elemento	Descripción	Valores clave
Type	Cómo ha conocido el enlace el direccionador.	DEFINED = configurado DYNAMIC TEMPORARY = todavía no puede coincidir con los enlaces configurados
Act_at_startup	Si el enlace está configurado para activarse cuando APPN arranca.	TRUE FALSE
Auto_act_supported	El enlace tiene la capacidad de activarse solamente cuando sea necesario.	--
Pan_uplink	Si el enlace está configurado como enlace superior (comunicación en sentido inverso de aspecto de EN con un NN) de Branch Extender (nodo de acceso periférico).	TRUE FALSE
Replace inbound CP name / node ID	Si el enlace está configurado de manera que estos campos de XID de un nodo LEN adyacente deban alterarse temporalmente mediante valores configurados en el direccionador.	TRUE FALSE
Retry link act unconditionally	Si siempre debe realizarse un reintento ante una anomalía de activación de enlace y una anomalía de enlace, sea cual sea la causa.	TRUE FALSE

<i>Tabla 67 (Página 2 de 2). Descripción de la salida</i>		
Adjacent node subnet affiliation	Si el enlace está configurado para que sea un enlace de un EBN con una subred de topología diferente.	NATIVE NON-NATIVE NEGOTIABLE
Real adj CP name	El nombre de CP recibido en una XID del nodo adyacente.	--
CP-CP sessions supported	El valor configurado de la definición de enlace o puerto del direccionador.	TRUE FALSE
Hpr_supp	Si se ha configurado soporte para el HPR.	TRUE FALSE
Hpr link	Si existe soporte negociado real para el HPR en este enlace.	TRUE FALSE
Link station state	El estado actual de la conexión del enlace lógico.	Los mismos valores de "list link"
Direction	La dirección en que se ha producido la activación del enlace.	INBOUND OUTBOUND
Tg_isr_type	El tipo de TG/enlace.	ENDPOINT_TG = el nodo adyacente actúa como EN INTERMEDIATE_ROUTING_TG = el direccionador actúa como NN o EBN y el nodo adyacente es un NN
Received CV22 sense code	El código de error de SNA de anomalía en intercambio de XID que se ha recibido del nodo adyacente en este enlace.	--

**list local\_link\_information**

Utilice este mandato para visualizar una lista de los enlaces lógicos existentes en el direccionador del DLUR con PU2.0 internas. Estas PU se utilizan para contener LU de la función de servidor TN3270.

**Ejemplo:**

```
APPN > li loc
  Name      SSCP PU Name   Node ID   Auto Act   Sense State
  =====
  PUSUD1    STFNET.PUSUD12  77DE711  TRUE      0 LOCAL_ACT_LS
  PUSUD21   STFNET.PUSUD1  77D7E11  TRUE      0 LOCAL_ACT_LS
  PUSU02    STFNET.PUSU02  77D7F12  TRUE      0 LOCAL_ACT_LS
  PUSU01    STFNET.PUSU01  77D7F11  TRUE      0 LOCAL_ACT_LS
```

<i>Tabla 68 (Página 1 de 2). Descripción de la salida</i>		
Título de columna	Descripción	Valores clave
Name	El nombre de estación de enlace configurado para el enlace interno con la PU dependiente.	--
SSCP PU name	El nombre de VTAM para esta PU, que se recibe en la ACTPU.	--

## Mandatos de supervisión de APPN

Tabla 68 (Página 2 de 2). Descripción de la salida		
Node ID	El bloque de ID y el número de ID configurados para esta PU dependiente interna.	--
Auto act	Si este enlace se activará automáticamente al iniciarse APPN.	TRUE FALSE
Sense	El código de detección de la última anomalía de enlace.	--
State	El estado actual del enlace lógico interno.	<b>Estados de fijación</b> LOCAL_RESET_LS = restablecido (inactivo) LOCAL_ACT_LS = activo <b>Estados de activación</b> LOCAL_SENT_CREATE_TG LOCAL_SENT_ACT_ASE <b>Estados de desactivación</b> LOCAL_SENT_DESTROY_TG LOCAL_PEND_DEACT

### list port information

Utilice este mandato para visualizar una lista de los puertos configurados de direccionador APPN lógicos y físicos con el estado de los mismos.

#### Ejemplo:

```

APPN > li port
  Intf      Name      DLC Type      HPR      State
  -----
      5      TR005      IBMTRNET      TRUE      ACT_PORT
      0      TR00      IBMTRNET      TRUE      ACT_PORT
  
```

Tabla 69 (Página 1 de 2). Descripción de la salida		
Elemento	Descripción	Valores clave
Intf	El número de interfaz lógica del direccionador para este puerto.	--
Name	El nombre de puerto APPN configurado.	--
DLC type	El tipo de interfaz física o configurada.	ATM ETHERAND = ethernet FDDI FR = frame relay HPR_IP = enterprise extender IBMTRNET = Red en Anillo PPP MPC+ = canal de diversas vías de acceso + SDLC X25 = QLLC X.25



Tabla 69 (Página 2 de 2). Descripción de la salida		
HPR	El estado del HPR que ha configurado en los enlaces dinámicos de este puerto.	TRUE FALSE
State	El estado de la interfaz física o lógica según la percepción de APPN.	<b>Estados de fijación</b> RESET_PORT = restablecido (inactivo) ACT_PORT = activo <b>Activación</b> SENT_ENABLE SENT_ACT_SAP <b>Desactivación</b> PEND_START_PORT_DEACT PEND_LS_DEACT_ORD_PORT PEND_LS_DEACT_IMM_PORT SENT_DEACT_SAP

**list port\_information nombre-puerto**

Utilice este mandato para obtener información detallada sobre la configuración y el estado de un solo puerto en particular.

**Ejemplo:**

```
APPN > li port t00004
```

```
Port Information
=====
port_name = T00004
dlc_name = IBMTRNET
port_num = 4
max_rcv_btu_size = 2048
ls_role = NEGOTIABLE
sap_value = 04
mac_addr = 401111111111
hpr_sap_value = C8
pan_uplink = FALSE
adjacent node subnet affiliation = NEGOTIABLE
subnet visit count = 3
hpr_supp = FALSE
port state = ACT_PORT
```

Tabla 70 (Página 1 de 2). Descripción de la salida		
Elemento	Descripción	Valores clave
DLC name	El tipo de puerto.	Los mismos valores del campo DLC type de "list port"
Port num	El número de interfaz lógica del direccionador para este puerto.	--
LS role	La función de estación de enlace local inicial en esta interfaz.	PRIMARY SECONDARY NEGOTIABLE
Pan uplink	Si los enlaces dinámicos de este puerto están configurados como enlaces superiores (comunicación en sentido inverso de aspecto de EN con NN) de Branch Extender (nodo de acceso periférico).	TRUE FALSE

Tabla 70 (Página 2 de 2). Descripción de la salida		
Adjacent node subnet affiliation	Si los enlaces dinámicos de este puerto están configurados para que sean enlaces de EBN con una subred de topología diferente.	NATIVE NON-NATIVE NEGOTIABLE
HPR support	Si está configurado soporte para el HPR en los enlaces dinámicos de este puerto.	TRUE FALSE
Port state	El estado de la interfaz física o lógica según la percepción de APPN.	Los mismos valores de <b>list port</b>

**list rtp**

Utilice este mandato para visualizar una lista de las entradas de la Tabla de asociados a RTP e información de resumen sobre todas las conexiones RTP activas con un punto final en el direccionador (la Tabla de conexiones RTP).

La Tabla de asociados a RTP no aparece si no tiene entradas. Se crea una entrada relativa a cada nodo remoto para el que son verdaderas las afirmaciones siguientes:

- El direccionador ha realizado una Definición de ruta de RTP para el nodo
- El nodo sólo utiliza una NCE para todas las conexiones RTP
- El nodo tiene, como mínimo, una conexión RTP activa con el direccionador

Tenga en cuenta que no se realiza una Definición de ruta de RTP durante la activación de RTP con RSETUP o CP-CP, por lo que no habrá ninguna entrada relativa a un nodo adyacente si las únicas conexiones RTP activas con éste están destinadas al transporte de definiciones de ruta o sesión de CP-CP. Tengase en cuenta también que todos los niveles del IBM 3746-900/950, y los niveles recientes de VTAM, utilizan diversas NCE.

**Ejemplo:**

```
APPN > 1i rtp
RTP PARTNER TABLE:
Remote Partner Name Remote Boundary Name TG Number
-----
          STFNET.NN12          STFNET.NN12          -1
          STFNET.VLNN045          STFNET.CP3174BC          21
RTP CONNECTION TABLE:
TCID          CP Name  ISR  APPC  Pathswitch  Alive  COS TPF TG Number
-----
31BE30E0      STFNET.NN12  0    1      180        180   CPSVCMG  21
31BE4428      STFNET.NN12  0    1      180        180   CPSVCMG  21
31BF4850      STFNET.NN12  0    0        0         180   RSETUP   21
31BF5B98      STFNET.NN12  0    1      180        180   SNASVCMG 21
31BF6EE0      STFNET.NN12  0    8      180        180   #CONNECT  21
```

Tabla 71 (Página 1 de 2). Tabla de asociados		
Elemento	Descripción	Valores clave

*Tabla 71 (Página 2 de 2). Tabla de asociados*

Remote partner name	El nombre de CP del nodo en que termina una conexión RTP.	--
Remote boundary name	El nombre de CP del siguiente nodo ISR adyacente al nodo asociado remoto o bien el nombre de LU de la aplicación remota que utiliza la conexión RTP.	--
TG number	El número de TG del TG con el siguiente nodo ISR adyacente al nodo asociado remoto. Un valor de "-1" indica que la sesión que ha causado la activación de RTP ha finalizado en el nodo asociado remoto; en este caso, "Remote boundary name" es el nombre de la LU de destino de la sesión del nodo asociado remoto.	--

*Tabla 72 (Página 1 de 2). Tabla de conexiones*

Elemento	Descripción	Valores clave
TCID	El ID de conexión de transporte, un identificador exclusivo para esta conexión RTP compartida por sus dos puntos finales.	--
CP name	El nombre de CP del nodo en que termina esta conexión RTP.	--
ISR	<p>El número de sesiones de LU-LU de ISR direccionadas sobre esta conexión RTP del direccionador. Este número incluye los siguientes tipos de sesiones:</p> <ul style="list-style-type: none"> <li>Sesiones de LU de nodos externos que entran con ISR y salen con HPR, tanto si se direccionan utilizando el DLUR como si no</li> <li>Sesiones de LU de TN3270 de este direccionador que salen con HPR, únicamente las direccionadas utilizando el DLUR (las sesiones de los enlaces de subárea no pueden utilizar el HPR)</li> </ul>	--

## Mandatos de supervisión de APPN

<i>Tabla 72 (Página 2 de 2). Tabla de conexiones</i>		
APPC	<p>El número de sesiones de LU6.2 con un punto final en este direccionador que están direccionadas sobre esta conexión RTP. Este número puede incluir los siguientes tipos de sesiones:</p> <ul style="list-style-type: none"> <li>• Sesiones de CP-CP para nodos de capacidad de torre con CF de HPR</li> <li>• Sesiones de conducto DLUR-DLUS</li> <li>• Sesiones de punto focal</li> <li>• Sesiones de Aping</li> </ul>	--
Pathswitch	El tiempo máximo en segundos para efectuar una conmutación de la vía de acceso antes de que falle la conexión RTP.	--
Alive	El tiempo en segundos entre los mensajes de pulsaciones cuando no hay tráfico del usuario.	--
COS TPF	<p>El nombre de clase de servicio para todas las sesiones de esta conexión RTP.</p> <p>Según las condiciones de temporización de definición de conexión, es normal ver conductos RTP paralelo (los mismos puntos finales) con la misma clase de servicio.</p>	<p>CPSVCMG = sesiones de CP-CP</p> <p>SNASVCMG = sesiones de DLUR-DLUS o FP</p> <p>#BATCH = prioridad baja estándar</p> <p>#CONNECT = prioridad media estándar</p> <p>#INTER = prioridad alta estándar</p> <p>existen otros nombres estructurados y nombres definidos por el usuario</p>
TG number	El número de enlace/TG para el primer salto de la conexión RTP fuera del direccionador.	--

**list rtp tcid**

Utilice este mandato para obtener información detallada de estadísticas y del estado de una o todas las conexiones RTP.

**Ejemplo:**

```

APPN > li rtp 31CC5DA8
=====
TCID          CP Name  ISR  APPC  Pathswitch  Alive  COS TPF TG Number
31CC5DA8     STFNET.VL15  0   2     200        180   CPSVCMG  21
RemoteTCID: 00000000 31C680C8, Role: ACTIVE, State: CONNECTED
FwdRSCV: 162B0100 12461080 150BE2E3 C6D5C5E3 *.....STFNET
          4BE5D3F1 F521          *.VL15.
Xmit:  SentBytes SentFrames  FramesQd  FramesWAck AllowdRate ActualRate Tokens?
      0x00003009 0x00000057      0          0      311Kbps      0Kbps  AVAIL
Recv:  RcvdBytes RcvdFrames  OutOfSeqQ  FramesDiscarded ARBmode
      0x0000349B 0x00000055      0          0          GREEN
Misc:  SmoothedRoundTrip  SR_timeouts  FramesResent  Pathswitches
      654ms              2              0
;
FwdMinLinkCapacity: 15974Kb/s, ReverseMinLinkCapacity: 15974Kb/s

Each set of data below is taken over 5 min intervals - New(top), Old(bottom)
Allwdsndrate Actlsndrate SmRoundTrip FramesResent PacketsDisc GapsReptd
  0KB/s        0KB/s        0ms          0          0          0
  0KB/s        0KB/s        0ms          0          0          0
  0KB/s        0KB/s        0ms          0          0          0
  0KB/s        0KB/s        0ms          0          0          0
  0KB/s        0KB/s        0ms          0          0          0
  0KB/s        0KB/s        0ms          0          0          0
  
```

Tabla 73 (Página 1 de 2). Descripción de la salida

Elemento	Descripción	Valores clave
Role	La función del direccionador en el establecimiento de esta conexión RTP.	ACTIVE PASSIVE
State	El estado actual de la conexión. Si la conexión RTP está experimentando actualmente una conmutación de la vía de acceso, se añade la serie "in path switch" al valor de estado (p.e., "CONNECTED, in path switch").	CONNECTED CONNECTING DISCONNECTING OPENED CALLING LISTENING
Tokens?	Si el direccionador tiene permiso para enviar en este instante de tiempo. Es normal que Tokens sea NOT AVAIL cuando el valor de FramesQd es distinto de cero, con tal de que las visualizaciones subsiguientes muestren SentBytes y SentFrames en aumento.	AVAIL NOT AVAIL
ARB mode	El estado que el direccionador notifica como receptor a su asociado basándose en la congestión de la red detectada por medio de cálculos ARB.	GREEN YELLOW RED
SR timeouts	El número de veces que el temporizador de peticiones cortas ha caducado. Este temporizador se inicia cuando el direccionador envía un mensaje de control a su asociado a RTP. La caducidad del temporizador indica que la respuesta no ha venido dentro del tiempo esperado.	--
MinLinkCapacity	La capacidad del TG más lento a lo largo de esta ruta de RTP.	--

## Mandatos de supervisión de APPN

<i>Tabla 73 (Página 2 de 2). Descripción de la salida</i>		
Allowed send rate	La velocidad de envío de datos máxima permitida por el receptor. Éste es un valor de promedio sobre el intervalo de 5 minutos.	--
Actual send rate	La velocidad de envío de datos calculada sobre la base de los bytes reales transmitidos entre las dos últimas peticiones relativas a velocidad. Si no hay datos para enviar, esta velocidad se reduce. Éste es un valor de promedio sobre el intervalo de 5 minutos.	--
Smoothed round trip	El promedio de tiempo para enviar datos al otro extremo de la conexión y obtener respuesta del mismo, promedio tomado sobre el intervalo de 5 minutos.	
Frames resent	El número de tramas que este direccionador ha reenviado en este intervalo de 5 minutos debido a los espacios notificados por el nodo asociado receptor (un solo espacio puede dar como resultado el reenvío de diversas tramas).	--
Packets disc	El número de paquetes recibidos que este direccionador ha desechado, en este intervalo de 5 minutos, debido a una falta de almacenamientos intermedios de APPN en el mencionado direccionador o a la detección de una infracción del protocolo.	--
Gaps reptd	El número de espacios de datos que este direccionador ha notificado como receptor, durante este intervalo de 5 minutos, al nodo asociado emisor.	--

### list session\_information

Utilice este mandato para visualizar una lista de las sesiones de ISR que fluyen por el direccionador. Estas sesiones son las que se han contado, siguiendo los enlaces, con el mandato **list isr** e incluyen:

- Sesiones que entran y salen del sistema mediante ISR
- Sesiones que entran en el sistema mediante ISR pero salen sobre una conexión RTP
- Sesiones de LU de TN3270 direccionadas por DLUR que salen del sistema mediante ISR

Este mandato no lista las sesiones de control de LU6.2 con un punto final en el direccionador; utilice **list appc** para ver estas sesiones. Para poder ver la salida completa de este mandato,

es necesario que haya configurado los parámetros de gestión de nodo APPN con el fin de guardar la información de los RSCV de las sesiones intermedias.

**Ejemplo:**

```
APPN > li sess
Origin CP Name      Primary LU      Secondary LU  Mode Name
-----
STFNET.VL15        STFNET.VL15    STFNET.MVS8   #INTER
STFNET.VL15        STFNET.VL15    STFNET.MVS8   SNASVCMG
STFNET.MVS8        STFNET.MVS8    STFNET.VL15   CPSVRMGR
STFNET.VL15        STFNET.VL15    STFNET.MVS8   CPSVRMGR
```

Tabla 74. Descripción de la salida		
Elemento	Descripción	Valores clave
Origin CP name	El nombre de CP del nodo que posee la LU primaria para esta sesión.	--
Primary LU	El nombre de LU de la LU primaria.	--
Secondary LU	El nombre de LU de la LU secundaria.	--
Mode name	El nombre de modalidad utilizado para definir esta sesión.  Tenga en cuenta que los nombres de modalidad de las sesiones de control de LU6.2 (p.e., de conducto DLUR-DLUS) no significan que estas sesiones terminen en el direccionador. En lugar de ello, pasan por el direccionador mediante ISR. Utilice <b>list appc</b> para ver las sesiones que terminan en el direccionador.	#CONNECT = prioridad media estándar #INTER = prioridad alta estándar CPSVCMG = sesión de CP-CP CPSVRMGR = sesión de DLUR-DLUS SNASVCMG = sesión de punto focal  están estructurados otros nombres de modalidad y también pueden estar definidos por el usuario

**list status**

Utilice este mandato para visualizar un resumen de la configuración general de APPN e información sobre su estado. La salida proporciona una visión “instantánea” del estado actual.

**Ejemplo:**

```
APPN > li stat
Fully Qualified CP NAME : STFNET.NETU24
Node up Time           : 6 hrs 50 min 21 Sec
Extended Border Node   : Not Supp   Branch Extender : Not Supp
DLUR                   : ACTIVE     TN3270E         : ACTIVE
Main Mem Stat          : OK          Buffer Mem Stat  : OK
```

Tabla 75 (Página 1 de 2). Descripción de la salida		
Elemento	Descripción	Valores clave
FQ CP name	El ID de red y nombre de CP configurados de este direccionador.	--
Node up time	El período de tiempo transcurrido desde el último reinicio de APPN.	--
Extended border node	Si el direccionador está configurado para que sea un EBN.	Supp = configurado Not Supp = no configurado

## Mandatos de supervisión de APPN

Tabla 75 (Página 2 de 2). Descripción de la salida		
Branch Extender	Si el direccionador está configurado para que sea un nodo extensor de rama.	Supp = configurado Not Supp = no configurado
DLUR	Si está configurada y activa la función DLUR.	ACTIVE = configurada y en ejecución NOT ACT = sin configuración o sin ejecución
TN3270E	Si está configurada y activa la función de servidor TN3270.	ACTIVE = configurada y en ejecución NOT ACT = sin configuración o sin ejecución
Main mem stat	El estado actual de la parte principal de la memoria de APPN.	OK CONSTRED = restringido CRITICAL
Buffer mem stat	El estado actual de la parte de almacenamientos intermedios de la memoria de APPN.	OK SLOWDOWN CONSTRED = restringido CRITICAL

### list topo node

Utilice este mandato para visualizar información de topología sobre un nodo determinado de una subred de la topología de este direccionador.

#### Ejemplo:

```
APPN > li topo node
NODE NAME []? stfnet.rbkim
CP NAME          NODE ROUTE CON TIME  RSN  BN  HPR  ICN  CDS NAT
                  TYPE RES  GES  LEFT
;                IVE
=====
STFNET.RBKIM      NN  128  N   15   23   Y  CF   N  N  Y
ACTIVE TGs ORIGINATING FROM THIS NODE

DESTINATION CP    CP_CP    HPR  TG_TYPE  TG NUM
=====
NETIDA.RB61      ACT     Y   APPN     21
STFNET.MVS3      ACT     Y   APPN     21
STFNET.RBB0B     NOTSUP  Y   APPN     21
STFNET.RBBRUNO  ACT     Y   APPN     21
```

Tabla 76 (Página 1 de 2). Descripción de la salida		
Elemento	Descripción	Valores clave
CP name	El nombre de punto de control del nodo, el valor que ha entrado el usuario.	--
Node type	El tipo estructurado del nodo.	NN EN VN = nodo virtual (p.e., red de conexiones)



<i>Tabla 76 (Página 2 de 2). Descripción de la salida</i>		
Route res	La resistencia a la adición de rutas (un valor superior significa mayor resistencia a la adición de nuevas rutas por el nodo). Normalmente, este valor se configura en el nodo y no es dinámico.	--
Conges	Si hay congestión o no, lo que notifica el nodo dinámicamente.	Y = sí N = no
Time left	Los días que quedan para que esta entrada de base de datos de topología caduque. Si tiene que forzar la desaparición de la entrada para que ésta se produzca más pronto, VTAM proporciona funciones de supresión de topología que pueden causar que el direccionador elimine entradas.	--
RSN	El número de secuencia de recurso para este nodo, que se utiliza para determinar si una actualización recibida contiene nueva información que no se haya visto con anterioridad.	--
BN	Si el nodo realiza la función Border Node.	Y = sí N = no
HPR sup	El nivel de soporte del HPR que el nodo puede realizar.	BASE = reenvío de ANR solamente TRAN = transporte - sólo puede tener puntos finales RTP para las sesiones de datos CF = flujo de control - puede tener puntos finales RTP para las sesiones de datos y de control
ICN	Nodo de intercambio - si el nodo es un nodo VTAM que realiza la función de APPN y de subárea SNA.	Y = sí N = no
CDS	Servidor de directorios central.	Y = sí N = no
Native	Si el nodo está en la subred de la topología del direccionador. Tenga en cuenta que un nodo puede tener el mismo ID de red y estar en una subred de topología diferente.	Y = sí N = no

Para obtener una descripción de los campos de la lista "Active TGs originating from this node", vea el mandato **list topo tg**.

#### **list topo status**

Utilice este mandato para visualizar un resumen de las estadísticas de base de datos de topología.

## Mandatos de supervisión de APPN

```

APPN > li topo st
Max num of Nodes allowed in Topo( 0 = limit is memory ) : 5400
Current number of Nodes in Topology : 25
Number of Node records purged from this node : 0
Number of TG records purged from this node : 0
The last flow reduction seq num sent out by this node : 259
Topology safe store frequency ( 0 = not saved) : 0
    
```

Tabla 77. Descripción de la salida

Elemento	Descripción	Valores clave
Max nodes allowed	El valor calculado del número máximo de nodos permitidos en la base de datos, el cual está basado en la cantidad de memoria de APPN, el tipo de producto y diversos límites relativos a valores mínimos y máximos.	--
Number of node records purged	El número de registros de nodo suprimidos debido a que han caducado o a operaciones de topología de red iniciadas por VTAM.	--
Number of TG records purged	El número de registros de nodo suprimidos debido a que han caducado o a operaciones de topología de red iniciadas por VTAM.	--
Last FRSN sent out	El número más reciente de secuencia de reducción de flujo enviado por este nodo a cualquier otro nodo.	--
Topology safe store frequency	El tiempo configurado en minutos entre las copias de seguridad de base de datos de topología creadas en el disco duro del direccionador.	0 = no se ha habilitado el almacenamiento seguro de la topología

### list topo tg pares distintivo-valor

Utilice este mandato para visualizar información de la base de datos de topología del direccionador sobre TG activos (enlaces, o grupos de transmisión) de una subred de esta topología.

Para limitar los datos visualizados, puede especificar uno o más de uno de los distintivos de filtro siguientes y los valores correspondientes.

Tabla 78. Descripción de la salida

Distintivo de filtro	Valor
-c	El nombre de CP del propietario de TG, que puede estar calificado con ID de red o no
-n	El ID de red del propietario de TG
-p	El nombre calificado al completo del asociado a TG

### Ejemplo:

```

APPN > li topo tg -c c20015
ACTIVE TG's
TG OWNER          TG DESTINATION  CP_CP  HPR  TG_TYPE  TG      RSN
                NUM
=====
STFNET.C20015     STFNET.VLNN045  ACT    Y   APPN     23     444
STFNET.C20015     STFNET.PDLUR2   ACT    N   APPN     1      436
    
```

Tabla 79. Descripción de la salida

Elemento	Descripción	Valores clave
TG owner	El nombre de CP del nodo que ha notificado este TG. Los dos puntos finales de un TG notifican el TG, en cada caso uno como propietario y el otro como destino.	--
TG destination	El nombre de CP del otro extremo del TG en relación con el propietario.	--
CP-CP	El soporte de sesiones de CP-CP existente en este TG.	ACT = activas NOTSUP = sin soporte SUPINACT = con soporte pero inactivas (p.e., los TG paralelo en que solamente uno lleva sesiones de CP-CP) UNK = se desconoce
HPR	El soporte del HPR existente en este TG.	Y = sí N = no
TG type	El tipo estructurado de este TG.	APPN INTER = intercambio, un enlace de subárea con APPN VIRT = virtual, p.e. un enlace con un nodo virtual de red de conexiones

**Log**

Utilice este mandato para visualizar la anotación cronológica de sucesos internos de APPN.

**Sintaxis:**

```

log
  status
  view
    
```

**log status**

APPN mantiene su propia anotación cronológica de sucesos internos además de la anotación cronológica de sucesos ELS del direccionador. Utilice este mandato para visualizar estadísticas de resumen actuales sobre la anotación cronológica de sucesos de APPN.

**Ejemplo:**

## Mandatos de supervisión de APPN

```

APPN > log st
Entries: 32, Discarded: 0, Filtered: 25959, Memory: 9348 of 273400
Filters enabled:
    none
Display direction: Descending
Top Entry:
    32|Jul 23 15:16:15 2F107-24 (E) SCM - UNBIND cleanup is being generated
Bottom Entry:
    1|Jul 23 08:55:45 2F104-14 (E) NOF unable to monitor EGPE environment
Current Time:
    Fri Jul 23 15:47:35 1999
    
```

Tabla 80. Descripción de la salida

Elemento	Descripción	Valores clave
Entry numbers	El número total de entradas, el número de eliminaciones por quedar llena la anotación cronológica, así como el número de operaciones de filtración a causa de duplicados.	--
Memory size	El tamaño actual de la anotación cronológica de errores y el tamaño máximo en bytes. El tamaño máximo está fijado en un 1%, aproximadamente, de la memoria de APPN.	--
Filters enabled	Una lista de los filtros de visualización de salida de anotación cronológica que el usuario ha establecido actualmente.	none Severity: <i>nivel de gravedad</i> Message: <i>ID de mensaje</i>
Display direction	El orden cronológico de la visualización de salida que el usuario ha establecido actualmente.	Descending (lo más reciente en la parte superior) Ascending
Top/bottom entries	La línea de resumen de cada una de estas entradas (el orden depende de la orientación de la visualización). Ello le permite ver el ámbito cronológico de las entradas que están actualmente en la anotación cronológica.	--
Current time	El día y la hora actuales con la misma base que las entradas de anotación cronológica.	--

### log view

Utilice el mandato **log view** para entrar en un submenú de mandatos que le permitirá navegar y ver la anotación cronológica de sucesos de APPN.

Cuando entre en la modalidad de visualización de anotación cronológica, puede utilizar los mandatos **bottom**, **top**, **goto**, **next** y **prev** para trasladarse y visualizar entradas de anotación cronológica en modalidad de resumen (una página de entradas de 1 ó 2 líneas cada vez). Utilice los mandatos **det next**, **det prev** y **det entry** para trasladarse y visualizar la información detallada de entradas de anotación cronológica individuales.

El submenú de visualización de anotación cronológica también contiene mandatos para controlar los valores de la visualización de anotación cronológica. Puede utilizar el mandato **filter** para seleccionar el nivel de gravedad mínimo que desee ver o para buscar un solo tipo de mensaje. Cada utilización del mandato **filter** altera temporalmente todos los valores anteriores; no se combina con los mandatos anteriores. Puede utilizar el mandato **set** para establecer las preferencias de visualización de anotación cronológica.

La sintaxis y las funciones del submenú son las siguientes:

<i>Tabla 81 (Página 1 de 2). Sintaxis del submenú Log view</i>		
<b>Mandato</b>	<b>Palabras clave y parámetros</b>	<b>Función</b>
<u>b</u> ottom		Trasladar a la parte inferior, mostrar página de resumen
<u>c</u> urrent		Volver a visualizar la página de resumen actual
<u>d</u> etail	<u>n</u> ext_entry	Visualizar en detalle la siguiente entrada
	<u>p</u> rev_entry	Visualizar en detalle la entrada anterior
	<u>e</u> ntry_id <i>núm_sec</i>	Visualizar en detalle la entrada especificada
<u>f</u> ilter	<u>a</u> ll	Borrar los filtros de salida (mostrarlo todo)
	<u>o</u> nly <u>s</u> everity <u>a</u> ction_ <u>r</u> equired	Mostrar las entradas con la gravedad de este tipo o superior
	<u>c</u> ritical	
	<u>e</u> rror	
	<u>w</u> arning	
	<u>i</u> nformational	
	<u>m</u> essage <i>id-mensaje</i>	Mostrar solamente las entradas con este mensaje
<u>g</u> oto_entry	<u>s</u> equence_num	Trasladar a entrada, mostrar página de resumen
<u>n</u> ext_page		Visualizar la siguiente página de resumen
<u>p</u> rev_page		Visualizar la página de resumen anterior
<u>s</u> et	<u>l</u> ines_in_page	Mostrar esta variedad de líneas en la página
	<u>d</u> irection <u>a</u> scending	Mostrar la entrada más reciente como la última
	<u>d</u> escending	Mostrar la entrada más reciente como la última
<u>t</u> op		Trasladar a la parte superior, visualizar página de resumen

<i>Tabla 81 (Página 2 de 2). Sintaxis del submenú Log view</i>		
<u>e</u> xit		Volver al menú de APPN principal de t 5

**Ejemplo:**

```

APPN > log v
LOG VIEW
LOG VIEW >?
BOTTOM
CURRENT
DETAIL
FILTER
GOTO_ENTRY
NEXT_PAGE
PREV_PAGE
SET
TOP
EXIT
LOG VIEW > top
32|Jul 23 15:16:15 2F107-24 (E) SCM - UNBIND cleanup is being generated
31|Jul 23 15:16:15 2F107-24 (E) SCM - UNBIND cleanup is being generated
30|Jul 23 15:08:15 2F10A-1A (I) Request Route
29|Jul 23 15:08:15 2F10A-07 (E) REQUEST_ROUTE_RSP failed
28|Jul 23 15:08:15 2F10A-1A (I) Request Route
27|Jul 23 15:08:15 2F10A-07 (E) REQUEST_ROUTE_RSP failed
26|Jul 23 15:08:15 2F10A-1A (I) Request Route
25|Jul 23 15:08:15 2F10A-07 (E) REQUEST_ROUTE_RSP failed
24|Jul 23 11:41:06 2F120-18 (C) Correlation table entry was not found.
23|Jul 23 11:37:46 2F120-18 (C) Correlation table entry was not found.
22|Jul 23 11:07:27 2F120-18 (C) Correlation table entry was not found.
21|Jul 23 11:07:27 2F126-0D (E) TNS0013I %1: Keepalive processing detected error
; the connection between IP addr %2 and LU %3 has been ended.

LOG VIEW > det e 21
-----
Sequence Number: 210
APPN Lifetime: 7206.950 seconds
Fri Jul 23 11:07:27 1999
ProbeID 226066B3
Message 2F126000-0000000D
Severity: Error

TNS0013I %1: Keepalive processing detected error ; the connection between IP addr
%2 and LU %3 has been ended.
(Sn) e124102
(Sn) 15.170.99.210
(Sn) STAT1
    
```

<i>Tabla 82 (Página 1 de 2). Descripción de la salida (la página de resumen, de izquierda a derecha)</i>		
<b>Elemento</b>	<b>Descripción</b>	<b>Valores clave</b>
Un número de secuencia	El número exclusivo asignado a este suceso cuando se graba en la anotación cronológica (no cuando se visualiza). Éste es el número que se utiliza con los mandatos "goto" y "detail".	--
Una fecha / hora	El momento en que se ha producido el suceso, según el reloj de este direccionador.	--

<i>Tabla 82 (Página 2 de 2). Descripción de la salida (la página de resumen, de izquierda a derecha)</i>		
Un ID de mensaje	El identificador de mensaje principal-menor para la condición que se ha producido. Consulte el manual "APPN Log Event Reference Guide" para obtener una descripción de cada posible mensaje. Añada tres ceros a la parte principal del ID y anteponga seis ceros a la parte menor para conseguir una correlación con los valores del manual Reference Guide.	--
Gravedad	La clasificación de APPN relativa al nivel de gravedad del suceso. Los valores clave aparecen listados por orden de gravedad en sentido decreciente.	A = acción necesaria C = crítico E = error W = aviso I = informativo
Un nombre de suceso	La descripción breve del suceso. Utilice el mandato "detail" y el manual Reference Guide para obtener más información.	--

<i>Tabla 83 (Página 1 de 2). Descripción de la salida (la información detallada de un suceso)</i>		
<b>Elemento</b>	<b>Descripción</b>	<b>Valores clave</b>
Sequence number	El mismo número descrito anteriormente respecto a la página de resumen.	--
APPN lifetime	El tiempo en segundos desde el último reinicio de APPN.	--
Una fecha / hora	Igual que en la página de resumen.	--
Probe ID	El ID de la ubicación exacta del software que ha anotado cronológicamente este error.	
Message ID	Igual que en la página de resumen, pero está ampliado con ceros iniciales y de cola para que coincida con el manual "APPN Log Event Reference Guide".	--
Severity	Los mismos valores que en la página de resumen, pero ampliados en palabras.	Vea más arriba

## Mandatos de supervisión de APPN

Tabla 83 (Página 2 de 2). Descripción de la salida (la información detallada de un suceso)		
Un nombre de suceso	La descripción breve del suceso, que está ampliada con los elementos de datos listados debajo. Utilice el manual Reference Guide para obtener más información.	--
Etiquetas de tipo de datos	Los identificadores de los diferentes tipos de datos anotados cronológicamente con cada mensaje. Consulte el manual Reference Guide para obtener una descripción de los elementos de datos que hay junto con cada mensaje.	(Ix) (Se) ( X) otros ...

### Memory

Utilice el mandato **Memory** para visualizar información sobre el uso de la memoria en APPN.

#### Sintaxis:

memory

#### Ejemplo:

APPN > mem

APPN memory status:

	Size (MB)	Percent in-use	State
Main	152	17	OK
Buffer	19	0	OK
Total	171	14	

APPN total shared memory size= 179200000, special use= 800

APPN main part: size = 159487200 crit\_thresh= 151512840 cons\_thresh= 143538480

APPN main part: inuse= 26516176 (incl: Trace tbl=65536, Error log= 1447)

APPN main part: peak memory usage= 26518048

APPN main part: event counts: crit= 0 cons= 0 OK = 1

APPN main part: OK for last 278211 seconds

APPN bufr part: size = 19712000 crit= 18726400 cons= 17740800 slow= 13404160

APPN bufr part: inuse= 1232 reserved (< slow)= 24992

APPN bufr part: peak memory usage= 26360

APPN bufr part: event counts: crit= 0 cons= 0 slow= 0 OK = 1

APPN bufr part: OK for last 278211 seconds

Tabla 84 (Página 1 de 4). Descripción de la salida		
Elemento	Descripción	Valores clave



<i>Tabla 84 (Página 2 de 4). Descripción de la salida</i>		
Total shared memory	<p>El tamaño configurado, en bytes, de la memoria de datos de APPN y servidor TN3270. Se establece cuando se configura APPN. No incluye el espacio de código de APPN o direccionador ni la memoria de datos/almacenamientos intermedios que necesitan otros componentes del direccionador.</p> <p>La parte de este elemento denominada "special use" no cuenta en la parte principal ni en la de almacenamientos intermedios y sirve para las estructuras de control del sistema APPN.</p>	--
Main part	<p>La parte de la memoria compartida de APPN que se utiliza para bloques de control, tablas de rastreo, mensajes internos y otros datos generales fijos y dinámicos.</p> <p>Esta parte incluye dos áreas de datos especiales: - una tabla de rastreo (Trace tbl) fijada en un 2% de la memoria compartida total o en 64 KB, el valor que sea mayor. Para Network Utility, está fijada en 20 MB. Esta tabla se asigna en el arranque de APPN. - una anotación cronológica de sucesos (Error log) que aumenta hasta un 1% de la memoria compartida total.</p>	--
Buffer part	<p>La parte de la memoria compartida de APPN que se utiliza para almacenamientos intermedios de paquetes/tramas.</p> <p>La parte de este elemento denominada "reserved" es un número dinámico de espacio de almacenamiento intermedio comprometido que estadísticamente sirve de reserva de un espacio de almacenamiento intermedio lógico más grande. "(&lt; slow)" indica que este valor debe permanecer por debajo del umbral de lentitud para el funcionamiento normal.</p>	--

## Mandatos de supervisión de APPN

<i>Tabla 84 (Página 3 de 4). Descripción de la salida</i>		
Main states	<p>El estado de la parte principal de la memoria de APPN en relación con los valores de umbral calculados.</p> <p>Cuando el estado de la parte principal va adquiriendo progresivamente una mayor congestión, APPN emprende algunas de estas acciones para ayudar a aliviar la congestión: poner los enlaces en estado de ocupación local y rechazar búsquedas de difusión de entrada.</p>	<p>OK</p> <p>Constrained</p> <p>Critical</p>
Buffer states	<p>El estado de la parte de almacenamientos intermedios de la memoria de APPN en relación con los valores de umbral calculados. Tenga en cuenta que se considera que el estado de la parte de almacenamientos intermedios es crítico cada vez que el estado de la parte principal es crítico, sea cual sea el nivel del uso de la memoria de almacenamientos intermedios.</p> <p>Cuando el estado de la parte de almacenamientos intermedios va adquiriendo progresivamente una mayor congestión, APPN emprende algunas de estas acciones para ayudar a aliviar la congestión: rechazar nuevas sesiones, hacer que el ritmo del flujo de datos de sesión sea más lento, notificar la congestión del nodo en las actualizaciones de topología, hacer que los remitentes de RTP vayan más despacio, poner los enlaces en estado de ocupación local e incluso desconectar las sesiones actuales con la prioridad más baja.</p>	<p>OK</p> <p>Slowdown</p> <p>Constrained</p> <p>Critical</p>
Inuse, peak usage	<p>El número actual de bytes utilizados y el nivel máximo que el valor de Inuse ha alcanzado alguna vez.</p>	--
Event counts	<p>El número de veces que ha aparecido un estado determinado desde el último reinicio de APPN.</p>	--

Tabla 84 (Página 4 de 4). Descripción de la salida

<estado> for last nn seconds	El período de tiempo durante el que la parte de la memoria ha permanecido en el estado actual. Si el nodo ha entrado alguna vez en un estado de agotamiento, se proporciona información adicional sobre la duración de este estado, el tiempo transcurrido desde entonces, etc.	--
------------------------------	---	----

### Rtp status

Utilice el mandato **rtp status** para visualizar información sobre la configuración global de RTP que actualmente se utiliza.

#### Sintaxis:

**rtp status**

#### Ejemplo:

```
APPN > rtp stat
Network          High      Medium    &
nbspc; Low
Liveness timer   180       180       180       180
Path Switch Timer 180       180       180       180
Retries          6         6         6         6
```

Tabla 85. Descripción de la salida

Elemento	Descripción
Network, etc.	Prioridad de transmisión de SNA.
Liveness timer	El tiempo en segundos entre los mensajes de pulsaciones cuando no hay tráfico del usuario.
Path switch timer	El tiempo máximo en segundos para efectuar una conmutación de la vía de acceso antes de que falle la conexión RTP.
Retries	El número de reintentos de petición corta a realizar antes de intentar efectuar una conmutación de la vía de acceso.

### Rtp switchpath

Utilice el mandato **rtp switchpath** con el fin de forzar una conmutación de la vía de acceso de HPR para una conexión RTP que tiene un punto final en este direccionador. La operación de conmutación de la vía de acceso selecciona la mejor vía de acceso actualmente disponible, que en realidad puede ser la vía de acceso actual. En cualquier caso, la conmutación de la vía de acceso causa una suspensión temporal del flujo de tráfico del usuario en la conexión RTP especificada.

Para utilizar este mandato, ejecute primero **list rtp** con el fin de determinar el TCID de la conexión RTP en la que desea forzar una conmutación de la vía de acceso.

## Mandatos de supervisión de APPN

Escriba "rtp switch" y proporcione este TCID cuando se le solicite. Para ver los resultados de la conmutación de la vía de acceso, utilice **list rtp tcid** y observe el estado de la conexión para determinar cuándo se completa la conmutación de la vía de acceso (el estado se activa). Puede ver la nueva vía de acceso en el RSCV o utilizando el mandato **rtp test**.

### Sintaxis:

**rtp switchpath**

### Rtp test

Utilice el mandato **rtp test** para realizar una prueba de ruta de HPR y visualizar información sobre cada salto de enlace existente en la vía de acceso de la conexión RTP. Utilice primero el mandato **list rtp** para determinar el TCID de la conexión RTP que desea probar. Este mandato lleva a cabo la misma acción que el mandato antiguo **test rtp**.

### Sintaxis:

**rtp test**

### Ejemplo:

```
APPN > rtp test
Enter TCID of the route to be tested [0]? 31B96928
Route Test issued
Waiting for 10 Seconds.....
Information
=====
Result      : SUCCESS
Detailed Information
=====
TG OWNER          TG DEST NAME          TGNUM  RT    DELTA  RESULT
                TG DEST NAME          TIME   TIME  TIME
=====
STFNET.VLNN105    STFNET.VL16           21     8     8     SUCCESS
STFNET.VL16       STFNET.VL15           21    68    60    SUCCESS
```

Tabla 86 (Página 1 de 2). Descripción de la salida

Elemento	Descripción	Valores clave
Result (valor general)	El estado o la razón de la anomalía con respecto a la operación de prueba de ruta.	SUCCESS IN PROGRESS NO RESPONSE INVALID NCE ID INVALID TCID NO ROUTE
TG owner	El nombre de CP del nodo más próximo en el salto de esta ruta.	--
TG dest name	El nombre de CP del nodo alejado en el salto de esta ruta.	--

<i>Tabla 86 (Página 2 de 2). Descripción de la salida</i>		
TG num	El número de este enlace negociado entre el propietario y el destino.	--
RT time	El tiempo de ida y vuelta en milisegundos desde el direccionador al destino del TG.	--
Delta time	El tiempo de ida y vuelta en milisegundos desde el propietario del TG al destino, es decir, la parte del elemento RT time que sólo es para este salto.	--
Result (valor de detalle)	El estado de la llegada al destino de este salto.	SUCCESS NO REPONSE

### Restart

Utilice el mandato **restart** para reiniciar APPN y TN3270 de manera disruptiva, sin reiniciar o volver a cargar el resto del software del direccionador. Si todavía no se ha detenido APPN, este mandato lo detiene antes de reiniciarlo.

Cuando APPN se reinicia, utiliza la información de configuración actual de la memoria, tanto si esta información se ha grabado en disco mediante el mandato `talk 6 write` (sólo en los modelos de direccionador con un disco duro) como si no ha sido así.

#### Sintaxis:

restart

### Stop

Utilice el mandato **stop** para detener APPN y TN3270 de manera disruptiva, sin que afecte al resto del direccionador.

#### Sintaxis:

stop

### TN3270E

Utilice el mandato **tn3270e** para acceder al indicador de mandatos `TN3270E>`, desde el que puede visualizar información sobre la configuración de TN3270E.

Vea la Tabla 87 en la página 276 para obtener una descripción de estos mandatos.

#### Sintaxis:

tn3270e

## Transmit

Utilice el mandato **transmit dump** para transmitir un archivo de vuelco de memoria de APPN desde el disco duro del direccionador a un servidor TFTP sobre una interfaz de red. Utilice el mandato **list dump** para buscar el número del archivo a transmitir. El destino de servidor TFTP se configura mediante los mandatos `talk 6` de APPN **set dump target** y **enable dump-memory**.

Este mandato no está disponible para los direccionadores que no tienen disco duro.

### Sintaxis:

`transmit dump-number`

## Mandatos de supervisión de TN3270E

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxxi.
Deactivate <i>nombre_lu</i>	Desactiva una LU utilizada por un cliente TN3270 y desconecta la conexión TCP correspondiente a este cliente.
List	Lista lo siguiente de la memoria de la configuración: <ul style="list-style-type: none"><li>• Connections</li><li>• Connections <i>nombre de LU</i></li><li>• Connections <i>dirección IP</i></li><li>• Maps</li><li>• Pools</li><li>• Pools <i>nombre de agrupación</i></li><li>• Ports</li><li>• Status</li></ul>
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxi.

## Deactivate LU

Utilice el mandato **deactivate LU** para desactivar una LU utilizada por un cliente TN3270 y para desconectar la conexión TCP correspondiente a este cliente. Utilice primero el mandato **list conn** para determinar el nombre de LU local sobre la base de la dirección IP, nombre de LU de VTAM o nombre de agrupación.

Este mandato proporciona el estado de cuando se completa, satisfactorio o con anomalía, aunque el usuario también puede utilizar los mandatos de listar para

comprobar el estado. Después de la desactivación, el cliente ya no debe aparecer en **list conn**, y **list lu** o **list pu nombrepu** deben reflejar el cambio en el estado de la LU.

**Sintaxis:**

**deactivate lu nombre\_lu local**

## List

Utilice el mandato **list** para visualizar información sobre las conexiones TN32870.

**Sintaxis:**

**list**  
connections  
 lu nombre\_LU\_interna  
mapping  
pools  
pools nombre\_agrupación  
ports  
pu  
pu nombre\_pu  
rejections  
status

**Mandato**

**Función**

**list connections** par *distintivo-valor*

Utilice este mandato para visualizar una lista completa o de subconjunto de las conexiones de cliente TN3270 activas.

Para limitar los datos visualizados, puede especificar uno o más de uno de los distintivos de filtro siguientes y los valores correspondientes:

<i>Tabla 88. Descripción de los distintivos</i>	
<b>Distintivo de filtro</b>	<b>Valor</b>
-l (distintivo no necesario, es posible escribir sólo el valor)	El nombre de la LU o de la agrupación del direccionador
-i (distintivo no necesario, es posible escribir sólo el valor)	La dirección IP de cliente o la subserie inicial de esta dirección. Por ejemplo, 9.67 servirá para todas las direcciones IP con el formato 9.67.*.*
-p	El nombre de LU primaria de VTAM
-s	El nombre de LU secundaria de VTAM (normalmente, no coincide con el nombre de LU del direccionador)

**Ejemplo:**

```

TN3270E > li conn
Local LU  Class  Assoc LU  Client Addr  Status  Prim LU  Sec LU  Idle Min
-----
PU1LU207  IW          9.37.182.187  LU-LU  NRAVM30  LU22207  8
PU1LU60   IW          9.37.176.39   LU-LU  NRAVM30  LU2260   52
PU1LU89   IW          9.37.178.49   LU-LU  NRAVM30  LU2289   288

```

Tabla 89. Descripción de la salida

Título de columna	Descripción	Valores clave
Local LU	El nombre de LU configurado o definido por sistema principal en el direccionador.	--
Class	El tipo de LU.	IW = estación de trabajo implícita EW = estación de trabajo explícita IP = impresora implícita EP = impresora explícita
Assoc LU	En el caso de una LU de estación de trabajo, el nombre de cualquier LU de impresora asociada.	--
Client addr	La dirección IP del cliente. Tenga en cuenta que una sola dirección IP de cliente puede tener diversas LU en uso si varía su puerto TCP de origen.	--
Status	El estado de la conexión de la LU.	estado SSCP-LU estado LU-LU en blanco = existe conexión TCP, pero la LU todavía no está conectada
Prim LU	El nombre de LU primaria conocido por VTAM	--
Sec LU	El nombre de LU secundaria conocido por VTAM	--
Idle min	El número de minutos transcurridos desde el transporte de datos del usuario de esta conexión.	--

#### **list lu nombre de LU interna**

Utilice este mandato para visualizar información detallada sobre la configuración y el estado de una sola LU interna. Utilice los mandatos **list conn** o **list pu nombre** con el fin de que le ayuden a determinar el nombre de LU del direccionador para una LU en particular.

#### **Ejemplo:**



```

TN3270E > li lu pu1lu207
LUNAME : PU1LU207      NAU : 207      LINK NAME : VM30PU1
POOL NAME : PUBLIC     MODEL : 3270002
SSCP_LU ST: NOT PCHSCON , LUENABLE , NOT ACTLURSP , NOT TRMNOTFY
              NOT NOTIFIED , ACTIVATD , NOT DEACTTNG , NOT ACTIVTNG
              NOT NMVTSNT , NOT NMVTRCV , COUNTED , NOT DACPUPEN
              NOT TERMPEND , NOT NMVTOFF
LU_LU ST : NOT SNTUNBND , BOUND , NOT UNBNDING , NOT BINDING
FLAGS : NOT SEGFOR , FAPBP , GETPCID , NOT BINDFRT
              NOT SESSTOP , NOT DETCHRCV , LSACON , HSACON
FLAGS1 : NOT MUEXPD , NOT PENDSF , WRAPNORM , NOT INOPST
              NOT SLI , NOT EXIT , OWNED , INITCOMP
VERB FLAGS: NOT EXIT , NOT SF , NOT TERM , NOT INIT , NOT PURG , NOT RD1
              NOT RD2 , NOT RD3 , NOT RD4 , BID , NOT WRI , NOT WR2
ACTLU : 4915      DACTLU : 0      BIND : 0
UNBIND : 0      NOTIFY : 1
MINI TRACE WRAPPED : NO NUMBER OF ENTRIES : 7
OTHERS : 14 : INIT ,NEW : INIT ,GETPCID : INIT ,PCIDREPY : INIT ,PCHSCOND
INIT ,SENNOTFY : INIT ,NOTFYRSP

```

Tabla 90. Descripción de la salida

Título de columna	Descripción	Valores clave
LU name	El nombre de LU configurado o definido por sistema principal en el direccionador, el valor que el usuario ha entrado.	--
NAU	La dirección SNA de NAU de 1 byte de esta LU en su PU (2-254). Este valor se visualiza ahora en decimal.	--
Link name	En el caso de los enlaces de sistema principal de subárea, el nombre de estación de enlace del enlace externo asociado con esta PU. En el caso de los enlaces de sistema principal de DLUR, el nombre de PU/estación del enlace interno con el DLUR.	--
Pool name	El nombre de la agrupación mediante la cual un cliente puede seleccionar esta LU.	--
Model	El modelo de impresora o pantalla 3270 al que da soporte esta LU.	--
SSCP_LU state	Las decodificaciones de valor de los bits individuales del estado de la sesión de SSCP-LU para esta LU, con destino al uso técnico.	--
LU_LU state	Las decodificaciones de valor de los bits individuales del estado de la sesión de LU-LU para esta LU, con destino al uso técnico.	--
Flags, Flags1, Verb flags	Otros distintivos de estado con destino al uso técnico.	--
El resto de la salida	Otra información sobre el estado con destino al uso técnico.	--

### list mapping

Utilice este mandato para ver las correlaciones entre dirección IP de cliente y LU de TN3270 configuradas del direccionador que están actualmente activas. También puede comprobar qué

entradas de correlación son aplicables a una dirección IP de cliente en particular.

Si desea limitar los datos visualizados a las entradas que el servidor utilizará para una dirección IP en particular, basta con especificar esta dirección IP cuando invoque este mandato.

**Ejemplo:**

```
TN3270E > li map
TN3270E Client IP Address to LU Name Maps
Client IP      Address      Resource      Last
Address      Mask          Name          Port    Map Type Resource
-----
8.1.1.99      255.255.255.255 <DEFLT>      23     Y  POOL WORKSTATION
9.9.9.9       255.255.255.255 LU45         0      Y  LU   WORKSTATION
9.1.1.1       255.255.255.255 LU47         0      Y  LU   PRINTER
4.4.4.4       255.255.255.255 LU46         0      Y  LU   WORKSTATION
7.7.7.7       255.255.255.255 LU48         0      Y  LU   PRINTER
2.2.2.2       255.255.0.0     POOL2        0      N  POOL PRINTER
1.1.1.1       1.1.1.1         POOL1        0      N  POOL WORKSTATION
0.0.0.0       0.0.0.0         <DEFLT>      0      N  POOL WORKSTATION
```

Tabla 91. Descripción de la salida

Elemento	Descripción	Valores clave
Client IP address	El germen de dirección IP de las direcciones IP de cliente coincidentes.	--
Address mask	La máscara de bits a aplicar al germen de dirección y a las direcciones de cliente de entrada para determinar si esta correlación corresponde a este cliente. Sólo se comparan las posiciones de bit en que el bit de máscara es 1.	255.255.255.255 = para comparar toda la dirección IP de cliente de entrada
Resource name	El nombre de LU o de agrupación configurado en el direccionador.	<DEFLT> = la agrupación por omisión configurada globalmente
Port	El puerto TCP de destino de servidor para que se comparen con esta entrada las conexiones que llegan.	0 = la entrada se aplica a todos los puertos de destino
Last map	En el caso de que se encuentre una coincidencia en esta entrada pero la agrupación/LU no pueda satisfacerla, si el servidor debe seguir con los intentos y comparar la conexión con entradas menos específicas.	Y = sí N = no
Type	Si el nombre de recurso es una LU o una agrupación.	LU POOL
Resource	El tipo de la LU o el tipo de las LU de la agrupación.	WORKSTATION PRINTER

**list pools**

Utilice este mandato para listar las agrupaciones con nombre configuradas de LU implícitas. Los clientes pueden solicitar cualquier LU de una agrupación si pasan el nombre de agrupación en la petición de conexión.

**Ejemplo:**

```

TN3270E > li pool

TN3270E Implicit pools
Default pool name : PUBLIC
Name                Class
-----
PUBLIC              WORKSTATION
POOL2               PRINTER
POOL1               WORKSTATION
POOL3               WORKSTATION
POOL4               WORKSTATION

```

Tabla 92. Descripción de la salida

Elemento	Descripción	Valores clave
Default pool name	El nombre de la agrupación por omisión global a la que se asocian todas las LU implícitas que no se han colocado en otra agrupación. Ésta es la agrupación a la que hace referencia la serie <DEFLT> en diversos mandatos y visualizaciones.	--
Name	El nombre configurado de la agrupación.	--
Class	El tipo configurado de las LU de la agrupación.	WORKSTATION PRINTER

### list pools nombreagrupación

Utilice este mandato para mostrar información detallada sobre la configuración de una sola agrupación de LU. Este mandato le permite ver cómo están distribuidas las LU de una agrupación entre las PU dependientes, cómo se denominan y qué tipo tienen. Para obtener información completa sobre las LU de una PU en particular, utilice el mandato **list pu nombre**.

#### Ejemplo:

```

TN3270E >li pools pool1
TN3270E Implicit Pool
-----
Pool Name : POOL1                      Pool Class : WORKSTATION
  Station Name : PU1
    LU Name Mask : @02LU
    Number of lus :200
    Model Type : 3270 mod 2

```

#### Ejemplo:

```

TN3270E >li pools pool2
TN3270E Implicit Pool
-----
Pool Name : POOL2                      Pool Class : PRINTER
  Station Name : PU1
    LU Name Mask : @03LU
    LU Address Range : 5-10,78-99
    Model Type : SCS

  Station Name : PU1
    LU Name: LU48
    NAU Address : 48
    Model Type : 3270

```

Tabla 93 (Página 1 de 2). Descripción de la salida

Elemento	Descripción	Valores clave
----------	-------------	---------------

Tabla 93 (Página 2 de 2). Descripción de la salida

Station name	En el caso de los enlaces de sistema principal de subárea, el nombre de estación de enlace asociado con la PU dependiente. En el caso de la conexión de sistema principal de DLUR, el nombre de PU local.	--
LU name mask	En el caso de las LU implícitas solamente, el germen de nombre configurado que el direccionador utiliza para generar nombres de LU dentro del número o rango de direcciones determinado.	--
LU address range	En el caso de las LU implícitas solamente, el rango de direcciones de NAU que el direccionador utiliza para generar LU en esta agrupación bajo esta PU.	--
Number of LUs	En el caso de las LU implícitas solamente, el número de LU generadas por el direccionador bajo esta PU.	--
LU name	En el caso de una LU explícita individual solamente, el nombre de LU configurado.	--
NAU address	En el caso de una LU explícita individual solamente, la dirección de NAU de 1 byte para la LU.	--
Model type	El tipo configurado de la LU o del grupo de LU.	<b>Para las pantallas:</b> 3270 mod 2 3270 mod 3 3270 mod 4 3270 mod 5 <b>Para las impresoras:</b> 3270 SCS

**list ports**

Utilice este mandato para visualizar todos los puertos TCP a los que los clientes TN3270 pueden conectarse y las características configuradas de cada puerto.

**Ejemplo:**

```

TN3270E > li ports
TN3270E Server Ports
Port Number  TN3270E  Resource Name  Disable Filtering
-----
23           Y          <DEFLT>       N
45           Y          <DEFLT>       N
66           Y          <DEFLT>       Y
88           Y          POOL1         N
99           Y          <DEFLT>       N
    
```

Tabla 94. Descripción de la salida		
Elemento	Descripción	Valores clave
Port number	El número del puerto TCP de destino del direccionador al que se conectan clientes.	--
TN3270E	Si este puerto está o no configurado para dar soporte a clientes "E".	Y = sí N = no
Resource name	El nombre de agrupación configurado para los clientes que se conectan a este puerto.	<DEFLT> = la agrupación por omisión implícita global los otros nombres están configurados por el usuario
Disable filtering	Si deben comprobarse las correlaciones de dirección IP de cliente para los clientes que se conectan a este puerto.	Y = sí N = no

### list pu

Utilice este mandato para visualizar todas las PU dependientes internas configuradas para LU de TN3270, incluidas las que utilizan el DLUR y las que utilizan enlaces de sistema principal de subárea.

#### Ejemplo:

```
TN3270E > li pu
PU NAME      STATUS      NODE ID  TOTAL  DDDL  -----LUs  IN-----
              LUs      ENABLED  ACTIV  OW
NED AVAILABL
-----
VM30PU1  ACTPU_RCVD  07711111  249   N    249      5    244
VM30PU2  ACTPU_RCVD  07722222  249   N    249      5    244
```

Tabla 95 (Página 1 de 2). Descripción de la salida		
Título de columna	Descripción	Valores clave
PU name	En el caso de las PU asociadas con enlaces de subárea, el nombre de estación de enlace configurado del enlace de sistema principal. En el caso de las PU asociadas con el DLUR, el nombre de PU local configurado.	--
Status	El estado actual de la sesión de SSCP-PU.	ACTPU_RCVD NOT ACTIVE
Node ID	El ID de nodo configurado interno que representa a esta PU dependiente para VTAM.	--
Total LUs	El número actual de LU definidas en el direccionador bajo esta PU. Se incluyen tanto LU configuradas como LU dinámicas iniciadas por sistema principal activas.	--
DDDLU enabled	Si esta PU está configurada para la definición de LU de tipo dinámico.	Y = sí N = n

Tabla 95 (Página 2 de 2). Descripción de la salida		
LU's active	El número de LU que el sistema principal ha activado a partir de ACTLU. Este número puede incluir tanto LU configuradas como LU con DDDLU iniciadas por sistema principal.	--
LU's owned	El número de LU que están asociadas con conexiones TCP de cliente.	--
LU's available	El número de LU que están activas o tienen posibilidad de DDDLU y se encuentran sin propietario, por lo cual están disponibles para que las utilicen clientes TN3270. Este número puede incluir LU configuradas cuya PU esté activa y dé soporte a DDDLU, pero no incluye LU con DDDLU iniciadas por sistema principal si no están activas.	--

**list pu nombre-pu** Utilice este mandato para visualizar información sobre la configuración y el estado de todas las LU que se encuentran bajo una PU dependiente determinada del direccionador. Estas LU son:

- LU implícitas configuradas, cuyos nombres genera el direccionador basándose en gérmenes de nombre configurados y cuyas direcciones de NAU asigna el direccionador basándose en rangos de direcciones o números de LU configurados
- LU explícitas configuradas, cuyos nombres y direcciones de NAU están completamente configurados
- LU dinámicas iniciadas por sistema principal, cuyos nombres y direcciones de NAU establece el sistema principal

**Ejemplo:**

```

TN3270E > li pu vm30pu1
PU NAME      STATUS      NODE ID  TOTAL  DDDLU  -----LU's  IN-----
              LUs      ENABLED  ACTIV  OW
NED AVAILABL
-----
VM30PU1      ACTPU_RCVD  07711111  249    N      249      5      249
-----
LU NAME      NAU  STATUS  OWN  POOL  SSCP_LU  LU_LU  FLAGS  FLAGS1
              ADD                                STATUS  STATUS
-----
PU1LU2      02  ACTIV  NO   PUBLIC  (04,20)  00     02     00
PU1LU3      03  ACTIV  NO   PUBLIC  (04,20)  00     02     00
PU1LU4      04  ACTIV  NO   PUBLIC  (04,20)  00     02     00
PU1LU5      05  ACTIV  NO   PUBLIC  (04,20)  00     02     00
PU1LU6      06  ACTIV  NO   PUBLIC  (04,20)  00     02     00
PU1LU7      07  ACTIV  NO   PUBLIC  (04,20)  00     02     00

```

Tabla 96 (Página 1 de 2). Descripción de la salida		
Elemento	Descripción	Valores clave

Tabla 96 (Página 2 de 2). Descripción de la salida		
LU Name	El nombre de la LU tal como lo conoce el direccionador. Este nombre está completamente configurado en el direccionador o es un nombre generado por el direccionador basándose en un valor de germen configurado o bien es un nombre pasado desde el sistema principal para una LU dinámica iniciada por sistema principal.	--
NAU add	La dirección SNA de 1 byte para esta LU de esta PU. Este valor está configurado en el direccionador, está seleccionado por el direccionador o viene pasado del sistema principal. El valor se visualiza ahora en decimal.	--
Status	El estado actual de esta LU por separado.	ACTIV NOT ACT
Own	Si esta LU se encuentra asociada con una conexión TCP de cliente TN3270.	YES NO
Pool name	El nombre de agrupación mediante el cual puede asignarse esta LU a un cliente.	En blanco para las LU explícitas
SSCP_LU status, LU_LU status, Flags, flags1	Los valores hexadecimales de los campos de estado con destino al uso técnico. Para ver la decodificación de estos valores, utilice el mandato <i>list lu nombre</i> .	--

### list rejections

Utilice este mandato para visualizar una lista de hasta 99 de las conexiones de cliente TN3270 que se han rechazado más recientemente. Puede servirle de ayuda para ver y corregir la razón por la cual se han rechazado. El orden de la lista presenta el rechazo más reciente en la parte superior de la misma, la cual muestra todos los rechazos, incluidos los diversos intentos del mismo cliente.

### **Ejemplo:**

```
TN3270E > li rej
Connection Rejection Table
```

```
-----
1 Time   : 7/23/1999 11:09:00
  Client : 15.170.99.210
  Reason : Client is not authorized by Filter entries
2 Time   : 7/23/1999 11:08:59
  Client : 15.170.99.210
  Reason : Client is not authorized by Filter entries
3 Time   : 7/23/1999 11:08:59
  Client : 15.170.99.32
  Reason : Client is not authorized by Filter entries
```

<i>Tabla 97. Descripción de la salida</i>		
Elemento	Descripción	Valores clave
Time	El día y la hora en que se ha producido el rechazo.	--
Client	La dirección IP del cliente.	--
Reason	El texto que describe la razón por la cual el servidor ha rechazado la conexión de cliente. Actualmente están definidas unas 40 razones.	<p>Por ejemplo, pueden presentarse razones como las siguientes:</p> <p>El nodo está terminando</p> <p>No se ha podido obtener memoria</p> <p>No hay LU disponibles</p> <p>No se encuentra/no está disponible la LU solicitada</p> <p>La validación del tipo de LU ha fallado</p> <p>Se ha alcanzado el valor de selección de LU</p> <p>Se ha agotado la agrupación de LU</p> <p>La memoria de APPN está restringida</p>

### list status

Utilice este mandato para visualizar un resumen de la configuración de la función de servidor TN3270 e información actual sobre su estado.

#### **Ejemplo:**

```
TN3270E > li st
TN3270E Server Status Summary

TN3270E IP Address: 9.37.179.142
NetDisp Advisor Port Number: 10008
Keepalive type: NOP           Frequency: 60
Automatic Logoff: N
Client IP Address mapping : N
Number of connections           : 10
Number of available LUA LU's    : 498
Number of LUA LU's pending termination : 0
Number of defined LU's         : 498
Number of connections in SSCP-LU state : 0
Number of connections in LU-LU state : 10
```

<i>Tabla 98 (Página 1 de 3). Descripción de la salida</i>		
Elemento	Descripción	Valores clave
IP address	La dirección IP del direccionador donde se conectan los clientes TN3270.	--
NetDisp advisor port number	El número de puerto TCP al que puede conectarse la función de equilibrio de carga de Network Dispatcher para realizar un sondeo relativo a la información de carga existente en este servidor.	--



Tabla 98 (Página 2 de 3). Descripción de la salida

Keepalive type	Si el servidor realiza sondeos relativos a los clientes para ver si todavía están activos y cómo los realiza.	None = el servidor no realiza sondeos relativos a clientes, por lo que sólo descubrirá la ausencia de un cliente cuando trate de enviar datos NOP = el servidor realiza sondeos relativos a clientes en el nivel de TCP Timing mark = el servidor realiza sondeos relativos a clientes en el nivel de TN3270
Frequency	El intervalo en segundos entre los sondeos de tipo keepalive.	--
Automatic logoff	Si el servidor desconecta o no los clientes después de un período de inactividad (inexistencia de flujo de datos en cualquier dirección).	Y = sí N = no
Client IP address mapping	Si el servidor está habilitado globalmente para correlacionar direcciones IP de entrada con nombres de LU/agrupación.	Y = sí N = no
Number of connections	El número actual de conexiones TCP activas con clientes TN3270.	--
Number of available LUA LUs	El número de LU activadas actualmente desde el sistema principal o con posibilidad de activación de forma dinámica. Se incluyen las LU que actualmente están utilizadas por clientes TN3270.	--
Number of LUA LU's pending termination	El número de LU que se van a desactivar, circunstancia en la que el direccionador espera la confirmación del sistema principal. Estas LU ya no están asociadas con conexiones de cliente TN3270.	--
Number of defined LU's	El número de LU que están configuradas en el direccionador o LU dinámicas iniciadas por sistema principal activas.	--
Number of connections in SSCP-LU state	El número de conexiones TCP activas asociadas con una LU que se encuentra en el estado SSCP-LU.  Cuando una aplicación se enlaza lógicamente con la LU asociada con una conexión y esta LU entra en el estado LU-LU, dicho número disminuye (aunque todavía esté activa la conexión SSCP-LU).	--

Tabla 98 (Página 3 de 3). Descripción de la salida

Number of connections in LU-LU state	El número de conexiones TCP activas asociadas con una LU que se encuentra en el estado LU-LU.	--
--------------------------------------	---	----

## Soporte de la reconfiguración dinámica de APPN

Este apartado describe la reconfiguración dinámica (DR) tal como afecta a los mandatos Talk 6 y Talk 5.

### Mandato Delete Interface de CONFIG (Talk 6)

APPN da soporte al mandato de CONFIG (Talk 6) **delete interface** con las consideraciones siguientes:

- Cuando se suprime una interfaz, los puertos y enlaces definidos sobre esta interfaz se suprimen al reiniciarse APPN.
- Si se emite el mandato **activate\_new\_config** de Talk 6 o el mandato **restart** de Talk 5 antes de volver a cargar el dispositivo, no volverán a definirse de manera satisfactoria las interfaces de valor superior a la interfaz suprimida.

### Mandato Activate Interface de GWCON (Talk 5)

APPN da soporte al mandato de GWCON (Talk 5) **activate interface** con la consideración siguiente:

Cuando se activa una interfaz, los puertos y enlaces de la SRAM de APPN en relación con esta interfaz se definen para el nodo APPN y se activan.

El mandato de GWCON (Talk 5) **activate interface** da soporte a todos los mandatos específicos de interfaz APPN.

### Mandato Reset Interface de GWCON (Talk 5)

APPN da soporte al mandato de GWCON (Talk 5) **reset interface** con la consideración siguiente:

- Cuando se restablece una interfaz, los puertos y enlaces definidos sobre ésta se desactivan. Si el enlace es un enlace TN3270E de subárea, el nodo APPN se reiniciará. Si se trata de un puerto normal, se suprimen las definiciones de puerto y enlace. Después de activarse la interfaz, las definiciones de puerto y enlace vuelven a definirse y se activan.

El mandato de GWCON (Talk 5) **reset interface** da soporte a todos los mandatos específicos de interfaz APPN.

### Mandatos Reset de GWCON (Talk 5) del componente

APPN da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos de APPN:

## **Mandato Restart de GWCON, Protocol Appn**

**Descripción:** Este mandato reinicia el nodo APPN.

**Efecto en la red:** El flujo de datos de APPN a través de este nodo quedará interrumpido. APPN se detiene y se reinicia.

### **Limitaciones:**

También se reflejarán los cambios efectuados en la configuración de APPN (Talk 6).

El mandato de **GWCON, protocol appn, restart** da soporte a todos los mandatos de APPN.

## **Mandatos Activate de CONFIG (Talk 6)**

APPN da soporte a los siguientes mandatos **activate** de CONFIG (Talk 6):

### **Mandato Activate\_new\_config de CONFIG, Protocol APPN, O BIEN Mandato Activate\_new\_config de CONFIG, Protocol APPN, TN3270E**

**Descripción:** Este mandato activa cualquier cambio efectuado en la configuración de APPN.

**Efecto en la red:** Si el cambio no puede activarse de manera dinámica, se reinicia APPN.

### **Limitaciones:**

- Si el cambio no puede activarse de manera dinámica, se reinicia APPN. Como ejemplos están los cambios en cualquiera de los parámetros de nodo, parámetros de DLUR por omisión o parámetros globales de tn3270e. Algunos de los mandatos de supresión también reinician el nodo APPN. La supresión de estaciones de enlace o puertos no reinicia el nodo APPN excepto si las estaciones de enlace son enlaces tn3270e de subárea.
- Si los cambios se efectúan en los parámetros de ajuste, es necesario volver a cargar o reiniciar el dispositivo.

Todos los mandatos de APPN reciben soporte del mandato siguiente: **CONFIG, protocol appn, activate\_new\_config O BIEN CONFIG, protocol appn, tn3270e, activate\_new\_config.**



---

## Utilización de AppleTalk Phase 2

Este capítulo describe los mandatos de configuración de AppleTalk Phase 2 (AP2) e incluye los apartados siguientes:

- “Procedimientos básicos de la configuración”
- “Filtros de zona de AppleTalk 2” en la página 293
- “Procedimientos de la configuración de muestra” en la página 294

---

### Procedimientos básicos de la configuración

En este apartado se perfilan los pasos iniciales necesarios para activar y ejecutar el protocolo AppleTalk Phase 2. La información sobre cómo efectuar cambios adicionales en la configuración se detallará en otros apartados de mandatos de este capítulo. Para que sean efectivos los nuevos cambios de configuración, debe reiniciarse el direccionador.

### Habilitación de parámetros de direccionador

Cuando configure un direccionador para que reenvíe paquetes de AppleTalk Phase 2, deberá habilitar ciertos parámetros sin tener en cuenta el número de interfaces o de qué tipo son éstas en el mismo. Si tiene diversos direccionadores para transferir paquetes de AppleTalk Phase 2, especifique estos parámetros para cada direccionador.

- **Habilitación global de AppleTalk Phase 2:** Para empezar, debe habilitar globalmente el software AppleTalk Phase 2 utilizando el mandato de configuración de AppleTalk Phase 2 **enable ap2**. Si el direccionador visualiza un error en este paso, es que la carga no incluye el software AppleTalk Phase 2. Si éste es el caso, póngase en contacto con el representante del servicio al cliente.
- **Habilitación de interfaces específicas:** A continuación, debe habilitar las interfaces específicas sobre las cuales AppleTalk Phase 2 va a enviar los paquetes. Utilice el mandato **enable interface número de interfaz** para realizar esta acción.

**Nota:** Cuando habilite AppleTalk sobre ATM, deberá habilitar las interfaces específicas relativas a las LAN emuladas sobre las cuales AppleTalk va a enviar paquetes. No debe habilitar AppleTalk sobre la interfaz ATM física. Todos los usos posteriores de la palabra “interfaz” en este capítulo se refieren a la interfaz LAN emulada, no a la interfaz ATM física.

- **Habilitación de la Suma de comprobación:** A continuación, puede determinar si el direccionador calculará sumas de comprobación de DDP de los paquetes originados. El software de suma de comprobación no funciona correctamente en algunas implementaciones de AppleTalk Phase 2, por lo que es posible que no desee originar paquetes con sumas de comprobación para permitir la compatibilidad con estas implementaciones. No obstante, normalmente deseará habilitar la generación de sumas de comprobación. Cualquier paquete reenviado con una suma de comprobación tendrá verificada su suma de comprobación.

### Establecimiento de parámetros de red

También debe especificar ciertos parámetros para cada red e interfaz que envíe y reciba paquetes de AppleTalk Phase 2. Después de haber especificado los parámetros, utilice el mandato de configuración de AppleTalk Phase 2 de listado para ver los resultados de la configuración.

- Establecimiento del rango de redes para los direccionadores de germinación: La coordinación de los rangos de redes y las listas de zonas para todos los direccionadores de una red se simplifica si se designan direccionadores específicos como direccionadores de germinación. Los direccionadores de germinación se configuran con rango de redes y lista de zonas mientras se dan valores nulos a todos los otros direccionadores. Los valores nulos indican que el direccionador debe realizar consultas en la red sobre valores de los direccionadores de germinación. Para cada red (segmento) de la internet AppleTalk interconectada, debe configurarse, como mínimo, una interfaz de direccionador como direccionador de germinación de dicha red. Normalmente, existen diversos direccionadores de germinación en una red por si uno de ellos falla. Además, un direccionador puede ser un direccionador de germinación para algunas de sus interfaces de red o para todas ellas. Utilice el mandato **set net-range** para asignar el rango de redes a los direccionadores de germinación.
- Establecimiento del número de nodo de inicio: Utilice el mandato **set node** para asignar el número de nodo de inicio del direccionador. El direccionador realizará una acción de AARP para este nodo, pero, si ya se utiliza, se elegirá un nuevo nodo.
- Adición de un nombre de zona: Puede añadir uno o más nombres de zonas para cada red de la internet. Puede añadir un nombre de zona para una red determinada a cualquier direccionador conectado a la misma; no obstante, sólo el direccionador de germinación tiene que contener la información de nombre de zona para una red conectada. Los direccionadores conectados obtienen dinámicamente el nombre de zona de los direccionadores adyacentes con el protocolo ZIP. Apple recomienda que, respecto a una red determinada, elija el mismo direccionador de germinación para el número de red y para el nombre de zona. No puede configurarse el nombre de zona para una red si no se configura también el número de red. Al añadir un nombre de zona para cada número de red, utilice el mandato de configuración de AppleTalk Phase 2 **add zone nombre**.

---

### AppleTalk sobre PPP

Existen dos modalidades para AppleTalk sobre PPP, direccionador completo y medio direccionador. En la modalidad de direccionador completo, la red punto a punto es visible para los otros direccionadores de AppleTalk. En la modalidad de medio direccionador, la red punto a punto es invisible para los otros direccionadores, aunque transmite información de direccionamiento y paquetes de datos de AppleTalk.

Si desea configurar la red para la modalidad de direccionador completo, proporcione a cada direccionador del enlace PPP un número de red común, un nombre de zona común y un número de nodo exclusivo. Si configura un extremo del enlace PPP con un número de red distinto de cero, también debe configurar este extremo

de manera que tenga un número de nodo distinto de cero y un nombre de zona. En este caso, el otro extremo del enlace debe contar con una de estas opciones:

- El mismo número de red y nombre de zona y un número de nodo diferente.
- Los números de red y nodo establecidos en cero. El direccionador aprenderá los números de red y nodo del direccionador configurado.

Si desea configurar la red para la modalidad de medio direccionador, configure ambos direccionadores del enlace PPP de manera que los números de red y nodo estén establecidos en cero y no se utilice ningún nombre de zona.

---

## Filtros de zona de AppleTalk 2

La filtración de nombres de zonas, aunque no es necesaria para AppleTalk, es una función muy conveniente para la seguridad y la administración de las redes internet AppleTalk de grandes proporciones. También se proporcionan limitaciones del acceso a redes por medio de los números de red.

### Información general

Se ha estructurado AppleTalk para que cada red se identifique de dos maneras. La primera es un número de red o rango de números de red consecutivos que deben ser exclusivos en toda la internet. El número de red combinado con el número de nodo identifica de forma exclusiva cualquier estación final en la internet.

El segundo identificador para la red consiste en uno o más nombres de zonas. Estas series de nombres de zonas no son exclusivas en toda la internet. La estación final se identifica de forma exclusiva por medio de la combinación de **objeto:tipo:serie-NombZonas**.

Un direccionador obtiene por primera vez información sobre una red cuando aparece el rango de la nueva red en la actualización del direccionamiento de RTMP de un direccionador contiguo. A continuación, el direccionador consulta al direccionador contiguo los nombres de zonas de la nueva red. Tenga en cuenta que el rango de la red se repite en cada nueva actualización de RTMP pero los nombres de zonas sólo se solicitan una vez.

Las estaciones finales obtienen los números de red de los paquetes difundidos de RTMP (información de direccionamiento) y, a continuación, eligen un número de nodo. Se realiza un sondeo de AARP (Punta de prueba de AARP) relativo a este par red/nodo para ver si cualquier otra estación final ya ha reclamado su uso. Si responde otra estación, la estación final elige otro par red/nodo y el proceso se repite hasta que no se reciben respuestas.

### Razón de los filtros de nombre de zona

Cuando la estación final AppleTalk normal desea utilizar un servicio (impresora, servidor de archivos) en la internet Apple, observa primero todas las zonas disponibles y selecciona una. A continuación, elige un tipo de servicio y solicita una lista de todos los nombres que anuncian el tipo en la zona elegida. Este mecanismo da lugar a varios problemas.

- Una internet grande puede tener muchas zonas. La presentación ante el usuario de una lista larga para que elija entorpece la selección de las necesarias (por lo tanto, impide que la lista sea utilizable).

- Es posible que el servidor no desee estar disponible en toda la internet (por razones de seguridad). Si la zona en la que está el servicio no es visible para el cliente, hay una mejora en la seguridad.
- Si se limitan las zonas visibles de un departamento para el resto de la internet, se permitirá que la administración de ésta deje que el departamento controle (o no) su propio dominio a la vez que no se aumenta la actividad general para el resto de la internet (lo que supone una reducción de la administración).

La filtración de números de red es un paso más en la mejora de la seguridad y la administración de la internet. La filtración de zonas sólo controla indirectamente el acceso a las redes. Un departamento sin normas puede añadir redes con los mismos nombres de zonas y nuevos números de red que entren en conflicto con otros departamentos. Puede utilizarse la filtración de números de red para evitar que estas adiciones aleatorias de nombres de zonas y números de red afecten al resto de la red.

### ¿Cómo se añaden los filtros?

El direccionador se configura con una lista exclusiva (que significa un bloqueo de las zonas especificadas) o inclusiva (que significa permitir solamente estas zonas) de las zonas para cada dirección de cada interfaz. La interfaz especificada no volverá a anunciar información sobre las zonas filtradas en la dirección definida. Si se filtran todas las zonas de la lista de zonas de una red, también se filtrará información sobre la red a través de la interfaz.

- Utilice los mandatos de configuración **add** y **delete** para crear la lista de filtración de una interfaz.
- Utilice los mandatos de configuración **enable** y **disable** para especificar cómo se aplicará la lista de filtración.

Utilice mandatos similares para crear los filtros de número de red.

#### Otros mandatos:

Puede utilizar el mandato de AP2 CONFIG> **list** para visualizar toda la información de filtración de las interfaces. Además, el mandato **list** acepta *interfaznúmero* como argumento con el fin de que pueda listar información para una interfaz solamente.

### Procedimientos de la configuración de muestra

Este apartado se ocupa de los pasos necesarios para activar y ejecutar AP2. Para obtener información sobre cómo efectuar cambios adicionales en la configuración, consulte el apartado "Mandatos de configuración de AppleTalk Phase 2" en la página 299. Para que sean efectivos los cambios de configuración, debe reiniciar el direccionador.

Para acceder al entorno de configuración de AP2, entre **protocol ap2** en el indicador Config>.

#### Habilitación de AP2

Cuando configure un direccionador para que reenvíe paquetes de AP2, deberá habilitar ciertos parámetros. Si tiene diversos direccionadores para transferir paquetes de AP2, especifique estos parámetros para cada direccionador. Para habilitar AP2:



1. Utilice el mandato **enable ap2** para habilitar AP2 globalmente en el direccionador. Por ejemplo:

```
AP2 config>enable ap2
```

2. Habilite las interfaces específicas sobre las que AP2 va a enviar paquetes. Por ejemplo:

```
AP2 config>enable interface 1
```

### Establecimiento de parámetros de red

Para configurar el direccionador como direccionador de germinación, debe establecer el rango de redes, un número de nodo de inicio y, como mínimo, un nombre de zona. Puede configurar algunas interfaces de un direccionador como direccionadores de germinación y dejar las otras interfaces como direccionadores sin germinación. Debe tener, como mínimo, un direccionador de germinación para cada red AppleTalk y debería configurar varios en una red por si uno de ellos falla.

**Nota:** No establezca un rango de redes ni un número de nodo para los medios direccionadores.

1. Utilice el mandato **set net-range** para establecer el rango de redes. Por ejemplo:

```
AP2 config>set net-range
Interface # [0]? 1
First Network range number (1-65279, or 0 to delete) []? 1
Last Network range number (1-165279) []? 5
```

Entre el mismo valor en First y Last para una red de un solo número.

2. Utilice el mandato **set node-number** para establecer el número de nodo de inicio de la interfaz. El direccionador realizará una acción de AARP para este nodo. Si ya se utiliza el número, el direccionador elegirá un nuevo número. Por ejemplo:

```
AP2 config>set node-number
Interface # [0]? 1
Node number (1-253, or 0 to delete) []? 1
```

3. Utilice el mandato **add zone** para añadir uno o más nombres de zonas de la red conectada a la interfaz. Si define un rango de redes para una interfaz, también debe definir los nombres de zonas para la interfaz. Si no ha definido un número de red, no defina nombres de zonas. Por ejemplo:

```
AP2 config>add zone
Interface # [0]? 1
Zone name []? Finanzias
```

Después de haber especificado los parámetros, puede utilizar el mandato **list** en el indicador `AP2 config>` para ver la configuración.

### Configuración de filtros de zona

La filtración de zonas le permite filtrar zonas en cada dirección de cada interfaz. Para filtrar paquetes de entrada, configure un filtro de la entrada. Para filtrar paquetes de salida, configure un filtro de la salida. La interfaz no volverá a anunciar información sobre las zonas filtradas en la dirección definida. Siga los pasos indicados a continuación para configurar un filtro de zona:

1. Añada filtros de zona a una interfaz. Utilice el mandato **add zfilter in** para añadir un filtro de zona de la entrada a una interfaz. Utilice el mandato **add zfilter out** para añadir un filtro de zona de la salida a una interfaz. Por ejemplo:

## Utilización de AppleTalk Phase 2

```
AP2 config>add zfilter in
Interface # [0]? 1
Zone name []? Admin
```

2. Habilite los filtros de zona que ha añadido. Con ello activa el filtro y controla si éste es inclusivo o exclusivo. Los filtros inclusivos reenvían solamente información sobre la zona del filtro. Los filtros exclusivos bloquean solamente información sobre la zona del filtro. Por ejemplo:

```
AP2 config>enable zfilter in exc
Interface # [0]? 1
```

A continuación, se ofrecen algunos ejemplos que explican cómo configurar filtros de zona en la internet que muestra la Figura 11.

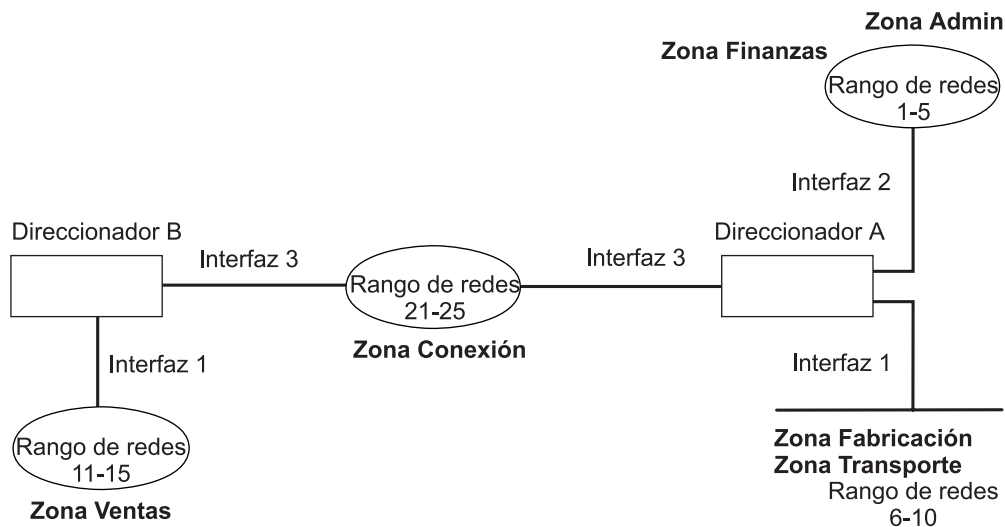


Figura 11. Ejemplo de filtración de zonas

### Ejemplo 1

A continuación, se muestra un ejemplo de cómo filtrar la Zona Fabricación con respecto a todas las otras redes. Para ello, configurará un filtro de la entrada en la Interfaz 1 del Direccionador A para excluir la Zona Fabricación.

1. En el Direccionador A, añada un filtro de zona de la entrada a la Interfaz 1.

```
AP2 config>add zfilter in
Interface # [0]? 1
Zone name []? Fabricación
```

2. Habilite el filtro de zona de la entrada y haga que sea exclusivo.

```
AP2 config>enable zfilter in exc
Interface # [0]? 1
```

Así se impide que entre información sobre la Zona Fabricación en el Direccionador A, por lo que se filtra la zona con respecto al resto de la internet.

### Ejemplo 2

El ejemplo siguiente muestra cómo filtrar la Zona Fabricación con respecto a la Red 11-15 y, no obstante, permitir que dicha zona sea visible en la Red 1-5. Para ello, configurará un filtro de la salida en la Interfaz 3 del Direccionador A para impedir que se reenvíe información sobre la Zona Fabricación desde la Interfaz 3. La interfaz continuará anunciando información sobre la Zona Fabricación en las Interfaces 1 y 2 del Direccionador A, con lo que la zona será visible en la Red 1-5.

1. Añada un filtro de zona de la salida a la Interfaz 3.

```
AP2 config>add zfilter out
Interface # [0]? 3
Zone name []? Fabricación
```

2. Habilite el filtro de zona de la salida y haga que sea exclusivo.

```
AP2 config>enable zfilter out exc
Interface # [0]? 3
```

Este filtro excluye información sobre la Zona Fabricación de la salida de la Interfaz 3.

### Ejemplo 3

El ejemplo siguiente muestra cómo configurar un filtro de manera que la Zona Admin sea visible en todas las redes, pero la Zona Finanzas no lo sea con respecto al resto de la internet.

1. Añada un filtro de zona de la entrada a la Interfaz 2 del Direccinador A.

```
AP2 config>add zfilter in
Interface # [0]? 2
Zone name []? Admin
```

2. Habilite el filtro de zona de la entrada y haga que sea inclusivo.

```
AP2 config>enable zfilter in inc
Interface # [0]? 2
```

Configurando este filtro de la entrada como inclusivo, sólo se reenvía al resto de la internet información sobre la Zona Admin por la Interfaz 2.

### Configuración de filtros de red

Los filtros de red son similares a los filtros de zona, con la excepción de que le permiten filtrar toda una red. Para configurar un filtro de red:

1. Añada un filtro de red. Utilice el mandato **add nfilter in** para añadir un filtro de red de la entrada a una interfaz. Utilice el mandato **add nfilter out** para añadir un filtro de red de la salida a una interfaz. Por ejemplo:

```
AP2 config>add nfilter out
Interface # [0]? 2
First Network range number (decimal) [0]? 11
Last Network range number (decimal) [0]? 15
```

El rango de redes que entre aquí debe coincidir con el rango que ha asignado a esa red.

2. Habilite el filtro de red que ha añadido y haga que sea inclusivo o exclusivo. Los filtros inclusivos reenvían solamente información sobre la red del filtro. Los filtros exclusivos bloquean solamente información sobre la red de un filtro y permiten reenviar toda la otra información sobre redes.

```
AP2 config>enable nfilter in exc
Interface # [0]? 2
```

A continuación, se ofrecen algunos ejemplos que explican cómo configurar filtros de red en la internet que muestra la Figura 12 en la página 298.

## Utilización de AppleTalk Phase 2

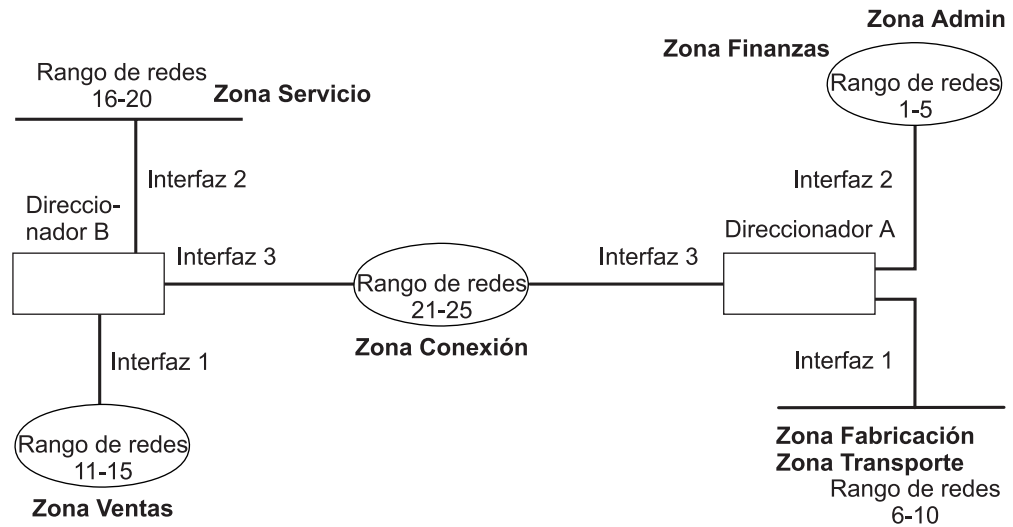


Figura 12. Ejemplo de filtración de redes.

Los pasos siguientes muestran cómo filtrar la Red 6-10 de manera que no sea visible en la Red 16-20 que muestra la Figura 12.

1. Añada un filtro de red de la salida para la Red 6-10 a la Interfaz 2 del Director B.

```
AP2 config>add nfilter out
Interface # [0]? 2
First Network range number (decimal) [0]? 6
Last Network range number (decimal) [0]? 10
```

2. Habilite el filtro de red de la salida como exclusivo.

```
AP2 config>enable nfilter out exc
Interface # [0]? 2
```

Este filtro impide que toda la información sobre la Red 6-10 se reenvíe a la Red 16-20 por la Interfaz 2.

---

## Configuración y supervisión de AppleTalk Phase 2

Este capítulo describe los mandatos de configuración y supervisión de AppleTalk Phase 2 (AP2). Incluye los apartados siguientes:

- “Acceso al entorno de configuración de AppleTalk Phase 2”
- “Mandatos de configuración de AppleTalk Phase 2”
- “Acceso al entorno de supervisión de AppleTalk Phase 2” en la página 308
- “Mandatos de supervisión de AppleTalk Phase 2” en la página 308

---

### Acceso al entorno de configuración de AppleTalk Phase 2

Para acceder al entorno de configuración de AppleTalk Phase 2, entre el mandato siguiente en el indicador Config>:

```
Config> ap2
AP2 Protocol user configuration
AP2 Config>
```

---

### Mandatos de configuración de AppleTalk Phase 2

Este apartado describe los mandatos de configuración de AppleTalk Phase 2.

Los mandatos de configuración de AppleTalk Phase 2 le permiten especificar parámetros de red para las interfaces de red que transmitan paquetes de AppleTalk Phase 2. La información que especifique con los mandatos de configuración se activará cuando reinicie el direccionador.

Entre los mandatos de configuración de AppleTalk Phase 2 en el indicador AP2 config>. Los mandatos se muestran en la Tabla 99 en la página 300.

## Mandatos de configuración de AppleTalk Phase 2 (Talk 6)

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi.
Add	Añade nombres de zonas, filtros de red y filtros de zona a una interfaz.
Delete	Suprime los nombres de zonas, interfaces, filtros de red y filtros de zona.
Disable	Inhabilita las interfaces, la suma de comprobación, el direccionamiento de horizonte dividido, los filtros de red o los filtros de zona o bien inhabilita AppleTalk Phase 2 globalmente.
Enable	Habilita las interfaces, la suma de comprobación, el direccionamiento de horizonte dividido, los filtros de red o los filtros de zona o bien habilita AppleTalk Phase 2 globalmente.
List	Visualiza la configuración actual de AppleTalk Phase 2.
Set	Establece el tamaño de antememoria, el rango de redes y el número de nodo.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

### Add

Utilice el mandato **add** para añadir el nombre de zona a la lista de zonas de la interfaz, para añadir el nombre de zona a la lista de zonas de la interfaz como valor por omisión de ésta o para añadir filtros de red y zona.

#### Sintaxis:

```
add           zone . . .  
               defaultzone . . .  
               nfilter in . . .  
               nfilter ot . . .  
               zfilter in . . .  
               zfilter ot . . .
```

**zone** *interfaz* *núm.* *nombzona*

Añade el nombre de zona a la lista de zonas de la interfaz. Si define un número de red para una interfaz, también debe definir los nombres de zonas para la interfaz. Si no ha definido un número de red, no defina nombres de zonas.

#### Ejemplo:

```
ap2config>add zone  
Interface # [0]? 0  
Zone name []? Finanzias
```

**defaultzone** *interfaz* *núm.* *nombzona*

Añade un nombre de zona por omisión a la interfaz. Si un nodo de la red solicita un nombre de zona que no es válido, el direccionador asigna el nombre de zona por omisión al nodo hasta que se elija otro

## Mandatos de configuración de AppleTalk Phase 2 (Talk 6)

nombre de zona. Si añade más de un valor por omisión a una interfaz, el último que se añade altera temporalmente el valor por omisión anterior. Si no añade un valor por omisión, el primer nombre de zona que se añade utilizando el mandato **zone** será el valor por omisión.

### Ejemplo:

```
ap2config>add defaultzone
Interface # [0]? 0
Zone name []? Central
```

### **nfilter in** *interfaznúm. primera rednúm. última rednúm.*

Añade un filtro de red a la entrada de la interfaz. El rango de redes que entre debe coincidir con el rango de redes que ha establecido para esa interfaz. No puede filtrar sólo una parte de un rango de redes. Por ejemplo, si ha establecido un rango de redes de 1–10 y ha configurado un filtro para 5–8, el direccionador filtra el rango de redes completo de 1–10.

### Ejemplo:

```
ap2config>add nfilter in
Interface # [0]? 0
First Network range number (decimal) [0]? 1
Last Network range number (decimal) [0]? 10
```

### **nfilter out** *interfaznúm. primera rednúm. última rednúm.*

Añade un filtro de red a la salida de la interfaz. El rango de redes que entre debe coincidir con el rango de redes que ha establecido para esa interfaz. No puede filtrar sólo una parte de un rango de redes. Por ejemplo, si ha establecido un rango de redes de 1–10 y ha configurado un filtro para 5–8, el direccionador filtra el rango de redes completo de 1–10.

### Ejemplo:

```
ap2config>add nfilter out
Interface # [0]? 0
First Network range number (decimal) [0]? 11
Last Network range number (decimal) [0]? 20
```

### **zfilter in** *interfaznúm. nombre de zona*

Añade un filtro de nombre de zona a la entrada o salida de la interfaz.

### Ejemplo:

```
ap2config>add zfilter in
Interface # [0]? 1
Zone name []? Marketing
```

### **zfilter out** *interfaznúm. nombre de zona*

Añade un filtro de nombre de zona a la salida de la interfaz.

### Ejemplo:

```
ap2config>add zfilter out
Interface # [0]? 0
Zone name []? Corporación
```

## Delete

Utilice el mandato **delete** para suprimir un nombre de zona de la lista de zonas de la interfaz, filtros de nombre de red o zona o toda la información de AppleTalk Phase 2 de una interfaz.

### Sintaxis:

```
delete zone . . .
nfilter in . . .
```

## Mandatos de configuración de AppleTalk Phase 2 (Talk 6)

```
nfilter out . . .  
zfilter in . . .  
zfilter out . . .  
interface
```

**zone** *interfaz*núm. *nombzona*

Suprime un nombre de zona de la lista de zonas de la interfaz.

**Ejemplo:**

```
ap2config>delete zone 2 nuevayork
```

**nfilter in** *interfaz*núm. *primera red*núm. *última red*núm.

Suprime un filtro de red de la entrada de la interfaz. Debe entrar los mismos números de rango de redes que ha establecido utilizando el mandato **add nfilter in**.

**Ejemplo:**

```
ap2config>delete nfilter in  
Interface # [0]? 0  
First Network range number (decimal) [0]? 1  
Last Network range number (decimal) [0]? 12
```

**nfilter out** *interfaz*núm.

Suprime un filtro de red de la salida de la interfaz. Debe entrar los mismos números de rango de redes que ha establecido utilizando el mandato **add nfilter out**.

**Ejemplo:**

```
ap2config>delete nfilter out  
Interface # [0]? 0  
First Network range number (decimal) [0]? 11  
Last Network range number (decimal) [0]? 20
```

**zfilter in** *interfaz*núm. *nombre de zona*

Suprime un filtro de nombre de zona de la entrada de la interfaz.

**Ejemplo:**

```
ap2config>delete nfilter in  
Interface # [0]? 1  
Zone name []? Marketing
```

**zfilter out** *interfaz*núm. *nombre de zona*

Suprime un filtro de nombre de zona de la salida de la interfaz.

**Ejemplo:**

```
delete zfilter out  
  
Interface # [0]? 1  
Zone name []? Marketing
```

**interface** Utilice este mandato para suprimir una interfaz. Ésta es la única manera de suprimir nombres de zonas que tienen caracteres no imprimibles.

**Ejemplo:**

```
ap2config>delete interface 1
```

## Disable

Utilice el mandato **disable** para inhabilitar AP2 en todas las interfaces o en una interfaz especificada, la suma de comprobación, la filtración, la conversión de APL/AP2 o el direccionamiento de horizonte dividido.

**Sintaxis:**

```
disable            ap2
```



- `checksum`
- `interface . . .`
- `nfilter in . . .`
- `nfilter out . . .`
- `zfilter in . . .`
- `zfilter out . . .`
- `split-horizon-routing . . .`

**ap2** Inhabilita la función de reenvío de paquetes de AppleTalk Phase 2 para todas las interfaces.

**Ejemplo:**

```
ap2config>disable ap2
```

**checksum**

Especifica que el direccionador no calculará la suma de comprobación en los paquetes que genere. Normalmente, el direccionador calcula la suma de comprobación en todos los paquetes que reenvía. Éste es el valor por omisión.

**Ejemplo:**

```
ap2config>disable checksum
```

**interface** *interfaznúmero*.

Inhabilita todas las funciones de AP2 en la interfaz de red especificada. La red continúa disponible para todos los otros protocolos.

**Ejemplo:**

```
ap2config>disable interface 2
```

**nfilter in** *interfaznúmero*.

Inhabilita, pero no suprime, los filtros de red de la entrada de esta interfaz.

**Ejemplo:**

```
ap2config>disable nfilter in
Interface # [0]? 2
```

**nfilter out** *interfaznúmero*.

Inhabilita, pero no suprime, los filtros de red de la salida de esta interfaz.

**Ejemplo:**

```
ap2config>disable nfilter out
Interface # [0]? 2
```

**zfilter in** *interfaznúmero*.

Inhabilita, pero no suprime, los filtros de zona de la entrada de esta interfaz.

**Ejemplo:**

```
ap2config>disable zfilter in
Interface # [0]? 1
```

**zfilter out** *interfaznúmero*.

Inhabilita, pero no suprime, los filtros de zona de la salida de esta interfaz.

**Ejemplo:**

```
ap2config>disable zfilter out 0
Interface # [0]? 1
```

## Mandatos de configuración de AppleTalk Phase 2 (Talk 6)

### **split-horizon-routing** *interfaznúmero*.

Inhabilita el direccionamiento de horizonte dividido en esta interfaz. Sólo tiene que inhabilitar el direccionamiento de horizonte dividido en las interfaces Frame Relay que estén en un concentrador dentro de una red Frame Relay con entramado parcial. La inhabilitación del direccionamiento de horizonte dividido hace que se propaguen todas las tablas de direccionamiento sobre esta interfaz.

#### **Ejemplo:**

```
ap2config>disable split-horizon-routing 0
```

## Enable

Utilice el mandato **enable** para habilitar la función de suma de comprobación, una interfaz especificada o la función de pasarela de AppleTalk 2 o bien para habilitar el protocolo AppleTalk Phase 2 globalmente.

### **Sintaxis:**

```
enable          ap2
                 checksum
                 interface . . .
                 nfilter in . . .
                 nfilter out . . .
                 split-horizon-routing . . .
                 zfilter . . .
```

**ap2** Habilita la función de reenvío de paquetes de AppleTalk Phase 2 sobre todas las interfaces.

#### **Ejemplo:**

```
ap2config>enable ap2
```

### **checksum**

Especifica que el direccionador calculará la suma de comprobación en los paquetes que genere. El direccionador calcula la suma de comprobación en todos los paquetes de AP2 que reenvía.

#### **Ejemplo:**

```
ap2config>enable checksum
```

### **interface** *interfaznúmero*.

Permite que el direccionador envíe paquetes de AppleTalk Phase 2 sobre interfaces específicas.

#### **Ejemplo:**

```
ap2config>enable interface 3
```

### **nfilter in** *exclusivo* o *exclusivo interfaznúmero*.

Habilita los filtros de red de la entrada y controla cómo se aplica el filtro a la interfaz. Los inclusivos reenvían las coincidencias. Los exclusivos eliminan las coincidencias.

#### **Ejemplo:**

```
ap2config>enable filter in inc
Interface # [0]? 1
```

**nfilter out** *exclusivo* o *exclusivo interfaznúmero*.

Habilita los filtros de red de la salida y controla cómo se aplica el filtro a la interfaz. Los inclusivos reenvían las coincidencias. Los exclusivos eliminan las coincidencias.

**Ejemplo:**

```
ap2config>enable filter out exec
Interface # [0]? 1
```

**split-horizon-routing** *interfaz número*.

Habilita el direccionamiento de horizonte dividido en la interfaz. El valor por omisión es el de estar *habilitado*.

**Ejemplo:**

```
ap2config>enable split-horizon-routing 1
```

**zfilter**

Habilita los filtros de zona asignados a una interfaz. Hay que especificar si el filtro es "in" o es "out" y si el filtro es inclusivo o exclusivo. Inclusivo significa que sólo se direccionarán los paquetes que coincidan con el filtro. Exclusivo significa que se desecharán todos los paquetes que coincidan con el filtro.

**Ejemplo:**

```
ap2config>enable zfilter in inc
Interface # [0]?
```

**Ejemplo:**

```
ap2config>enable zfilter out exec
Interface # [0]? 0
```

## List

Utilice el mandato **list** para visualizar la configuración actual de AP2. En el ejemplo, el direccionador es un direccionador de germinación sobre las interfaces 0 y 1

**Nota:** El mandato **list** acepta *interfaznúmero* como argumento.

**Sintaxis:**

**list**

**Ejemplo:**

## Mandatos de configuración de AppleTalk Phase 2 (Talk 6)

```
ap2config>list
APL2 globally enabled
Checksumming disabled
Cache size 500

List of configured interfaces:

Interface      netrange      / node      Zone
0              1000-1000    / 1        "LíneaSerie"(Def)
Input ZFilters disabled
Input NFilters (inclusive)
Output ZFilters disabled
Output NFilters disabled
Split-horizon-routing enabled
1              10-19       / 52      "EtherTalk", "Ventas"(Def)
Input ZFilters disabled
Input NFilters (inclusive)
Output ZFilters disabled
Output NFilters disabled
Split-horizon-routing enabled
2              unseeded net / 0
Input ZFilters disabled
Input NFilters (inclusive)
Output ZFilters disabled
Output NFilters disabled
Split-horizon-routing disabled
```

### **APL2 globally**

Indica si AppleTalk Phase 2 se ha habilitado o inhabilitado globalmente.

### **Checksumming**

Indica si la suma de comprobación se ha habilitado o inhabilitado.

### **Cache size**

El número de entradas de antememoria de vía de acceso rápida.

### **List of configured interfaces**

Lista cada número de interfaz y su rango de redes, número de nodo y nombre(s) de zona(s) así como la zona por omisión.

Para cada interfaz, también lista si los filtros de zona y los filtros de red de la entrada y la salida se han habilitado o inhabilitado. Si se han habilitado, indica si son inclusivos o exclusivos.

### **Input/output Zfilters**

Indica los filtros de zona asignados a una interfaz. Inclusivo significa que sólo se direccionarán los paquetes que coincidan con el filtro. Exclusivo significa que se desecharán todos los paquetes que coincidan con el filtro. Se visualiza el nombre de la zona filtrada. Entrada significa que el filtro se aplica al tráfico que entre en la interfaz. Salida significa que el filtro se aplica al tráfico que salga de la interfaz.

### **Input/output Nfilters**

Indica los filtros de red asignados a una interfaz. Inclusivo significa que sólo se direccionarán los paquetes que coincidan con el filtro. Exclusivo significa que se desecharán todos los paquetes que coincidan con el filtro. Se visualiza el rango de redes filtrado. Entrada significa que el filtro se aplica al tráfico que entre en la interfaz. Salida significa que el filtro se aplica al tráfico que salga de la interfaz.

### **Split-horizon-routing**

Muestra si el direccionamiento de horizonte dividido se ha habilitado o inhabilitado en cada interfaz.

## Set

Utilice el mandato **set** para definir el tamaño de antememoria de vía de acceso rápida o parámetros específicos de AppleTalk Phase 2 que incluyen el rango de redes de los direccionadores de germinación y el número de nodo.

### Sintaxis:

```
set          cache-size . . .
              net-range . . .
              node . . .
```

### **cache-size** *valor*

*Cache-size* corresponde al número total de redes y nodos AppleTalk que pueden comunicarse simultáneamente a través de este direccionador por medio de la función de vía de acceso rápida. (La vía de acceso rápida es un método destinado al cálculo previo de cabecezas MAC para reenviar paquetes con mayor rapidez.) El valor por omisión es 500, que permite que un máximo de 500 redes y nodos se comuniquen simultáneamente a través del direccionador por medio de la vía de acceso rápida. Si el número de redes y nodos es superior al tamaño de la antememoria, el direccionador sigue reenviando los paquetes, pero no utiliza la vía de acceso rápida. Los valores válidos para el tamaño de la antememoria son: 0 (inhabilitación) y del 100 al 10 000. Aunque no es recomendable, el establecimiento del tamaño de la antememoria en cero inhabilita la función de vía de acceso rápida y no se utiliza memoria para la antememoria. Sólo tiene que cambiar este valor por omisión para redes muy grandes. Cada entrada de tamaño de antememoria utiliza 36 bytes de memoria.

### Ejemplo:

```
ap2config>set cache-size 700
```

### **net-range** *interfaz*núm. *primer número* *último número*

Asigna el rango de redes de los direccionadores de germinación utilizando los valores siguientes:

- *interfaz*núm. - Designa la interfaz de direccionador con la que se trabajará.
- *primer número* - Asigna el número más bajo del rango de redes. Los valores permitidos van desde el 1 al 65279 (hexadecimal 10xFEFF).
- *último número* - Establece el número más alto del rango de redes. Los valores permitidos van desde el *primer número* al 65279.

Una red de un solo número tiene el mismo valor como primer número y como último número. Un primer valor de cero suprime el rango de redes para la interfaz y convierte la interfaz "de germinación" en una interfaz "sin germinación". El primer número y el último número son inclusivos en el rango de redes.

El establecimiento del primer valor en cero en una interfaz Point-to-Point (PPP) permite que esta interfaz funcione en la modalidad de "medio direccionador". En la modalidad de medio direccionador, ninguno de los dos extremos de una red PPP se configura con un rango de redes o una lista de zonas, lo que reduce la cantidad de configuración nece-

## Mandatos de supervisión de AppleTalk Phase 2 (Talk 5)

saría. Ambos direccionadores deben funcionar en la misma modalidad dentro de la red PPP.

**Nota:** Al conectar un 2216 con un IBM 6611 utilizando una interfaz PPP, establezca el 2216 en la modalidad de “medio direccionador”, que es la *única* modalidad de funcionamiento soportada por el IBM 6611 para las comunicaciones de AppleTalk sobre una interfaz PPP.

### Ejemplo:

```
ap2config>set Net-Range 2 43 45
```

**node** *interfaznúmero. nodonúmero.*

Asigna el número de nodo de inicio para el direccionador. El direccionador realizará una acción de AARP para este nodo, pero, si ya se utiliza, se elegirá un nuevo nodo. A continuación, se explican los argumentos que se entran después de este mandato:

- *interfaznúmero.* - Designa la interfaz de direccionador con la que se trabajará.
- *nodonúmero.* - Designa el primer número de nodo con el que se realiza un intento. Los valores permitidos van desde el 1 al 253. Un valor de cero en *nodonúmero.* suprime el número de nodo para la interfaz y obliga al direccionador a elegir uno de forma aleatoria.

### Ejemplo:

```
ap2config>set node 2 2
```

---

## Acceso al entorno de supervisión de AppleTalk Phase 2

Para acceder al entorno de supervisión de AppleTalk Phase 2, entre el mandato siguiente en el indicador + (GWCON):

```
+ protocol ap2  
AP2>
```

---

## Mandatos de supervisión de AppleTalk Phase 2

Este apartado describe los mandatos de supervisión de AppleTalk Phase 2, que le permiten ver los parámetros y las estadísticas de las interfaces y redes que transmiten paquetes de AppleTalk Phase 2. Los mandatos de supervisión visualizan los valores de configuración para los niveles físicos, de trama y de paquete. También tiene la opción de ver los valores de los tres niveles de protocolo a la vez.

Entre los mandatos de supervisión de AppleTalk Phase 2 en el indicador AP2>. Los mandatos se muestran en la Tabla 100 en la página 309.

Tabla 100. Resumen de los mandatos de supervisión de AppleTalk Phase 2

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi.
Atecho	Envía peticiones con eco y observa si hay respuestas.
Cache	Visualiza las entradas de tabla de antememoria.
Clear Counters	Borra todos los contadores de usos de la antememoria y los contadores de desbordamientos de paquetes.
Counters	Visualiza la cuenta de desbordamientos de paquetes de AP2 para cada interfaz.
Dump	Visualiza el estado actual de la tabla de direccionamiento para todas las redes de la internet y sus nombres de zonas asociados.
Interface	Visualiza las direcciones actuales de las interfaces.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

## Atecho

El mandato **atecho** envía peticiones con eco de AppleTalk a un destino especificado y observa si hay una respuesta. Puede utilizarse este mandato para verificar la conectividad básica de AppleTalk y para aislar problemas en la internet AppleTalk.

### Sintaxis:

**atecho** *red\_dest nodo\_dest*

**red\_dest** Especifica el número de red AppleTalk de destino, en decimal. Es un parámetro necesario.

### nodo\_dest

Especifica el número de nodo AppleTalk de destino, en decimal. Es un parámetro necesario.

**Nota:** En muchos nodos AppleTalk, la dirección de red (número de red y número de nodo) se asigna dinámicamente y puede que no se encuentre disponible de forma fácil. No obstante, hay varias maneras de utilizar el mandato **atecho** eficazmente:

1. La dirección AppleTalk para los nodos direccionadores se encuentra configurada de manera estática en muchos casos. La conectividad entre los nodos direccionadores es muy importante para la conectividad general de la red.
2. Estableciendo el número de nodo de destino de atecho en 255, puede consultar a todos los nodos del número de red especificado de una red AppleTalk conectada directamente. Las respuestas recibidas indicarán el número de nodo del nodo. Estos números de nodo pueden utilizarse para enviar peticiones con eco a tales nodos desde direccionadores distanciados con el fin de verificar la conectividad.

**red\_origen** El número de red AppleTalk de origen. Éste es un parámetro opcional. Si no se especifica, el direccionador utiliza el número de red de interfaz de la interfaz de salida que conduce a la red de destino. Si la interfaz

## Mandatos de supervisión de AppleTalk Phase 2 (Talk 5)

de salida es una interfaz PPP de medio direccionador sin número, el direccionador utiliza cualquiera de sus nodos de red de interfaz LAN.

**nodo\_origen** El número de nodo AppleTalk de origen. Éste es un parámetro opcional. Si no se especifica, el direccionador utiliza el número de nodo de interfaz de la interfaz de salida que conduce a la red de destino. Si la interfaz de salida es una interfaz PPP de medio direccionador sin número, el direccionador utiliza cualquiera de sus nodos de red de interfaz LAN.

**tamaño** El número de bytes a utilizar en las peticiones con eco de AppleTalk. Éste es un parámetro opcional. El valor por omisión es de 56 bytes.

**velocidad** La velocidad del envío de peticiones con eco de AppleTalk. Éste es un parámetro opcional. El valor por omisión es de un segundo.

**Nota:** Si entra **atecho** sin parámetros, se le solicitarán todos los parámetros. Entre valores para los parámetros necesarios y entre valores para los parámetros opcionales o bien acepte los valores por omisión.

## Cache

El mandato **cache** visualiza información sobre las entradas de tamaño de antememoria.

### Sintaxis:

cache

### Ejemplo: cache

Destination	Interface	Usage	Next Hop
122/22	1	1	27/5
138/51	0	1	27/5
23/7	1	1	Direct

### Destination

La dirección de nodo AppleTalk (número de red/número de nodo).

**Net** El número de la interfaz utilizada para el reenvío al nodo de destino.

**Usage** El número de veces que esta entrada de antememoria se ha utilizado durante este período de tiempo, que es de cinco segundos. Una entrada no utilizada se suprime después de 10 segundos.

**Next Hop** La dirección AppleTalk del direccionador de siguiente salto utilizado para reenviar un paquete al nodo de destino, o es Direct si el nodo de destino está conectado a la interfaz directamente.

## Clear Counters

El mandato **clear-counters** borra todos los contadores de usos de la antememoria y los contadores de desbordamientos de paquetes.

### Sintaxis:

clear-counters



## Counters

Utilice el mandato **counters** para visualizar el número de desbordamientos de paquetes de cada red que envía y recibe paquetes de AppleTalk Phase 2. Este mandato visualiza el número de veces que la cola de la entrada de la función de reenvío de AppleTalk Phase 2 estaba llena cuando se han recibido paquetes de la red especificada.

### Sintaxis:

counters

### Ejemplo: counters

AP2 Input Packet Overflows

Net	Count
FR/0	0
Eth/0	4
PPP/0	22

## Dump

Utilice el mandato **dump** para obtener información de la tabla de direccionamiento sobre las interfaces del direccionador que reenvía paquetes de AppleTalk Phase 2.

**Nota:** `dump interfaznúmero`. visualiza la parte de la red general e información sobre zonas que es visible en la interfaz mencionada.

### Sintaxis:

dump

### Ejemplo: dump

Dest Net	Cost	State	Next hop	Zone
10-19	0	Dir	0/0	"Ethertalk", "Ventas"
40-49	1	Good	10/13	"Marketing", "ServCliente", "TokenTalk"
20-29	2	Sspct	10/13	"Fuchsia", "Troncal", "InspTécnica", "MKTING"

3 entries

También puede utilizar el mandato **dump** con una interfaz específica para visualizar las rutas que son visibles en esta interfaz. Puede utilizar esta función para asegurarse de que los filtros estén configurados correctamente porque muestra si las zonas o redes filtradas son visibles o no en una interfaz.

### Ejemplo: dump 0

View for interface 0

Dest net	Cost	State	Next hop	Zone
214-214	1	Good	152/152	"eth-214"
153-153	0	Dir		"eth153"
152-152	0	Dir		"ser152"

3 entries

**Dest Net** Especifica el número de red de destino, en decimal.

**Cost** Especifica el número de saltos de direccionador hasta esta red de destino.

## Mandatos de supervisión de AppleTalk Phase 2 (Talk 5)

- State** Especifica el estado de la entrada de la tabla de direccionamiento. Incluye lo siguiente:
- Next hop** Especifica el siguiente salto para los paquetes dirigidos a redes que no están conectadas directamente. Para las redes conectadas directamente, es el número de nodo 0.
- Zones** Especifica el nombre de esa red que es comprensible para un usuario. Los nombres de zonas están encerrados entre comillas dobles por si hay espacios incorporados o caracteres no imprimibles. Si el nombre de zona contiene caracteres que superan el juego de caracteres ASCII de 7 bits (tienen 8 bits), el nombre de zona que se visualice dependerá de las características del terminal de supervisión.

## Interface

Utilice el mandato **interface** para visualizar las direcciones de todas las interfaces del direccionador en que se ha habilitado AppleTalk Phase 2. Si la interfaz está presente pero se ha inhabilitado, este mandato muestra dicho estado.

**Nota:** `interface interfaznúmero`. visualiza la filtración activa de esta interfaz. Visualiza la red, el nodo, la zona por omisión y los filtros activos de una interfaz.

### Sintaxis:

`interface`

### Ejemplo: interface

```
Interface      Addresses
PPP/0         0/1 on net 1000-1000 default zone "LíneaSerie"
Eth/0         10/52 on net 10-19 default zone "Ventas"
PPP/1         0/0 in startup range
TKR/0         0/0 on net 20-29 default zone "Troncal"
```

También puede entrar el mandato `interface` seguido de un número de interfaz específico para ver la configuración de AP2 de esta interfaz.

### Ejemplo: interface 1

```
Eth/0 1/30 on net 1-5 default zone "marketing"

Input Net filters inclusive 1-5
Output Zone filters inclusive "financias"
Output Net filters exclusive 1-5
```

---

## Utilización de VINES

Este capítulo describe los mandatos de configuración del protocolo Banyan VINES e incluye los apartados siguientes:

- “Visión general de VINES”
- “Protocolos de capa de red VINES” en la página 314
- “Procedimientos básicos de la configuración” en la página 321
- “Acceso al entorno de configuración de VINES” en la página 323
- “Ejecución de Banyan VINES en el direccionador con función de puente” en la página 321
- “Mandatos de configuración de VINES” en la página 323.

**Nota:** Si necesita información más detallada sobre los protocolos VINES, consulte la siguiente publicación de Banyan: *VINES Protocol Definition*, número de pedido: 003673

---

## Visión general de VINES

### VINES sobre protocolos e interfaces de direccionador

El protocolo VINES direcciona paquetes de VINES sobre las interfaces y los protocolos siguientes:

- PPP Banyan Vines Control Protocol (PPP BVCP)
- Frame Relay
- Ethernet/802.3
- Red en Anillo 802.5
- X.25
- Cliente de emulación de LAN de ATM Ethernet
- Cliente de emulación de LAN de ATM Red en Anillo
- FDDI

También da soporte a paquetes a través del puente Source Routing Bridge (SRB) de 802.5.

El protocolo VINES está implementado en la capa de red (capa 3) del modelo OSI. VINES direcciona paquetes de la capa de transporte de un nodo a la capa de transporte de otro nodo. Cuando VINES direcciona los paquetes a sus nodos de destino, los paquetes pasan por las capas de red de los nodos intermedios, donde se comprueban por si hay errores de bit. Un paquete de VINES IP puede contener un máximo de 1500 bytes, que incluyen la cabecera de capa de red y todas las cabeceras y datos de protocolos de capas superiores.

### Nodos de servicio y clientes

La red VINES consta de nodos de servicio y nodos clientes. Un nodo de servicio proporciona resolución de direcciones y servicios de direccionamiento a los nodos clientes. Un nodo cliente es un nodo físicamente contiguo de la red VINES. Todos los direccionadores son nodos de servicio. Un nodo Banyan puede ser un nodo de servicio o un nodo cliente.

Cada nodo de servicio tiene una dirección de red de 32 bits y una dirección de subred de 16 bits. El IBM 2216 tiene una dirección de red configurable. Esta direc-

ción identifica al direccionador como nodo de red de servicio para Vines. Banyan ha asignado el rango del 30800000 al 309FFFFFF a IBM para que lo utilicen sus direccionadores. Este direccionador utiliza el rango del 30900000 al 3097FFFF.

**Nota:** Es muy importante que no se asigne la misma dirección de red a dos direccionadores. La dirección de red de un nodo de servicio Banyan es el número de serie hexadecimal de 32 bits del nodo de servicio. La dirección de subred para todos los nodos de servicio es 1.

La dirección de red de cada nodo cliente es, en general, la dirección de red del nodo de servicio de la misma red. No obstante, si un nodo cliente está en una LAN que tiene más de un nodo de servicio, se le asigna la dirección de red del nodo de servicio que responda primero a la petición de asignación de dirección del nodo cliente. La dirección de subred de cada nodo cliente es un valor hexadecimal del 8000 al FFFE.

---

## Protocolos de capa de red VINES

Esta implementación de VINES consta de los cuatro protocolos de capa de red siguientes. Las próximas secciones describen estos protocolos y sus implementaciones.

- “VINES Internet Protocol (VINES IP)”. Direcciona paquetes a través de la red.
- “Routing Update Protocol (RTP)” en la página 316. Distribuye información topológica para dar soporte a los servicios de direccionamiento proporcionados por VINES IP.
- “Internet Control Protocol (ICP)” en la página 319. Proporciona funciones de diagnóstico y soporte a ciertas entidades de protocolos de capa de transporte, como, por ejemplo, la función para facilitar la notificación de algunos errores de red y condiciones topológicas.
- “VINES Address Resolution Protocol (VINES ARP)” en la página 319. Asigna direcciones internet VINES a los nodos clientes que todavía no tienen direcciones.

## VINES Internet Protocol (VINES IP)

El protocolo VINES IP direcciona paquetes a través de la red utilizando el número de red de destino de la cabecera de VINES IP. VINES IP se compone de una cabecera de capa de red de 18 bytes que sirve de prefijo de cada paquete. La Tabla 101 en la página 315 resume los campos de esta cabecera.

### Implementación de VINES IP

Cuando VINES IP recibe un paquete, lo comprueba por si hay errores de tamaño y excepciones. Un error de tamaño es un paquete que tiene menos de 18 bytes o más de 1500 bytes. Si contiene un error de tamaño, VINES IP desecha el paquete. Un error de excepción es, por ejemplo, una suma de comprobación equivocada o una cuenta de saltos que ha caducado.

Si el paquete no contiene errores de tamaño ni excepciones, VINES IP comprueba la dirección de destino y reenvía el paquete de la manera siguiente:

- Si la dirección de destino es igual que la dirección VINES IP local y la suma de comprobación es válida, el nodo local acepta el paquete.

- Si la dirección de destino es igual que la dirección de difusión y la suma de comprobación es válida, VINES IP acepta el paquete, lo procesa localmente y comprueba el campo de cuenta de saltos de la cabecera de IP. Si la cuenta de saltos es superior a 0, VINES IP disminuye la cuenta de saltos en uno y vuelve a difundir el paquete a todos los medios locales a excepción del medio por el cual se ha recibido el paquete.
- Si la dirección de destino no es igual que la dirección VINES IP local ni la dirección de difusión, VINES IP comprueba sus tablas de direccionamiento para ver cuál es el siguiente salto. Si la cuenta de saltos es 0, VINES IP desecha el paquete. De lo contrario, disminuye la cuenta de saltos en uno y reenvía el paquete al siguiente salto.

Si la dirección VINES IP de destino no se encuentra en la tabla de direccionamiento y está establecido el bit de error en el campo de control de transporte, VINES IP elimina el paquete y devuelve un mensaje de destino inasequible de ICP al origen. Si no está establecido el bit de error en el campo de control de transporte, VINES IP desecha el paquete y no envía ningún mensaje al origen.

*Tabla 101 (Página 1 de 2). Resumen de los campos de cabecera de Vines IP*

<b>Campo de cabecera de VINES IP</b>	<b>Núm. de bytes</b>	<b>Descripción</b>
Suma de comprobación	2	Detecta la corrupción de los errores de bit de un paquete.
Longitud de paquete	2	Indica el número de bytes del paquete con inclusión de la cabecera y los datos de VINES IP.

Tabla 101 (Página 2 de 2). Resumen de los campos de cabecera de Vines IP

Campo de cabecera de VINES IP	Núm. de bytes	Descripción
Control de transporte	1	<p>Consta de los cinco subcampos siguientes:</p> <p><b>Clase</b> Determina el tipo de nodo al que se envían los paquetes difundidos de VINES IP.</p> <p><b>Error</b> Si está establecido el bit de error, se envía un paquete con notificación de excepción a la entidad de protocolo de capa de transporte cuando no puede direccionarse un paquete hacia un nodo de servicio o un nodo cliente.</p> <p><b>Métrica</b> Solicita que el nodo de servicio del nodo cliente de destino devuelva al origen un coste del direccionamiento del nodo de servicio al nodo cliente de destino.</p> <p><b>Redireccionamiento</b> Indica si el paquete contiene un mensaje de RTP especificando una ruta mejor a utilizar.</p> <p><b>Cuenta de saltos</b> Especifica el rango por el que puede pasar un paquete. La cuenta de saltos abarca desde el 0x0 hasta el 0xf.</p>
Tipo de protocolo	1	Especifica el protocolo de capa de red VINES del paquete como VINES IP, RTP, ICP o VINES ARP.
Número de red de destino	4	Un número de red de 4 bytes de la dirección VINES IP del destino.
Número de subred de destino	2	Un número de subred de 2 bytes de la dirección VINES IP del destino.
Número de red de origen	4	Un número de red de 4 bytes de la dirección VINES IP del origen.
Número de subred de origen	2	Un número de subred de 2 bytes de la dirección VINES IP del origen.

## Routing Update Protocol (RTP)

RTP reúne y distribuye la información de direccionamiento que VINES IP utiliza para calcular rutas a través de la red. RTP permite que cada direccionador difunda de manera periódica tablas de direccionamiento a todos los contiguos. El direccionador determina el contiguo de destino que utilizará para direccionar el paquete.

Los nodos de servicio mantienen dos tablas: una tabla de direccionamiento y una tabla de contiguos. Ambas tablas tienen temporizadores que establecen un período de tiempo para el contenido con el fin de eliminar entradas obsoletas. Las actuali-

zaciones del direccionamiento para las interfaces X.25 tienen lugar cuando hay un cambio en la base de datos de direccionamiento, como, por ejemplo, cuando un nodo se activa/desactiva o cuando cambia la métrica.

### Tabla de direccionamiento

La tabla de direccionamiento contiene información sobre los nodos de servicio. En la Figura 13 se muestra una tabla de direccionamiento de muestra. Después de la figura siguen las descripciones de los campos de esta tabla.

Net	Address	Next Hop	Nbr Addr	Nbr Intf	Metric	Age (secs)
S	30622222		30622222:0001	Eth/0	20	30
H	0027AA21		0027AA21:0001	Eth/1	2	120
P	0034CC11		0034CC11:0001	X.25/0	45	0
3 Total Routes						
<b>S ⇒ Entry is suspended, H ⇒ Entry is in Hold-down, P ⇒ Entry is permanent</b>						

Figura 13. Tabla de direccionamiento de muestra

### Campo de tabla de direccionamiento Descripción

#### Net Address

La dirección de red es un número de 32 bits exclusivo. La letra S, H o P que precede al campo de dirección de red indica lo siguiente:

- S** Indica que el nodo de servicio se encuentra en el estado de suspendido y se anuncia, durante 90 segundos, como desactivado. Después de 90 segundos, el direccionador elimina la entrada de este nodo de servicio de la tabla de direccionamiento.
- H** Indica que el nodo de servicio se encuentra en el estado de retenido y se anuncia, durante 2 minutos, como desactivado. Después de 2 minutos, el direccionador anuncia el nodo de servicio como operativo. Si un nodo de servicio se encuentra en el estado de suspendido y recibe un paquete de RTP, el nodo de servicio entra en el estado de retenido.
- P** Indica que la interfaz X.25 entra en el estado de permanente durante 4-1/2 minutos después de la inicialización. Después de 4-1/2 minutos, el contiguo entra en el estado de permanente y su duración se queda en 0 mientras permanece en este estado. Si la interfaz X.25 se desactiva, se elimina la entrada de la tabla de direccionamiento.

#### Next Hop Nbr Addr

La dirección del nodo de servicio contiguo que es el siguiente salto en la vía de acceso de menor coste hacia la red.

#### Nbr Intf

El medio al que está conectado el nodo de servicio contiguo de siguiente salto.

#### Metric

El coste estimado, en incrementos de 200 milisegundos, del direccionamiento del paquete de VINES al nodo de servicio de destino.

### Age (secs)

La duración actual, en segundos, para la entrada. Si un direccionador no recibe una actualización sobre un nodo de servicio que está en la tabla de direccionamiento al menos cada 360 segundos (6 minutos), el direccionador elimina la entrada de este nodo de servicio de la tabla de direccionamiento.

### Tablas de contiguos

La tabla de contiguos contiene información sobre los nodos de servicio y nodos clientes contiguos conectados con el direccionador. La Figura 14 muestra una tabla de contiguos de muestra y después siguen las descripciones de los campos de esta tabla.

Nbr	Address	Intf	Metric	Age(secs)	H/W Addr	RIF
30633333	:0001	TKR/0	4	30	0000C009	5012
0035CC10	:8000	Eth/1	2	120	0000C007	8221
2 Total Neighbors						

Figura 14. Tabla de contiguos de muestra

### Campo de tabla de contiguos Descripción

#### Nbr Address

La dirección del nodo contiguo. En la Figura 14, la dirección 30633333:0001 es un nodo de servicio y la dirección 0035CC10:8000 es un nodo cliente.

#### Intf

El medio al que está conectado el nodo contiguo.

#### Metric

El coste estimado, en incrementos de 200 milisegundos, del direccionamiento del paquete de VINES al nodo contiguo.

#### Age (secs)

La duración actual, en segundos, para la entrada. Si un direccionador no recibe una actualización del direccionamiento de un contiguo al menos cada 360 segundos (6 minutos), el direccionador elimina la entrada de este contiguo de la tabla de contiguos y, si el contiguo es un nodo de servicio, de la tabla de direccionamiento.

#### H/W Addr

La dirección LAN del nodo si el contiguo está conectado a una LAN. Si el protocolo Frame Relay está en ejecución, H/W Addr es el identificador de conexión de enlace de datos (DLCI). Para las interfaces X.25, H/W Addr es la dirección X.25 del contiguo.

#### RIF

El campo de información de direccionamiento. Una secuencia de números de segmento y puente, en hexadecimal, que indican una vía de acceso a través de la red entre dos estaciones. El RIF es necesario para el direccionamiento de origen.



## Implementación de RTP

Las entidades de RTP emiten los paquetes siguientes:

- *Paquetes de petición de RTP.* Peticiones a los nodos de servicio para obtener la topología actual de la red. Durante la inicialización, una interfaz X.25 genera paquetes de petición de direccionamiento cada 90 segundos para cada destino X.25 de la interfaz X.25. Cuando la interfaz X.25 recibe un paquete de respuesta sobre direccionamiento, se envían tres actualizaciones de base de datos de direccionamiento al completo, cada 90 segundos, a los nodos de servicio que han enviado los paquetes de respuesta sobre direccionamiento. Una vez que la interfaz X.25 haya recibido paquetes de respuesta sobre direccionamiento de todos los nodos de destino X.25, no se enviarán más peticiones de direccionamiento a estas direcciones X.25.
- *Paquetes de actualización de RTP.* Paquetes enviados por nodos clientes a los nodos de servicio para notificar su existencia a los nodos de servicio. Los nodos de servicio también envían paquetes de actualización de RTP para notificar su existencia a otros nodos y para anunciar sus bases de datos de direccionamiento.
- *Paquetes de respuesta de RTP.* Paquetes que envían los nodos de servicio en respuesta a los paquetes de petición de RTP.
- *Paquetes de redireccionamiento de RTP.* Informan a los nodos de las vías de acceso mejores entre ellos para los paquetes de direccionamiento.

A menos que estén conectados por un circuito permanente, cada uno de los nodos de servicio y nodos clientes difunde una actualización de RTP cada 90 segundos. Ésta notifica a los contiguos la existencia del nodo y su tipo (nodo de servicio o nodo cliente) y, en el caso de los nodos de servicio, anuncia sus bases de datos de direccionamiento. Cuando un direccionador recibe un paquete de actualización de un nodo de servicio, RTP extrae la dirección VINES IP y busca en la tabla de direccionamiento una entrada existente que corresponda a este nodo de servicio. Si existe, RTP actualiza la entrada y restablece el temporizador de la misma. Si una entrada no existe, RTP crea una e inicializa el temporizador para la misma.

## Internet Control Protocol (ICP)

ICP genera mensajes de información de la red en dos tipos de paquetes destinados al direccionador local:

- *Paquete de destino inasequible.* Indica que un paquete no ha podido llegar a su destino y que se ha devuelto a su origen. A continuación, el direccionador emite un mensaje del ELS y desecha el paquete.
- *Paquete de métrica de retardo.* Un paquete procedente de un nodo de origen de petición de la métrica del direccionamiento del nodo de servicio de destino al nodo cliente de destino.

## VINES Address Resolution Protocol (VINES ARP)

El protocolo VINES ARP asigna direcciones VINES IP exclusivas a los nodos clientes. VINES ARP incluye los tipos de paquetes siguientes:

- *Paquete de petición de consulta.* Paquetes que los nodos clientes difunden al inicializarse.
- *Paquete de respuesta para consulta.* La respuesta del nodo de servicio a un paquete de petición de consulta.

- *Paquete de petición de asignación.* La respuesta del nodo cliente a un paquete de respuesta para consulta.
- *Paquete de respuesta de asignación.* Incluye las direcciones de red y subred que el nodo de servicio ha asignado a un nodo cliente.

Para asignar una dirección VINES IP a un nodo cliente, VINES ARP implementa el algoritmo siguiente:

1. El nodo cliente difunde un paquete de petición de consulta.
2. Los nodos de servicio responden con un paquete de respuesta para consulta que contiene la dirección MAC de destino del nodo cliente y una dirección VINES IP de difusión.
3. El nodo cliente emite un paquete de petición de asignación para el nodo de servicio que haya respondido con un paquete de respuesta para consulta.
4. El nodo de servicio responde con un paquete de respuesta de asignación que contiene las direcciones VINES de red y subred.

Cada nodo cliente mantiene un temporizador que tiene un valor por omisión de dos segundos. El temporizador se inicia cuando un nodo cliente transmite un paquete de petición de consulta o de petición de asignación. El nodo cliente detiene y restablece el temporizador cuando recibe un paquete de respuesta para consulta. Cuando un período de tiempo de espera excedido sobrepasa los dos segundos, el nodo cliente se inicializa, difunde un paquete de petición de consulta y restablece el temporizador. La Tabla 102 resume los estados en que entran los nodos de servicio y nodos clientes durante la implementación de VINES ARP.

<i>Tabla 102. Estados de los nodos clientes y los nodos de servicio VINES ARP</i>	
<b>Estados de los nodos clientes</b>	
Inicialización	El nodo cliente se está inicializando.
Consulta	El nodo cliente transmite un paquete de petición de consulta.
Petición	El nodo cliente ha recibido un paquete de respuesta para consulta de un nodo de servicio y transmite un paquete de petición de asignación al nodo de servicio que ha respondido.
Asignado	El nodo cliente ha recibido un paquete de respuesta de asignación que contiene las direcciones VINES de red y subred.
<b>Estados de los nodos de servicio</b>	
Inicialización	El protocolo VINES ARP se está inicializando.
Escucha	El nodo de servicio espera paquetes de petición de consulta de los nodos clientes.
Servicio	El nodo de servicio ha recibido un paquete de petición de consulta y ha enviado un paquete de respuesta para consulta.
Asignación	El nodo de servicio emite un paquete de respuesta de asignación que contiene las direcciones VINES de red y subred.

## Procedimientos básicos de la configuración

Los pasos para configurar inicialmente cada direccionador que envíe y reciba paquetes de VINES son los siguientes:

1. Asigne una dirección hexadecimal de 32 bits exclusiva a cada direccionador de la red VINES. Utilizando el mandato **set network-address** *núm. hex*, entre una dirección de red del 30900000 al 3097FFFF. La dirección de red de los servidores Banyan es el número de serie hexadecimal de 32 bits del nodo de servicio. Este número se lee automáticamente en la clave de servidor de nodos.
2. Habilite globalmente el protocolo VINES utilizando el mandato **enable VINES**.
3. Habilite las tarjetas de interfaz que van a transmitir y recibir los paquetes de VINES utilizando el mandato **enable interface** *interfaznúm.*.

Para que sean efectivos los cambios de configuración, debe reiniciar el direccionador. Entre **reload** después del indicador de OPCON (\*) y responda **yes** a la solicitud siguiente:

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

Para ver la configuración, entre el mandato **list** después del indicador VINES `config>`.

## Ejecución de Banyan VINES en el direccionador con función de puente

Los servidores Banyan VINES deben tener esta opción de Banyan para comunicarse con otros servidores o direccionadores:

LAN de servidor a servidor.

Para comunicarse a través de una WAN X.25, los servidores VINES conectados directamente a la WAN necesitan estas dos opciones:

WAN de servidor a servidor

Soporte de X.25 en el servidor (hardware y software).

## Ejecución de Banyan VINES sobre enlaces WAN

Cuando configure un enlace PPP, Frame Relay o X.25 para utilizarlo con VINES, debe establecer la velocidad de HDLC del enlace aunque establezca el cronometraje en externo.

Si establece la velocidad de HDLC en cero, VINES supone que la velocidad es de 56 kbps. No establezca la velocidad en un valor superior al de la línea.



## Configuración y supervisión de VINES

Este capítulo describe los mandatos de configuración y supervisión de VINES e incluye los apartados siguientes:

- “Acceso al entorno de supervisión de VINES” en la página 327
- “Mandatos de supervisión de VINES” en la página 327

### Acceso al entorno de configuración de VINES

Para acceder al entorno de configuración de VINES, entre el mandato siguiente en el indicador Config>:

```
Config> protocol vin
VINES Protocol user configuration
VINES Config>
```

### Mandatos de configuración de VINES

Este apartado resume los mandatos de configuración de VINES y ofrece una explicación de los mismos. Entre estos mandatos en el indicador VINES config>.

*Tabla 103. Resumen de los mandatos de configuración de VINES*

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi.
Add	Añade una conversión de dirección X.25.
Delete	Suprime una conversión de dirección X.25.
Disable	Inhabilita el protocolo VINES en todas las interfaces o en una sola interfaz e inhabilita la suma de comprobación.
Enable	Habilita el protocolo VINES en todas las interfaces o en una sola interfaz y habilita la suma de comprobación.
List	Visualiza la configuración actual de VINES.
Set	Asigna las direcciones de red a los direccionadores de la red VINES y establece el número máximo de nodos de servicio y nodos clientes físicamente contiguos.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

### Add

Añade una conversión de dirección X.25.

#### Sintaxis:

```
add                interface ...
#                  Especifica el número de interfaz.
```

## Mandatos de configuración de VINES (Talk 6)

### **dir-X.25-remota**

Puede incluir hasta 15 dígitos. Si la conexión de circuito virtual se ha configurado como PVC, la dirección VINES *dir-X.25-remota* debe coincidir con la dirección de PVC configurada en la solicitud de X.25. Si las direcciones no coinciden, el sistema toma por omisión el valor de un circuito virtual conmutado (SVC).

### **descriptor de contexto**

Un nombre que el usuario puede configurar y que identifica de forma exclusiva a cada servidor remoto.

**Ejemplo:** `add interface 0 4508907898 test`

## Delete

Suprime una conversión de dirección X.25.

### **Sintaxis:**

`delete`                    `interface ...`

**#**                    Especifica el número de interfaz.

### **dir-X.25-remota**

Puede incluir hasta 15 dígitos. Si la interfaz especificada no se ha configurado utilizando el mandato de VINES **add interface**, el terminal visualiza el mensaje `That X.25 address has not been configured.`

**Ejemplo:** `delete interface 1 4799999999 compress`

## Disable

Utilice el mandato **disable** para inhabilitar el protocolo VINES en todas las interfaces o en una sola interfaz o para inhabilitar la suma de comprobación.

### **Sintaxis:**

`disable`                    `checksumming ...`  
                              `interface ...`  
                              `vines`

### **checksumming** *interfaznúmero.*

Inhabilita la suma de comprobación en los paquetes que genere la interfaz especificada, sin contar los paquetes difundidos. Para todas las interfaces, el valor por omisión es la inhabilitación de la suma de comprobación.

**Ejemplo:** `disable checksumming 0`

### **interface** *interfaznúmero.*

Inhabilita el protocolo VINES en la interfaz especificada.

**Ejemplo:** `disable interface 1`

**vines**                    Inhabilita el protocolo VINES en todas las interfaces.

**Ejemplo:** `disable vines`

## Enable

Utilice el mandato **enable** para habilitar el protocolo VINES en todas las interfaces o en una sola interfaz o para habilitar la suma de comprobación.

### Sintaxis:

```
enable          checksumming ...
                interface ...
                vines
```

### **checksumming** *interfaznúmero*.

Habilita la suma de comprobación en los paquetes que genere la interfaz especificada.

**Ejemplo: enable checksumming 0**

### **interface** *interfaznúmero*.

Habilita el protocolo VINES en la interfaz especificada.

**Ejemplo: enable interface 1**

**vines** Habilita el protocolo VINES globalmente. Si recibe un mensaje de error después de entrar este mandato, póngase en contacto con el representante del servicio al cliente. Es posible que el software VINES no esté en la carga del software.

**Ejemplo: enable vines**

## List

Utilice el mandato **list** para visualizar la configuración actual de VINES.

### Sintaxis:

```
list
```

### Ejemplo: list

```
VINES: enabled/disabled
VINES network number (hex):
Maximum Number of Routing Table Entries:
Maximum Number of Neighbor Service Nodes:
Maximum Number of Neighbor Client Nodes:

List of interfaces configured for VINES:

intf 0      (checksumming enabled/disabled)
intf 1      (checksumming enabled/disabled)
intf 2      (checksumming enabled/disabled)
```

### *VINES X.25 Configuration*

Interface	Remote X.25 Address	Remote Handle
0	4508907898	test

```
VINES config>
```

**VINES** Indica si VINES se ha habilitado o inhabilitado globalmente.

### **VINES network number (hex)**

Una dirección hexadecimal de 32 bits configurable para los direccionadores de la red VINES.

## Mandatos de configuración de VINES (Talk 6)

### Maximum Number of Routing Table entries

Un valor configurado que especifica el número máximo de entradas permitidas en la tabla de direccionamiento de VINES.

### Maximum Number of Neighbor Service Nodes

Un valor configurado que especifica el número máximo de nodos de servicio contiguos conectados con el direccionador.

### Maximum Number of Neighbor Client Nodes

Un valor configurado que especifica el número máximo de nodos clientes conectados con el direccionador.

### List of interfaces configured for VINES

Visualiza las interfaces en que se ha habilitado VINES y si la suma de comprobación se ha habilitado o inhabilitado.

### VINES X.25 Configuration

Esta información representa lo siguiente:

**Interface** La interfaz que se ha configurado para X.25.

#### Remote X.25 Address

La dirección de DTE del servidor remoto.

#### Remote Handle

Un nombre que el usuario puede configurar y que identifica de forma exclusiva al servidor remoto.

## Set

Utilice el mandato **set** para asignar las direcciones de red a los direccionadores de la red VINES y para especificar el número máximo de nodos de servicio y nodos clientes.

### Sintaxis:

```
set          client-node-neighbors ...  
              network-address ...  
              routing-table-size ...  
              service-node-neighbors ...
```

### **client-node-neighbors** núm.

Especifica el número máximo de nodos clientes de la red. **Client-node-neighbors** incluye todos los nodos de cada red conectada directamente a través del direccionador. El rango es del 1 al 65535 y el valor por omisión es 25.

**Nota:** Es recomendable que establezca este número en un valor significativamente superior al número de nodos de la red. Ello permitirá que la red continúe funcionando sin necesidad de volver a configurar y reiniciar los direccionadores cuando se añadan nodos adicionales. El aumento de este número depende del tamaño de la red y de las dimensiones del desarrollo previsto. Como norma general, establezca **client-node-neighbors** en un valor que supere en un 25% el número real de estaciones de cliente de las LAN que sean locales para el direccionador.

**Ejemplo:** `set client-node-neighbors 20`



**network-address** *núm. hex*

Asigna una dirección de red a cada direccionador de la red VINES. *núm. hex* es un valor hexadecimal de 32 bits del 30900000 al 3097FFFF.

**Ejemplo:** set network-address 30922222

**routing-table-size** *núm.*

Especifica el número máximo de nodos de servicio y direccionadores de la red VINES. El rango es del 1 al 65535 y el valor por omisión es 300.

**Nota:** Asegúrese de que el número que especifique sea lo suficientemente elevado como para alojar 2216 y servidores VINES adicionales en relación con el desarrollo de la red.

**Ejemplo:** set routing-table-size 250

**service-node-neighbors** *núm.*

Especifica el número máximo de nodos de servicio físicamente contiguos. Este número incluye los 2216 y servidores VINES que son el primer punto de contacto después de atravesar una WAN. El rango es del 1 al 65535 y el valor por omisión es 50.

**Ejemplo:** set service-node-neighbors 100

---

## Acceso al entorno de supervisión de VINES

Para acceder al entorno de supervisión de VINES,

```
* t 5
```

A continuación, entre el mandato siguiente en el indicador +:

```
+ protocol vin
VINES>
```

---

## Mandatos de supervisión de VINES

Este apartado describe los mandatos de supervisión de VINES. Entre estos mandatos en el indicador VINES>.

*Tabla 104. Resumen de los mandatos de supervisión de VINES*

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxxi.
Counters	Visualiza errores de direccionamiento y el número de veces que la cola de la entrada de VINES estaba llena cuando se han recibido paquetes de la interfaz especificada.
Dump	Visualiza el contenido actual de las tablas de direccionamiento y contiguos de VINES.
Route	Visualiza una entrada de la tabla de direccionamiento de VINES.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxi.

### Counters

Utilice el mandato **counters** para visualizar errores de direccionamiento y el número de veces que la cola de la entrada de VINES estaba llena cuando se han recibido paquetes de la interfaz especificada.

#### Sintaxis:

#### counters

#### Ejemplo: counters

```
Routing Errors
Count          Type
-----
2             Net Unreachable
3             Hop Count Expired
3             Routing Update from Orphan Client
0             Routing Redirect Received
0             Routing Response Received

VINES Input Packet Overflows
Net           Count
---
Eth/0         5
Eth/1         1
```

#### *Net Unreachable*

El número de veces que el direccionador ha recibido un paquete destinado a un nodo que no se ha encontrado en la tabla de direccionamiento.

#### *Hop Count Expired*

El número de veces que el direccionador ha desechado un paquete porque ha caducado la cuenta de saltos.

#### *Routing Update from Orphan Client*

El número de veces que el direccionador ha recibido un paquete de actualización procedente de un nodo cliente cuyo nodo de servicio no existía. Puede producirse una actualización del direccionamiento de un cliente huérfano cuando el direccionador arranca y tiene noticia del nodo cliente antes que del nodo de servicio o cuando el nodo de servicio de un cliente está inactivo y se ha eliminado una entrada de la base de datos de la tabla de direccionamiento.

#### *Routing Redirect Received*

El número de veces que el direccionador ha recibido paquetes de redireccionamiento de nodos de servicio.

#### *Routing Response Received*

El número de veces que se han generado paquetes de respuesta como resultado de paquetes de petición iniciados por el direccionador.

#### *VINES input packet overflows*

El número de veces que la cola de la entrada de la función de reenvío de VINES estaba llena cuando se han recibido paquetes de la interfaz especificada. Los paquetes se desechan a continuación.

## Dump

Utilice el mandato **dump** para visualizar el contenido de las tablas de direccionamiento y contiguos de VINES.

### Sintaxis:

```
dump          _neighbor-tables
                _routing-tables
```

### neighbor-tables

Visualiza información sobre cada nodo de servicio y nodo cliente contiguos conectados con el direccionador.

#### Ejemplo: dump neighbor-tables

Nbr	Address	Intf	Metric	Age(secs)	H/W Addr	RIF
30622222	:0001	TKR/0	4	30	0000C00	95012
0035CC10	:8000	Eth/0	2	120	0000C00	78221

2 Total Neighbors

#### Nbr Address

La dirección del nodo contiguo. En el ejemplo anterior, la dirección 30622222:0001 es un nodo de servicio y la dirección 0035CC10:8000 es un nodo cliente.

#### Intf

El medio al que está conectado el nodo contiguo.

#### Metric

El coste estimado, en 200 milisegundos, del direccionamiento del paquete de VINES al nodo contiguo.

#### Age (secs)

La duración actual, en segundos, para la entrada. Si un direccionador no recibe una actualización del direccionamiento de un contiguo al menos cada 360 segundos (6 minutos), el direccionador elimina la entrada de este contiguo de la tabla de contiguos y, si el contiguo es un nodo de servicio, de la tabla de direccionamiento.

#### H/W Addr

La dirección LAN del nodo si el contiguo está conectado a una LAN. Si el protocolo Frame Relay está en ejecución, H/W Addr es el identificador de conexión de enlace de datos (DLCI). Para las interfaces X.25, H/W Addr es la dirección X.25 del contiguo.

#### RIF

El campo de información de direccionamiento. Una secuencia de números de segmento y puente, en hexadecimal, que indican una vía de acceso a través de la red entre dos estaciones. El RIF es necesario para el direccionamiento de origen.

### routing-tables

Visualiza información sobre cada nodo de servicio reconocido por el direccionador.

#### Ejemplo: dump routing-table

## Mandatos de supervisión de VINES (Talk 5)

Net Address	Next Hop Nbr Addr	Nbr Intf	Metric	Age (secs)
S 30622222	30622222:0001	Eth/0	20	30
H 0027AA21	0027AA21:0001	Eth/1	2	120
P 0034CC11	0034CC11:0001	X.25/0	45	0

3 Total Routes

S ==> Entry is suspended, H ==> Entry is Holddown, P ==> Entry is permanent

### Net Address

La dirección de red es un valor hexadecimal de 32 bits configurable y exclusivo del 30900000 al 3097FFFF. Banyan ha asignado este rango de números a IBM. Es muy importante que no se asigne la misma dirección de red a dos direccionadores de una red. La dirección de red de un nodo de servicio Banyan es el número de serie hexadecimal de 32 bits del nodo de servicio. La letra S, H o P que precede al campo de dirección de red indica lo siguiente:

- S:** El nodo de servicio se encuentra en el estado de suspendido y se anuncia, durante 90 segundos, como desactivado. Después de 90 segundos, el direccionador elimina la entrada de este nodo de servicio de la tabla de direccionamiento.
- H:** El nodo de servicio se encuentra en el estado de retenido y se anuncia, durante 2 minutos, como desactivado. Después de 2 minutos, el direccionador anuncia el nodo de servicio como operativo. Si un nodo de servicio se encuentra en el estado de suspendido y recibe un paquete de RTP, el nodo de servicio entra en el estado de retenido.
- P:** Después de la inicialización, la interfaz X.25 entra en el estado de permanente durante 4 minutos y 1/2. Después de 4 minutos y 1/2, el contiguo entra en el estado de permanente y su duración se queda en 0 mientras permanece en este estado. Si la interfaz X.25 se desactiva, se elimina la entrada de la tabla de direccionamiento.

### Next Hop Nbr Addr

La dirección del nodo de servicio contiguo que es el siguiente salto en la vía de acceso de menor coste hacia la red.

**Nbr Intf** El medio al que está conectado el nodo de servicio contiguo de siguiente salto.

**Metric** El coste estimado, en 200 milisegundos, del direccionamiento del paquete de VINES al nodo de servicio de destino.

### Age (secs)

La duración actual, en segundos, para la entrada. Si un direccionador no recibe una actualización del direccionamiento sobre un nodo de servicio que está en la tabla de direccionamiento al menos cada 360 segundos (6

minutos), el direccionador elimina la entrada de este nodo de servicio de la tabla de direccionamiento.

## Route

Utilice el mandato **route** para ver una entrada de la tabla de direccionamiento.

### Sintaxis:

**route**                      dirección dada

### **dirección dada**

La dirección de red del nodo de servicio.

### **Ejemplo: route 30622222**

Net Address	Next Hop	Nbr Addr	Nbr Intf	Metric	Age (secs)
30622222	30622222:0001		Eth/0	2	30

## Mandatos de supervisión de VINES (Talk 5)

---

## Utilización de DNA IV

Este capítulo describe la implementación de Digital Network Architecture Phase IV (DNA IV) por parte de IBM e incluye los apartados siguientes:

- “Visión general de DNA IV”
- “Implementación de DNA IV por parte de IBM” en la página 337
- “Configuración de DNA IV” en la página 346
- “Mandatos de configuración y supervisión de DNA IV” en la página 351

---

## Visión general de DNA IV

DNA IV es un conjunto de componentes de software que transfieren información entre redes conectadas por medios físicos. Transfiriendo información, el software DNA IV facilita la comunicación entre dispositivos de red como, por ejemplo, PC (Personal Computer), servidores de archivos e impresoras.

El protocolo DNA IV es el protocolo subyacente para los productos de software DECnet de Digital Equipment Corporation así como los productos compatibles con DNA. El protocolo DNA IV incluye lo siguiente:

- Software de direccionamiento para las redes de protocolo DNA IV.
- NCP, una implementación del programa DNA IV Network Control Program. Para obtener más información, consulte la documentación correspondiente de DECnet-VAX, publicada por Digital Equipment Corporation.
- Soporte para DNA IV Maintenance Operations Protocol (MOP).

DNA IV lleva a cabo estas dos funciones principales:

- Mantiene una base de datos de direccionamiento completa sobre todos los nodos de su área. (Si el direccionador funciona como direccionador de nivel 2, mantiene la base de datos para todas las áreas asimismo.)
- Direcciona los paquetes de datos de DECnet de entrada a los destinos correspondientes a partir de su propia base de datos de direccionamiento. Ignora los paquetes dirigidos al direccionador que no son paquetes hello o paquetes de direccionamiento.

DNA IV da soporte a lo siguiente:

- Diversas áreas de una red Ethernet, Red en Anillo o FDDI.
- Las operaciones básicas de MOP. DNA IV responde a un mensaje de ID de petición de MOP con un mensaje de ID del sistema de MOP. DNA IV también envía un mensaje de ID del sistema de MOP cuando se activa un circuito. Puede supervisar mensajes de MOP utilizando el módulo de configuración de Ethernet bajo DECnet-VAX NCP. El programa NCP del direccionador no incluye ningún módulo de configuración de Ethernet.
- El protocolo LAT. El protocolo LAT no forma parte de la familia de protocolos DNA IV. Es un protocolo de sólo Ethernet pensado únicamente para comunicaciones a corta distancia (tiempo de ida y vuelta limitado). (El protocolo CTERM proporciona soporte de terminales de área amplia utilizando los protocolos DNA IV a través de los direccionadores. El mandato **set host** de DECnet-VAX proporciona el protocolo CTERM.)

Merecen una consideración especial las siguientes limitaciones de DNA IV:

- DNA IV no da soporte a los protocolos NSP, Session o NICE.
- DNA IV no da soporte al protocolo de línea DDCMP en sus líneas síncronas conectadas directamente.
- DNA IV no proporciona funciones compatibles con Phase III porque no da soporte a los protocolos de enlace de datos DDCMP utilizados por todos los nodos Phase III.
- NCP (la implementación de DECnet Network Control Program del direccionador) implementa un subconjunto de los mandatos y funciones del programa NCP original.

## Terminología y conceptos de DNA IV

Esta sección contiene una breve descripción de la terminología de DNA IV.

### Sistema de dirección

Cada nodo tiene una dirección de nodo de 16 bits, que es la misma para todas las interfaces de ese nodo. Una dirección consta de 2 campos: 6 bits de número de área y 10 bits de número de nodo. Las direcciones se imprimen en decimal con un punto que separa el área y el nodo, de manera que, por ejemplo, 1.7 indica el nodo 7 del área 1. Si no se facilita ninguna área, se supone el área 1. Está permitida cualquier dirección dentro del rango del 1.1 al 63.1023. Tanto los nodos como las áreas deben numerarse empezando desde 1, con pocos espacios, si los hay. Esto es porque el número máximo de nodos y el número máximo de áreas son opciones de la configuración y controlan el tamaño de muchas estructuras de datos de direccionamiento.

No existe una correlación directa entre las direcciones y el cableado físico. Las rutas se calculan en relación con los nodos, no con los cables.

### Sistema de dirección de enlace de datos Ethernet

Cada interfaz Ethernet se establece en la misma dirección física de 48 bits, que es la concatenación de un prefijo de 32 bits (AA-00-04-00) y la dirección de nodo DNA IV de 16 bits. En la dirección de nodo tiene lugar una conmutación de bytes (para la conversión de PDP11 al orden de los bytes de Ethernet). De este modo, el nodo DNA IV 1.1 tiene la dirección Ethernet AA-00-04-00-01-04.

También se utiliza el vertimiento múltiple (distinto de difusión) en el direccionamiento. Las tres direcciones de vertimiento múltiple utilizadas por DNA IV son AB-00-00-02-00-00, AB-00-00-03-00-00 y AB-00-00-04-00-00.

### Sistema de dirección de enlace de datos Red en Anillo 802.5

La implementación de DNA sobre Red en Anillo IEEE 802.5 se ajusta a la especificación *DECnet Digital Networking Architecture (Phase IV) Token-Ring Data Link and Node Product Functional Specification*, Versión 1.0.0, que incluye el soporte para las direcciones MAC arbitrarias (AMA).

Hay dos tipos de sistemas de direcciones MAC, el sistema de dirección DNA IV convencional, que es la concatenación de un prefijo de 32 bits (AA-00-04-00) y la dirección de área/nodo DNA IV de 16 bits, o bien el AMA, que permite que el protocolo DNA se ejecute sobre nodos IEEE 802.5 sin que el protocolo DNA cambie las direcciones MAC de los mismos. Esto es necesario si sigue determinados con-



venios de protocolos de IBM. Puede seleccionar el tipo de sistema de dirección que va a utilizar por medio del proceso de configuración de DNA (NCP>).

Otro tipo de representación de sistema de dirección es el orden de los bits nativos. Se deshace la estructura de bytes de este tipo de dirección cuando se envía sobre la capa física. Por ejemplo, el prefijo canónico de 32 bits mostrado anteriormente (con guiones) se expresa como 55:00:20:00 en el orden de los bits nativos, con los bytes separados entre sí por el signo de dos puntos.

**Nota:** Cuando configure DNA IV para que se ejecute sobre la Emulación de LAN de ATM, debe utilizarse el AMA.

### Sistema de dirección de enlace de datos FDDI

La implementación de DNA sobre FDDI incluye el soporte para las direcciones MAC arbitrarias (AMA).

Hay dos tipos de sistemas de direcciones MAC, el sistema de dirección DNA IV convencional, que es la concatenación de un prefijo de 32 bits (AA-00-40-00) y la dirección de área/nodo DNA IV de 16 bits, o bien el AMA, que permite que el protocolo DNA se ejecute sobre nodos FDDI sin que el protocolo DNA cambie las direcciones MAC de los mismos. Esto es necesario si sigue determinados convenios de protocolos de IBM. Puede seleccionar el tipo de sistema de dirección que va a utilizar por medio del proceso de configuración de DNA (NCP>).

Otro tipo de representación de sistema de dirección es el orden de los bits nativos. Se deshace la estructura de bytes de este tipo de dirección cuando se envía sobre la capa física. Por ejemplo, el prefijo canónico de 32 bits mostrado anteriormente (con guiones) se expresa como 55:00:20:00 en el orden de los bits nativos, con los bytes separados entre sí por el signo de dos puntos.

### Sistema de dirección de enlace de datos X.25

El direccionador da soporte a DECnet Phase IV sobre X.25 y puede interoperar con direccionadores que ejecuten la implementación de DECnet Phase IV sobre X.25 por parte de Digital.

Configure la dirección de DTE local y la remota con el mandato **set/define circuit** cuando configure un circuito DECnet. En el parámetro *call-userdata* se especifica la dirección de DTE local en octetos (caracteres) hexadecimales. En el parámetro *DTE-address* se especifica la dirección remota en octetos hexadecimales. Ambas direcciones de DTE local y remota pueden tener un máximo de 14 octetos hexadecimales de longitud con dos caracteres ASCII que representen un solo octeto hexadecimal.

## Direccionamiento

DNA IV maneja tanto el reenvío de paquetes de datos de DNA IV como el direccionamiento automático con otros nodos DNA IV. El direccionador realiza las siguientes funciones de DNA IV:

- Anuncia su presencia enviando mensajes hello sobre cada red en que se ha habilitado DNA IV.
- Mantiene una lista de nodos DNA IV adyacentes a partir de los paquetes hello que recibe de otros nodos DNA IV.
- Intercambia información de direccionamiento con otros direccionadores.

- Reenvía paquetes entre los nodos.

Todos los nodos finales y de direccionamiento difunden mensajes hello para la dirección de vertimiento múltiple de todos los direccionadores. Esto permite que cada direccionador ubique los otros nodos de su área.

En cada red de difusión (por ejemplo, Ethernet, Red en Anillo), un direccionador se declara a sí mismo como el direccionador designado para esa línea. El direccionador designado difunde su presencia para que los nodos finales lo reconozcan y lo utilicen como su pasarela por omisión. Cualquier nodo final que va a enviar un paquete a un nodo que no está en esa línea lo envía automáticamente al direccionador designado para el reenvío.

En una red DNA de diversas áreas, asigne prioridades a los direccionadores de manera que el direccionador designado sea un direccionador de nivel 2 o sea probablemente el siguiente salto mejor para los destinos utilizados comúnmente. Esto reduce la posibilidad de que el tráfico de nodos finales tenga que servirse de un salto adicional.

Las decisiones sobre el direccionamiento están basadas en el algoritmo de menor coste. Cada enlace (por ejemplo, punto a punto, red de difusión, salto) tiene un coste. Cada direccionador difunde (sólo a los otros direccionadores) su coste y el número de saltos para llegar a cada nodo de su área. De esta manera, cada direccionador encuentra la vía de acceso de menor coste, sujeta a una cuenta máxima de saltos.

### Tablas de direccionamiento

Un direccionador reenvía cualquier paquete de datos de DNA IV que reciba al nodo apropiado basándose en su tabla de direccionamiento. Para mantener su tabla de direccionamiento, un direccionador escucha y envía actualizaciones de nivel 1 de y hacia cada nodo de su área. Si el tipo del direccionador se establece en AREA, también intercambia actualizaciones del direccionamiento de nivel 2.

Cada direccionador mantiene una tabla de direccionamiento con una entrada para cada nodo (hasta el número máximo de direcciones) y cada siguiente salto posible (todos los circuitos y hasta el número máximo de direccionadores de difusión). Cada entrada de esta tabla contiene el coste y el salto para llegar a un nodo por medio de un circuito o nodo de siguiente salto. La tabla de direccionamiento emite un temporizador del direccionamiento de difusión una vez por segundo.

### Direccionadores de áreas

Si el direccionador se configura como direccionador de áreas, mantiene una base de datos similar para todas las áreas hasta el número máximo de áreas y puede intercambiar información de direccionamiento de áreas con direccionadores de otras áreas. Las áreas se manejan casi igual que los nodos, con la excepción de que los mensajes proporcionan costes para las áreas pero no para los nodos.

El concepto de áreas da como resultado dos tipos de nodos de direccionamiento:

- Un direccionador de nivel 1 sólo tiene información sobre un área, por lo que hace un seguimiento de los nodos de su área. Además, ignora las adyacencias a través de las áreas.

- Un direccionador de nivel 2 mantiene una base de datos de direccionamiento de áreas y puede tener las adyacencias a través de las áreas. Los direccionadores de nivel 2 anuncian rutas hacia todas las otras áreas, por lo que los direccionadores de nivel 1 envían todo el tráfico de áreas exteriores a los direccionadores de nivel 2.

Los nodos finales solamente pasan paquetes a un direccionador.

Un direccionador de nivel 2 que puede alcanzar a otras áreas anuncia una ruta hacia un nodo 0 dentro de su área. Cuando los direccionadores de nivel 1 tienen que enviar un paquete a otra área, lo direccionan hacia el nodo 0 más cercano. Ésta no es necesariamente la mejor ruta hacia esa área. A partir de ahí, el algoritmo de direccionamiento de nivel 2 envía el paquete a su área de destino.

## Configuración de parámetros de direccionamiento

En cada sistema, puede establecer los parámetros de direccionamiento siguientes:

- El número máximo de nodos del área
- El número máximo de direccionadores adyacentes a este direccionador
- El número máximo de redes en cualquier nodo existente
- El número máximo de nodos finales alejados de este nodo final por un salto
- El coste de un salto en cada red a la que está conectado este nodo
- Los valores de varios temporizadores implicados en el envío de mensajes hello y en la acción de esperar estos mensajes de otros nodos

---

## Implementación de DNA IV por parte de IBM

El programa de interfaz de usuario principal para la implementación de DNA IV del direccionador se llama NCP. El NCP del direccionador es un subconjunto limitado de los mandatos del programa DECnet Network Control Program (NCP). El NCP del direccionador le permite ver y modificar los diversos argumentos operativos de DNA IV y leer diversos contadores específicos de DNA.

Las siguientes son algunas de las funciones del NCP del direccionador:

- El NCP implementa nuevas entidades: el módulo de control del acceso y el módulo de filtro de direccionamiento.
- El NCP no tiene el mandato **set executor buffer size** porque el direccionador no origina tráfico de DECnet. El direccionador puede reenviar el paquete más grande que ningún implementador de DECnet puede generar frente a las limitaciones de tamaño de almacenamiento intermedio de todos los nodos adyacentes.
- El NCP permite el calificador **all** en los submandatos **node**, **area** y **circuit**.

El NCP del direccionador es similar al programa NCP proporcionado por DECnet-VAX, con las diferencias siguientes:

- El NCP del direccionador no incluye el mandato **set node name**, por lo que no puede asignar nombres a nodos ni visualizar nombres de nodos con las direcciones.

- El NCP del direccionador no incluye los mandatos **clear** o **purge** ni permite que los mandatos **set** tengan el argumento **all**. La base de datos permanente siempre se copia en la base de datos volátil cuando el direccionador se inicia, se reinicia o se arranca.
- Un mandato del NCP del direccionador sólo puede tener un argumento.
- El NCP no tiene el concepto de líneas. Para ver los datos que visualiza el mandato del programa DECnet-VAX NCP **show line**, utilice los mandatos de GWCON **interface** y **network**.
- El NCP del direccionador no da soporte a mandatos de paso a través de redes:
  - El NCP del direccionador no incluye el mandato **tell**, que solicita mandatos del NCP a otros nodos.
  - De manera similar, el NCP del direccionador no da soporte a las peticiones de protocolo de los otros direccionadores de DNA consistentes en que, de parte de éstos, se ejecuten mandatos del NCP en el direccionador.

### Importante

Antes de configurar DNA IV, ha de tener conocimiento de las funciones de seguridad opcionales tratadas en:

- “Gestión del tráfico mediante el control del acceso”
  - Proporciona seguridad adicional limitando el acceso dentro de los direccionadores de la red.
- “Gestión del tráfico mediante filtros de direccionamiento de áreas” en la página 342
  - Limita el acceso a un grupo de áreas por parte de las otras áreas
  - Permite la combinación de dos espacios de direcciones DECnet

Si ya está familiarizado con estos temas, sáltese estas dos secciones y siga en “Configuración de DNA IV” en la página 346.

## Gestión del tráfico mediante el control del acceso

El control del acceso protege un grupo de nodos de los otros nodos de la red. Los direccionadores permiten que todos los nodos de una red sean accesibles entre sí. Normalmente, las principales formas de seguridad son contraseñas y el uso conservador del acceso de tipo proxy de DNA IV en el nivel de sistema principal.

No obstante, debido a diferencias existentes respecto al nivel de seguridad de las máquinas, es posible que tenga que proporcionar seguridad adicional limitando el acceso dentro de los direccionadores de la red. La función de reenvío de DNA le permite hacerlo utilizando controles del acceso.

En general, los controles del acceso no son recomendables por las desventajas siguientes:

- Los controles del acceso afectan al rendimiento del direccionamiento porque se comprueba cada paquete. Cuanto más compleja es la configuración de los controles del acceso, mayor es su efecto en el rendimiento.

- Los controles del acceso son difíciles de configurar y los errores en la configuración son difíciles de diagnosticar.
- Los controles del acceso no pueden ocultar un nodo de los protocolos de direccionamiento. El nodo permanece visible en todos los direccionadores de su área.

**Nota:** Los controles del acceso no garantizan la seguridad; sólo dificultan las intromisiones. Los protocolos de direccionamiento DNA IV utilizados en Ethernet y otros medios de difusión no tienen incorporadas funciones de seguridad.

El control del acceso evita el reenvío de paquetes de datos (formato largo) de DNA IV tomando como base la dirección de origen, la dirección de destino y la interfaz. El control del acceso no afecta a los paquetes de direccionamiento porque utilizan un formato de paquete diferente. Esto da una mayor seguridad a la configuración del control del acceso, ya que no se puede interrumpir el protocolo de direccionamiento.

Para implementar el control del acceso, se efectúan máscaras de direcciones y comparaciones relativas a éstas. Es decir, se efectúa una máscara de la dirección en cuestión con números 1 en las posiciones de bit para la prueba y números 0 en el área libre. A continuación, la dirección se compara con un valor fijo. Por ejemplo, se puede utilizar una máscara de 63.1023 (todo números 1) y compararla con un resultado de 6.23, que sólo podrá ser verdadero para el nodo 6.23. Puede utilizar una máscara de 63.0 y un resultado de 9.0, que será verdadero para cualquier nodo del área 9.

Estos valores de máscara y comparación vienen en pares para la dirección de origen y la de destino. Forman, entonces, listas de interfaz. Cada interfaz sólo puede tener una lista de control del acceso, que se aplica a los paquetes recibidos en esa interfaz. Esta lista puede ser inclusiva o exclusiva. Una lista inclusiva es un conjunto de pares de direcciones que designa un corredor para el flujo de tráfico. Una lista exclusiva es un conjunto de pares de direcciones que no permite flujo de tráfico.

En una lista inclusiva, la dirección de origen y la de destino se comprueban utilizando los valores de máscara y comparación. Si coinciden el origen y el destino de una entrada cualquiera, se reenvía el paquete. En una lista exclusiva, la dirección de origen y la de destino se comprueban utilizando los valores de máscara y comparación. Si coinciden el origen y el destino de una entrada cualquiera, se elimina el paquete. La elección entre exclusiva e inclusiva debe hacerse basándose en qué lista será más corta. No obstante, el control del acceso exclusivo es, normalmente, más fácil de configurar.

Cuando se eliminan paquetes debido a los controles del acceso, se establece el bit de petición de devolución a emisor (RQR) en la cabecera de paquete de datos de formato largo y se devuelve el paquete. A continuación, la petición de conexión falla inmediatamente porque normalmente los paquetes de inicio de conexión de NSP se envían con el bit RQR establecido.

### Configuración del control del acceso

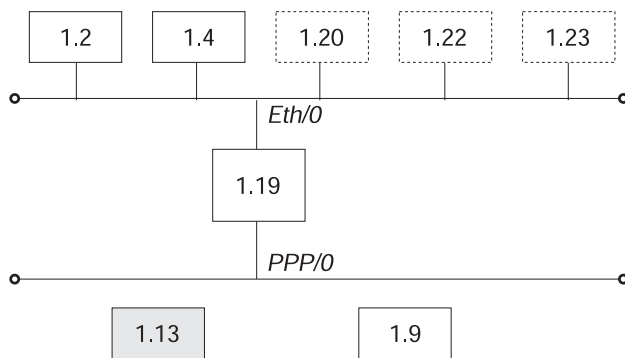
El control del acceso limita el acceso a un sistema principal o grupo de sistemas principales en particular. Debe asignar el control del acceso a todas las rutas hacia este sistema principal, no únicamente a la ruta preferente. De lo contrario, el control del acceso funciona cuando está activa la ruta primaria, pero falla cuando se utiliza la ruta secundaria.

En el mapa de la red, trace una línea para aislar la región segura del resto de la red. Lo ideal es que la línea pase por el conjunto mínimo de adyacencias posible para que haya el número menor de interfaces en ejecución con el control del acceso. Para las redes de difusión (Ethernet y Red en Anillo), trace la línea por el cable de interconexión hacia el nodo para identificar la interfaz a filtrar. Para cada interfaz por la que pase la línea del control del acceso, utilice el NCP con el fin de definir la misma lista de control del acceso.

**Nota:** Puesto que todas las aplicaciones DECnet utilizan el protocolo NSP, que requiere conectividad bidireccional, no es necesario definir controles del acceso en ambas direcciones.

### Control del acceso inclusivo

En la Figura 15, el nodo 1.13 desea comunicarse con los nodos 1.2 y 1.4 únicamente. El control del acceso le permite proteger nodos de todos los nodos conectados por direccionadores. Por lo tanto, en la Figura 15 puede proteger el nodo 1.13 de todos los nodos a excepción del nodo 1.9 porque estos dos nodos comparten la misma red física. Si desea configurar el control del acceso correspondiente a este ejemplo, cree un filtro inclusivo para la interfaz Eth/0 del direccionador 1.19 tal como se muestra en la parte inferior de la Figura 15



Información de filtro inclusivo

Resultado origen	Máscara origen	Resultado destino	Máscara destino
1.2	63.1023	1.13	63.1023
1.4	63.1023	1.13	63.1023
0.0	0.0	1.9	63.1023

Figura 15. Ejemplo del control del acceso inclusivo

Las entradas primera y segunda de la información de filtro inclusivo mostrada en la Figura 15 permiten que los nodos 1.2 y 1.4 envíen paquetes al nodo 1.13. La

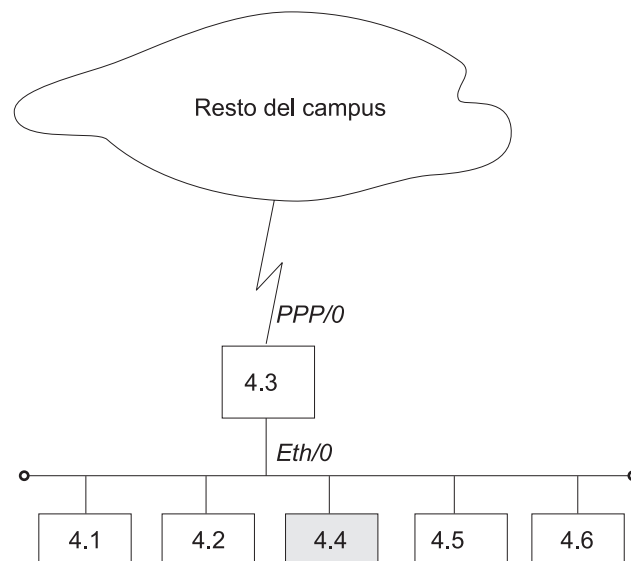
tercera entrada permite que cualquier nodo realice envíos para el nodo 1.9 (no se intenta proteger el nodo 1.9).

Si desea configurar el ejemplo proporcionado para el direccionador 1.19, entre los siguientes mandatos y parámetros del NCP:

```
NCP> def mod access-cont circ eth/0 type inclusive
NCP> def mod access-cont circ eth/0 filter 1.2 63.1023 1.13 63.1023
NCP> def mod access-cont circ eth/0 filter 1.4 63.1023 1.13 63.1023
NCP> def mod access-cont circ eth/0 filter 0.0 0.0 1.9 63.1023
NCP> def mod access-cont circ eth/0 state on
```

### Control del acceso exclusivo

La Figura 16 muestra la manera en que el control del acceso exclusivo aísla el nodo 4.4 del resto del campus.



Información de filtro exclusivo

Resultado origen	Máscara origen	Resultado destino	Máscara destino
0.0	0.0	4.4	63.1023

Figura 16. Ejemplo del control del acceso exclusivo

Configure el control del acceso correspondiente a este ejemplo creando un filtro exclusivo para la interfaz PPP/0 del direccionador 4.3 tal como se muestra en la Figura 16. Si desea configurar el ejemplo proporcionado para el direccionador 4.3 de la Figura 16, entre los siguientes mandatos y parámetros del NCP:

```
NCP> def mod access-cont circ ppp/0 type exclusive
NCP> def mod access-cont circ ppp/0 filter 0.0 0.0 4.4 63.1023
NCP> def mod access-cont circ ppp/0 state on
```

### Gestión del tráfico mediante filtros de direccionamiento de áreas

Los filtros de direccionamiento de áreas permiten configuraciones especiales de la red DNA. Puesto que se trata de un tema avanzado, muy pocas redes DNA IV necesitan filtros de direccionamiento. Existen dos aplicaciones primarias de la filtración de áreas en DNA IV:

- Seguridad, que limita el acceso a un grupo de áreas por parte de las otras áreas.
- Permitir la combinación de dos espacios de direcciones DECnet.

**Nota:** La configuración de los filtros de direccionamiento de áreas es muy difícil y sutil. Es muy fácil interrumpir completamente el direccionamiento de áreas. Si no comprende cómo funciona el direccionamiento de DECnet, especialmente en el nivel de área, no intente utilizar filtros de direccionamiento. Puede encontrar documentación sobre el protocolo de direccionamiento DECnet en la publicación *DECnet Digital Network Architecture Phase-IV Routing Layer Functional Description*, Número de pedido AAX435ATK, December 1983, Digital Equipment Corporation, Maynard, Massachusetts.

Los filtros de direccionamiento de áreas le permiten configurar un direccionador de manera que controle la información sobre las áreas DECnet a las que se envían mensajes de direccionamiento de nivel 2 o de las que se aceptan estos mensajes. Puede configurar filtros de entrada y salida por separado para cada interfaz. Cada filtro especifica a qué áreas se pasará información de direccionamiento o de qué áreas se aceptará esta información.

Cuando una red envía una actualización del direccionamiento de nivel 2 y hay un filtro de direccionamiento, la entrada (RTGINFO) de cualquier área que no esté en el filtro tiene el coste de 1023 y una cuenta de saltos de 63. Se colocan el coste y los saltos correctos en la entrada de cualquier área del filtro.

Cuando la red recibe un mensaje de direccionamiento de nivel 2 y hay un filtro de direccionamiento, cualquier entrada de un área que no esté en el filtro se trata como si el coste fuera de 1023 y la cuenta de saltos de 63 (inasequible). Cualquier entrada de direccionamiento del paquete que esté en el filtro se procesa normalmente.

Los filtros de direccionamiento sólo afectan al proceso de los mensajes de direccionamiento de nivel 2. No existen filtros para mensajes de direccionamiento de nivel 1. Los filtros de direccionamiento no tienen ningún efecto sobre el proceso de hello del direccionador y no evitan que los direccionadores de áreas desarrollen adyacencias. Afectan a la base de datos de direccionamiento de áreas. Si los filtros evitan que un direccionador de áreas aprenda información sobre otra área, impedirán que éste se conecte y entonces el direccionador no podrá anunciarse como direccionador de áreas.

#### Seguridad mediante la filtración de áreas

Al igual que los controles del acceso, los filtros de direccionamiento proporcionan seguridad. No obstante, los filtros de direccionamiento tienen algunas desventajas en comparación con los controles del acceso:

- La filtración de áreas es menos flexible que los controles del acceso porque requiere que la asignación de las áreas se corresponda con la arquitectura de seguridad adecuada.



- La filtración de áreas es más difícil de comprender y de configurar.
- El nivel de seguridad es inferior porque un sistema principal que ignore la ausencia de información de direccionamiento puede enviar los paquetes al direccionador correcto de todas maneras.

No obstante, la filtración de áreas es más eficaz porque no hay necesidad de comprobar cada paquete. En el ejemplo siguiente, se produce la filtración de áreas en un área que contiene estaciones de trabajo que forman parte de una red grande que contiene máquinas con información confidencial. Puede haber una máquina fuera del área a la que las máquinas confidenciales tengan que acceder para obtener información.

En la Figura 17, el área 13 contiene estaciones de trabajo que tienen que ser capaces de acceder al área 7. El nodo 13.1 es el direccionador y los otros nodos son las estaciones de trabajo. El nodo 13.1 tiene un filtro para aceptar cualquier ruta hacia el área 7. Por lo tanto, si el nodo 13.1 recibe un paquete de cualquier nodo del área 13 que no está destinado al área 7, el nodo 13.1 no puede reenviar el paquete y envía un mensaje de error al nodo emisor.

Para configurar el direccionador 13.1 de la Figura 17, entre los siguientes mandatos y parámetros del NCP:

```
NCP> def mod routing-filter circ eth/1 incoming area 7
NCP> def mod routing-filter circ eth/1 incoming state on
```

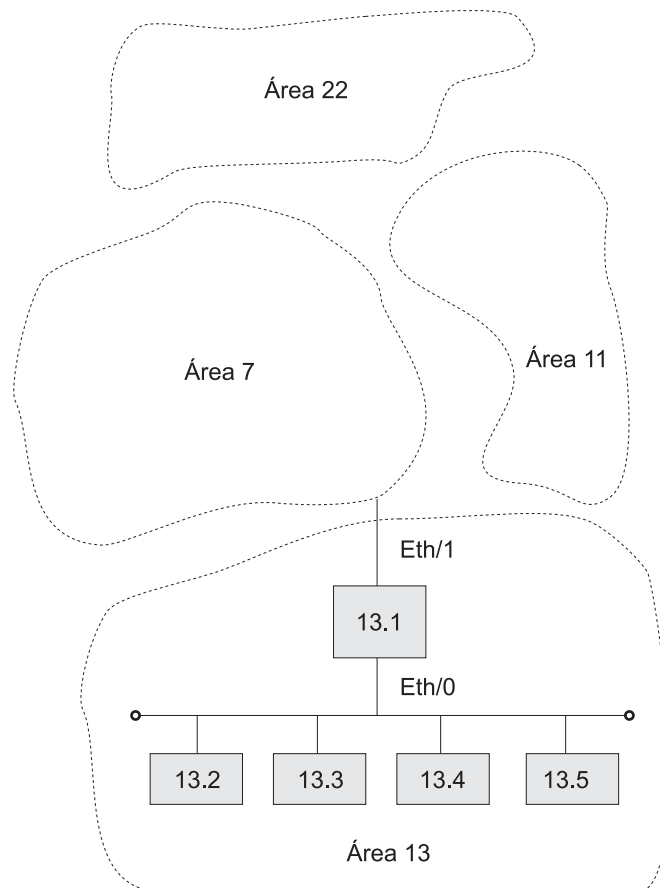


Figura 17. Ejemplo del filtro de direccionamiento de áreas para la seguridad

### Combinación de dominios DECnet

DECnet tiene un espacio de direcciones de nodo de 16 bits con una jerarquía fija de 6 bits de área y 10 bits de nodo. Por comparación, IP tiene un espacio de direcciones de nodo de 32 bits con una jerarquía flexible de diversos niveles.

Actualmente, muchas redes establecidas se han desarrollado hasta el punto de utilizar las 63 áreas. El problema es que, cuando diferentes recursos se conectan entre sí, quieren conectar sus redes DECnet, pero no pueden debido a conflictos con el número de área.

La única solución es volver a diseñar la arquitectura DECnet. (Esto está dirigido por DECnet Phase V.) No obstante, utilizando filtros de direccionamiento de áreas, es posible permitir que se solapen dos dominios DECnet.

Dominio no es un término estándar de DECnet; aquí se utiliza como nombre para una red de área amplia DECnet, presumiblemente una con muchas áreas. El propósito es combinar dos de estos dominios para que haya un área común que pueda alcanzar a partes de ambos dominios. No obstante, hay más de 63 áreas en la unión de los dos dominios. Puesto que la filtración de áreas no es fácil de administrar y es restrictiva, no debe tomar en consideración su uso si hay suficientes números de área disponibles para la unión de los dominios.

Para llevar a cabo la configuración que permita solapar dos dominios, primero debe decidir con qué áreas va a efectuar la intersección. Estas áreas son las que podrán participar de ambos dominios. Estos números de área no deben utilizarse en ninguna otra parte de los dos dominios.

La Figura 18 en la página 346 muestra que las áreas de la intersección son las áreas 1 y 2. El resto de las áreas pueden estar duplicadas entre los dos dominios. En el ejemplo, hay dos áreas 3, 4 y 5, una en cada dominio. Tenga en cuenta que nunca es posible permitir una conexión directa entre un nodo del área 3 del dominio A y el área 3 del dominio B. Lo mejor que puede hacer es proporcionar a las áreas de la intersección la posibilidad de comunicarse con partes de cada dominio.

Al diseñar la intersección, tenga cuidado con que ningún dominio se apoye en rutas a través de la intersección para mantener la conectividad entre las áreas que no están en la intersección. Puesto que se filtran las rutas que están dentro y fuera de la intersección, probablemente no ofrecen una asequibilidad normal entre todas las áreas del dominio.

Para decidir cómo configurar los filtros de direccionamiento, trace un mapa preciso de la configuración. En este mapa, ubique todas las áreas y profile los dos dominios. A continuación, decida cuál es la barrera de la filtración que tiene que establecer. Con cuidado, rodee la intersección de los dos dominios y localice todas las adyacencias de nivel 2 que atraviesen la barrera de la filtración. Éstas son las vías de acceso de comunicaciones de un salto entre direccionadores de nivel 2 que combinan áreas.

En el ejemplo, hay seis adyacencias que atraviesan la barrera, del 1.18 al 5.7, del 1.18 al 5.8, del 1.18 al 8.3, del 2.17 al 3.12, del 2.21 al 4.7 y del 2.21 al 4.9.

El primer paso para diseñar los filtros de áreas es configurar filtros que impidan que las áreas de un dominio se propaguen en el otro dominio. Las únicas rutas de área que deben dejar la intersección son las de las áreas de la intersección. En el

ejemplo, éstas son las áreas 1 y 2. Por lo tanto, deben enviarse solamente rutas de las áreas 1 y 2 desde nodos tales como el 2.17 y el 3.12.

En enlaces punto a punto como, por ejemplo, el 2.17 y el 3.12, no importa qué extremo filtre, pero probablemente es más seguro filtrar en el extremo emisor. Por lo tanto, habrá un filtro en la interfaz del 2.17 que permitirá reenviar solamente las rutas de las áreas 1 y 2. Lo mismo ocurrirá en las dos interfaces del 2.21 y en el enlace del 1.18 con el 8.3.

Cuando el salto entre dos áreas es Ethernet u otro medio de difusión, como, por ejemplo, del 1.18 al 5.7 y al 5.8, debe tomar la decisión sobre otra base. La mayoría de las redes Ethernet tienen la mayoría de los nodos de direccionamiento de nivel 2 en un área, y unos cuantos en la segunda área. Aquí, la filtración debe realizarse en los que son unos cuantos antes que en los muchos. El ejemplo indica que el nodo 1.18 es el intruso en la red Ethernet del área 5, por lo que debe ser el que filtre.. El nodo 1.18 sólo enviará direccionadores de las áreas 1 y 2 en la red Ethernet.

Puede filtrar en ambos extremos de una adyacencia. Esto añade una capa adicional de seguridad contra una reconfiguración accidental. No obstante, si sólo configura un extremo para la filtración, sólo filtra este extremo.

Una vez facilitados estos filtros, los dos dominios no pueden interferirse entre sí. No obstante, para un nodo de la intersección no está claro a qué área 3 se accederá cuando se intente una conexión con el nodo 3.4. Depende de los costes de la ruta actual y del circuito. Por supuesto, esto no es lo ideal. No importa que sólo pueda haber un nodo 3.4 en el dominio A y no en el dominio B. El direccionamiento entre las áreas se lleva a cabo solamente sobre la base de las áreas; sólo los direccionadores que están dentro de un área conocen las rutas hacia los nodos de esa área.

Por consiguiente, debe establecer un segundo conjunto de filtros para decidir qué instancia de un área (dominio A o B) es asequible desde la intersección para cada área que no está en la intersección. Por lo tanto, podrá decidir que los nodos de la intersección puedan alcanzar a las áreas 3 y 4 del dominio A y al área 5 del dominio B. En el ejemplo, esto se hará configurando los direccionadores 1.18 y 2.21 de manera que sólo acepten rutas hacia las áreas 3, 4, 6 y 8 del dominio A. Los direccionadores 2.17 y 2.21 sólo aceptarán rutas hacia las áreas 5 y 9 del dominio B.

Por lo tanto, los nodos de la intersección ven un universo que contiene las áreas 1 y 2 de la intersección, las áreas 3, 4, 6 y 8 del dominio A y las áreas 5 y 9 del dominio B.

Para configurar el direccionador 1.18 de la Figura 18 en la página 346, entre los siguientes mandatos y parámetros del NCP:

```
NCP> def mod routing-filter circ eth/0 outgoing area 1,2
NCP> def mod routing-filter circ eth/0 outgoing state on
NCP> def mod routing-filter circ eth/0 incoming area 3,4,6,8
NCP> def mod routing-filter circ eth/0 incoming state on
NCP> def mod routing-filter circ ppp/0 outgoing area 1,2
NCP> def mod routing-filter circ ppp/0 outgoing state on
NCP> def mod routing-filter circ ppp/0 incoming area 3,4,6,8
NCP> def mod routing-filter circ ppp/0 incoming state on
```

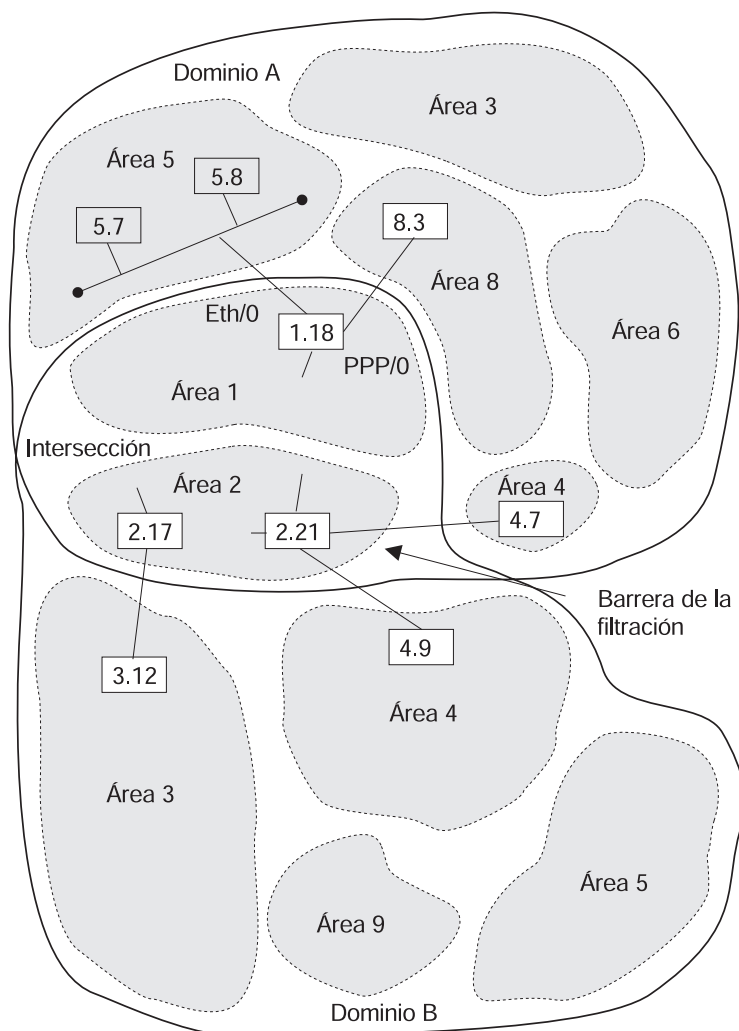


Figura 18. Ejemplo de la combinación de dominios DECnet

Todavía no existe la manera de que un nodo del área 5 del dominio A pueda comunicarse directamente con un nodo del área 5 del dominio B. Para que los nodos de estas dos áreas se comuniquen, debe realizar una serie de retransmisiones relay de nivel de aplicación utilizando el mandato **set host**. Por ejemplo:

- Ejecute el mandato **set host** para que, desde un nodo del área 5 del dominio A, se inicie remotamente la sesión de un nodo del área 8 del dominio A.
- Ejecute el mandato **set host** para que, desde un nodo del área 8 del dominio A, se inicie remotamente la sesión de un nodo del área 1 ó 2.
- Ejecute el mandato **set host** para que, desde un nodo del área 1 ó 2, se inicie remotamente la sesión de un nodo del área 5 del dominio B.

## Configuración de DNA IV

El protocolo DNA IV se ejecuta sobre las interfaces Red en Anillo, Frame Relay, Ethernet, PPP, clientes de emulación de LAN de ATM Red en Anillo, clientes de emulación de LAN Ethernet y X.25. Las secciones siguientes describen los procedimientos para configurar el protocolo DNA IV de manera que funcione sobre las interfaces Red en Anillo, FDDI y X.25.

**Nota:** Cuando trabaje con redes mixtas de DNA IV y DNA V, debe efectuar toda la configuración y supervisión de DNA IV siguiendo el proceso descrito en este capítulo.

### Consideraciones sobre los algoritmos de DNA IV y DNA V

DNA IV utiliza un algoritmo de direccionamiento de vector de distancia. DNA V puede utilizar un algoritmo de direccionamiento de vector de distancia o un algoritmo de direccionamiento de estado de enlace. El direccionador con función de puente seleccionará el algoritmo según los protocolos que se habiliten y se inhabiliten y cualquier combinación que pueda resultar de estos dos protocolos. Vea la Tabla 105 para obtener información detallada.

Tabla 105. Consideraciones sobre los algoritmos de DNA IV y DNA V

Estado de DECnet IV	Estado de OSI/DNA V	Algoritmo seleccionado
Habilitado	Inhabilitado	Vector de distancia (automáticamente)
Inhabilitado	Habilitado	Estado de enlace (automáticamente)
Habilitado	Habilitado	Utilice el mandato <b>set algorithm</b> para configurar esta información en la SRAM.

### Configuración de DNA IV para Red en Anillo

El procedimiento para ejecutar el protocolo DNA IV sobre Red en Anillo (TR) 802.5 incluye mandatos de los procesos de configuración de DNA IV y Red en Anillo.

- Desde el indicador de OPCON (\*), entre en el proceso de configuración.

```
* talk 6
Config>
```

- Entre **list device** para ver los números de interfaz de las interfaces Red en Anillo. Anote el número de interfaz de cada interfaz Red en Anillo.

```
Config> list device
```

- Utilice el mandato **network** con el número de interfaz de la interfaz Red en Anillo que desea configurar. Esto le colocará en el proceso de configuración de Red en Anillo.

```
Config> network 0
TKR config>
```

- Utilice el mandato **list** para verificar la información sobre la configuración de Red en Anillo.

```
TKR config> list
```

```
Token-Ring configuration:
```

```
Packet size (INFO field): 2052
Speed: 4 Mb/sec
Media: Shielded
```

```
RIF Aging Timer: 120
Source Routing: Enabled
Mac Address 000000000000
```

- Salga del proceso de configuración de Red en Anillo y entre en el proceso de configuración de DNA del NCP.

```
TKR config> exit
Config> protocol DN
NCP>
```

6. Utilice el mandato **define** para definir un circuito DNA sobre la interfaz Red en Anillo:

```
NCP> define circuit tkr/0 state on
```

7. Opcionalmente, utilice el mandato **define** para establecer el tipo de direccionamiento del circuito. Para el soporte de Phase IV o el bilingüe, tiene que cambiar el tipo de direccionamiento por omisión (estándar) por el AMA o el bilingüe.

```
NCP> define circuit tkr/0 router type bilingual
```

o-

```
NCP> define circuit tkr/0 router type AMA
```

8. Utilice el mandato **list** para comprobar los parámetros.

```
NCP> list circuit tkr/0 characteristics
Circuit Permanent Characteristics
Circuit           = TKR/0
State             = On
Cost              = 4
Router priority   = 64
Hello timer       = 15
Max routers       = 16
Router type       = Standard
```

9. Reinicie el direccionador para que sean efectivos todos los parámetros configurados.

**Nota:** Si desea inhabilitar el direccionamiento de origen o establecer el temporizador de RIF en un valor distinto del valor por omisión, utilice el mandato **source-routing** y el mandato **set RIF-timer** en el proceso de configuración de Red en Anillo.

### Configuración de DNA IV para X.25

El procedimiento para ejecutar el protocolo DNA IV sobre circuitos X.25 incluye mandatos de los procesos de configuración de X.25 y DNA IV.

1. Desde el indicador de OPCODE (\*), entre en el proceso de configuración. Vaya a "t 6" y entre en X.25 config (net núm.). Si es la primera vez que va a configurar X.25, realice las siguientes acciones:

- a. DEFINA la dirección de DTE del direccionador.

```
X.25 Config> set address
```

- b. DEFINA cada protocolo que estará soportado sobre X.25:

```
X.25 Config> add protocol
```

**IP** Normalmente, es una buena idea añadir este protocolo para que pueda verificar si la configuración general de X.25 es correcta

#### DN

Nota: Deje que los parámetros de protocolo tomen el valor por omisión.

- c. DEFINA la correlación de dirección remota de protocolo con dirección X.25 remota para los protocolos que lo requieran:

```
X.25 Config> add address
```

para IP:

- Dirección IP = 128.185.247.22
- Dirección X.25 = 22

para DN:

- Dirección DN = 5.22
- Dirección X.25 = 22

- d. VERIFIQUE si un extremo del circuito X.25 es un DTE y el otro extremo es un DCE.

```
X.25 Config> list all
```

Compruebe el campo de personalidad nacional para ver el tipo de dispositivo. Para el tipo de personalidad nacional GTE-Telenet, podrá ver:

```
National Personality: GTE Telenet (DTE)
```

```
-0-
```

```
National Personality: GTE Telenet (DCE)
```

Para cambiar el tipo de dispositivo por DCE, entre:

```
X.25 Config> set equipment-type dce
```

Lista todos los parámetros configurados para X.25

```
National Personality: GTE Telenet (DTE) National Personality: GTE Telenet (DCE)
```

De lo contrario, elija un direccionador para que actúe como DCE y modifíquelo como tal,

```
X.25 Config> set national-personality dce
```

- e. REINICIE el direccionador para que sean efectivos todos los parámetros configurados.

- f. Para VERIFICAR si la configuración es válida después de un reinicio, vaya a la parte del supervisor y observe si el enlace se está activando.

```
* t 5
+ c
```

Esto le proporciona el estado del enlace en ese momento. Si ve que el estado del enlace X.25 pasa de “prueba” a “inactivo”, vaya a los mensajes del ELS y compruebe si hay un error obvio. Si el estado del enlace X.25 pasa de “prueba” a “activo”, es probable que la configuración de x.25 sea válida.

2. Para VERIFICAR si el enlace X.25 es operativo:

- a. INTENTE realizar una acción de PING con cada extremo del enlace X.25 desde el supervisor de IP:

```
IP> interface
```

Verifique si se habían configurado las direcciones X.25 correctas en el protocolo IP.

```
IP> ping dirección IP del enlace X.25 remoto
```

3. Para CONFIGURAR DECnet PhaseIV en el direccionador:

- a. DEFINA los parámetros de ejecutor de DECnet:

```
NCP> define exec address área.nodo La dirección DECnet del direccionador
```

```
NCP> define exec type DEC-ROUTING-IV Configura el direccionador como direccionador de tipo DEC de NIVEL 1
```

**Nota:** Este ejemplo es para configurar un direccionador de

manera que interactúe con otros direccionadores con soporte para el direccionamiento de DEC estándar sobre redes X.25. Un direccionador que dé soporte al estándar debe estar definido como de tipo DEC-ROUTING-IV (nivel 1) o DEC-AREA (nivel 2). El tipo de direccionamiento por omisión es ROUTING-IV, y AREA permite la interoperación con muchos IBM 2216 existentes y otros direccionadores compatibles.

```
NCP> define exec state on
```

Reinicie el direccionador para que, cuando configure el circuito X.25, sean visibles todos los parámetros específicos de DEC. Para verificar la configuración del ejecutor, NCP> **show executor characteristics**

b. DEFINA circuitos PhaseIV X.25.

Debe configurar el circuito X.25 como PVC o SVC. Si este circuito se configura como PVC, el otro extremo también debe ser un PVC. Si este circuito se configura como SVC de entrada, el otro extremo debe configurarse como SVC de salida

```
NCP> define cir x25/0 usage IN-SVC  
NCP> define cir x25/0 DTE-address "DTE X.25 remoto"  
NCP> define cir x25/0 call-data  
NCP> define cir x25/0 verification enabled
```

Habilitar la verificación es opcional.

c. DEFINA circuitos para el estado activo:

- para Red en Anillo

```
NCP> define cir TKR/0 router type bilingual
```

- para TODOS los circuitos

```
NCP> define cir xxx state on
```

Reinicie el direccionador para que sean efectivos todos los parámetros de DECnet, VERIFIQUE si la configuración de X.25 dentro del protocolo DECnet es la que desea.

```
NCP> list circuit x25/0 characteristics
```



## Configuración y supervisión de DNA IV

### Mandatos de configuración y supervisión de DNA IV

Este apartado describe los mandatos de configuración y supervisión del NCP. Entre los mandatos en el indicador NCP>. Puede accederse a **todos** los mandatos del NCP desde el entorno de configuración o desde el entorno de supervisión.

Tabla 106. Mandatos de configuración y supervisión del NCP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxxi.
define	Define elementos en la base de datos no volátil (permanente), incluidos: <ul style="list-style-type: none"> <li>• Listas de control del acceso y filtros de direccionamiento</li> <li>• Elementos de circuito</li> <li>• Argumentos globales para DNA</li> <li>• Datos de configuración de los nodos</li> </ul>
purge module	Elimina listas de control del acceso y filtros de direccionamiento de la base de datos permanente.
set	Establece o cambia elementos de la base de datos volátil, incluidos: <ul style="list-style-type: none"> <li>• Elementos de circuito</li> <li>• Argumentos globales para DNA</li> <li>• Datos de configuración de los nodos</li> </ul>
show	Visualiza el estado de la base de datos volátil y los nodos volátiles de la base de datos de direccionamiento.
show/list	Visualiza los elementos de la base de datos volátil (show) o permanente (list), incluidos: <ul style="list-style-type: none"> <li>• El estado actual de los circuitos especificados</li> <li>• El estado actual de la base de datos volátil/permanente para DNA</li> <li>• Las listas de control del acceso de DECnet que se han definido en la base de datos permanente para el direccionador</li> <li>• Los filtros de direccionamiento de áreas de DECnet que se han definido en la base de datos permanente para el direccionador</li> </ul>
zero	Borra los contadores de circuitos de la base de datos volátil, los contadores globales de la base de datos volátil y los contadores del módulo de lista de control del acceso. <b>No borra los valores de los argumentos establecidos con los mandatos <b>set</b> o <b>define</b>.</b>
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxi.

### Tenga en cuenta la información siguiente sobre los mandatos:

1. Los mandatos **define** no son efectivos hasta la próxima vez que se reinicia el direccionador.
2. Los mandatos **list**, **define** y **purge** modifican o visualizan datos de la base de datos permanente (la RAM estática del direccionador). La base de datos permanente se almacena en la configuración y permanece efectiva durante los reinicios, las cargas de software y los ciclos de la alimentación.
3. Los mandatos **show** y **list** son los más útiles para supervisar el protocolo DNA IV.
4. Utilice **set**, **show** y **zero** para modificar, visualizar o borrar datos de la base de datos volátil.
5. El mandato **zero** borra las estadísticas guardadas en la base de datos volátil, pero **no** borra los valores de los argumentos establecidos con los mandatos **set** o **define**.

## Define/Set

Esta sección explica los mandatos **define** y **set**.

Utilice el mandato **define** para definir listas de control del acceso y filtros de direccionamiento así como para definir los parámetros de circuito, ejecutor y nodo. **Define** se utiliza para establecer la SRAM (necesita rearranque).

### Sintaxis:

```
define          especificador-circuito . . .  
                ejecutor . . .  
                module access-control . . .  
                module routing-filter . . .  
                node . . .
```

**Set** puede utilizarse para la RAM volátil (cambio inmediato sin rearranque).

### Sintaxis:

```
set            especificador-circuito . . .  
                ejecutor . . .  
                node . . .
```

**especificador-circuito** *argumento*

Las opciones para *especificador-circuito* son las siguientes:

#### **active circuits**

Especifica todos los circuitos que están activos y cuyo estado es el de activado (sólo set).

#### **all circuits**

Especifica todos los circuitos del direccionador.

### **circuit name**

El nombre del circuito. Por ejemplo: Eth/0, TKR/0, PPP/1.

### **known circuits**

(sólo **set**) Especifica todos los circuitos del direccionador.

Los *argumentos* son los siguientes:

### **call-userdata**

Utilizado durante la inicialización de circuito de los circuitos X.25 estáticos. Si se define un circuito como SVC de salida, la petición de llamada inicial y todas las subsiguientes contienen los datosusuario-llamada definidos cuando se habilita el circuito. Cuando se define un circuito como SVC de entrada, uno de los criterios a la hora de aceptar una petición de llamada para entrada es una coincidencia con los datosusuario-llamada definidos.

Actualmente los datosusuario-llamada deben establecerse en el DTE del direccionador local tanto para el SVC de entrada como para el de salida.

Entre un número par de caracteres (octetos) hexadecimales hasta un máximo de 14 caracteres.

### **cost [rango]**

Establece el coste de la recepción de un paquete en este circuito. El algoritmo de direccionamiento lo utiliza para determinar el coste de un circuito al elegir rutas (el coste no es lo mismo que una métrica de IP). Rango: del 1 al 25. Valor por omisión: 4.

Los valores siguientes son puntos de partida que se sugieren:

<i>Tipo de circuito</i>	<i>Coste</i>
Ethernet	4
Red en Anillo 4/16	4
FDDI	4
Síncrono 56 Kb	6
Síncrono T1	5
X.25	25

### **Ejemplo:**

```
define circuit tkr/0 cost 5
```

### **DTE Address**

Especifica la dirección del DTE remoto en el circuito X.25. Ésta siempre es la dirección del sistema remoto. Es un número de tipo decimal hasta un máximo de 14 caracteres.

### **hello timer [rango]**

Especifica la frecuencia (en segundos) con la que se envían mensajes hello del direccionador en este circuito. Rango: de 1 a 8191 segundos. Valor por omisión: 15 segundos (recomendable).

### maximum recalls

(sólo **define**) Especifica cuántos intentos realiza el direccionador para restablecer una llamada relacionada con un SVC estático de salida después de una anomalía de una llamada inicial. Después del número máximo de llamadas, el direccionador no realiza más intentos para establecer el SVC sin la intervención del usuario. Los valores válidos se encuentran en el rango del 1 al 20, y el valor por omisión es 1. Véase también el argumento recall timer.

### maximum routers [rango]

(sólo **define**) Especifica cuántos direccionadores más puede haber en este circuito. Rango: del 1 al 33. Valor por omisión: 16.

**Nota:** El usuario no puede configurar este parámetro en un circuito X.25 cuando el *tipo* de ejecutor está establecido en DEC-routing-IV o DEC-area. En este caso, el número máximo de direccionadores es 1.

Si es un direccionador de nivel 1, sólo cuentan los direccionadores de este circuito de la misma área. Si es un direccionador de nivel 2, cuentan todos los direccionadores de este circuito. El direccionador no cuenta en el límite.

Los requisitos de eficacia y memoria del direccionador mejoran si se establece un número bajo. Establezca este argumento en un valor que supere el número total de direccionadores adyacentes del circuito. No establezca este argumento en un valor inferior al número de direccionadores del circuito; esto puede dar como resultado anomalías de direccionamiento.

**Nota:** Para un circuito punto a punto (línea síncrona), establezca este argumento en 1. El resultado es un ahorro de memoria significativo en un direccionador con diversas líneas punto a punto.

La suma del número máximo de direccionadores a partir de todos los circuitos debería ser inferior al argumento de ejecutor relativo al número máximo de direccionadores de difusión, aunque este límite no es necesariamente obligatorio.

### recall timer

Determina el retardo en segundos entre los intentos de llamada para establecer un circuito estático de salida X.25.

Para **define**, los valores válidos se encuentran en el rango de 1 a 60 segundos. El valor por omisión es de 1 segundo. Véase también el argumento maximum recalls.

Para **set**, los valores válidos se encuentran en el rango de 0 a 65595 segundos. El valor por omisión es de 60 segundos.

### router priority [rango]

Especifica la prioridad del direccionador a la hora de solicitar convertirse en el direccionador designado para los nodos

finales de este circuito. Rango: del 1 al 127, donde 127 es la prioridad superior. Valor por omisión: 64.

Si dos direccionadores tienen la misma prioridad, es preferible el direccionador con la dirección de nodo superior. La prioridad de direccionador no tiene efecto en las decisiones sobre direccionamiento de áreas o en el acceso al direccionador de nivel 2 conectado más cercano.

Utilice la prioridad de direccionador con el fin de elegir el direccionador designado partiendo de que será, probablemente, el siguiente salto mejor para los nodos finales del circuito. Si hay dos direccionadores en un circuito, uno con 500 nodos tras de sí y el otro con 20, el direccionador con 500 nodos debe tener la prioridad de direccionador superior. No obstante, esto no es necesario porque, una vez que un paquete de nodo final alcance a un direccionador, se reenviará hacia su destino.

Este argumento es irrelevante en las líneas punto a punto, donde no habrá nodos finales. (De todas formas, se selecciona un direccionador designado.)

### router type

Especifica la clase de direccionamiento que el direccionador tiene que efectuar: estándar, AMA o bilingüe.

- *Standard*. Especifica que el direccionador va a utilizar el sistema de dirección phase IV convencional, en que la dirección MAC se crea a partir del número de área y número de nodo. El direccionador toma por omisión este tipo.

- *AMA*. Especifica que el direccionador puede direccionar paquetes que utilicen el sistema de dirección phase IV en que la dirección MAC es arbitraria y se aprende de la capa de enlace de datos.

- *Bilingual*. Especifica que el direccionador puede direccionar los paquetes que utilicen el sistema de dirección phase IV convencional y el sistema de dirección phase IV con AMA.

### state

Cuando se establece en **on**, especifica que el circuito está habilitado para que DNA lo utilice. Cuando se establece en **off**, especifica que el circuito está inhabilitado para la utilización por parte de DNA. **off** es el valor por omisión.

### usage

Especifica si un circuito X.25 es:

- PVC: Un circuito virtual permanente
- OUT-SVC: Un circuito estático de salida
- IN-SVC: Un circuito estático de entrada

Este parámetro se aplica cuando el tipo de ejecutor está establecido en *DEC-routing-IV* o *DEC-area*. (Véase **ejecutor type** para el circuito si desea obtener más información.)

### **verification**

Especifica si el direccionador compara una serie de verificación del direccionador con los datos de verificación de un mensaje de inicialización de entrada. Si no coinciden, el circuito X.25 debe reinicializarse. Especifique **enabled** o **disabled**.

### **executor** *argumento*

Define o establece argumentos (es decir, el valor de ejecutor) de forma global para DNA en la base de datos permanente (**define**) o volátil (**set**).

La mayoría de estos argumentos reducen la eficacia del direccionador y aumentan la carga en los circuitos conforme se va incrementando su valor. También pueden hacer que aumenten los requisitos de memoria. No deben utilizarse innecesariamente en mayor medida que los valores necesarios para la configuración de la red real.

Para **set**, el ejecutor debe encontrarse en el estado off si se van a modificar los argumentos numéricos o el tipo en la base de datos volátil. (A diferencia de DECnet-VMS, el mandato **set executor state on** es válido cuando el estado del ejecutor es off.) Estos cambios son efectivos inmediatamente sin rearrancar el direccionador.

### **address** [área.nodo]

Establece la dirección de nodo del ejecutor, el ID de nodo de este direccionador. Rango del valor de área: del 1 al 63. El área y el nodo deben ser inferiores al número máximo de áreas del ejecutor. El rango del valor de nodo es del 1 al 1023. El valor por omisión 0.0 no está permitido.

**Nota:** No se habilitará DNA si no se establece la dirección de ejecutor en un valor permitido.

### **area maximum cost** [número]

El coste máximo permitido entre este direccionador de nivel 2 y cualquier otro direccionador de nivel 2. Si la ruta mejor hacia un área tiene un coste superior a este valor, esta área se considerará inasequible. Máximo: 1022. Valor por omisión: 1022. Este argumento no se aplica a los direccionadores de nivel 1. Debería ser superior al coste máximo permitido hacia el área más distanciada. Un valor que se sugiere es 25 multiplicado por el "número máximo de saltos hacia área".

### **area maximum hops** [número]

El número máximo de saltos permitidos entre este direccionador de nivel 2 y cualquier otro direccionador de nivel 2. Si la ruta mejor hacia un área necesita un número de saltos superior a este valor, esta área se considerará inasequible. Máximo: 30. Valor por omisión: 30. Este argumento no se aplica a los direccionadores de nivel 1. Debería ser, aproximadamente, el doble de la longitud mayor de vía de acceso (en saltos) esperada.

El direccionamiento utiliza la cuenta de saltos únicamente para agilizar la desaparición de las rutas hacia áreas inasequibles. El número máximo de saltos hacia área puede

reducirse para hacer que áreas inasequibles se conviertan en inasequibles con mayor rapidez.

### **broadcast routing timer [rango]**

Especifica la frecuencia con la que se envían mensajes de direccionamiento de nivel 1 (y 2 en un direccionador de nivel 2), en segundos. Se refiere a la frecuencia con la que se enviarán en ausencia de cualquier cambio de coste o adyacencia. Esto protege la base de datos de direccionamiento de la corrupción. Como mínimo, se envían actualizaciones parciales del direccionamiento automáticamente si cambia algún coste o adyacencia. Rango: del 1 al 65535. Valor por omisión: 180. Los valores inferiores aumentan la actividad general para este direccionador y para todos los adyacentes. Los valores superiores permiten un aumento del tiempo necesario para corregir la base de datos de direccionamiento si se pierde un mensaje de actualización parcial del direccionamiento.

### **maximum address number [rango]**

(sólo **define**) Es la dirección de nodo superior (dentro de esta área) para la que este direccionador mantendrá rutas. La base de datos de direccionamiento no incluirá rutas hacia nodos de esta área con una parte de dirección de nodo que sea más alta. Rango: del 1 al 1023. Valor por omisión: 32. Debe superar la dirección de nodo más alta del área del direccionador. Si la establece demasiado grande, afectará a la eficacia del direccionador y utilizará demasiada memoria. Este argumento no es efectivo hasta que se reinicia el direccionador.

### **maximum area number [número]**

(sólo **define**) Es el área superior para la que se mantendrán rutas si este direccionador es de nivel 2. La base de datos de direccionamiento no incluirá rutas hacia áreas superiores a ésta. Máximo: 63. Valor por omisión: 63. Debe superar el número de área más alto de la red general. Este argumento no es efectivo hasta que se reinicia el direccionador.

### **maximum broadcast nonrouters [número]**

(sólo **define**) El número máximo de nodos finales que pueden ser adyacentes (alejados por un salto) respecto a este direccionador. Ésta es la suma a partir de todos los circuitos de difusión. Si hay más nodos finales, algunos de éstos no serán asequibles para este direccionador, lo que puede causar problemas imprevisibles de direccionamiento. Este argumento no es efectivo hasta que se reinicia el direccionador. Rango: del 1 al 1023. Valor por omisión: 63.

### **maximum broadcast routers [número]**

(sólo **define**) El número máximo de direccionadores que pueden ser adyacentes (alejados por un salto) respecto a este direccionador. Ésta es la suma a partir de todos los circuitos de difusión. Si hay más direccionadores, no se aceptarán rutas de los direccionadores en exceso. Esto puede causar problemas imprevisibles de direccionamiento. Este

argumento no es efectivo hasta que se reinicia el direccionador. Valor por omisión: 32. Máximo: 33 multiplicado por el número de circuitos. Este valor debería ser igual o superior a la suma del “número máximo de direccionadores de circuito” a partir de todos los circuitos, aunque no es necesariamente obligatorio. Este parámetro tiene un gran efecto sobre la utilización de memoria y no debe ser mucho más grande de lo necesario. Puesto que el valor por omisión es bastante alto, es posible que tenga que reducirlo si ha establecido un gran “número máximo de dirección”.

### **maximum cost [número]**

El coste máximo permitido entre este direccionador y cualquier otro nodo del área. Si la ruta mejor hacia un nodo tiene un coste superior a este valor, este nodo se considerará inasequible. Máximo: 1022. Valor por omisión: 1022. Debería ser superior al coste máximo permitido hacia el nodo más distanciado. Un valor que se sugiere es 25 multiplicado por el “número máximo de saltos”.

### **maximum hops [número]**

El número máximo de saltos permitidos entre este direccionador y cualquier nodo del área. Si la ruta mejor hacia un nodo necesita un número de saltos superior a este valor, este nodo se considerará inasequible. Máximo: 30. Valor por omisión: 30. Debería ser, aproximadamente, el doble de la longitud mayor de vía de acceso (en saltos) esperada. El direccionamiento utiliza la cuenta de saltos únicamente para agilizar la desaparición de las rutas hacia nodos inasequibles. El número máximo de saltos puede reducirse para hacer que nodos inasequibles se conviertan en inasequibles con mayor rapidez.

### **maximum visits [número]**

Especifica que se eliminará cualquier paquete reenviado por este direccionador que hayan reenviado más direccionadores de los que indica el número máximo de visitas. Se utiliza para detectar paquetes que están en bucles de direccionamiento, lo que se produce cuando desaparecen rutas. El número máximo de visitas es 63. Éste es el valor por omisión. Este argumento debe ser un valor superior, multiplicado por dos, al número máximo de saltos y número máximo de saltos hacia área.

**state on** Habilita DNA. Puede emitirse en cualquier momento, siempre y cuando el direccionador tenga una dirección de nodo válida.

**state off** Inhabilita DNA. Puede emitirse en cualquier momento. El estado por omisión es off.

Para **set**, quedará inhibida la opción **set executor** si la inicialización de DNA falla por falta de memoria disponible para las tablas de direccionamiento.



**type** (sólo **define**) En los circuitos X.25, hace que el direccionador actúe de una de las cuatro maneras que hay de acuerdo con el valor seleccionado. Las opciones son:

**DEC-routing-iv**

configura el direccionador como direccionador de nivel 1 compatible con DEC.

**DEC-area**

configura el direccionador como direccionador de nivel 2 (de áreas) compatible con DEC.

**Routing-iv**

configura el direccionador como direccionador de nivel 1 sin compatibilidad con DEC en circuitos X.25. Éste es el valor por omisión.

**Area**

configura el direccionador como direccionador de nivel 2 (de áreas) sin compatibilidad con DEC en circuitos X.25.

Un direccionador de nivel 2 acepta adyacencias con direccionadores de otras áreas y mantiene rutas hacia todas las áreas. Si puede alcanzar a otras áreas, también se anuncia a sí mismo ante los direccionadores de nivel 1 como ruta hacia otras áreas.

Para los direccionadores de nivel 1, sólo se aceptan adyacencias con direccionadores de la misma área.

**Ejemplo: define executor state on**

```
define executor type DEC-area
```

```
define executor maximum broadcast routers 10
```

**type area** (sólo **set**) Hace que el direccionador actúe como direccionador de nivel 2. Aceptará adyacencias con direccionadores de otras áreas y mantendrá rutas hacia todas las áreas. Si puede alcanzar a otras áreas, también se anunciará a sí mismo ante los direccionadores de nivel 1 como ruta hacia otras áreas.

El estado de DNA debe establecerse en *off* antes de cambiar *type*.

**type routing-IV**

(sólo **set**) Hace que el direccionador actúe como direccionador de nivel 1, que es el valor por omisión. Sólo se aceptarán adyacencias con direccionadores de la misma área.

El estado de DNA debe establecerse en *off* antes de cambiar *type*.

**Ejemplo: set executor state on**

```
set executor maximum broadcast routers 10
```

### **module access-control especificador-circuito argumento**

(sólo **define**) Define listas de control del acceso, que se utilizan para limitar el reenvío de paquetes entre ciertos orígenes y destinos. Cada lista de acceso está asociada con un circuito, y se aplica a los paquetes de datos de formato largo de DECnet recibidos en este circuito. El control del acceso no se aplica a ningún paquete hello ni de direccionamiento.

Los argumentos para especificador-circuito son los siguientes:

#### **all circuits**

Especifica todos los circuitos del direccionador.

#### **circuit name**

Especifica el circuito nombrado.

#### **known circuits**

Especifica todos los circuitos del direccionador.

Los elementos siguientes son los argumentos entre los que realiza una selección después de entrar el mandato **define module access-control** y el valor de especificador-circuito:

**state on** Habilita la lista de control del acceso en este circuito.

**state off** Inhabilita la lista de control del acceso en este circuito.

#### **type exclusive**

Especifica que se eliminará cualquier paquete que coincida con uno o más filtros de la lista de control del acceso para esta interfaz.

#### **type inclusive**

Especifica que sólo se reenviarán los paquetes que coincidan con uno o más filtros de la lista de control del acceso para esta interfaz.

#### **filter [resultado-origen máscara-origen resultado-dest máscara-dest]**

Añade un filtro a la lista para el circuito especificado. El filtro se añade al final de la lista existente.

Se efectúa una máscara para la dirección de origen con máscara-origen y se compara con resultado-origen. Lo mismo se hace con máscara-dest y resultado-dest. La acción depende de qué tipo de control del acceso esté en uso en el circuito.

Los elementos siguientes son las opciones entre las que realiza una selección después de entrar el mandato **define module access-control** y **filter** para especificador-circuito:

#### **resultado-origen**

Dirección con la que la dirección de origen se compara después de recibir una máscara.

#### **máscara-origen**

Máscara utilizada para la dirección de origen.

#### **resultado-dest**

Dirección con la que la dirección de destino se compara después de recibir una máscara.

### máscara-dest

Máscara utilizada para la dirección de destino.

**Ejemplo:** `define module access-control circuit eth/0 state on`

### `module routing-filter` *especificador-circuito argumento*

(sólo **define**) Define filtros de direccionamiento, que se utilizan para limitar el envío de rutas de áreas por parte de direccionadores de nivel 2 (Executor Type Area).

### all circuits

Especifica todos los circuitos del direccionador.

### circuit name

Especifica el circuito nombrado.

### known circuits

Especifica todos los circuitos del direccionador.

Los elementos siguientes son las opciones de orientación entre las que realiza una selección después de entrar el mandato **define module routing-filter** y el valor de especificador-circuito:

**incoming** Afecta al filtro de información de direccionamiento recibida en este circuito.

**outgoing** Afecta al filtro de información de direccionamiento enviada en este circuito.

Los elementos siguientes son los argumentos entre los que realiza una selección después de entrar el mandato **define module routing-filter** y el valor de especificador-circuito:

### area [lista-áreas]

Especifica que el filtro permite que pase información de direccionamiento para el conjunto de áreas de lista-áreas. La lista-áreas es una lista de áreas o rangos de áreas separados por comas. Un rango se especifica mediante dos números de área separados por un guión. También puede ser que la lista-áreas no tenga ningún valor, lo que especificará que no pasará información sobre ninguna área. A continuación, se indican ejemplos para lista-áreas:

**1,4,9,60** Áreas 1, 4, 9 y 60

**1-7,9-13,23**

Áreas 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13 y 23

**state on** Especifica que el filtro está activo.

**state off** Especifica que el filtro está inhabilitado, pero continúa almacenado en la base de datos permanente. La única manera de eliminar el filtro es mediante el mandato **purge**.

**Ejemplo:** `define module routing-filter circuit eth/0 state on`

### `node` *argumento*

Permite definir o establecer información de configuración sobre nodos en la base de datos volátil (**set**) o permanente (**define**). El único nodo para el que se mantiene cualquier tipo de información es el nodo del ejecutor, ya que no se almacenan nombres de nodos. El nodo especi-

fica la dirección de nodo del direccionador (del ejecutor). Consulte la descripción del mandato **define executor**.

**Ejemplo: define node state on**

**Ejemplo: set node state on**

## Purge

Utilice el mandato **purge** para eliminar listas de control del acceso y filtros de direccionamiento de la base de datos permanente.

### Sintaxis:

```
purge          module access-control . . .  
                module routing-filter . .
```

**module access-control *especificador-circuito***

Elimina listas de control del acceso de la base de datos permanente. Puede suprimir una lista de control del acceso entera; no puede suprimir un filtro por separado.

#### **all circuits**

Especifica todos los circuitos del direccionador.

#### **circuit name**

Especifica el circuito nombrado.

**Ejemplo: purge module access-control all circuits**

**module routing-filter *especificador-circuito***

Elimina filtros de direccionamiento de la base de datos permanente. Puede eliminar un filtro especificado o puede eliminarlos todos.

Las opciones para especificador-circuito son las siguientes:

**all** Especifica todos los filtros de direccionamiento de la memoria de la configuración.

#### **circuit name**

Especifica el filtro de direccionamiento del circuito nombrado.

**Ejemplo: purge module routing-filter all**

## Set

Utilice el mandato **set** para añadir, establecer o modificar especificadores de circuito, argumentos globales, módulos de enlace de datos o nodos en la base de datos de DNA volátil.

### Sintaxis:

```
set           especificador-circuito . . .  
              executor . . .  
              node . . .
```

Para obtener una descripción de las opciones de estos argumentos, consulte la sección "Define/Set" en la página 352.

## Show

Utilice el mandato show para visualizar el estado de la base de datos volátil y los nodos volátiles de la base de datos de direccionamiento.

### Sintaxis:

```
show          especificador-área . . .
              especificador-nodo . . .
```

### especificador-área *argumento*

Examina el estado de la base de datos de direccionamiento de áreas volátil. Con ello puede averiguar qué áreas son asequibles y cuáles son las rutas hacia las diversas áreas.

Las opciones para especificador-área son las siguientes:

#### active areas

Proporciona información sobre las áreas que actualmente son asequibles.

**all areas** Proporciona información sobre todas las áreas (hasta el número máximo de áreas del ejecutor).

**area** Proporciona información sobre el área especificada. Si no se proporciona el área, se le solicitará.

#### known areas

Proporciona información sobre las áreas que actualmente son asequibles.

Los elementos siguientes son las opciones de submandato entre las que realiza una selección después de entrar el mandato **show** y el especificador de área:

#### characteristics

Muestra el estado actual del área especificada. (Es lo mismo que summary.)

**status** Proporciona información detallada sobre las áreas especificadas, incluidos coste y saltos.

**summary** Muestra el estado actual de las áreas especificadas. Éste es el valor por omisión.

### Ejemplo: show active areas

```
Active Area Volatile Summary
Area State      Circuit Next
                Node
1  reachable    Eth/0  1.22
2  reachable    2.26
3  reachable    X25/0 2.30
```

### Ejemplo: show active areas status

```
Active Area Volatile Status
Area State      Cost Hops Circuit Next
                Node
1  reachable    3   1   Eth/0  1.22
2  reachable    0   0   2.26
3  reachable    2   1   PPP/0  3.9
6  reachable   12   3   PPP/0  3.9
3  reachable   11   1   X25/0  2.30

Area Volatile Status
Area State      Cost Hops Circuit Next
                Node
5  unreachable 1023 31
```

Los elementos siguientes definen la información visualizada cuando utiliza el mandato **show**.

- area** Indica el área de esta línea de la pantalla.
- circuit** Indica el circuito al que estará conectado el siguiente salto hacia este nodo. No se facilita ningún circuito para la propia área del direccionador.
- cost** Indica el coste para esta área.
- hops** Indica los saltos hacia esta área.
- next node**  
Indica el direccionador que será el siguiente salto (destino intermedio) hacia el área especificada.
- state** Indica que ésta será asequible o inasequible.

### **especificador-nodo** *argumento*

Muestra el estado de la base de datos de direccionamiento de nodos volátil; incluye información sobre los nodos asequibles y las rutas hacia los mismos.

Cualquiera de las siguientes puede ser una opción para especificador-nodo:

#### **active nodes**

Proporciona información sobre todos los nodos que actualmente son asequibles.

**all nodes** Proporciona información sobre todos los nodos (hasta el número máximo de dirección del ejecutor). Una pantalla de all nodes incluye información sobre el "pseudo-nodo" área.0. Cualquier direccionador de nivel dos que alcanza a otras áreas anuncia una ruta hacia el nodo área.0. Los direccionadores de nivel uno utilizan estas rutas para reenviar todos los paquetes al direccionador de nivel uno más próximo con conocimiento de cómo llevar ese paquete al área correcta. No existe otra manera de examinar el nodo 0, ya que no es una dirección de nodo permitida.

#### **node nodo**

Proporciona información sobre el nodo especificado. Si no se proporciona el nodo, se le solicitará.

#### **known nodes**

Proporciona información sobre los nodos que actualmente son asequibles.

Los argumentos son los siguientes:

#### **characteristics/ summary**

Ambas opciones de submandato muestran el estado actual de los nodos especificados.

**status** Proporciona información detallada sobre los nodos especificados, incluidos coste y saltos.

#### **Ejemplo: show node status**

Este ejemplo muestra el estado detallado de un nodo específico.

```
Which node [1.9]? 2.26
Node Volatile Status
Executor node      = 2.26 (gato)
State              = on
Physical address   = AA-00-04-00-1A-08
Type               = DEC-area
```

**Ejemplo: show active nodes**

Este ejemplo muestra los nodos asequibles.

```
Active Node Volatile Summary
Executor node      = 2.26 (gato)
State              = on
Identification     = DECnet-MC68360 V1 R2.0 NP00523 [P10]

Node   State   Circuit Next
Addr  Address
2.14  reachable Eth/0  2.14
2.34  reachable PPP/0  2.34
2.37  reachable PPP/0  2.34
1.22  reachable Eth/0  1.22
```

**Ejemplo: show adjacent nodes status**

Este ejemplo muestra la información de direccionamiento detallada sobre todos los nodos adyacentes. Sólo se mostrarán los nodos con un solo salto. El tipo de nodo se reconoce y visualiza únicamente para los nodos adyacentes porque esta información sólo está contenida en mensajes hello.

```
Adjacent Node Volatile Status

Executor node      = 2.26 (gato)
State              = on
Physical address   = AA-00-04-00-1A-08
Type               = DEC-area

Node   State   Type      Cost Hops Circuit Next
Addr  Address
2.14  reachable routing IV  3   1  Eth/0  2.14
2.34  reachable routing IV  2   1  PPP/0  2.34
2.42  reachable nonrouting IV 2   1  PPP/0  2.42
1.22  reachable area      3   1  Eth/0  1.22
```

## Show/List

Utilice el mandato **show circuit** para recuperar información sobre el estado actual de los circuitos especificados de la base de datos volátil. El mandato **list circuit** recupera los datos almacenados en la base de datos permanente para los circuitos.

**Sintaxis:**

```
show          all
               area
               circuit . . .
               executor . . .
               known argumento
               module argumento
               node argumento
```

**Sintaxis:**

```
list         all
               area
               circuit argumento
               executor argumento
               module
               node argumento
```

### especificador-circuito *argumento*

Donde las opciones para especificador-circuito son las siguientes:

#### **active circuits**

Especifica todos los circuitos que actualmente están activos (según la base de datos volátil).

#### **all circuits**

Especifica todos los circuitos del direccionador.

#### **circuit name**

Especifica el circuito nombrado.

#### **known circuits**

Especifica todos los circuitos del direccionador.

Los elementos siguientes son las opciones de submandato entre las que realiza una selección después de entrar el mandato y el especificador de circuito:

#### **characteristics**

Proporciona información detallada sobre todos los valores de los argumentos del circuito.

**counters** Muestra los contadores del circuito.

**status** Muestra información detallada sobre el circuito de la base de datos volátil.

**summary** Muestra información de resumen sobre el circuito de la base de datos volátil. Éste es el valor por omisión si no se suministra ningún argumento.

#### **Ejemplo: show all circuits**

```
Circuit Volatile Summary
Circuit State      Adjacent
                  Node
X25/0  on          5.25
Eth/0   on          1.22
Eth/0   on          2.14
Eth/0   on          1.13
PPP/0   off
```

#### **Ejemplo: list circuit eth/0 characteristics**

```
Circuit Permanent Characteristics
Circuit              = Eth/0
State                 = On
Cost                  = 4
Router priority       = 64
Hello timer           = 15
Maximum routers       = 16
Router type           = Standard
```

#### **Ejemplo: show active circuits status**

```
Active Circuit Volatile Status
Circuit State      Adjacent  Block
                  Node      Size
Eth/0  on          1.22    1498
Eth/0  on          2.14    1498
Eth/0  on          1.13    1498
X25/0  on          5.25    1498
```

#### **Ejemplo: show all circuits characteristics**

Este ejemplo muestra las características actuales de los circuitos de esta máquina. Incluye todos los argumentos de la configuración así como las adyacencias actuales y el temporizador de escucha (el triple del temporizador de hello de la adyacencia).



```
Circuit Volatile Characteristics
Circuit          = Eth/0
State            = on
Designated router = 2.26
Cost             = 4
Router priority  = 64
Hello timer      = 15
Maximum routers  = 16
Adjacent node    = 1.22
Listen timer     = 45
Adjacent node    = 2.14
Listen timer     = 45
Adjacent node    = 2.39
Listen timer     = 90

Circuit          = PPP/0
State            = off
Designated router =
Cost             = 4
Router priority  = 64
Hello timer      = 15
Maximum routers  = 8
```

### Ejemplo: `show circuit eth/0 counters`

Este ejemplo muestra los contadores mantenidos para los circuitos. Tenga en cuenta que algunos contadores mantenidos por DECnet-VAX no lo están aquí, pero, en lugar de ello, se leen mediante el mandato **network** de GWCON.

```
Circuit Volatile Counters
Circuit = Eth/0
525249 Seconds since last zeroed
0 Terminating packets received
0 Originating packets sent
3693 Transit packets received
4723 Transit packets sent
0 Transit congestion loss
0 Circuit down
0 Initialization failure
0 Packet corruption loss
```

### adjacent node

El ID de nodo de un nodo que tiene una adyacencia con este nodo en el circuito visualizado. Mientras que las adyacencias con los nodos finales hacen que automáticamente ese nodo sea asequible, la adyacencia con un direccionador no hace que automáticamente ese nodo sea asequible. Un direccionador no se considera asequible a menos que se haya recibido un mensaje de direccionamiento sobre una adyacencia activa de ese direccionador. Por consiguiente, los nodos pueden mostrarse adyacentes en la base de datos de circuitos, pero no estarán en la base de datos de nodos asequibles (muestra los nodos activos).

### block size

El tamaño máximo de bloque de datos que el nodo adyacente asociado está dispuesto a recibir. Normalmente son 1498 bytes, que son los 1500 bytes estándares de un paquete de Ethernet menos el campo de 2 bytes de longitud utilizado con DECnet.

**circuit** Los circuitos a los que se aplican estos datos.

### designated router

Visualiza el que este nodo considera el direccionador designado para esta área en este circuito. (Puede haber algunas discrepancias transitorias cuando arranca un nuevo direccionador.) Normalmente será el mismo para todos los direccionadores del circuito. Los nodos finales envían todos

los paquetes dirigidos a destinos que no están en el circuito local al direccionador designado.

### **hello timer**

El temporizador de hello para este circuito. Los mensajes hello del direccionador se envían con esta frecuencia en el circuito.

### **listen timer**

El período de tiempo que designa la frecuencia con la que deben recibirse mensajes hello de direccionador o nodo final de esta adyacencia en este circuito. Es el triple del temporizador de hello establecido para este circuito en la máquina adyacente.

### **router priority**

La prioridad del direccionador para este circuito, utilizada al competir por el estado de direccionador designado.

### **router type**

El tipo del direccionador para este circuito - estándar, phase IV con AMA o bilingüe.

### **maximum routers**

El número máximo de direccionadores permitidos en este circuito.

### **state**

ON u OFF. En la base de datos volátil, el estado será ON si se habilita el circuito y pasa la autoprueba. Si el circuito ha fallado la autoprueba o el dispositivo no está, el estado será OFF.

En la base de datos permanente, indica si DNA intentará habilitar el circuito.

### **executor** *argumento*

Recupera información sobre el estado actual de la base de datos volátil para DNA con el mandato `show executor`. El mandato `list executor` recupera los datos almacenados en la base de datos permanente para DNA.

A continuación, se listan las opciones o argumentos de submandato entre los que realiza una selección después de entrar el mandato `show/list executor`:

### **characteristics**

La información detallada sobre los valores de todos los argumentos que pueden ajustarse de la base de datos de direccionamiento.

**counters** Facilita los contadores globales de sucesos y errores para DNA. No hay contadores permanentes, por lo que el mandato `list executor counters` es irrelevante.

**status** Facilita información clave sobre el estado de DNA.

**summary** Facilita un breve resumen del estado de DNA. Éste es el valor por omisión.

**Ejemplo:** `show executor`

```
Node Volatile Summary
Executor node      = 2,26 (gato)
State              = on
Identification     = DECnet-MC68360 V1 R2.0 NP00523 [P10]
```

## Ejemplo: **show executor characteristics**

Este ejemplo muestra la configuración completa de la base de datos del direccionador. El mandato **list executor characteristics** genera básicamente la misma visualización.

```
Node Volatile Characteristics
Executor node      = 2,26 (gato)
State              = on
Identification     = DECnet-MC68360 V1 R2.0 NP00523 [P10]
Physical address   = AA-00-04-00-1A-08
Type               = DEC-area
Routing version    = V2.0.0
Broadcast routing timer = 180
Maximum address    = 64
Maximum cost       = 1022
Maximum hops       = 30
Maximum visits     = 63
Maximum area       = 63
Max broadcast nonrouters = 64
Max broadcast routers = 32
Area maximum cost  = 1022
Area maximum hops  = 30
Maximum buffers    = 103
Buffer size        = 2038
```

## Ejemplo: **list executor status**

Este ejemplo muestra el estado del direccionador en la base de datos permanente:

```
Node Permanent Status
Executor node      = 2,26 (gato)
State              = on
Type               = DEC-area
```

## Ejemplo: **show executor counters**

Este ejemplo muestra los contadores que mantiene DNA.

```
Node Volatile Counters
Executor node      = 2,26 (gato)
525948 Seconds since last zeroed
0 Aged packet loss
0 Node unreachable packet loss
0 Node out-of-range packet loss
0 Oversized packet loss
0 Packet format error
0 Partial routing update loss
0 Verification reject
```

Los elementos siguientes definen los campos que se visualizan cuando utiliza el mandato **show/list executor**.

### **area maximum cost**

El coste máximo permitido para un área.

### **area maximum hops**

El número máximo de saltos permitidos hacia un área.

### **broadcast routing timer**

La frecuencia con la que se envían mensajes de direccionamiento en ausencia de cambios.

### **buffer size**

El tamaño de almacenamiento intermedio para el direccionador.

### **executor node**

La dirección del nodo y el nombre del nodo. El nombre del nodo es el nombre establecido por medio del mandato de **CONFIG set hostname**.

### **identification**

La identificación del software del direccionador enviada en los mensajes de ID del sistema de MOP.

**maximum area**

El área superior para la que se mantienen rutas.

**maximum broadcast nonrouters**

El número máximo de nodos finales que pueden ser adyacentes respecto a este direccionador.

**maximum broadcast routers**

El número máximo de direccionadores que pueden ser adyacentes respecto a este direccionador.

**maximum buffers**

El número de almacenamientos intermedios de paquetes del direccionador.

**maximum cost**

El coste máximo permitido para un nodo.

**maximum hops**

El número máximo de saltos permitidos hacia un nodo.

**maximum visits**

El número máximo de direccionadores a través de los que puede direccionarse un paquete entre origen y destino.

**physical address**

La dirección Ethernet física establecida en todos los circuitos Ethernet cuando se inicia DNA. Deriva del ID de nodo.

**routing version**

La versión siempre es la Versión 2.0.0.

**state**

El estado de DNA, on u off.

**type**

ROUTING IV o AREA, correspondientes al nivel 1 y nivel 2.

**module access-control especificador-circuito *argumento***

Facilita el listado de las listas de control del acceso que se han definido en la base de datos permanente para el direccionador además de los contadores que utilizan. Las opciones para especificador-circuito son las siguientes:

**all circuits**

Especifica todos los circuitos del direccionador.

**circuit [nombre]**

Especifica el circuito nombrado.

**known circuits**

Especifica todos los circuitos del direccionador.

Los elementos siguientes son los argumentos entre los que realiza una selección después de entrar el mandato **show/list module access-control** y el valor de especificador-circuito:

**counters**

Facilita los contadores utilizados por las listas de control del acceso.

**status**

Muestra información detallada sobre las listas de control del acceso, incluidos los filtros de la lista de control del acceso.

**summary**

Muestra información de resumen sobre el estado de las listas de control del acceso. Éste es el valor por omisión.

**Ejemplo:** `show module access-control circuit eth/0 counters`  
**Ejemplo:** `list module access-control circuit eth/0 counters`

```
Module Access-Control Volatile Counters
Circuit = Eth/0
6337      Seconds since last zeroed
0         Packets processed
0         Packets rejected
0         Access control loop iterations
```

### module routing-filter especificador-circuito *argumento*

Lista los filtros de direccionamiento de áreas de DECnet que se han definido en la base de datos permanente para el direccionador.

#### **all circuits**

Especifica todos los circuitos del direccionador.

#### **circuit [nombre]**

Especifica el circuito nombrado.

#### **known circuits**

Especifica todos los circuitos del direccionador.

Los elementos siguientes son los argumentos entre los que realiza una selección después de entrar el mandato **show/list module routing-filter** y el valor de especificador-circuito:

**status** Muestra información detallada sobre los filtros de direccionamiento, incluida la lista de áreas.

**summary** Muestra información de resumen sobre el estado de los filtros de direccionamiento. Éste es el valor por omisión.

**Ejemplo:** `show module routing-filter circuit eth/0 status`

**Ejemplo:** `list module routing-filter circuit eth/0 status`

## Zero

Utilice el mandato **zero** para borrar los contadores de circuitos de la base de datos volátil, los contadores globales de la base de datos volátil y los contadores del módulo de lista de control del acceso.

### **Sintaxis:**

```
zero                especificador-circuito
                    _executor
                    _module _access-control especificador-circuito
```

#### **especificador-circuito**

#### **all circuits**

Especifica todos los circuitos del direccionador.

#### **circuit [nombre]**

Especifica el circuito nombrado.

#### **known circuits**

Especifica todos los circuitos del direccionador.

**Ejemplo:** `zero all circuits`

## Mandatos de configuración y supervisión de DNA IV

**executor** Establece todos los contadores globales de la base de datos volátil en el valor de cero. No hay opciones.

**Ejemplo:** zero executor

**module access-control especificador-circuito**

**all circuits**

Especifica todos los circuitos del direccionador.

**circuit [nombre]**

Especifica el circuito nombrado.

**Ejemplo:** zero module access-control all circuits

## Utilización de OSI/DECnet V

Este capítulo describe la implementación, por parte del direccionador, de la Capa de red sin conexiones de Interconexión de Sistemas Abiertos (OSI) de la Organización Internacional para la Normalización (ISO). DECnet Phase V da soporte a OSI (que a partir de aquí denominaremos DECnet V/OSI) y los usuarios de las redes DNA V pueden utilizar este capítulo para obtener información sobre los protocolos OSI de la ISO. Este capítulo contiene los apartados siguientes:

- “Visión general de OSI”
- “Sistema de dirección NSAP” en la página 374
- “Direcciones de vertimiento múltiple” en la página 376
- “Direccionamiento de OSI” en la página 377
- “Protocolo IS-IS” en la página 377
- “Protocolo ESIS” en la página 387
- “Circuitos X.25 para DECnet V/OSI” en la página 388
- “Configuración de OSI/DECnet V” en la página 390
- “Acceso al entorno de configuración de OSI” en la página 393
- “Mandatos de configuración de OSI/DECnet V” en la página 393

### Visión general de OSI

Una red OSI está compuesta por subredes interconectadas. Una subred está compuesta por sistemas principales conectados, que se denominan sistemas finales (ES), y direccionadores, que se denominan sistemas intermedios (IS), tal como muestra la Figura 19.

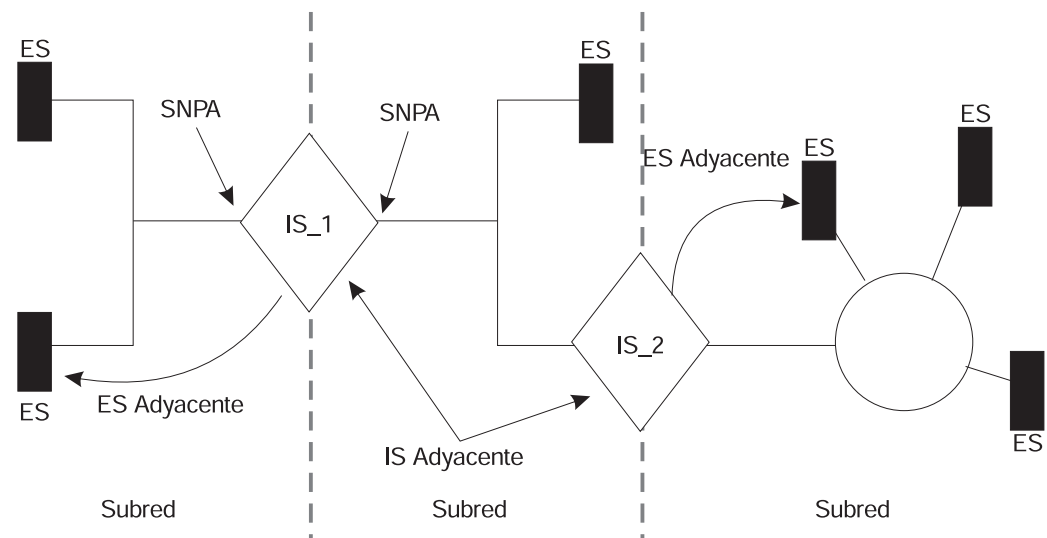


Figura 19. Red OSI

Los ES contienen todas las capas del modelo de referencia OSI y contienen las aplicaciones de sistema principal. Los IS realizan las funciones de las tres capas inferiores del modelo de referencia OSI y manejan el direccionamiento de las unidades de datos de protocolo de red (NPDU) entre subredes. Los IS se conectan lógicamente a la subred en el punto de conexión de subred (SNPA). El SNPA es el punto de acceso a la capa de enlace de datos.

Según la configuración del IS, cada IS puede ejecutar tres protocolos: ES-IS, IS-IS y Connectionless-Mode Network Protocol (CLNP).

El protocolo ES-IS permite que los ES e IS conectados a la misma subred descubran dinámicamente la existencia de los otros entre sí. Un ES conectado a la misma subred que un IS es adyacente respecto al IS. El protocolo de direccionamiento IS-IS permite que los IS realicen las siguientes acciones:

- Descubran dinámicamente la existencia y disponibilidad de los IS adyacentes.
- Intercambien información de direccionamiento con los otros IS.
- Utilicen la información intercambiada para calcular rutas basándose en la vía de acceso más corta.

El protocolo CLNP es un protocolo de datagramas que transporta paquetes entre los IS.

---

## Sistema de dirección NSAP

La NPDU contiene direcciones de red OSI (también denominadas NSAP). NSAP hace referencia a un punto de la capa de red donde el usuario accede a la capa de red. NSAP son puntos exclusivos de un sistema que representan puntos finales de comunicación accesibles a través de la capa de red. El número de NSAP puede variar según el sistema.

Una autoridad que gestiona un sistema de dirección, como, por ejemplo, el National Institute of Standards and Technology (NIST) del Gobierno de los Estados Unidos, administra direcciones NSAP y determina cómo se asignan e interpretan las direcciones dentro de su dominio. Si es conveniente, estas autoridades pueden realizar una mayor división del dominio en subdominios y designar las autoridades correspondientes para que los administren.

Existen dos direcciones NSAP dentro de la NPDU, una dirección de destino y una dirección de origen. La longitud de cada dirección puede variar de 2 octetos a 20 octetos y, normalmente, se representa en notación hexadecimal. A continuación, se muestra un ejemplo de una NSAP de 6 octetos que puede entrarse en la configuración de OSI del direccionador.

AA000400080C

Puesto que la longitud de la dirección es variable, las partes de la cabecera de PDU denominadas Indicador de longitud de dirección de destino e Indicador de longitud de dirección de origen se utilizan para indicar la longitud, en octetos, de cada dirección.

Una dirección NSAP está compuesta por dos partes, una Parte de dominio inicial (IDP) y una Parte específica de dominio (DSP), tal como muestra la Figura 20.

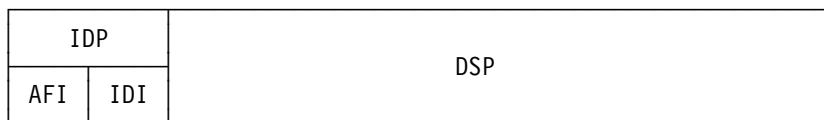


Figura 20. Estructura de una dirección NSAP



## IDP

La IDP está compuesta por dos partes, el Identificador de autoridad y formato (AFI) y el Identificador de dominio inicial (IDI).

El AFI especifica el tipo de IDI y la autoridad del sistema de dirección de red responsable de la asignación de los valores del IDI.

El IDI especifica el dominio del sistema de dirección de red a partir del cual se asignan los valores de la DSP y la autoridad del sistema de dirección de red responsable de la asignación de los valores de la DSP de este dominio.

## DSP

La autoridad del sistema de dirección de red identificada por el IDI determina la DSP. No obstante, lo importante es que la DSP incluye información de sistema de dirección específica para el dominio.

## Formato de sistema de dirección IS-IS

El protocolo IS-IS divide la dirección NSAP en tres partes: dirección de área, ID del sistema y selector (vea la Figura 21). La dirección de área y el ID del sistema, junto con un selector de 0, vienen referidos como Título de entidad de red (NET). Un NET es la dirección de la capa de red en sí y se asigna cuando se configura un IS en la red OSI.

IDP	DSP	
Dirección de área	ID del sistema	Selector

Figura 21. Interpretación del sistema de dirección NSAP en IS-IS

### Dirección de área

En el protocolo IS-IS, la dirección de área es el segmento de la NSAP que incluye toda la IDP o un segmento de ésta y el segmento de la DSP hasta el ID del sistema.

La dirección de área es el segmento de la NSAP que identifica a un área específica de un dominio. Esta dirección debe tener, como mínimo, 1 octeto de longitud y todos los ES e IS de la misma área deben tener la misma dirección de área.

### ID del sistema

El ID del sistema es el segmento de la NSAP que identifica a un sistema específico de un área. Los ID del sistema deben tener los atributos siguientes:

- De 1 octeto a 8 octetos de longitud.
- La misma longitud en todo el dominio. Los direccionadores utilizan una longitud de configuración por omisión de 6 octetos.
- Ser exclusivos para cada sistema en todo el dominio.

### Selector

El selector es un campo de 1 octeto que actúa como selector de la entidad que va a recibir la PDU, como, por ejemplo, la capa de transporte o la capa de red de IS en sí. El direccionador establece este campo en 0.

## NSAP del GOSIP Versión 2

El Perfil de Interconexión de Sistemas Abiertos del Gobierno (GOSIP) Versión 2 proporciona, para uso del Gobierno, el formato de sistema de dirección NSAP ilustrado en la Figura 22. Las autoridades responsables de la dirección han definido claramente los campos y han especificado el formato de sistema de dirección bajo la DSP establecida por el National Institute of Standards and Technology (NIST).

IDP		DSP						
AFI 47	IDI 0005	Ver 80	Aut.	Reservado	Dominio (2)	Área (2)	ID sist. (6)	Selector (1)

Figura 22. Formato de dirección GOSIP

- AFI** Este campo de 1 octeto tiene la designación 47 (hexadecimal). Este valor significa que la dirección se basa en el formato de ICD y que la DSP utiliza una sintaxis binaria.
- IDI** Este campo de 2 octetos tiene la designación 0005 (hexadecimal). Este valor está asignado al Gobierno de los EE.UU. y el formato está establecido por NIST.
- VER** Este campo de 1 octeto tiene la designación 80 (hexadecimal). Este valor identifica al formato de DSP.
- Aut. (Autoridad)** Este campo de 3 octetos identifica a la autoridad que controla la distribución de las direcciones NSAP.
- Reservado** Este campo de 2 octetos se proporciona para el alojamiento de un desarrollo futuro.
- Dominio** Este campo de 2 octetos contiene el identificador de dominio de direccionamiento.
- Área** Este campo de 2 octetos contiene el ID de área.
- ID sist.** Este campo de 6 octetos identifica al sistema.
- Selector** Este campo de 1 octeto selecciona la entidad que va a recibir la NPDU.

---

## Direcciones de vertimiento múltiple

El sistema de dirección de vertimiento múltiple es el método que los IS de nivel 1 (L1) y nivel 2 (L2) utilizan para distribuir actualizaciones del estado de los enlaces (LSU) y mensajes hello a otros sistemas o LAN. Cuando una LSU o un mensaje hello se vierte de manera múltiple, recibe el paquete un grupo de estaciones de destino. Por ejemplo, se vierte de manera múltiple una LSU de L1 en otros IS de L1 únicamente. Se vierte de manera múltiple un mensaje hello de sistema intermedio (ISH) en ES de la misma subred únicamente.

Puede configurar direcciones de vertimiento múltiple para cada subred con el mandato **set subnet**. La Tabla 107 en la página 377 lista las direcciones de vertimiento múltiple para FDDI, Ethernet y Red en Anillo.

Tabla 107. Direcciones de vertimiento múltiple en IS-IS

Destino	Ethernet 802.3	Red en Anillo 802.5	FDDI	Descripción de dirección
Todos los ES	09002B000004	C00000004000	9000D4000020	Para todos los sistemas finales de la subred.
Todos los IS	09002B000005	C00000008000	9000D40000A0	Para todos los sistemas intermedios de la subred.
Todos los IS de L2	0180C2000015	C00000008000	800143000028	Para todos los sistemas intermedios de L2 de la subred.
Todos los IS de L1	0180C2000014	C00000008000	8001430000A8	Para todos los sistemas intermedios de L1 de la subred.

## Direccionamiento de OSI

OSI direcciona paquetes utilizando el protocolo IS-IS. El direccionamiento por medio del protocolo IS-IS se basa en:

- Un ID del sistema para el direccionamiento dentro de un área
- Una dirección de área para el direccionamiento dentro de un dominio
- El prefijo de dirección asequible para el direccionamiento fuera del dominio

El protocolo IS-IS utiliza tablas de direccionamiento para reenviar los paquetes a sus destinos correctos. Las entradas de tabla de direccionamiento se crean a partir de la información de la base de datos de estado de los enlaces o a partir de direcciones asequibles configuradas por el usuario. La base de datos de estado de los enlaces se crea a partir de la información recibida de la actualización del estado de los enlaces (LSU). Consulte la sección “Bases de datos de estado de los enlaces” en la página 382.

## Protocolo IS-IS

El protocolo IS-IS es un protocolo de direccionamiento dinámico de estado de enlace que detecta y aprende las rutas mejores hacia destinos asequibles. IS-IS puede percibir rápidamente cambios en la topología de un dominio y, después de un período corto de convergencia, calcular nuevas rutas. Para realizar esto, el IS utiliza los paquetes siguientes:

- Actualizaciones del estado de los enlaces (LSU) que el IS utiliza para mantener actualizada la información de la base de datos de estado de los enlaces.
- PDU de número de secuencia (SNP) para mantener sincronizada la base de datos y para asegurarse de que cada IS adyacente tenga conocimiento del Paquete del estado de los enlaces (LSP) más reciente de cada direccionador.
- Mensajes hello que los IS utilizan para descubrir, inicializar y mantener adyacencias con IS contiguos.

### Áreas IS-IS

Un área IS-IS es un conjunto de sistemas de subredes contiguas. La topología de cada área se oculta de las de las otras áreas para reducir tráfico de direccionamiento. Un IS de nivel 1 (L1) se utiliza para direccionar dentro de un área. Un IS de nivel 2 (L2) se utiliza para direccionar entre áreas o sobre la red troncal. Un IS que direcciona dentro de un área y sobre la red troncal se considera un IS de L1/L2.

### Dominio IS-IS

Un dominio IS-IS es un conjunto de normas, administradas por la misma autoridad, que todos los ES e IS deben seguir para asegurar la compatibilidad. Hay dos tipos de dominios que tienen que describirse, el dominio administrativo y el dominio de direccionamiento.

#### **Dominio administrativo**

Un dominio administrativo controla la organización de IS en dominios de direccionamiento así como las direcciones NSAP y de subred que utilizan estos dominios de direccionamiento.

#### **Dominio de direccionamiento**

Un dominio de direccionamiento es un conjunto de IS y ES controlados por las normas siguientes:

- Todos los dispositivos utilizan el mismo tipo de métrica de direccionamiento.
- Todos los dispositivos utilizan el mismo protocolo de direccionamiento, como, por ejemplo, IS-IS.

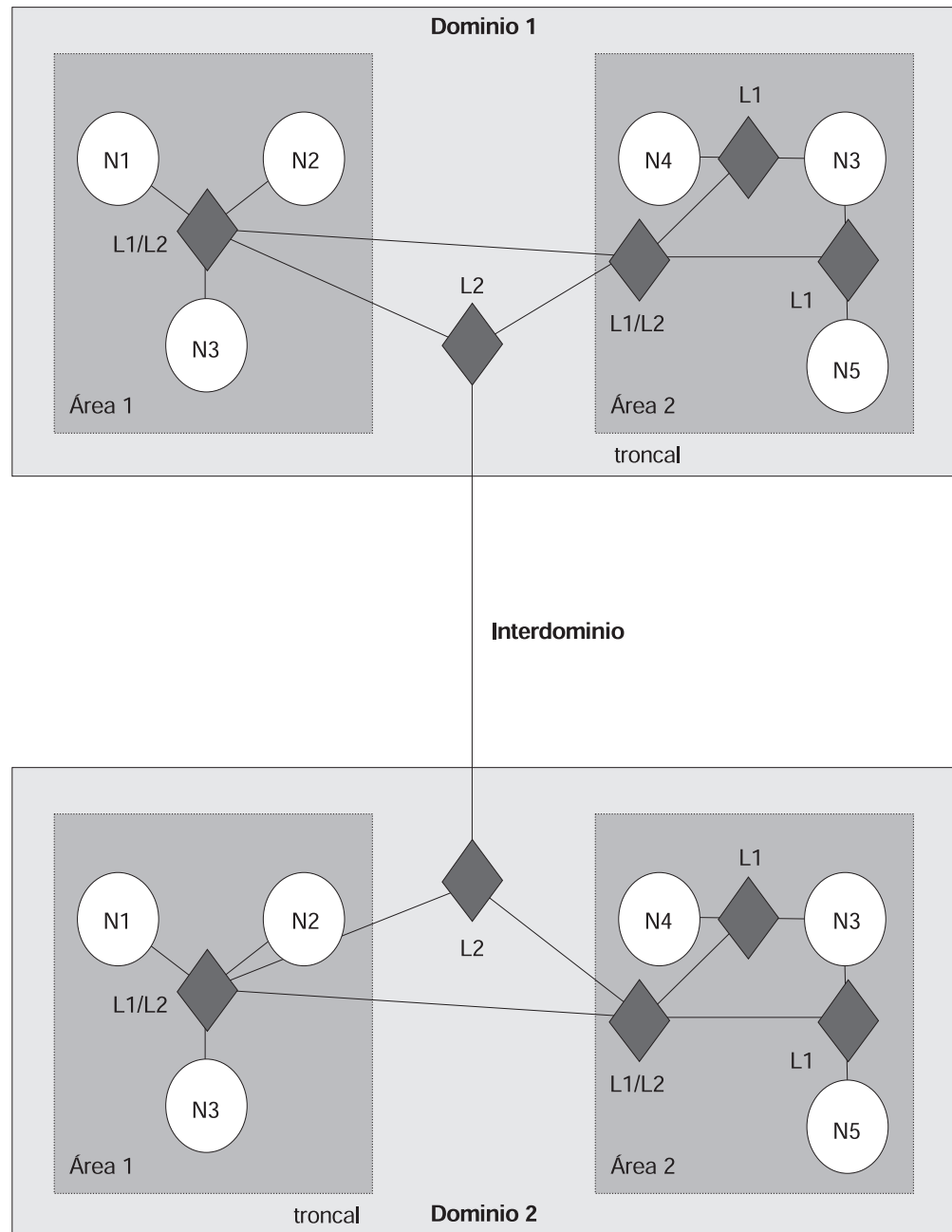


Figura 23. Dominio OSI

### Áreas sinónimas

Cuando un IS de L1 sirve a más de un área, estas áreas adicionales se denominan áreas sinónimas. Un direccionador puede dar soporte a un número cualquiera de áreas sinónimas mientras exista una solapa de una dirección de área, como mínimo, entre direccionadores adyacentes. Por ejemplo, en la Figura 24 en la página 380, el Área 1 y el Área 2 son áreas sinónimas entre sí y las Áreas 3 y 4 también son sinónimas entre sí.

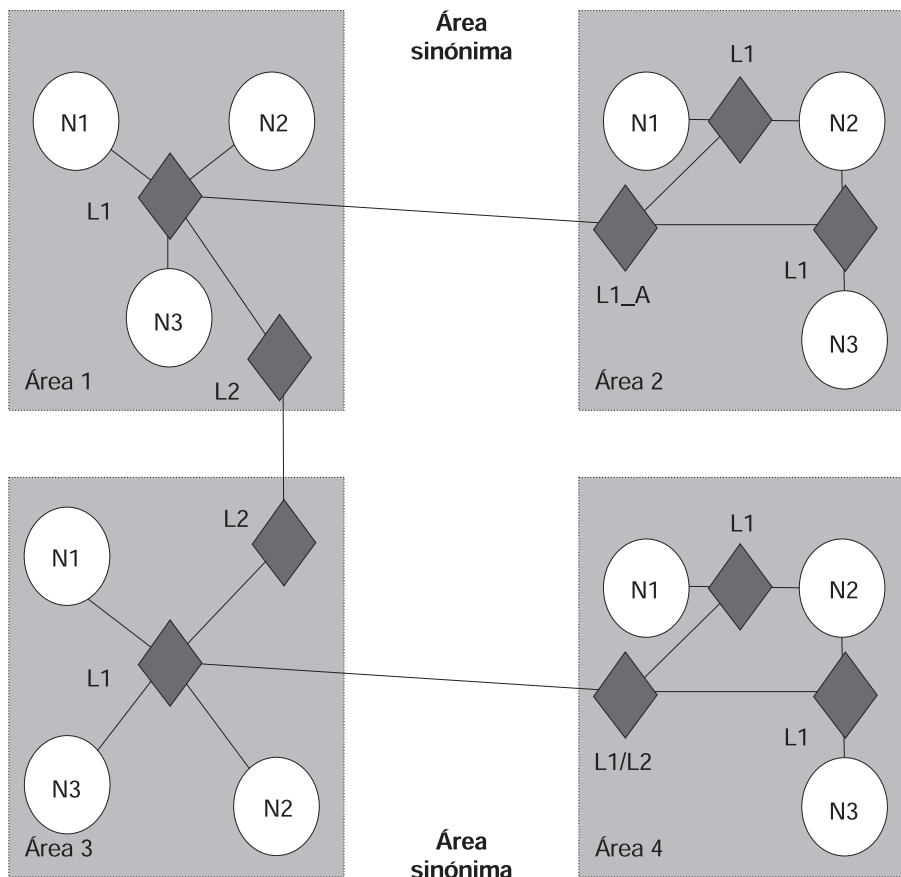


Figura 24. Áreas sinónimas

El IS de L1\_A del área 2 debe haber añadido la dirección del área 1 a su configuración y el IS de L1 del área 1 debe haber añadido la dirección del área 2 a su configuración. Para que las áreas 3 y 4 sean sinónimas, debe añadirse la dirección de cada área al otro IS de L1.

## Mensaje hello de IS a IS (IIH)

El mensaje IIH permite que un IS determine la existencia de otros IS y establezca adyacencias. Hay tres tipos de mensajes IIH: L1, L2 y punto a punto.

Cada IS contiene un temporizador de hello local y un temporizador de mantenimiento. Cada vez que el temporizador de hello caduca, se vierte de manera múltiple un IIH sobre la interfaz del IS para cualquier IS adyacente. Cuando se recibe el mensaje hello, el destinatario establece o actualiza (renueva) la información de la adyacencia. Esta información permanece actual durante el período de tiempo (segundos) especificado por el temporizador de mantenimiento. Si el temporizador de mantenimiento caduca, se descarta la adyacencia.

## Mensaje IIH de L1

El mensaje IIH de L1 se vierte de manera múltiple sobre la interfaz cuando caduca su temporizador de hello local. El IS de L1 coloca la información siguiente en su IIH:

- ID de origen
- Cualquier dirección de área manual a la que sirva

- Tipo de IS (sólo L1 ó L1/L2)
- Prioridad
- ID de LAN
- Si es aplicable, el ID del sistema del IS de L1 designado (pseudonodo)

Tras recibir el mensaje, el IS de L1 adyacente extrae el ID de origen del IS emisor. A continuación, este IS crea su propio mensaje IIH y coloca su ID de origen en el campo de ID de origen. El ID de origen del emisor se coloca en el campo de contiguo de IS. La devolución del ID del emisor es una verificación para el emisor de que el IS adyacente tiene conocimiento de su existencia (adyacencia de 2 direcciones).

Cuando el primer IS recibe el IIH, extrae también el ID de origen y observa el campo de contiguo de IS. Tras descubrir su propio ID de origen en el campo de contiguo de IS, este IS establece una adyacencia con el otro IS.

**Nota:** Para que el IS de L1 adyacente pueda aceptar el paquete, el paquete debe tener una dirección de área común y la misma longitud de ID del sistema que el IS adyacente.

## Mensaje IIH de L2

El IIH de L2 se vierte de manera múltiple sobre sus interfaces para la propia identificación ante otros IS de L2. En el IS de L2, la función es la misma que la de un IIH de L1. El IS de L2 coloca la información siguiente en el IIH:

- ID de origen
- Cualquier dirección de área manual a la que sirva
- Tipo de IS (sólo L2 ó L1/L2)
- Prioridad
- ID de LAN
- Si es aplicable, el ID del sistema del IS de L2 designado

**Nota:** Para que el IS de L2 adyacente pueda aceptar el paquete, dicho paquete debe tener la misma longitud de ID del sistema que el IS adyacente.

## Mensaje IIH punto a punto

Un mensaje IIH punto a punto se envía sobre una interfaz de no difusión de un IS (Frame Relay o X.25) para la propia identificación ante otros IS. Este IS facilita el IIH de modo que contenga la información siguiente:

- ID de origen
- Cualquier dirección de área manual a la que sirva
- Tipo de IS (sólo L1, sólo L2 ó L1/L2)
- ID de circuito local

## IS designado

Un IS designado se selecciona entre todos los IS conectados a la misma LAN para la realización de tareas adicionales. En particular, genera actualizaciones del estado de los enlaces en nombre de la LAN, la cual recibirá el trato de pseudonodo. Un pseudonodo es un método para modelar toda la LAN como un nodo en la red con menos enlaces lógicos. Al minimizar los enlaces lógicos en todo el dominio, se reduce la complejidad de cálculo del algoritmo de estado de enlace.

Cuando existe más de un IS en una LAN, cada IS compara lo siguiente para determinar qué IS se convertirá en el IS designado:

- Todos los IS comparan sus prioridades. El IS con la prioridad superior se convierte en el IS designado.
- Si los IS tienen la misma prioridad, comparan sus direcciones MAC de origen. El IS con la dirección MAC numéricamente superior se convierte en el IS designado para esa LAN y se indica por medio del ID de LAN.

### Bases de datos de estado de los enlaces

Cada IS de L1 y de L2 contiene una base de datos de estado de los enlaces. El elemento primario de la base de datos es la actualización del estado de los enlaces (LSU). El direccionador tiene la responsabilidad de crear su propia LSU y procesar las LSU de otros IS para mantener la base de datos. La base de datos de L1 contiene información sobre ES. Cada base de datos de L1 es idéntica para todos los IS de L1 de la misma área. La base de datos de L2 contiene información sobre áreas y direcciones asequibles. Cada base de datos de L2 es idéntica para todos los IS de L2 configurados del dominio IS-IS. Con información de las bases de datos, el algoritmo de direccionamiento Dijkstra calcula las vías de acceso más cortas hacia todos los destinos y crea las tablas de direccionamiento.

### Acumulación de estados de los enlaces

Para asegurarse de que cada IS de L1 y de L2 mantenga una base de datos idéntica, se acumulan LSU por toda un área o una red troncal. La acumulación es un mecanismo que utiliza un IS de L1 ó L2 para propagar una LSU por todos los IS de L1 ó L2. Un IS de L1 acumula LSU para los IS de L1 únicamente. Un IS de L2 acumula LSU para los IS de L2 únicamente. Un IS de L1/L2 acepta tanto LSU de L1 como LSU de L2.

### Actualización del estado de los enlaces de L1 (no pseudonodo)

La LSU de L1 se acumula para todos los IS de L1. El IS de L1 facilita la siguiente información en la LSU:

- ID de origen
- Cualquier dirección de área manual a la que sirva
- Tipo de IS (L1)
- ID del sistema y costes del acceso para las adyacencias de IS
- Si es aplicable, los ID del sistema de los pseudonodos adyacentes
- ID del sistema para cualquier adyacencia de ES manual

### Actualización del estado de los enlaces de L1 (pseudonodo)

La LSU de pseudonodo de L1 se acumula para todos los IS de L1 ubicados en el área. Cualquier IS de L1 ubicado en la misma LAN que reciba la LSU propaga la LSU por todos los IS de L1 adyacentes en sus otras subredes. El IS de L1 coloca la siguiente información en la LSU:

- ID de origen
- Tipo de IS (L1)
- ID del sistema y coste del acceso para todos los IS que no son pseudonodos ubicados en la LAN
- ID del sistema para cualquier adyacencia de ES aprendida por medio del protocolo ES-IS



### Actualización del estado de los enlaces de L2 (no pseudonodo)

La LSU de L2 se acumula para todos los IS de L2. El IS de L2 coloca la siguiente información en la LSU:

- ID de origen
- Conjunto de direcciones de área a las que sirve
- Tipo de IS (L2)
- ID del sistema y el coste del acceso para las adyacencias de IS
- Si es aplicable, el ID del sistema del pseudonodo
- Prefijos de dirección para los IS ubicados en un dominio externo

### Actualización del estado de los enlaces de L2 (pseudonodo)

La LSU de pseudonodo de L2 se vierte de manera múltiple sobre la interfaz y se propaga por todos los IS de L2 ubicados fuera de la subred. Cualquier IS que no sea un pseudonodo de L2 ubicado en la misma red que reciba la LSU retransmite la LSU a todos los L2 ubicados fuera de la subred. El IS de L2 coloca la siguiente información en la LSU:

- ID de origen
- Tipo de IS (L2)
- ID del sistema y métricas para los IS que no son pseudonodos ubicados en la misma subred

### IS de L2 conectados y sin conectar

Un IS de L2 conectado es un direccionador que tiene conocimiento de otras áreas. Un IS de L2 sin conectar es un direccionador que no tiene conocimiento de ninguna área que no sea la suya.

Durante el direccionamiento, un IS de L2 sin conectar direcciona paquetes al IS de L2 conectado más cercano.

## Tablas de direccionamiento

Un IS que sólo sea de L1 utiliza una sola tabla de direccionamiento, la tabla de direccionamiento de nivel 1. Un IS que sólo sea de L2 contiene tres tablas de direccionamiento: una tabla de direccionamiento de direcciones de área de L2, una tabla de direccionamiento de prefijos de dirección asequible de métrica interna de L2 y una tabla de direccionamiento de prefijos de dirección asequible de métrica externa de L2. Un IS de L1/L2 contiene la tabla de direccionamiento de L1 y todas las tablas de direccionamiento de L2. Las entradas de tabla de direccionamiento se crean a partir de la información de la base de datos de estado de los enlaces.

### Direccionamiento de L1

A continuación, se resumirá el direccionamiento de L1:

1. Un IS de L1 recibe un paquete y compara la parte de dirección de área de la dirección de destino de la cabecera del paquete con el conjunto de direcciones de área del direccionador.
2. Si el paquete va destinado al área del direccionador, éste extrae el ID del sistema de la dirección. Buscando una coincidencia, el direccionador compara el ID del sistema con los ID del sistema de la tabla de direccionamiento de L1.
3. Si aparece una coincidencia, el IS direcciona el paquete al ES o al IS de siguiente salto. Si no aparece ninguna coincidencia, se elimina el paquete.

4. Si el paquete no va destinado a esta área, el L1 reenvía el paquete al IS de L2 más próximo o, si este direccionador es un IS de L1/L2, comprueba las tablas de direccionamiento de L2 tal como se describe en la siguiente sección. Si el L1 no puede determinar dónde direccionar el paquete, dicho paquete se elimina.

### Direccionamiento de L2

Un IS de L2 contiene tres tablas de direccionamiento: una tabla de direccionamiento de direcciones de área de L2, una tabla de prefijos de dirección asequible de métrica interna (interna) y una tabla de prefijos de dirección asequible de métrica externa (externa).

A continuación, se resumirá el direccionamiento de L2:

1. Un IS de L2 recibe un paquete y compara la dirección de destino de la cabecera del paquete con el conjunto de direcciones de área de la tabla de direccionamiento de direcciones de área. Si existe una coincidencia, el paquete se reenvía al direccionador troncal de siguiente salto. Si no existe ninguna coincidencia, el direccionador comprueba la tabla de direccionamiento interna.
2. La tabla de direccionamiento interna contiene entradas de prefijos de dirección asequible que conducen a otros dominios. Si la tabla de direccionamiento interna contiene una coincidencia, el paquete se reenvía por la red troncal al dominio correspondiente. Si no existe ninguna coincidencia, el direccionador comprueba la tabla de direccionamiento externa.
3. La tabla de direccionamiento externa contiene entradas para prefijos de dirección asequible que también conducen a otros dominios. Si la tabla de direccionamiento externa contiene una coincidencia, el paquete se reenvía por la vía de acceso hacia el dominio correspondiente. Si no existe ninguna coincidencia, se elimina el paquete.

Consulte la sección "Direccionamiento interno y externo" en la página 385 para obtener una explicación detallada de la tabla de direccionamiento interna y la externa.

### Métrica del direccionamiento

La métrica del direccionamiento es un valor asociado con una función del circuito para indicar el coste del direccionamiento sobre este circuito. Por ejemplo, la métrica del direccionamiento basada en los gastos monetarios de un circuito utilizará un número bajo para indicar un gasto monetario bajo y un número elevado para indicar el gasto monetario elevado del direccionamiento de un paquete sobre ese circuito.

El protocolo de direccionamiento IS-IS utiliza cuatro métricas del direccionamiento: métrica por omisión, métrica de retardo, métrica de gasto y métrica de errores.

La implementación actual del protocolo OSI sólo utiliza la métrica por omisión de IS-IS. Por convenio, la métrica por omisión está destinada a medir la capacidad del circuito para manejar tráfico. Todos los IS del dominio de direccionamiento deben ser capaces de calcular rutas basándose en la métrica por omisión. Las otras métricas del direccionamiento son opcionales. Aunque no se utilizan en esta implementación del protocolo OSI, se describen a continuación solamente con fines informativos.

- La métrica de retardo mide el retardo del tránsito del circuito asociado.

- La métrica de gasto mide el coste monetario de la utilización del circuito asociado.
- La métrica de errores mide la probabilidad de errores residuales del circuito asociado.

### Direccionamiento interno y externo

El direccionamiento interno o externo implica la existencia de un IS de L2 que direcciona un paquete entre dos dominios individuales. Cuando tiene que direccionarse un paquete hacia otro dominio, el IS de L2 intenta que la dirección coincida con un prefijo de dirección asequible de la tabla de direccionamiento interna o de la externa. Las rutas internas y externas están basadas en el coste (métrica del direccionamiento) para el destino. El coste de una ruta interna toma en consideración el coste del direccionamiento dentro del dominio y el coste del direccionamiento al destino. El coste de una ruta externa sólo se basa en el coste del direccionamiento al destino fuera del dominio de direccionamiento. El IS elige la vía de acceso con el menor coste.

Por ejemplo, un paquete está destinado a ir desde el nodo A del dominio 1 hasta el nodo D del dominio 2 (Figura 25 en la página 386). El nodo A puede elegir dos vías de acceso para enviar el paquete, hacia el nodo B y luego hasta el D o hacia el nodo C y luego hasta el D. La manera en que los nodos B y C anuncian el coste de sus rutas al D determina la manera en que el nodo A decide direccionar el paquete, interna o externamente. Hay tres opciones posibles:

- Los nodos B y C anuncian el coste de sus rutas al D como de tipo interno. El coste interno de la ruta A-B-D es 35, que es el coste del direccionamiento del A al B más el coste del direccionamiento del B al D. El coste interno de la ruta A-C-D es 40, que es el coste del direccionamiento del A al C más el coste del direccionamiento del C al D. En este caso, el nodo A elegirá direccionar sobre la vía de acceso A-B-D porque el coste es menor.
- Los nodos B y C anuncian el coste de sus rutas como de tipo externo. El coste externo para A-B-D es 30, que es el coste del direccionamiento del B al D. El coste externo para A-C-D es 20. En este caso, el nodo A elegirá direccionar sobre la vía de acceso A-C-D porque el coste de esta ruta es menor.
- Los nodos B y C anuncian el coste de sus rutas como de tipo interno y externo. Se añaden el coste interno y el externo de las rutas a las tablas de direccionamiento respectivas. Puesto que se prefieren las rutas internas a las externas, el direccionador elige la ruta interna de A-B-D.

**Nota:** Ya que no existe un protocolo de direccionamiento exterior, todas las rutas de prefijo entre dominios deben configurarse de forma estática.

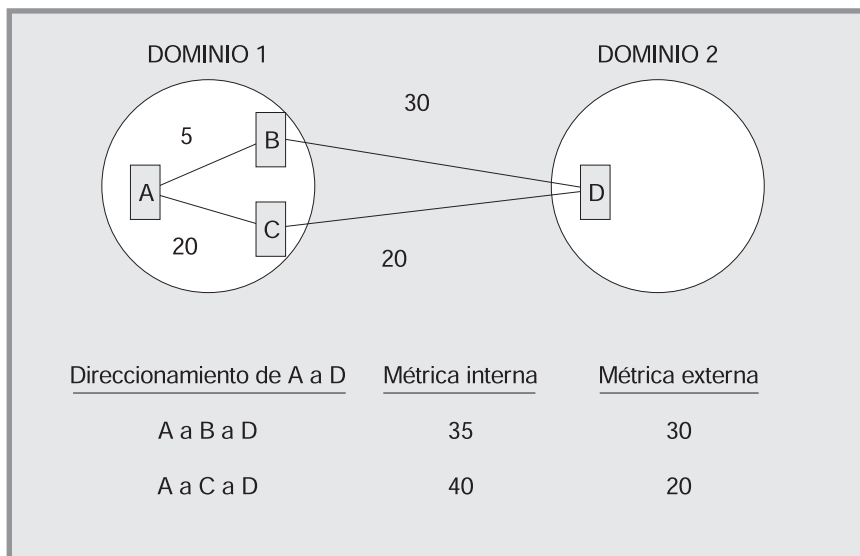


Figura 25. Métricas del direccionamiento interna y externa

## Codificación de prefijos de dirección

Cuando entre rutas de prefijo de dirección en el direccionador, tome atentamente en consideración la diferencia entre codificar normas para las NSAP y para las rutas de prefijo. Los cuatro ejemplos siguientes ilustran la codificación de prefijos de dirección.

### Codificación de un IDI de longitud fija

Para muchos prefijos de dirección, codificar el prefijo y la NSAP correspondiente es lo mismo. Por ejemplo, va a utilizar una dirección GOSIP 1.0 y desea crear una ruta hacia una organización del DdD. El IDI de la Org es 1234 y el IDI del DdD es 0006. La dirección NSAP codificada es

4700061234CCCC222222222222

El prefijo de dirección codificado es el resultado del truncamiento de la NSAP

4700061234

Las normas de codificación son para todos los formatos de NSAP con un IDI de longitud fija y para cualquier prefijo de dirección que termine después de la IDP.

### Codificación de un AFI

Un prefijo de dirección basado totalmente en el AFI sólo se codifica sobre el campo de AFI de 1 octeto. Por ejemplo, si es necesario un prefijo de dirección para todas las direcciones de formato X.121 (utilizadas en redes X.25), utilizará el AFI de X.121 con el valor de 37.

### Codificación de un IDI de longitud variable

Las direcciones NSAP que tienen formatos de IDI de longitud variable, como, por ejemplo, X.121, F.69, E.163 y E.164, utilizan un esquema de codificación más complicado. Cuando se codifican IDI de longitud variable como NSAP, se rellena la dirección hacia la izquierda con ceros; no obstante, cuando el IDI se codifica como prefijo de dirección, no hay relleno hacia la izquierda.

Por ejemplo, desea direccionar llamadas para X.25 desde los EE.UU. a una portadora de X.25 de los Países Bajos. La portadora tiene un Código de identificador de red de datos (NDIC) de 2041. La codificación del prefijo de dirección será

372041

Un abonado a X.25 que tenga un número telefónico nacional (NTN) de 117010 en esta portadora tendrá una NSAP de

3700002041117010

Observe que el IDI de la NSAP se ha rellenado hacia la izquierda con ceros hasta los 14 dígitos porque el número de los datos internacional resultante (2041117010) estaba por debajo de los 14 dígitos.

No obstante, si desea un prefijo de dirección que sólo remita a este abonado a X.25, la codificación será la NSAP (3700002041117010) porque el prefijo no termina en la IDP.

### **Prefijos de dirección por omisión**

Se utiliza un prefijo de dirección por omisión si se desea originar una ruta por omisión hacia todas las direcciones fuera del dominio. Los prefijos de dirección por omisión tienen una longitud de cero, por lo que no hay nada para codificar.

## **Contraseñas de autenticación**

Para proporcionar una capa mínima de seguridad a la red, OSI proporciona la opción de las contraseñas de autenticación. Cuando se habilite la autenticación, el IS no aceptará ningún paquete de IS-IS que no contenga la contraseña correcta. El campo de autenticación de la NPDU contiene las contraseñas de autenticación. Hay dos tipos de contraseñas de autenticación, la de transmisión y la de recepción.

Se añade una contraseña de transmisión a los paquetes de IS-IS transmitidos por el IS. Una contraseña de recepción es un listado de las contraseñas de transmisión que el IS acepta. Por ejemplo, con la autenticación habilitada, si no se ha añadido una contraseña de transmisión al paquete o no hay el listado de las contraseñas de transmisión en la base de datos de contraseña de recepción, se elimina el paquete. Hay tres tipos de contraseñas de transmisión y de recepción: dominio, área y circuito.

Una contraseña de dominio proporciona seguridad para la información de direccionamiento de L2. Una contraseña de área proporciona seguridad para la información de direccionamiento de L1. Una contraseña de circuito proporciona seguridad para los mensajes hello de IS-IS.

---

## **Protocolo ESIS**

El protocolo ES-IS permite que los ES e IS conectados a la misma subred descubran dinámicamente la existencia y disponibilidad de los otros entre sí. Esta información también permite que los ES obtengan información, los unos de los otros, sin un IS disponible.

La información de redireccionamiento por ruta permite que un IS informe a un ES de una ruta mejor al reenviar NPDU a un destino en particular. Por ejemplo, una ruta mejor puede ser otro IS de la misma subred que el ES o el ES de destino ubicado en la misma subred.

### Mensaje hello

Se pasa información de direccionamiento a los ES e IS mediante los mensajes hello.

Están presentes en cada ES e IS un temporizador de configuración (CT) local y un temporizador de mantenimiento (HT). Cada vez que caduca el CT, se vierte de manera múltiple un mensaje hello en la LAN. Cuando recibe el mensaje hello, el destinatario establece su valor de HT de acuerdo con el valor transmitido en el campo de HT del mensaje. Se espera que el destinatario retenga esta información hasta que caduque el HT para asegurar el funcionamiento correcto del protocolo ES-IS.

### Mensaje hello de sistema final (ESH)

El mensaje ESH se vierte de manera múltiple desde el ES para todos los IS de L1 cuando caduca el CT local. El ES crea este mensaje para informar a un IS de cualquier NSAP servida por él. Tras recibir este mensaje, el IS extrae la información de NSAP y SNPA y almacena el par en la tabla de direccionamiento de L1 para sustituir cualquier otra información que actualmente esté almacenada allí.

### Mensajes hello de sistema intermedio (ISH)

El mensaje ISH se vierte de manera múltiple en todos los ES adyacentes cuando caduca el CT local. El IS crea este mensaje para informar al ES de su NET. Tras recibir este mensaje, el ES extrae la información de NET y SNPA y almacena el par en una de las tablas de direccionamiento locales para sustituir cualquier otra información que actualmente esté almacenada allí.

---

## Circuitos X.25 para DECnet V/OSI

Para las redes X.25, el direccionador establece circuitos virtuales conmutados X.25 (SVC) sobre circuitos de direccionamiento.

**Nota:** Si desea habilitar DECnet V/OSI para X.25, debe entrar en el proceso de DECnet IV y definir el direccionador de manera que sea un direccionador DEC-AREA o DEC-ROUTING-IV. Debe hacer esto (y reiniciar el direccionador) para permitir que los mandatos realicen la configuración de DECnet V/OSI. Utilice el mandato **define executor type**.

## Circuitos de direccionamiento

Los circuitos de direccionamiento son conexiones punto a punto entre nodos que implementan el protocolo CLNS de la ISO. El direccionador emplea estos tipos de circuitos de direccionamiento:

- Circuitos de entrada estáticos
- Circuitos de salida estáticos
- Circuitos asignados dinámicamente

Los circuitos estáticos de entrada y de salida sólo tienen asociado un SVC y conllevan los datos de usuario y los datos que no son de usuario (como, por ejemplo, mensajes de protocolo de direccionamiento). Los circuitos estáticos se activan y desactivan explícitamente por medio de los mandatos de configuración de DECnet V/OSI. Los circuitos de direccionamiento asignados dinámicamente se establecen a la llegada de los datos y se eliminan cuando no se transmiten ni se reciben datos.

Un circuito asignado dinámicamente puede tener diversos SVC, pero sólo puede conllevar los datos de usuario.

DECnet V/OSI controla las llamadas para cada uno de los tipos de circuitos de direccionamiento utilizando *filtros* y *plantillas*. Los filtros se utilizan para procesar llamadas de entrada; las plantillas se utilizan para establecer llamadas de salida.

## Filtros

Un *filtro* es un conjunto de parámetros que el usuario puede configurar y que definen los criterios para aceptar todas las llamadas de entrada relativas al circuito de direccionamiento X.25 especificado.

Los parámetros definidos en un filtro incluyen la dirección del DTE que llama, una prioridad de filtro y los datos de usuario de llamada.

### Filtros y circuitos de direccionamiento

Puede haber llamadas de entrada para un circuito de entrada estático o para un circuito asignado dinámicamente (DA). Pueden definirse uno o más filtros para el mismo circuito de direccionamiento. Por ejemplo, un circuito DA puede tener diversas adyacencias y puede definirse más de un filtro para ese circuito de direccionamiento.

### Prioridades de los filtros

Los filtros de la lista relativos a circuitos de entrada estáticos y circuitos DA están entremezclados y ordenados por prioridades de modo descendente. Cuando se recibe una llamada de entrada, el direccionador realiza una búsqueda en la lista de filtros, la prioridad superior primero. Para evitar asignar erróneamente un circuito estático a un circuito DA, es recomendable que los filtros de todos los circuitos estáticos tengan asignada una prioridad más alta que los filtros de todos los circuitos DA.

### Restricciones de los filtros en las llamadas

Para un circuito de entrada estático, el filtro debe especificar una dirección determinada de DTE que llama, pero el primer octeto de los datos de usuario de llamada debe contener el Discriminador de protocolo de ISO 8473 (129). Con el fin de conseguir un funcionamiento correcto de los diversos circuitos DA, deben configurarse restricciones adicionales para cada filtro definido. Esto asegura que los criterios de selección especificados en estos filtros permitan que se efectúe la distinción necesaria entre las llamadas de entrada.

**Nota:** Si un circuito DA se conecta incorrectamente a un circuito estático, la arquitectura no intenta identificar la condición ni rectificar el problema. El mensaje normal que expresa una “anomalía en la inicialización” puede generarse en la parte del circuito estático debido a la ausencia de respuesta a sus consultas para la inicialización del enlace. El SVC estático se elimina a continuación.

## Plantillas

Una plantilla es un conjunto de parámetros que el usuario puede configurar para las llamadas de salida. Establece los parámetros de forma que el circuito del direccionador remoto acepte las llamadas de entrada. Los parámetros definidos en una plantilla incluyen la dirección del DTE que llama y los datos de usuario de llamada.

Sólo puede definir una plantilla por circuito de direccionamiento estático de salida.

### Inicialización del enlace

La inicialización del enlace es un procedimiento perteneciente a Digital Equipment Corporation (y no forma parte de OSI). La inicialización del enlace sigue inmediatamente al establecimiento de un SVC. Se utiliza principalmente para establecer la relación de DECnet con un sistema remoto en un enlace punto a punto.

Cuando se recibe un mensaje de XID/inicialización, puede efectuarse la verificación en dos niveles: sobre la base de un circuito o sobre la base de un sistema. Básicamente, el proceso de verificación compara los datos de verificación de entrada con los datos especificados localmente para el circuito o para el sistema que llama. Los datos de verificación aparecen en el campo de datos de verificación del mensaje de XID.

**Nota:** Este release del software del direccionador no da soporte a la verificación por medio del sistema.

---

### Configuración de OSI/DECnet V

**Nota:** Cuando trabaje con redes DNA IV y redes DNA V en conjunto, toda la configuración y supervisión de DNA IV debe realizarse desde el proceso de configuración de DNA IV en NCP>. Para obtener información sobre cómo configurar DNA IV, consulte el capítulo "Utilización de DNA IV" en la página 333. El uso del término "OSI" en este capítulo hace referencia a los entornos de OSI y DNA V a menos que se indique lo contrario.

### Procedimiento básico de la configuración

Esta sección perfila los pasos de configuración mínimos que tiene que seguir para activar y ejecutar el protocolo OSI/DNA V sobre una LAN (Ethernet o Red en Anillo o FDDI), redes de conmutación de paquetes X.25 y Frame Relay. Antes de empezar los procedimientos de configuración, utilice el mandato **list device** desde el proceso **config** para listar los números de interfaz de los diferentes dispositivos. Si desea explicaciones adicionales sobre mandatos de configuración, consulte los mandatos de configuración descritos en este capítulo.

**Nota:** Para que sean efectivos los nuevos cambios de configuración, debe reiniciar el direccionador.

Siga el procedimiento básico de la configuración indicado a continuación antes de empezar con los procedimientos especializados que se describen en las próximas secciones.

Establecimiento del título de entidad de red (NET)

Establezca el NET del direccionador utilizando el mandato **set network-entity-title**. El NET está compuesto por el ID del sistema del direccionador y su dirección de área. Utilice el mandato **list globals** para verificar si el NET se ha configurado correctamente.

Habilitación global de OSI

Permita que el software OSI se ejecute en el direccionador por medio del mandato **enable OSI**. Utilice el mandato **list globals** para verificar si se ha habilitado el protocolo OSI.



## Configuración de OSI sobre una LAN Ethernet o Red en Anillo FDDI

Para configurar el protocolo OSI de manera que se ejecute sobre una LAN Ethernet o Red en Anillo o FDDI, establezca la subred. Existe una correspondencia de una-para-una entre subredes e interfaces. Utilice el mandato **set subnet** para configurar todas las subredes LAN(Ethernet, Red en Anillo o FDDI). Utilice las direcciones de vertimiento múltiple por omisión para Ethernet. Cuando configure una Red en Anillo, utilice estas direcciones:

Parámetro	Dirección funcional 802.5
Todos los ES [09002B000004]	C00000004000
Todos los IS [09002B000005]	C00000008000
Todos los IS de L1 [0180C2000014]	C00000008000
Todos los IS de L2 [0180C2000015]	C00000008000

Cuando configure FDDI, utilice estas direcciones:

Parámetro	Dirección de vertimiento múltiple FDDI
Todos los ES [09002B000004]	9000D4000020
Todos los IS [09002B000005]	9000D40000A0
Todos los IS de L1 [0180C2000014]	800143000028
Todos los IS de L2 [0180C2000015]	8001430000A8

Utilice el mandato **list subnet detailed** o **list subnet summary** para verificar si ha configurado las subredes correctamente.

## Configuración de OSI sobre X.25 ó Frame Relay

Para configurar el protocolo OSI de manera que se ejecute sobre la interfaz X.25 ó Frame Relay, realice las acciones siguientes:

Establezca la subred.

Utilice el mandato **set subnet** para establecer la interfaz en X.25 ó FRL (Frame Relay). Utilice los valores por omisión para toda la información necesaria. Utilice el mandato **list subnet detailed** o **list subnet summary** para verificar si ha configurado las subredes correctamente.

Establezca el circuito virtual.

Utilice el mandato **set virtual-circuit** para configurar un circuito virtual X.25 ó Frame Relay.

**Nota:** El direccionador le solicitará una dirección de DTE. Para frame relay, entre el número de DLCI (Identificador de control de enlace de datos). Para X.25, entre la dirección de DTE de PSN.

## Configuración de un direccionador de DNA V para un entorno de DNA IV

Cuando configure un direccionador de DNA V, es posible que tenga que configurar una interfaz para que se ejecute en un entorno de DNA IV. Por ejemplo, si el direccionador va a conectarse a una red DNA V y a una red DNA IV o bien si se conecta un ES DNA IV a un direccionador de DNA V.

Antes de empezar con los pasos siguientes, utilice la sección precedente que corresponda para configurar OSI sobre una LAN, X.25 ó Frame Relay.

1. Entre en el proceso de configuración de DN. Salga de `OSI config>` y entre en `NCP>`. Utilice el mandato **protocol DN**.
2. Defina la dirección DNA global. Utilice el mandato **define executor address** para configurar el número de área y nodo DNA del direccionador.
3. Habilite DNA globalmente. Utilice el mandato **define executor state** para permitir que el protocolo DNA se ejecute en el direccionador.
4. Habilite el direccionamiento interáreas. Si el algoritmo de direccionamiento de L2 es el vector de distancia de nivel 2, utilice el mandato **define executor type area** para asegurarse de que este direccionador pueda intercambiar información de direccionamiento de nivel 2 de DNA IV.
5. Habilite el circuito DNA IV. Habilite el circuito que el direccionador utilizará para intercambiar la información de direccionamiento. Utilice el mandato **define circuit tipo state on**.

### Consideraciones sobre los algoritmos de DNA IV y DNA V

DNA IV utiliza un algoritmo de direccionamiento de vector de distancia. DNA V puede utilizar un algoritmo de direccionamiento de vector de distancia o un algoritmo de direccionamiento de estado de enlace. Se selecciona el algoritmo según los protocolos que se habiliten y se inhabiliten y cualquier combinación que pueda resultar de estos dos protocolos:

DNA IV inhabilitado y OSI/DNA V habilitado

Esta combinación se considera un entorno de OSI/DNA V puro y el algoritmo se establece automáticamente en estado de enlace de nivel 1 y 2 sin tener en cuenta cómo esté configurado el mandato **set algorithm**.

DNA IV habilitado y OSI/DNA V inhabilitado

Esta combinación se considera un entorno de DNA IV puro y el algoritmo se establece automáticamente en vector de distancia sin tener en cuenta cómo esté configurado el mandato **set algorithm**.

DNA IV habilitado y OSI/DNA V habilitado

Éste es un entorno mixto y la información sobre el algoritmo se configura y se lee en la SRAM. Utilice el mandato **set algorithm** para configurar esta información en la SRAM.

## Configuración y supervisión de OSI/DECnet V

Este capítulo describe los mandatos de configuración y supervisión de OSI/DECnet V e incluye los apartados siguientes:

- “Acceso al entorno de supervisión de OSI/DECnet V” en la página 421
- “Mandatos de supervisión de OSI/DECnet V” en la página 421

### Acceso al entorno de configuración de OSI

Para obtener información sobre cómo acceder al entorno de configuración de OSI, consulte “Cómo empezar (Introducción a la interfaz de usuario)” en la publicación *Nways Multiprotocol Access Services Guía del usuario de software*.

### Mandatos de configuración de OSI/DECnet V

Este apartado resume los mandatos de configuración de OSI y ofrece una explicación de los mismos. Los mandatos de configuración de OSI le permiten crear o modificar una configuración de OSI. Entre todos los mandatos de configuración de OSI después del indicador `OSI Config>`. Los valores por omisión para cualquier mandato y sus parámetros van encerrados entre corchetes inmediatamente después de la solicitud.

Los mandatos de configuración manipulan la base de datos de OSI permanente (SRAM).

*Tabla 108 (Página 1 de 2). Resumen de los mandatos de configuración de OSI*

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi.
Add	Añade áreas soportadas por este nodo; contraseñas de recepción con fines de autenticación; direcciones de prefijo para otros dominios; y alias
Change	Modifica algunos de los parámetros configurados con el mandato <b>add</b> .
Clear	Borra una contraseña de recepción, una contraseña de transmisión o la SRAM
Delete	Suprime áreas, PVC, direcciones de prefijo, adyacencias, alias, subredes y parámetros de circuito de direccionamiento X.25.
Disable	Inhabilita una subred, el protocolo OSI o un circuito de direccionamiento X.25.
Enable	Habilita una subred, el protocolo OSI o un circuito de direccionamiento X.25.
List	Visualiza la configuración actual en relación con las adyacencias, los alias, las contraseñas, los pvc, las direcciones de prefijo, las subredes, el algoritmo, phaseivpfx, la información global o los circuitos de direccionamiento X.25.

Tabla 108 (Página 2 de 2). Resumen de los mandatos de configuración de OSI	
Mandato	Función
Set	Configura las propiedades asociadas con los parámetros de OSI (conmutadores, globales, NET, temporizadores, subredes, contraseña de transmisión, direcciones de prefijo, adyacencias, pvc, el algoritmo y phaseivpfx)
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxi.

## Add

Utilice el mandato **add** para configurar direcciones de área y prefijo, contraseñas de recepción y alias de dirección.

### Sintaxis:

```
add          alias
              area...
              filter...
              prefix-address
              receive-password
              routing-circuit...
              template...
```

**alias** Añade una serie ASCII que designa una dirección de área o un ID del sistema en particular. La serie ASCII puede contener *a-z*, *A-Z*, *0-9* y otros caracteres más, que incluyen el guión ( - ), la coma ( , ) y el signo de subrayado ( \_ ). No utilice caracteres de escape.

El desplazamiento indica la posición, en semioctetos (porciones), donde empieza la serie ASCII dentro de la dirección (los alias utilizados para ID del sistema tienen un desplazamiento de 1). La serie debe tener el mismo tamaño o ser más larga que el segmento que designa o recibirá el mensaje `invalid segment length`. El tamaño máximo de alias permitido son 20 bytes.

**Nota:** Cuando utilice una entrada de alias, debe encerrarla entre corchetes. Por ejemplo: **I1\_update**  
**47[nuevonomb]99999000012341234.**

### Ejemplo:

```
add alias
Alias [ ]:
Segment [ ]:
Offset [1]:
```

**Alias** La serie de caracteres que desea utilizar

**Segment** El segmento de NSAP que el alias va a sustituir

**Offset** La ubicación del alias (en semioctetos de 4 bits) dentro de la NSAP. El desplazamiento se determina a partir del principio de la NSAP (izquierda) tal como se visualiza en el terminal.

### **area** *dir-área*

Añade direcciones de área adicionales (18 bytes como máximo) soportadas por el nodo. Un nodo de L1 que da soporte a otras áreas las considera sinónimas. Una dirección de área es la parte de área del NET configurado. Si intenta añadir una dirección de área duplicada, el direccionador visualizará un mensaje de error.

#### **Ejemplo:**

```
add area 47000580999999000012341234
```

**Nota:** Cuando añada áreas sinónimas a un nodo de L1, utilice el mandato **set globals** para configurar el número máximo de áreas sinónimas permitidas para este nodo. Todos los direccionadores de un área deben utilizar el mismo número máximo de áreas sinónimas. No pueden establecerse adyacencias si son diferentes.

### **filter** *nombre-filtro nombre-circuito-direccionamiento DTE-que-llama*

*DatosUsuario-llamada prioridad*

Añade parámetros en los que el direccionador basa su aceptación de llamadas a X.25 de entrada para un circuito de direccionamiento, tanto si es un circuito de entrada estático como si es un circuito asignado dinámicamente (DA).

El *nombre-filtro* es el nombre que da al filtro. El *nombre-circuito-direccionamiento* es el nombre del circuito de direccionamiento con el que está asociado el filtro.

El *DTE-que-llama* es la dirección del direccionador que llama.

El direccionador local comprueba la dirección de DTE de una llamada de entrada con una lista de filtros con prioridades para todos los circuitos. Una *prioridad* de filtro más alta en la lista significa que se efectúa primero una conexión con la dirección del DTE que llama para ese filtro. Es recomendable asignar una prioridad más alta a los filtros relacionados con circuitos estáticos que a los relacionados con circuitos DA. Esto puede impedir que se asigne a un circuito DA una llamada de entrada relacionada con un circuito estático.

Los *DatosUsuario-llamada* pueden tener uno de estos tres valores - *osi*, *dec* o *user*:

- Con *osi*, el direccionador automáticamente configura un discriminador de protocolo de la ISO para los datos de llamada y requiere que la llamada proceda de un nodo OSI.
- Con *dec*, el direccionador espera que las llamadas de entrada procedan de un direccionador de Digital Equipment Company.
- Con *user*, se le solicita una entrada adicional de un máximo de 16 octetos. Entre texto para restringir la aceptación de llamadas de entrada. El campo de *DatosUsuario-llamada* de la llamada de entrada debe coincidir con el texto especificado.

#### **Ejemplo:**

```
add filter
Filter Name [ ]:
Routing Circuit Name [ ]:
DTE Address [ ]:
Call UserData (OSI/DEC/USER):
```

## Mandatos de configuración de OSI/DECnet V (Talk 6)

Si selecciona **user**, aparecerá una solicitud adicional para que entre datos de usuario, seguida de la solicitud Priority:

```
(max 16 octets) [ ]?  
Priority (1-10) [5]?
```

### prefix-address

Añade rutas estáticas a destinos fuera del dominio IS-IS. Este parámetro le solicita información diferente según el tipo de subred (X.25, LAN o FRL) que se haya configurado utilizando el mandato **set subnet**.

**Nota:** Si no se entra ningún prefijo de dirección, se supone el prefijo por omisión.

### Ejemplo:

#### Subred LAN:

```
add prefix-address  
Interface Number [0]:  
Address Prefix [ ]:  
MAC Address [ ]:  
Default Metric [20]:  
Metric Type [Internal]:  
State [ON]:
```

#### Subred X.25:

```
add prefix-address  
Interface Number [0]:  
Address Prefix [ ]:  
Mapping Type[Manual]:  
DTE Address[]:  
Default Metric[20]:  
Metric Type [Internal]:  
State [ON]:
```

#### Subred Frame Relay:

```
add prefix-address  
Interface Number [0]:  
Address Prefix [ ]:  
DTE Address [ ]:  
Default Metric [20]:  
Metric Type [Internal]:  
State [ON]:
```

**Nota:** Si no existe la subred, recibirá el mensaje de error Subnet does not exist - cannot define a reachable address.

### Interface Number

Define la interfaz sobre la que se accede a la dirección

### Address Prefix

Define el prefijo de NSAP (20 bytes como máximo).

### MAC Address

Define la dirección MAC de destino. Debe especificar esta dirección si la interfaz corresponde a una subred LAN. Esta solicitud sólo aparecerá si la interfaz está conectada a una subred LAN.

### Mapping Type

Define cómo está determinada la dirección física de destino, manual o X.121.

Si es manual, el protocolo solicitará la dirección de DTE.

## Mandatos de configuración de OSI/DECnet V (Talk 6)

Si es X.121, el protocolo no le solicitará la dirección de DTE. La dirección de DTE en esta instancia se extrae de la NSAP.

### DTE Address

Define la dirección de DTE de destino. Debe especificar esta dirección si la interfaz es X.25 y el tipo de correlación es manual. Esta solicitud sólo aparecerá si la interfaz está configurada para X.25 y el tipo de correlación es manual.

### Default Metric

Define el coste de la dirección.

### Metric Type

Define si el coste de la métrica se utiliza para el direccionamiento externo (E) o el interno (I).

### State

Cuando se establece en ON, se anuncia esta dirección de prefijo a otros direccionadores de L2. Cuando se establece en OFF, es una dirección de prefijo no funcional.

## routing-circuit

Añade un canal de comunicaciones para circuitos virtuales conmutados (SVC) X.25 que la capa de direccionamiento utiliza para enviar y recibir datos.

El parámetro de circuito de direccionamiento sólo es aplicable si configura el direccionador como direccionador de tipo DEC. Puede especificar uno de estos tipos de circuitos de direccionamiento:

- un circuito estático de entrada
- un circuito estático de salida
- un circuito asignado dinámicamente

Un circuito estático de entrada maneja llamadas de entrada de tipo X.25. Un filtro de llamadas (vea **add filter**) especifica los datos que el direccionador utiliza para aceptar o rechazar llamadas de entrada para el circuito. Un circuito estático de salida inicia llamadas de salida de tipo X.25. El direccionador utiliza una plantilla de llamada (vea **add template**) para efectuar llamadas de salida. Un circuito asignado dinámicamente puede tener en ejecución diversos SVC simultáneamente. A diferencia de lo que sucede con los circuitos estáticos, el direccionador sólo utiliza un circuito asignado dinámicamente cuando entra tráfico en el direccionador o cuando sale del mismo. Cierra el circuito asignado dinámicamente después de que caduque un temporizador de inactividad.

El mandato **add routing-circuit** le solicita valores para sus parámetros.

### Ejemplo:

```
add routing-circuit
Interface number [0]?
Circuit Name [ ]?
Circuit Type (STATIC/DA) [STATIC]?
Circuit Direction (OUT/IN) [OUT]?
```

Si selecciona **STATIC** y **OUT**, aparecerán las solicitudes adicionales siguientes:

## Mandatos de configuración de OSI/DECnet V (Talk 6)

Recall Timer (0-65535) [60]?  
Max Call Attempts (0-255) [10]?  
Initial Min Timer (1-65535) [55]?  
Enable IS-IS [YES]?  
Level 2 only [NO]?  
External Domain [NO]?  
Default Metric [20]?  
ISIS Hello Timer [3]?  
Enable DECnetV Link Initialization [YES]?  
Modify Receive Verifier (YES/NO) [NO]?  
Transmit Verifier (YES/NO) [NO]?  
Explicit Receive Verification (TRUE/FALSE) [TRUE]?

Si selecciona **STATIC** e **IN**, aparecerán las solicitudes adicionales siguientes:

Initial Min Timer (1-65535) [55]?  
Enable IS-IS [YES]?  
Level 2 only [NO]?  
External Domain [NO]?  
Default Metric [20]?  
ISIS Hello Timer [3]?  
Enable DECnetV Link Initialization [YES]?  
Modify Receive Verifier (YES/NO) [NO]?  
Modify Transmit Verifier (YES/NO) [NO]?  
Explicit Receive Verification (TRUE/FALSE) [TRUE]?

Si selecciona **DA** para el tipo de circuito, aparecerán las solicitudes adicionales siguientes:

Recall Timer (0-65535) [60]?  
Reserve Timer (1-65536) [600]?  
Idle Timer (1-65536) [30]?  
Max SVCs (1-65535) [1]?

### Interface Number

Especifica la interfaz X.25 lógica para este circuito de direccionamiento.

### Circuit Name

Configura el nombre alfanumérico de este registro de circuito de direccionamiento.

### Circuit Type

Especifica si este circuito de direccionamiento es un circuito **STATIC** o **DYNAMICALLY ALLOCATED**.

### Circuit Direction

Especifica **IN** u **OUT** para determinar si el SVC del circuito estático se establecerá con una petición de llamada de entrada o una petición de llamada de salida. En ambos casos, el SVC se establece inicialmente después de la acción del operador, pero el circuito no está habilitado por completo hasta que ambos extremos del mismo se han inicializado satisfactoriamente.

### Recall Timer

Define el período en segundos durante el cual debe esperar un circuito estático de salida o un circuito **DA** antes de intentar una nueva petición de llamada. Es resultado de haberse producido una anomalía en la petición de llamada inicial o de haber eliminado una llamada subsiguiente.



### **Max Call Attempts**

Si falla una petición de llamada, Max Call Attempts define el número máximo de peticiones de llamada subsiguientes que intenta el circuito estático de salida antes de no efectuar más intentos. En este punto, se anota cronológicamente una anomalía de llamada y es necesaria la intervención del operador para activar el circuito estático de salida.

### **Initial Min Timer**

Especifica el período de tiempo (en segundos) durante el cual un circuito estático de salida espera a que se inicialice un enlace (recepción de un ESH o un ISH) después de que se haya aceptado la petición de llamada. Si Initial Min Timer caduca antes de que el enlace se haya inicializado completamente, el SVC se elimina y se genera un suceso que indica una anomalía en la inicialización.

### **Enable IS-IS**

Define si se habilita el protocolo IS-IS en este circuito de direccionamiento. Cuando se activa, se habilita el protocolo IS-IS; cuando se desactiva, no se habilita el protocolo IS-IS.

### **Level2 Only**

Especifica si se utiliza este circuito de direccionamiento para el direccionamiento de nivel 2 únicamente.

### **External Domain**

Especifica si el direccionador transmite/recibe mensajes dirigidos hacia/procedentes de un dominio que es externo a su dominio de direccionamiento IS-IS.

### **Default Metric**

Define el coste de esta dirección.

### **ISIS Hello Timer**

Define el intervalo de tiempo entre las transmisiones de mensajes hello de ISIS.

### **Enable DECnetV Link Initialization**

Define si se habilita (YES) o no (NO) la inicialización de enlace de tipo DEC para este circuito.

### **Modify Receive Verifier**

Especifica los datos de verificación con los que se realizará una comprobación después de que se reciba un XID cuando se verifica según circuito.

### **Modify Transmit Verifier**

Especifica los datos de verificación que se incluirán en el XID.

### **Explicit Receive Verification**

Define si la verificación es según circuito o según sistema. TRUE especifica una verificación según circuito, y FALSE especifica según sistema.

### **Reserve Timer**

Define el período de tiempo existente después de que caduque el temporizador de inactividad durante el cual el direccionador todavía considera que un nodo remoto de un

circuito DA está "activo". El direccionador puede reenviar datos sobre el circuito DA hasta que caduque el temporizador de reserva.

### Idle Timer

Define el período de tiempo durante el cual puede estar desocupada (sin transmisión de datos) una adyacencia DA antes de que se elimine.

### Max SVCs

Define el número máximo de adyacencias de SVC soportadas por este circuito DA. Si no puede efectuarse ninguna llamada porque se ha alcanzado el número máximo de adyacencias de SVC, se genera un suceso que indica la acción de "sobrepasar el número máximo de adyacencias de SVC".

### receive-password

Añade una serie de caracteres ASCII (16 caracteres como máximo) que autentica todos los paquetes de entrada. Un paquete de entrada cuya contraseña coincida con una del conjunto de las contraseñas de recepción se procesa en el IS; cualquier paquete de entrada cuya contraseña no coincida se elimina.

#### Ejemplo:

```
add receive-password
```

**Nota:** Obtendrá un mensaje de error si utiliza un valor no válido para *Password type*.

```
Password type [Domain]:  
Password [ ]:  
Reenter password:
```

#### Password type

Designa uno de los dos tipos de contraseñas: *domain* o *area*.

Las contraseñas de dominio se utilizan con LSP de L2 (paquetes del estado de los enlaces de nivel 2) y SNP (PDU de número de secuencia).

Las contraseñas de área se utilizan con LSP de L1 y SNP.

#### Password

Designa la serie de caracteres que va a utilizar para la autenticación. El tamaño máximo de serie permitido son 16 caracteres.

**template** *nombre-plantilla nombre-circuito-direccionamiento DTE-destino*  
*DatosUsuario-llamada*

Crea una plantilla según la cual el direccionador efectúa llamadas de salida para un circuito de direccionamiento estático de salida. Las plantillas para circuitos estáticos de salida son análogas a los filtros para circuitos estáticos de entrada.

El *nombre-plantilla* es el nombre que da a la plantilla. El *nombre-circuito-direccionamiento* es el nombre del circuito de direccionamiento con el que está asociada la plantilla.

El *DTE-destino* es una dirección para el direccionador remoto de un máximo de 14 dígitos.

Los *DatosUsuario-llamada* deben coincidir con los datos de llamada configurados para un filtro en el circuito remoto. *DatosUsuario-llamada* puede tener uno de estos tres valores - *osi*, *dec* o *user*.

- Con *osi*, el direccionador automáticamente configura un discriminador de protocolo de la ISO para los datos de llamada y requiere que la llamada se dirija a un direccionador de OSI.
- Con *dec*, los datos de usuario identifican las llamadas de salida como procedentes de un direccionador de Digital Equipment Company.
- Con *user*, se le solicita una entrada adicional de un máximo de 16 octetos. Entre texto que coincida con los datos de usuario del filtro correspondiente en un direccionador remoto.

### Ejemplo:

```
add template
  Template Name []?
  Routing Circuit Name []?
  DTE Address []?
  Call UserData (OSI/DEC/USER) ?
```

Si elige **user**, aparecerá esta solicitud adicional:

```
(max 16 octets) [] ?
```

Entre hasta 16 octetos de texto para los datos de usuario.

## Change

Le permite modificar los parámetros de los registros de ISO/DNV creados en la base de datos permanente.

### Sintaxis:

```
change          filter
                  prefix-address
                  routing-circuit
                  template
```

### **filter** nombre-filtro

Cambia los valores de los parámetros de filtro de circuito de direccionamiento. Puede entrar un nombre de filtro o dejar que el direccionador le solicite el nombre de filtro.

Los valores entre corchetes [] son los valores actuales de los parámetros; el valor configurado que se lee en la base de datos permanente.

### Ejemplo: change filter

```
Filter Name [valoractual]?
DTE Address [valoractual]?
Call Userdata (OSI/DEC/USER)? [valoractual]?
```

Si selecciona **user**, aparecerá esta solicitud adicional para que entre datos de usuario, seguida de la solicitud Priority:

```
(max 16 octets) [valoractual] ?
```

### prefix-address

Cambia los datos de dirección para las subredes. El direccionador le solicita los datos de dirección.

#### Ejemplo: change prefix-address

##### Subred LAN:

Interface Number [0]:  
Address Prefix [ ]:  
MAC Address [ ]:  
Default Metric [20]:  
Metric Type [Internal]:  
State [ON]?

##### Subred X.25:

Interface Number [0]:  
Address Prefix [ ]:  
Mapping Type [Manual]:  
DTE Address [ ]:  
Default Metric [20]:  
Metric Type [Internal]:  
State [ON]?

##### Subred Frame Relay:

Interface Number [0]:  
Address Prefix [ ]:  
DTE Address [ ]:  
Default Metric [20]:  
Metric Type [Internal]:  
State [ON]?

### Interface Number

Indica la interfaz sobre la que se accede a la dirección.

### Address Prefix

Indica el prefijo de NSAP de destino (20 bytes como máximo).

### MAC Address

Indica la dirección MAC de destino. Debe especificar esta dirección si la interfaz corresponde a una subred LAN. Esta solicitud sólo aparecerá si la interfaz está conectada a una subred LAN.

### Mapping Type

Indica cómo está determinada la dirección física de destino, *manual* o *X.121*.

Si es manual, el protocolo le solicitará la dirección de DTE.

Si es X.121, el protocolo no le solicitará la dirección de DTE. La dirección de DTE en esta instancia se extrae de la NSAP.

### DTE Address

Define la dirección de DTE de destino. Debe especificar esta dirección si la interfaz es X.25 y el tipo de correlación es manual. Esta solicitud sólo aparecerá si la interfaz está configurada para X.25 y el tipo de correlación es manual.

### Default Metric

Indica el coste de la dirección.

### Metric Type

Indica si el coste de la métrica se utiliza para el direccionamiento externo (E) o el interno (I).

## Mandatos de configuración de OSI/DECnet V (Talk 6)

**State** Cuando se establezca en ON, esta dirección recibirá paquetes. Cuando se establece en OFF, es una dirección no funcional.

### **routing-circuit** *nombrcircuitodireccionamiento*

Cambia los valores de la configuración para un circuito de direccionamiento. Puede entrar un nombre de circuito de direccionamiento o dejar que el direccionador le solicite un nombre. Los valores entre corchetes [] son los valores actuales tomados de la base de datos permanente.

#### **Ejemplo: change routing-circuit**

```
Routing Circuit Name [valoractual]?
Recall Timer (0-65535) [valoractual]?
Max Call Attempts (0-255) [valoractual]?
Initial Min Timer (1-65535) [valoractual]?
Enable ES-IS [valoractual]?
Enable IS-IS [valoractual]?
Level 2 only [valoractual]?
External Domain [valoractual]?
Default Metric [valoractual]?
ISIS IS Hello Timer [valoractual]?
ISIS Hello Timer [valoractual]?
Enable DECnetV Link Initialization [valoractual]?
Modify Receive Verifier (YES/NO) [valoractual]?
Modify Transmit Verifier (YES/NO) [valoractual]?
Explicit Receive Verification (TRUE/FALSE) [valoractual]?
```

### **template** *nombre-plantilla*

Cambia los valores de la plantilla para un circuito de direccionamiento estático de salida. Puede entrar un nombre de plantilla o dejar que el direccionador le solicite un nombre de plantilla. Los valores entre corchetes [] son los valores actuales de los parámetros; los valores configurados que se leen en la base de datos permanente.

#### **Ejemplo: change template**

```
Template Name [valoractual]?
DTE Address [valoractual]?
Call UserData (OSI/DEC/USER)? [valoractual]
```

Si selecciona **user**, aparecerá esta solicitud adicional para que entre datos de usuario, seguida de la solicitud Priority:

```
(max 16 octets) [valoractual] ?
Priority (1-10) [valoractual]?
```

## Clear

Utilice el mandato clear para borrar la SRAM o bien para eliminar la contraseña de recepción o de transmisión.

### **Sintaxis:**

```
clear          rreceive-password
                sram
                transmit-password
```

### **receive-password**

Elimina todas las contraseñas de recepción configuradas anteriormente por medio del mandato **add receive-password**.

**Nota:** Recibirá un mensaje de error si utiliza un tipo de contraseña no válido.

## Mandatos de configuración de OSI/DECnet V (Talk 6)

### Ejemplo: `clear receive`

Password Type [Domain]:

### Password Type

Especifica el tipo de contraseña que se utiliza: *Domain* o *Area*. Consulte el mandato **add receive-password** para obtener una descripción de estas contraseñas.

## SRAM

Utilice este parámetro para borrar la configuración de OSI de la SRAM.

**Atención:** Utilice este mandato **sólo** si piensa borrar la configuración.

### Ejemplo:

```
clear sram
Warning: All OSI SRAM Information will be erased.
Do you want to continue? (Y/N) [N]?
```

## Transmit-password

Elimina la contraseña de transmisión configurada anteriormente por medio del mandato **set transmit-password**. La salida para este parámetro es la misma que la del parámetro `receive-password`.

**Nota:** Recibirá un mensaje de error si utiliza un tipo de contraseña no válido.

### Ejemplo:

```
clear password transmit
Password Type [Domain]:
```

## Delete

Utilice el mandato **delete** para eliminar parámetros configurados anteriormente por medio del mandato **set** o **add**.

### Sintaxis:

delete                    adjacency  
                              alias  
                              area  
                              filter (sólo configuración de DEC)  
                              prefix-address  
                              routing-circuit  
                              subnet  
                              template (sólo configuración de DEC)  
                              virtual-circuit

### **adjacency**

Elimina una adyacencia de ES configurada estáticamente que se haya configurado anteriormente con el mandato **set adjacency**.

### Ejemplo:

```
delete adjacency
Interface Number [0]?
Area Address [ ]?
System ID [ ]?
```

### Interface number

Indica la interfaz de la adyacencia.

### Area address

Indica la dirección de área de la adyacencia.

### System ID

Indica la parte del NET que identifica a la adyacencia dentro del área.

**alias** Elimina la serie ASCII que designa la parte de una dirección de área o un ID del sistema.

### Ejemplo:

```
delete alias  
ALIAS [ ]?
```

### area *dirección*

Elimina la dirección de área (*dirección*) configurada anteriormente con el mandato **add area**.

### Ejemplo:

```
delete area 47000580999999000012341234
```

### filter *nombre-filtro*

Elimina el registro de un filtro de la base de datos permanente.

### Ejemplo:

```
delete p_systems
```

### prefix-address

Elimina la dirección de prefijo configurada anteriormente con el mandato **set prefix-address**.

### Ejemplo: delete prefix-address

```
Interface Number [0]?  
Address Prefix [ ]
```

### Interface number

Indica el número de interfaz sobre el que está configurada la dirección de prefijo.

### Address Prefix

Indica el prefijo de NSAP de destino.

### Interface number

Indica el número de interfaz sobre el que está configurado el PVC.

### DTE address

Indica la dirección de DTE de la red X.25 a la que desea conectarse o el DLCI de la red Frame Relay a la que desea conectarse.

### routing-circuit *nombre-circuito-direccionamiento*

Elimina un circuito de direccionamiento X.25 establecido con **add routing-circuit** de la base de datos permanente.

### Ejemplo:

```
delete routing-circuit p_system2
```

## Mandatos de configuración de OSI/DECnet V (Talk 6)

### **subnet** *interfaznúmero.*

Elimina una subred que se haya configurado anteriormente con el mandato **set subnet**. *interfaznúmero.* indica el número de interfaz de la subred configurada.

#### **Ejemplo:**

```
delete subnet 1
```

### **template** *nombre-plantilla*

Elimina de la base de datos permanente la plantilla para un circuito de direccionamiento de salida mediante el cual el direccionador genera mensajes de X.25 de salida.

#### **Ejemplo:**

```
delete template x25_5
```

### **virtual-circuit**

Elimina un circuito virtual X.25 ó Frame Relay que se haya configurado anteriormente con el mandato **set virtual-circuit**.

#### **Ejemplo:**

```
delete virtual-circuit  
Interface number [0]?  
DTE address []?
```

#### **Interface number**

El número de interfaz sobre el que está configurado el circuito virtual.

#### **DTE address**

La dirección de DTE de la red X.25 a la que desea conectarse o el DLCI de la red Frame Relay a la que desea conectarse.

## Disable

Utilice el mandato **disable** para inhabilitar las funciones habilitadas anteriormente con el mandato **enable**.

### **Sintaxis:**

```
disable          osi  
  
                  routing-circuit  
  
                  subnet
```

**osi**            Inhabilita el protocolo OSI en el direccionador.

**routing-circuit** *nombre-circuito-direccionamiento*

Inhabilita el circuito de direccionamiento especificado.

Utilice el mandato **add routing-circuit** para configurar circuitos de direccionamiento.

**subnet** *interfaznúmero.*

Inhabilita el protocolo OSI en la subred especificada (*interfaznúmero.*).

#### **Ejemplo:**

```
disable subnet 0
```



## Enable

Utilice el mandato **enable** para habilitar el protocolo OSI o una subred OSI.

### Sintaxis:

```
enable      osi
              routing-circuit...
              subnet...
```

**osi** Habilita el protocolo OSI en el direccionador.

**routing-circuit** *nombre-circuito-direccionamiento*

Habilita el circuito de direccionamiento especificado.

Utilice el mandato **add routing-circuit** para configurar circuitos de direccionamiento.

### Ejemplo:

```
enable routing-circuit p_system2
```

**subnet** *interfaz*núm.

Habilita el protocolo OSI en la subred especificada (*interfaz*núm.).

### Ejemplo:

```
enable subnet 0
```

## List

Utilice el mandato **list** para visualizar la configuración actual del protocolo OSI.

### Sintaxis:

```
list      adjacencias
           algorithm
           alias
           filter (sólo configuración de DEC)
           globals
           password
           phaseivpfx
           prefix-address
           routing-circuits (sólo configuración de DEC)
           subnets
           templates (sólo configuración de DEC)
           timers
           virtual-circuits
```

### adjacencies

Visualiza todas las adyacencias de ES configuradas estáticamente.

### Ejemplo:

```
list adjacencies
Ifc  Area Address  System ID  MAC Address
0    0001-0203-0405  0001-0203-0405
1    0002-4000-0000  0000-0019-3004
```

## Mandatos de configuración de OSI/DECnet V (Talk 6)

**lfc** Indica el número de interfaz que conecta con la adyacencia.

### Area Address

Indica la dirección de área de esta adyacencia de ES.

### System ID

Indica la parte del NET que identifica a la adyacencia.

### MAC Address

Indica la dirección MAC (SNPA) de la adyacencia.

## algorithm

Visualiza el algoritmo de direccionamiento que está configurado en la SRAM para el protocolo DNA V. Si sólo ejecuta el protocolo OSI, este parámetro no está soportado.

### Ejemplo:

```
list algorithm
Level 1 algorithm LINK_STATE
Level 2 algorithm DISTANCE_VECTOR
```

### Level 1 Algorithm

Indica la configuración actual del algoritmo de direccionamiento para el nivel 1, Link State (el valor por omisión) o Distance Vector.

### Level 2 Algorithm

Indica la configuración actual del algoritmo de direccionamiento para el nivel 2, Link State o Distance Vector (el valor por omisión).

**Nota:** Según esté habilitado o inhabilitado DNA IV, el algoritmo de direccionamiento visualizado aquí puede ser diferente del que se ejecute en el direccionador.

**alias** Visualiza los alias configurados y sus segmentos de dirección correspondientes.

### Ejemplo:

```
list aliases
Alias      Segment      Offset
joplin    AA0004000104      1
moon      0000931004F0      1
trane     000093E0107A      1
```

**filter** Visualiza los filtros definidos para circuitos X.25.

### Ejemplo:

```
list filters
Rout Cir Name  Filter Name  DTE Addr  Pri  Call Data
routeCir2     filter1     25        5    81
```

**globals** Visualiza el NET, las direcciones de área, los valores de conmutación, los parámetros globales y la configuración de temporizadores actuales del direccionador.

### Ejemplo:

## Mandatos de configuración de OSI/DECnet V (Talk 6)

### list globals

DNAV State: Enabled\* Network Entity Title: 4700050001:0000931004F0  
Manual Area Addresses:  
1. 4700050001 2. 7700050011

### Switches:

ESIS Checksum = On ESIS Init Option = Off  
Authentication = Off

### Globals:

IS Type = L2	System ID Length = 6
L1 LSP Size = 1492 bytes	L2 LSP Size = 1492 bytes
Max IS Adjs = 50	Max ES Adjs = 200
Max Areas = 50	Max ESs per Area = 50
Max Ifc Prefix Adds = 100	Max Ext Prefix Adds = 100
Max Synonymous Areas = 3	Max Link State Updates = 100

### OSI State o DNAV State

Indica si se ejecuta el protocolo OSI o DNA V en el direccionador.

### Network Entity Title

Indica la dirección de área y el ID del sistema que componen el NET del direccionador.

### Manual Area Addresses

Las áreas en las que opera el direccionador. La primera dirección de área refleja la dirección de área del NET configurado del direccionador. Las direcciones de área adicionales se han añadido con el mandato **add area**.

**Globals:** Indica los parámetros globales que están actualmente configurados:

#### IS Type

La designación del direccionador en el entorno de OSI: L1 ó L2.

#### Domain ID Length

El tamaño (en bytes) de la parte de ID del sistema del NET.

**Nota:** Todos los direccionadores del dominio deben coincidir en la longitud del ID de dominio.

#### L1 LSP Size/L2 LSP Size

Visualiza el tamaño máximo de almacenamiento intermedio de LSP de L1 y L2.

#### Max IS Adjacencies/Max ES Adjacencies

Visualiza el número máximo de adyacencias de ES e IS que están permitidas para todos los circuitos.

#### Max Areas

Visualiza el número máximo de áreas del dominio de direccionamiento.

#### Max ESs per Area

Visualiza el número máximo de ES permitidos en un área.

#### Max Int Prefix Adds

Visualiza el número máximo de direcciones de prefijo internas.

#### Max Ext Prefix Adds

Visualiza el número máximo de direcciones de prefijo externas.

### Max Synonymous Areas

Visualiza el número máximo de áreas de nivel 1 a las que sirve este direccionador.

### password

Visualiza el número de contraseñas de transmisión y recepción configuradas para cada área y dominio OSI. Puede configurar contraseñas de recepción utilizando el mandato **add receive-password**. Las contraseñas de transmisión se configuran por medio del mandato **set transmit-password**.

#### Ejemplo:

```
list password
Number of Passwords Configured:
  -- Domain --
  Transmit = 3
  Receive  = 2
  -- Area --
  Transmit = 4
  Receive  = 6
```

### phaseivpfx

Visualiza el prefijo de dirección de DNA phase IV configurado que el protocolo OSI utiliza para direccionar paquetes a una red DNA IV conectada.

#### Ejemplo:

```
list phaseivpfx
Local Phase IV Prefix: 49
```

### prefix-address

Visualiza todos los SNPA para las rutas configuradas estáticamente.

#### Ejemplo:

```
list prefix:-addresses
Ifc Type Metric State Address Prefix Dest Phys Address
0 INT 20 On 470006 302198112233
1 EXT 50 OFF 470006 302198223344
```

**Ifc** Indica el número de interfaz donde puede accederse a la dirección.

**Type** Indica el tipo de métrica, interna (INT) o externa (EXT).

**Metric** Indica el coste de la dirección asequible.

#### Address prefix

Indica el prefijo de NSAP de destino. La longitud de este prefijo puede ser de 20 bytes.

#### Dest Phys Address

Indica la dirección de DTE de destino si esta interfaz es X.25 y la correlación configurada es manual.

### routing-circuits

Visualiza un resumen de todos los circuitos de direccionamiento o información detallada de cada circuito de direccionamiento.

#### Ejemplo:

## Mandatos de configuración de OSI/DECnet V (Talk 6)

### list routing circuits

Summary or Detailed [Summary]? Summary

Ifc	Name	Type	Enabled
0	routecir1	STATIC-OUT	YES
0	routecir2	STATIC-IN	YES
0	routecir3	DA	YES

Summary or Detailed [Summary]? Detailed

```
Routing Circuit Name [] routecir2
Interface #:          0
Enabled:              YES
Type:                 STATIC
Direction:           Incoming
Initial Minimum Timer: 55
Enable IS-IS:        YES
L2 Only:              NO
External Domain:     NO
Metric:               20
IS-IS Hello Timer:   3
DECnetV Link Initialization: YES
Receive Verifier:
Transmit Verifier:
Explicit Receive Verification: TRUE
```

### Interface # / Ifc

La interfaz X.25 lógica para este circuito de direccionamiento.

**Name** El nombre alfanumérico de este registro de circuito de direccionamiento.

**Enabled** Indica el estado del circuito de direccionamiento: YES si está habilitado, NO si está inhabilitado.

**Type** Indica si el circuito es STATIC-IN, STATIC-OUT o DA (asignado dinámicamente).

**Direction** Indica cómo establece el direccionador un circuito de direccionamiento estático: mediante una petición de llamada de entrada (IN) o una petición de llamada de salida (OUT).

En cualquier caso, el SVC se establece inicialmente después de la acción del operador, pero el circuito no está habilitado por completo hasta que ambos extremos del mismo se han inicializado satisfactoriamente.

### Initial Min Timer

El período de tiempo (en segundos) durante el cual un circuito estático de salida espera a que se inicialice un enlace (recepción de un ESH o un ISH) después de que se haya aceptado la petición de llamada. Si Initial Min Timer caduca antes de que el enlace se haya inicializado completamente, el SVC se elimina y se genera un suceso que indica una anomalía en la inicialización.

### Enable IS-IS

Indica si se ha habilitado el protocolo IS-IS en este circuito.

**L2 Only** Indica si se utiliza este circuito de direccionamiento para el direccionamiento de nivel 2 únicamente.

### External Domain

Indica si el direccionador transmite/recibe mensajes dirigidos hacia/procedentes de un dominio que es externo a su dominio de direccionamiento IS-IS.

**Metric** Facilita el coste de esta dirección.

## Mandatos de configuración de OSI/DECnet V (Talk 6)

### ISIS Hello Timer

Facilita el intervalo de tiempo entre las transmisiones de mensajes hello de ISIS.

### DECnetV Link Initialization

Indica si se ha habilitado (YES) o inhabilitado (NO) la inicialización de enlace de tipo DEC para este circuito.

### Receive Verifier

Visualiza los datos de verificación a comprobar con un XID recibido cuando se verifica según circuito.

### Transmit Verifier

Visualiza los datos de verificación a incluir en el XID cuando se verifica según circuito.

### Explicit Receive Verification

Indica si la verificación se lleva a cabo según circuito o según sistema. TRUE indica una verificación según circuito, FALSE indica una verificación según sistema.

### Subnet *informe.subred interfaznúm.*

Visualiza información de subred.

- *informe.subred* tiene dos opciones, Summary y Detailed.
  - *Summary* visualiza información sobre todas las subredes configuradas.
  - *Detailed* visualiza información sobre las subredes LAN únicamente.
- *interfaznúm.* es la interfaz que conecta a la subred.

### Ejemplo:

```
list subnet summary
Ifc State Type ESIS  ISIS  L2 Only  Ext Dom  Metric  EIH (sec)  IIH(sec)
0   On  LAN  Enb  Enb  False   False   20      10         3
2   On  X25
3   On  Fr1
```

**Ifc** Indica el número de interfaz de la subred.

**State** Indica el estado de la interfaz, ON u OFF.

**Type** Indica el tipo de subred: LAN, X25, etc.

**ESIS** Indica el estado del protocolo ES-IS, habilitado (Enb) o inhabilitado (Dis).

**ISIS** Indica el estado del protocolo IS-IS, habilitado (Enb) o inhabilitado (Dis).

**L2 Only** Indica si el direccionador sólo realiza operaciones de nivel 2; puede ser que sí (true) o que no (false).

**Ext Dom** Indica si el direccionador realiza operaciones fuera del dominio de direccionamiento IS-IS (dominio externo).

**Metric** Indica el coste de la utilización de esta subred.

**EIH** Indica a qué intervalos se envían mensajes hello de ES sobre la subred.

**IIH** Indica a qué intervalos se envían mensajes hello de IS sobre la subred.

## Ejemplo:

```
list subnet detailed
Interface Number [0]? 0

Detailed information for subnet 0:
  ISIS Level 1 Multicast: 018002B000014
  ISIS Level 2 Multicast: 018002B000015
  All ISs Multicast:      009002B000005
  All ESs Multicast:      009002B000004
  Level 1 Priority: 64
  Level 2 Priority: 64
```

### ISIS Level 1 Multicast

Indica la dirección de vertimiento múltiple a utilizar cuando se transmiten y se reciben PDU de IS-IS de L1.

### ISIS Level 2 Multicast

Indica la dirección de vertimiento múltiple a utilizar cuando se transmiten y se reciben PDU de IS-IS de L2.

### All ISs Multicast

Indica la dirección de vertimiento múltiple a utilizar cuando se reciben mensajes hello de ES.

### All ESs Multicast

Indica la dirección de vertimiento múltiple a utilizar cuando se transmiten mensajes hello de IS.

### Level 1 Priority/Level 2 Priority

Indica la prioridad del direccionador para convertirse en el direccionador designado en la LAN.

## templates

Visualiza una lista de las plantillas definidas en este direccionador.

### Ejemplo:

```
list template
Route Cir Name      Template Name      DTE Addr      Call UserData
routetest2          temptest2          25             81
```

## timers

Visualiza la configuración de los temporizadores de OSI/DNA V (lo que se ejecute en el direccionador, OSI o DNA V).

### Ejemplo:

```
list timers
Timers:
Complete SNP (sec) = 10      Partial SNP (sec) = 2
Min LSP Gen (sec) = 30      Max LSP Gen (sec) = 900
Min LSP Xmt (sec) = 30      Min Br LSP Xmt (msec) = 33
Waiting Time (sec) = 60     DR ISIS Hello (sec) = 1
ES Config Timer (sec) = 10
```

**Timers:** Indica la configuración de los temporizadores de OSI excluidos los temporizadores por circuito.

### Complete SNP

El intervalo entre generaciones de SNP completas.

### Partial SNP

El intervalo mínimo entre envíos de SNP parciales.

### Min LSP Generation/Max LSP Generation

Los intervalos mínimo y máximo entre generaciones de LSP.

### Min LSP Transmission

El intervalo mínimo entre retransmisiones de LSP.

## Mandatos de configuración de OSI/DECnet V (Talk 6)

### Min Broadcast LSP Transmission

El intervalo mínimo entre retransmisiones de LSP en un circuito de difusión.

### Waiting Time

El período de tiempo durante el que debe retardarse el proceso de actualización antes de que entre en el estado de activo.

### DR ISIS Hello

El intervalo entre generaciones de PDU de mensajes hello de IS-IS si este direccionador es un direccionador designado.

### ES Config Timer

El intervalo mínimo entre las ocasiones en que un ES debe enviar un paquete hello cada vez que se activa una interfaz.

### virtual-circuits

Visualiza información sobre todos los circuitos virtuales X.25.

**Ejemplo:** `list virtual-circuits`

## Set

Utilice el mandato **set** para configurar el direccionador de manera que ejecute el protocolo OSI.

### Sintaxis:

**set**                    aadjacency  
                          algorithm  
                          globals  
                          network-entity-title  
                          phaseivpfx  
                          subnet  
                          switches  
                          timers  
                          transmit-password (sólo configuración de DEC)  
                          virtual-circuit (sólo configuración del IBM 2216)

### adjacency

Añade o cambia una adyacencia de ES. Añade una adyacencia de ES para todos los ES LAN que no ejecutan el protocolo ES-IS.

### Ejemplo:

```
set adjacency
Interface Number [0]:
Area Address [ ]:
System ID [ ]:
MAC Address [ ]:
```

### Interface Number

Indica el número de interfaz que conecta con la adyacencia.

### Area Address

Indica el área donde está ubicada la adyacencia.



### System ID

Indica la parte de ID del sistema del NET que se utiliza para identificar a la adyacencia.

### MAC Address

Indica la dirección MAC (SNPA) de la adyacencia.

### algorithm

**Nota:** Éste es un mandato de DNA phase V. Este mandato sólo funcionará si se incluye el protocolo DNA phase V en la carga del software. Le permite seleccionar el tipo de algoritmo de direccionamiento que va a utilizar para el protocolo de direccionamiento DNA, estado de enlace (DNA V) o vector de distancia (DNA IV).

#### Ejemplo:

```
set algorithm
Level 1 Algorithm [link_state]?
Level 2 Algorithm [distance_vector]?
```

#### Level 1 Algorithm

Selecciona el tipo de algoritmo de direccionamiento, link\_state (para las redes DNA V) o distance\_vector (para las redes DNA IV).

#### Level 2 Algorithm

Selecciona el tipo de algoritmo de direccionamiento, link\_state (para las redes DNA V) o distance\_vector (para las redes DNA IV).

**globals** Configura los parámetros globales que necesita el protocolo OSI.

#### Ejemplo:

```
set globals
IS Type [L2]:
System ID Length [6 bytes]:
Max Synonymous Areas [3]:
L1 LSP Buffer Size [1492 bytes]:
L2 LSP Buffer Size [1492 bytes]:
Max IS Adjacencies [50]:
Max ES Adjacencies [200]:
Max Areas in Domain [50]:
Max ESs per Area [500]:
Max Internal Prefix Addresses [100]:
Max External Prefix Addresses [100]:
Max Link State Updates [100]?
```

#### IS Type (L1 ó L2)

Selecciona el nivel del direccionador, nivel 1 ó nivel 2.

#### System ID Length

Selecciona la longitud de la parte de ID de dominio del NET. Esta longitud debe ser igual para todos los direccionadores del mismo dominio.

#### Max Synonymous Areas

Selecciona el número máximo de áreas de nivel 1 a las que servirá este direccionador.

#### L1 LSP Buffer Size

Selecciona el tamaño de almacenamiento intermedio de los LSP de nivel 1 y las SNP que origine el direccionador. El rango va desde el 512 hasta el 1492. Si el tamaño de

## Mandatos de configuración de OSI/DECnet V (Talk 6)

paquete de interfaz es inferior al configurado aquí, OSI no se ejecutará y el direccionador generará el mensaje ISIS.053 del ELS.

### **L2 LSP Buffer**

Selecciona el tamaño de almacenamiento intermedio de los LSP de nivel 2 y las SNP que origine el direccionador. El rango va desde el 512 hasta el 1492. Si el tamaño de paquete de interfaz es inferior al configurado aquí, OSI no se ejecutará y el direccionador generará el mensaje ISIS.053 del ELS.

### **Max IS Adyacencias**

Selecciona el número total de adyacencias de IS permitidas para todos los circuitos. Este número se utiliza para proporcionar el tamaño de la agrupación de adyacencias de IS libres.

### **Max ES Adyacencias**

Selecciona el número total de adyacencias de ES permitidas para todos los circuitos. Este número se utiliza para proporcionar el tamaño de la agrupación de adyacencias de ES libres.

### **Max Areas in Domain**

Selecciona el número total de áreas del dominio de direccionamiento. Este número se utiliza para proporcionar el tamaño de la tabla de direccionamiento de L2.

### **Max ESs per Area**

Selecciona el número total de ES de cualquier área. Este número se utiliza para proporcionar el tamaño de la tabla de direccionamiento de L1.

### **Max Internal Reachable Addresses**

Selecciona el número que se va a utilizar para proporcionar el tamaño de la tabla de direccionamiento de métrica interna.

### **Max External Reachable Addresses**

Selecciona el número que se va a utilizar para proporcionar el tamaño de la tabla de direccionamiento de métrica externa.

### **Max Link State Updates**

Selecciona el número que se va a utilizar para proporcionar el tamaño de la base de datos de estado de los enlaces.

### **network-entity-title**

Configura el NET del direccionador. El NET está compuesto por el ID del sistema del direccionador y su dirección de área.

#### **Ejemplo:**

```
set network-entity-title  
Area-address [ ]  
System-ID [ ]:
```

#### **Area-address**

Indica una parte de dirección de área del NET del direccionador. Se incluye como la primera dirección en el

## Mandatos de configuración de OSI/DECnet V (Talk 6)

conjunto de direcciones de área manuales del direccionador. Cada dirección de área puede tener un máximo de 19 bytes.

### System-ID

Define la parte del NSAP que identifica a este direccionador específico. El ID del sistema puede tener un máximo de 19 bytes, pero la longitud debe coincidir con la longitud de ID de dominio que ha configurado con el mandato **set globals**.

### phaseivpfx

Configura la dirección de prefijo que permite que el protocolo OSI dirija paquetes a la red DNA IV conectada. El valor por omisión es 49 (hexadecimal).

#### Ejemplo: **set phaseivpfx**

Local Phase IV prefix [49]?

### subnet

Añade o cambia una subred. Este parámetro le solicita información diferente según el tipo de subred que configure: X.25 ó LAN.

#### Ejemplo:

##### Subred X.25:

```
set subnet
Interface number [0]:
Interface Type [X25]:
```

##### Subred LAN:

```
Interface number [0]:
Interface Type [LAN]:
Enable ES-IS [N]?
Enable IS-IS [N]?
Level 2 Only [N]?
External Domain [N]?
Default Metric [20]:
ISIS IS Hello Timer [10 sec]:
ISIS Hello Timer [3 sec]:
Modify Transmit password [No]?
Modify the set of receive passwords [No]?
L1 Priority [64]:
L2 Priority [64]:
All ESs [0x09002B000004]:
All ISs [0x09002B000005]:
All L1 ISs [0x0180C2000014]:
All L2 ISs [0x0180C2000015]:
```

##### Subred Frame Relay:

```
Interface number [0]:
Interface Type [FRL]:
```

#### Interface number

Enlaza lógicamente la subred con la interfaz especificada.

#### Enable ES-IS

Indica si el protocolo ES-IS va a ejecutarse sobre la interfaz, sí (Y) o no (N).

#### Enable IS-IS

Indica si el protocolo IS-IS va a ejecutarse sobre la interfaz, sí (Y) o no (N).

#### Interface Type

Indica el tipo de subred: LAN, X.25 y Frame Relay (FRL). LAN incluye Ethernet y Red en Anillo.

### Level 2 Only

Indica si la subred sólo debe ejecutarse con el nivel 2, sí (Y) o no (N). Una designación de no, permite que el direccionador dirija sobre esta subred según el nivel 1 y el nivel 2.

### External Domain

Indica si el circuito realizará operaciones fuera del dominio de direccionamiento IS-IS.

### Default Metric

Indica el coste de la subred. El rango del coste es 20–63.

### IS Hello Timer

Indica el período entre las transmisiones de PDU de mensajes hello de IS.

### ISIS Hello Timer

Indica el período entre las transmisiones de PDU de mensajes hello de IS-IS de L1 y L2.

### Modify Transmit password

Elimina o cambia una contraseña de transmisión de circuito. Cuando selecciona yes, esta opción le solicita lo siguiente:

```
Delete or change the transmit password  
[change]?
```

### Modify the set of receive passwords

Elimina todas las contraseñas de recepción de circuito o añade una. Cuando selecciona yes, esta opción le solicita lo siguiente:

```
Delete all or add 1 receive password  
[add]?
```

### L1 Priority/L2 Priority

Indica la prioridad del direccionador para convertirse en el direccionador designado en la LAN.

**All ESs** Indica la dirección de vertimiento múltiple a utilizar cuando se transmiten mensajes hello de IS. La dirección por omisión refleja la dirección de vertimiento múltiple ethernet/802.3. Si va a conectarse a una LAN 802.5, utilice **C00000004000**. Si va a conectarse a una LAN FDDI, utilice **9000D4000020**.

**All ISs** Indica la dirección de vertimiento múltiple a utilizar cuando se reciben mensajes hello de ES. La dirección por omisión refleja la dirección de vertimiento múltiple ethernet/802.3. Si va a conectarse a una LAN 802.5, utilice **C00000008000**. Si va a conectarse a una LAN FDDI, utilice **9000D40000A0**.

### All L1 ISs

Indica la dirección de vertimiento múltiple a utilizar cuando se transmiten y se reciben PDU de IS-IS de L1. La dirección por omisión refleja la dirección de vertimiento múltiple ethernet/802.3. Si va a conectarse a una LAN 802.5, utilice **C00000008000**. Si va a conectarse a una LAN FDDI, utilice **800143000028**.

### All L2 ISs

Indica la dirección de vertimiento múltiple a utilizar cuando se transmiten y se reciben PDU de IS-IS de L2. La dirección por

omisión refleja la dirección de vertimiento múltiple ethernet/802.3. Si va a conectarse a una LAN 802.5, utilice **C00000008000**. Si va a conectarse a una LAN FDDI, utilice **8001430000A8**.

**switches** Activa o desactiva las opciones de OSI.

### Ejemplo:

```
set switches
ES-IS Checksum Option [OFF]?
ES-IS Init Option [OFF]?
ISIS Authentication [OFF]?
```

### IS-IS Checksum Option

Cuando se activa, el direccionador genera sumas de comprobación para todos los paquetes de ES-IS originados.

### ES-IS Init Option

Cuando se activa, el direccionador envía un mensaje hello de IS dirigido a un nuevo ES contiguo.

### IS-IS Authentication

Si se activa, cada paquete de IS-IS incluye la contraseña de transmisión configurada para el dominio, el área y los circuitos. Además, no se realiza ninguna comprobación con contraseñas de recepción.

**timers** Configura los temporizadores de OSI, excluidos los temporizadores de circuito.

### Ejemplo:

```
set timers
Complete SNP [10 sec]:
Partial SNP [2 sec]:
Minimum LSP Generation [30 sec]:
Maximum LSP Generation [900 sec]:
Minimum LSP Transmission [5 sec]:
Minimum Broadcast LSP Transmission [33 msec]:
Waiting Time [60 sec]:
Designated Router ISIS Hello [1 sec]:
Suggested ES Configuration Timer (sec) [10]:
```

### Complete SNP

Selecciona el intervalo entre las generaciones de PDU de número de secuencia (SNP) completas por parte del direccionador designado en un circuito de difusión.

### Partial SNP

Selecciona el intervalo mínimo entre envíos de PDU de número de secuencia (SNP) parciales.

### Minimum LSP Generation

Selecciona el intervalo mínimo entre sucesivas generaciones de paquetes del estado de los enlaces (LSP) con el mismo ID de LSP que genera el direccionador.

### Maximum LSP Generation

Selecciona el intervalo máximo entre LSP generados por el direccionador.

### Minimum LSP Transmission

Selecciona el intervalo mínimo entre las retransmisiones de un LSP.

### Minimum Broadcast LSP Transmission

Selecciona el intervalo mínimo de transmisión, en milisegundos, entre transmisiones de LSP en un circuito de difusión.

### Waiting Time

Selecciona el número de segundos durante los que debe retardarse el proceso de actualización en el estado de espera antes de que entre en el estado de activo.

### Designated Router ISIS Hello

Selecciona el intervalo entre las generaciones de PDU de mensajes hello de IS-IS por parte del direccionador si éste es un direccionador designado en una LAN.

### Suggested ES Configuration Timer

Establece el campo de opción del mensaje hello de IS que indica al ES que cambie la velocidad a la que envía mensajes hello de ES.

### transmit-password

Establece o cambia una contraseña de transmisión.

#### Ejemplo:

```
set transmit-password
Password type [Domain]:
Password [ ]:
Reenter password:
```

#### Password type

Selecciona el tipo de contraseña: *domain* o *area*.

Las contraseñas de dominio se utilizan con LSP de L2 y SNP. Las contraseñas de área se utilizan con LSP de L1 y SNP.

#### Password

Indica la serie de caracteres que va a utilizar para la autenticación. El tamaño máximo de serie permitido puede ser de 16 caracteres.

### virtual-circuit

Configura un PVC o un SVC X.25 o bien un PVC Frame Relay.

#### Ejemplo:

```
set virtual-circuit
Interface Number [0]:
DTE Address [ ]:
Enable ISIS (Y or N) [Y]?
L2 only (Y or N) [N]?
External Domain (Y or N) [N]?
Default Metric [20]:
ISIS Hello Timer [3 sec]?
Modify transmit password (y or n) [N]?
Modify the set of receive passwords [No]?
```

#### Interface Number

Indica la interfaz X.25 ó Frame Relay sobre la que se configura el circuito virtual.

**DTE Address**

Indica la dirección de DTE de destino para X.25 ó el DLCI (identificador de control de enlace de datos) para Frame Relay. Esta dirección debe ser la misma que la definida para el circuito virtual en la configuración de X.25 o de Frame Relay.

**Default Metric**

Indica el coste del circuito.

**Enable IS-IS**

Indica si el protocolo IS-IS va a ejecutarse sobre la interfaz, sí (Y) o no (N).

**L2 only**

Indica si el circuito sólo debe ejecutarse con el nivel 2, sí (Y) o no (N). Una designación de no permite que el direccionador direcciona según el nivel 1 y el nivel 2.

**External Domain**

Indica si el circuito realizará operaciones fuera del dominio de direccionamiento IS-IS.

**Acceso al entorno de supervisión de OSI/DECnet V**

Para obtener información sobre cómo acceder al entorno de supervisión de OSI/DECnet V, consulte *Cómo empezar (Introducción a la interfaz de usuario)* en la publicación *Nways Multiprotocol Access Services Guía del usuario de software*.

**Mandatos de supervisión de OSI/DECnet V**

Este apartado describe los mandatos de supervisión de OSI/DECnet V. Utilícelos para reunir información de la base de datos.

Los mandatos de supervisión visualizan o modifican la base de datos volátil.

<i>Tabla 109 (Página 1 de 2). Resumen de los mandatos de supervisión de OSI/DECnet V</i>	
Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxxi.
Addresses	Visualiza el NET y las direcciones de área del direccionador.
Change Metric	Modifica el coste de un circuito.
CLNP-Stats	Visualiza estadísticas de CLNP para OSI.
DNAV-info	Visualiza el algoritmo de direccionamiento de nivel 1 y nivel 2 de DNAV que es efectivo actualmente.
Designated-router	Visualiza el direccionador designado para la LAN.
ES-adjacencies	Visualiza todas las adyacencias de ES de la base de datos de adyacencias.
ES-IS-Stats	Visualiza estadísticas asociadas con el protocolo ESIS.

## Mandatos de supervisión de OSI/DECnet V (Talk 5)

<i>Tabla 109 (Página 2 de 2). Resumen de los mandatos de supervisión de OSI/DECnet V</i>	
Mandato	Función
IS-adjacencies	Visualiza todas las adyacencias de IS de la base de datos de adyacencias.
IS-IS-Stats	Visualiza estadísticas asociadas con el protocolo ISIS.
L1-routes	Visualiza todas las rutas de L1 de la base de datos de nivel 1.
L2-route	Visualiza todas las rutas de L2 de la base de datos de nivel 2.
L1-summary	Visualiza un resumen de la base de datos de estado de los enlaces de nivel 1.
L2-summary	Visualiza un resumen de la base de datos de estado de los enlaces de nivel 2.
L1-update	Visualiza la información contenida en el paquete de actualización del estado de los enlaces de L1.
L2-update	Visualiza la información contenida en el paquete de actualización del estado de los enlaces de L2.
Ping-1139	Hace que el direccionador envíe una petición con eco a un destino y espere una respuesta.
Route	Visualiza la ruta que toma un paquete hacia un destino especificado.
Send echo packet	Codifica un mensaje de petición con eco en el paquete de CLNP.
Show routing circuits	Visualiza el estado de los circuitos de direccionamiento definidos por el usuario para la interfaz especificada. Se aplica cuando el direccionador está configurado como direccionador de tipo DEC.
Subnets	Visualiza todas las subredes definidas por el usuario.
Toggle	Habilita o inhabilita la función de sustitución de alias de NSAP.
Traceroute	Visualiza la ruta que recorre un paquete hacia su destino.
Virtual-circuits	Visualiza todos los circuitos virtuales definidos por el usuario. Se aplica cuando el direccionador está configurado como direccionador de tipo IBM 2216.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxi.

## Addresses

Utilice el mandato **addresses** para listar el NET y las direcciones de área del direccionador que se han configurado para éste.

### Sintaxis:

**addresses**

### Ejemplo:

```
addresses
Network Entity Title:
4700-0500-01 000-9310-04F0
Area Addresses:
4700-0500-01
4900-02
```



**Network Entity Title**

Identifica al direccionador. El NET está compuesto por una dirección de área y un ID del sistema.

**Area Address**

Indica las direcciones dentro del dominio de direccionamiento. El direccionador puede tener un máximo de tres direcciones de área configuradas en cualquier momento.

**Change Metric**

Utilice el mandato **change metric** para modificar el coste de un circuito.

**Sintaxis:**

change metric

**Ejemplo:**

```
change metric
Circuit [0]?
New Cost [0]?
```

**Circuit** Indica el número de circuito que desee cambiar.

**New Cost**

Indica el nuevo coste del circuito. Rango: del 1 al 63.

**CLNP-Stats**

Utilice el mandato **clnp-stats** para visualizar las estadísticas del protocolo de OSI Connectionless Layer Network Protocol (CLNP).

**Sintaxis:**

clnp-statistics

**Ejemplo:**

```
clnp-statistics

Received incomplete packet                0
Received packet with bad NSAP length      0
Received packet with bad checksum         0
Received packet with bad version number   0
Received packet with bad type             0
Received packet with expired lifetime     0
Received packet with bad option           0
Received packet with unknown destination  0
Received packet with no segmentation permitted 0
Received data packet cannot be forwarded  0
CLNP input queue overflow                 0
No buffer available to send error packet   0
No route to send error packet             0
Received OK CLNP packet                   0
Cannot forward error packet               0
ISO unknown initial protocol ID          0
Received error packet                     0
Received local data packet                0
Sent error packet                         0
received echo packet - destination unknown 0
cannot send an echo packet, handler error 0
sent ECHO reply packet                    0
sent ECHO request packet                  0
received ECHO Request                     0
received ECHO reply                       0
Error PDU dropped - SP, MS or E/R flag set 0
```

### **Received incomplete packet**

Indica que se ha recibido un fragmento de un paquete de datos reconocido como paquete de datos del protocolo CLNP de la ISO.

### **Received packet with bad NSAP length**

Indica que se ha recibido un paquete de datos del protocolo CLNP de la ISO con una longitud de NSAP incorrecta.

### **Received packet with bad checksum**

Indica que se ha recibido un paquete de datos del protocolo CLNP de la ISO con una suma de comprobación incorrecta.

### **Received packet with bad version number**

Indica que se ha recibido un paquete de datos del protocolo CLNP de la ISO con un número de versión incorrecto o no soportado.

### **Received packet with bad type**

Indica que se ha recibido un paquete de datos del protocolo CLNP de la ISO con un campo de tipo incorrecto o no soportado.

### **Received packet with expired lifetime**

Indica que se ha recibido un paquete de datos del protocolo CLNP de la ISO con una duración caducada.

### **Received packet with bad option**

Indica que se ha recibido un paquete de datos del protocolo CLNP de la ISO con un parámetro opcional incorrecto.

### **Received packet with unknown destination**

Indica que se ha recibido un paquete de datos del protocolo CLNP de la ISO, pero no se ha podido direccionar. La tabla de direccionamiento no contiene ninguna entrada para el destino.

### **Received packet with no segmentation permitted**

Indica que se ha recibido un paquete de datos del protocolo CLNP de la ISO que necesitaba segmentación. No se ha establecido el distintivo de segmentación permitido.

### **Received data packet cannot be forwarded**

Indica que se ha recibido un paquete de datos del protocolo CLNP de la ISO, pero no se ha podido direccionar a causa de un error del manejador.

### **No buffer available to send error packet**

Ha fallado un intento de enviar un paquete de error del protocolo CLNP de la ISO a causa de la falta de almacenamientos intermedios de E/S del sistema.

### **No route to send error packet**

Ha fallado un intento de enviar un paquete de error del protocolo CLNP de la ISO porque no ha podido direccionarse.

### **Received OK CLNP packet**

Indica que se ha recibido un paquete de datos del protocolo CLNP de la ISO y ha pasado la comprobación de errores.

### **Cannot forward error packet**

Indica que no se ha podido direccionar un paquete de error del protocolo CLNP de la ISO a causa de un error del manejador.

**ISO unknown initial protocol ID**

Indica que se ha recibido un paquete del protocolo CLNP de la ISO con un identificador de protocolo inicial desconocido o no soportado.

**Received error packet**

Indica que se ha recibido un paquete de error del protocolo CLNP de la ISO para este direccionador.

**Received local data packet**

Indica que se ha recibido un paquete de datos del protocolo CLNP de la ISO con una NSAP de destino que indica una de las NSAP del direccionador.

**Sent error packet**

Indica que se ha enviado un paquete de error del protocolo CLNP de la ISO al recibirse un paquete incorrecto.

**Designated-router**

Utilice el mandato **designated-router** si desea visualizar el direccionador designado para las subredes LAN que están conectadas físicamente a este direccionador y ejecutan IS-IS de forma activa.

**Sintaxis:**

designated-router

**Ejemplo:****designated-router**

Designated Router Information:

Hdw	Int#	Circ	L1DR	L2DR
Eth/1	1	2	0000931004F002	0000931004F002
TKR/0	0	1	Elvis-01	Elvis-01

**Hdw** Indica el tipo y la instancia de la LAN conectada a este direccionador.

**Int#** Indica el número de interfaz de este direccionador que conecta a la LAN.

**Circ** Indica el número de circuito asignado por el direccionador. Este número siempre es uno más que el número de interfaz para las subredes LAN.

**L1DR** Indica el ID de LAN del direccionador designado. Si está habilitado el uso de un alias, este mandato visualiza el alias del segmento en particular. El ID de LAN es el ID del sistema del direccionador designado en concatenación con un ID de circuito asignado localmente de 1 byte.

**L2DR** Su descripción es la misma que la del L1DR explicado anteriormente.

**Nota:** Si todavía no se ha elegido el direccionador designado, se visualizará "Not Elected" en lugar de un ID de LAN.

**DNAV-info**

Utilice el mandato **dnav-info** para visualizar el algoritmo de direccionamiento que se ejecuta actualmente en el direccionador.

**Sintaxis:**

dnav-info

**Ejemplo:**

## Mandatos de supervisión de OSI/DECnet V (Talk 5)

### **dnav-info**

DNA V Level 1 Routing Algorithm: Distance-vector

DNA V Level 2 Routing algorithm: Distance-vector

**Nota:** Según esté habilitado o inhabilitado DNA IV, el algoritmo de direccionamiento visualizado aquí puede ser diferente del que se haya configurado en la memoria mediante el mandato **set algorithm** del indicador `config>` de OSI/DECnet V.

Si está habilitado DNA IV - el algoritmo de direccionamiento es el que se ha configurado en la memoria.

Si está inhabilitado DNA IV - el algoritmo de direccionamiento se establece en estado de enlace y puede ser diferente del que se ha establecido en la memoria.

## ES-Adyacencias

Utilice el mandato **es-adjacencies** para visualizar todas las adyacencias de sistema final (ES) que se hayan configurado o se hayan aprendido mediante el protocolo ESIS.

### **Sintaxis:**

**es-adjacencies**

### **Ejemplo:**

#### **es-adjacencies**

End System Adjacencies

System ID	MAC Address	Interface	Lifetime	Type
6666-6666-6666	1234-FEAA-041C	0	50	DNAIV

### **System ID**

El ID del sistema de la adyacencia de ES.

### **MAC Address**

Indica la dirección MAC del ES en la subred.

**Interface** Indica el número de interfaz del direccionador donde se ha aprendido la adyacencia de ES.

**Lifetime** Indica el período de tiempo, en segundos, que ha dejado el direccionador antes de que se deseche la información recibida en el último mensaje hello de ES. En el caso de una adyacencia de ES estática o configurada manualmente, este campo expresa **Static**.

**Type** Indica el tipo de adyacencia de ES: OSI, DNAIV, DNAIV', y MANUAL para las adyacencias configuradas estáticamente.

## ES-IS-Stats

Utilice el mandato **es-is-stats** para visualizar las estadísticas del protocolo ESIS.

### **Sintaxis:**

**es-is-stats**

### **Ejemplo:**

### es-is-stats

```

ESIS input queue overflow          0
Received incomplete packet        0
Received packet with bad checksum 0
Received packet with bad version  0
Received packet with bad type     0
No iob available to send hello    0
Cannot send hello due to packet handler error 0
Sent hello                        3672
Received packet with bad header   0
Received hello with bad nsap     0
Received hello packet with bad option 0
Received hello                   0
Received hello with unsupported domain source 0
No resources to install route     0
Received hello with conflicting route 0
Timed out route reactivated       0
No resources to send redirect     0
Redirect not sent - handler error  0
Sent redirect                    0
Timed out route                  0
Timed out route                  0
Unable to allocate resources for a new ES adjacency 0
hello PDU dropped, received over point-to-point circ 0
ESIS hello PDU dropped, no matching area address 0
dropped hello packet - manual ES adjacency exists 0

```

#### **ESIS input queue overflow**

Se ha eliminado el paquete de ESIS porque se ha desbordado la cola de la entrada de tareas.

#### **Received incomplete packet**

Se ha recibido un fragmento de un paquete reconocido como paquete de ESIS.

#### **Received packet with bad checksum**

Se ha recibido un paquete de ESIS con una suma de comprobación incorrecta.

#### **Received packet with bad version**

Se ha recibido un paquete de ESIS con una versión incorrecta o no soportada.

#### **Received packet with bad type**

Se ha recibido un paquete de ESIS con un campo de tipo incorrecto o no soportado.

#### **No iob available to send hello**

Ha fallado un intento de enviar un paquete de ESIS a causa de la falta de almacenamientos intermedios de E/S del sistema.

#### **Cannot send hello due to packet handler error**

No se ha podido enviar un mensaje hello de ESIS a causa de un error del manejador.

#### **Sent hello**

Se ha emitido un mensaje hello de ESIS desde una interfaz.

#### **Received packet with bad header**

Se ha recibido un paquete hello de ESIS con un campo recibido o tiempo de mantenimiento incorrecto.

#### **Received hello with nsap**

Se ha recibido un paquete hello de ESIS con una NSAP incorrecta o una NSAP que ha desbordado el campo.

## Mandatos de supervisión de OSI/DECnet V (Talk 5)

### **Received hello packet with bad option**

Se ha recibido un paquete de datos de CLNP de ESIS con un parámetro de opción incorrecta.

### **Received hello**

Se ha recibido un paquete hello de ESIS en la interfaz.

### **Received hello with unsupported domain source**

Se ha recibido un paquete hello de ESIS de un origen de dominio no especificado.

### **No resources to install route**

Se ha recibido un paquete hello de ESIS, pero no había recursos para instalar la ruta.

### **Received hello with conflicting route**

Se ha recibido un paquete hello de ESIS, pero no ha podido entrar en la base de datos. Una ruta dinámica o estática definida anteriormente de la base de datos está en conflicto con la ruta del mensaje hello.

### **Timed out route reactivated**

Se ha recibido un paquete hello de ESIS con una ruta en la que anteriormente se había sobrepasado el tiempo de espera.

### **No resources to send redirect**

No se ha podido enviarse un paquete de redireccionamiento de ESIS a causa de la falta de recursos.

### **Redirect not sent handler error**

No se ha podido enviarse un paquete de redireccionamiento de ESIS a causa de un error del manejador.

### **Sent redirect**

Se ha emitido un paquete de redireccionamiento de ESIS desde la interfaz.

### **Timed out route**

Una ruta de mensaje hello de ESIS ha sobrepasado el tiempo de espera.

### **Unable to allocate resources for a new ES adjacency**

Se ha recibido un paquete hello de ES-IS, pero el direccionador no tenía suficientes recursos para establecer una adyacencia de ES con el nodo emisor.

### **hello PDU dropped, received over point-to-point circ**

Se ha eliminado un paquete hello de ES-IS porque el circuito implicado es un circuito punto a punto.

### **ESIS hello PDU dropped, no matching area address**

Se ha eliminado un paquete hello de ES-IS porque el área no coincidía con la dirección de área del direccionador. El protocolo ES-IS sólo se aplica a un área.

### **dropped hello packet-manual ES adjacency exists.**

Se ha eliminado un paquete hello de ES-IS porque existe una adyacencia de ES estática con el nodo emisor.

## IS-Adjacencies

Utilice el mandato **IS-adjacencies** para listar todas las adyacencias de IS aprendidas mediante el protocolo ISIS.

### Sintaxis:

is-adjacencies

### Ejemplo:

```
is-adjacencies
Intermediate System Adjacencies
System ID      MAC Address    Int  Level Usage  State  Life  Type
0000-9310-04C8 AA00-0400-EF04 0    L1   L1/L2 DOWN   5390  OSI
0000-9310-04C8 AA00-0400-EF04 0    L2   L1/L2 DOWN   5390  DNAIV
AA00-0400-0504 AA00-0400-0504 1    L2   L2     UP     5390  OSI
```

### System ID

El ID del sistema de la adyacencia de IS.

### MAC Address

Indica la dirección MAC de la adyacencia de IS.

**Int** Indica el número de interfaz del direccionador que conecta con la adyacencia de IS.

**Level** Para las LAN, indica el nivel del sistema contiguo a partir del tipo de mensaje hello, L1 ó L2. Para punto a punto, indica el tipo del sistema contiguo: L1 únicamente o, si no, L2.

**Usage** Indica el tipo de circuito a partir del paquete hello: L1 únicamente, L2 únicamente o bien L1 y L2.

**State** Indica el estado operativo de la adyacencia de IS, activo o inactivo.

**Life** Indica el período de tiempo, en segundos, antes de desechar el último mensaje hello de IS.

**Type** Indica el tipo de protocolo de direccionamiento de la adyacencia de IS: OSI o DNA IV.

## IS-IS-Stats

Utilice el mandato **is-is-stats** para visualizar información asociada con el protocolo ISIS.

### Sintaxis:

is-is-stats

### Ejemplo:

## Mandatos de supervisión de OSI/DECnet V (Talk 5)

### is-is-stats

#### Link State Database Information

no. of level 1 LSPs	1	no. of level 2 LSPs	0
no. of L1 Dijkstra runs	21	no. of L2 Dijkstra runs	0
no. of L1 LSPs deleted	0	no. of L2 LSPs deleted	0
no. of routing table entries allocated	6		

#### Packet Information

level 1 lan hellos rcvd	0	level 1 lan hellos sent	10967
level 2 lan hellos rcvd	0	level 2 lan hellos sent	10967
pnt to pnt hellos rcvd	0	pnt to pnt hellos sent	0
level 1 LSPs rcvd	0	level 1 LSPs sent	40
level 2 LSPs rcvd	0	level 2 LSPs sent	0
level 1 CSNPs rcvd	0	level 1 CSNPs sent	0
level 2 CSNPs rcvd	0	level 2 CSNPs sent	0
level 1 PSNPs rcvd	0	level 1 PSNPs sent	0
level 2 PSNPs rcvd	0	level 2 PSNPs sent	0

### no. of level 1/level 2 LSPs

Indica el número de paquetes del estado de los enlaces de L1 y L2 que se encuentran en la base de datos.

### no. of L1/L2 Dijkstra runs

Indica el número de veces que el direccionador ha calculado las tablas de direccionamiento de L1 y L2.

### no. of L1/L2 LSPs deleted

Indica el número de paquetes del estado de los enlaces de L1 y L2 que se han suprimido de la base de datos.

### no. of routing table entries allocated

Indica el número de entradas que contiene actualmente la tabla de direccionamiento.

### level 1/level 2 lan hellos rcvd

Indica el número de mensajes hello de LAN que ha recibido el direccionador.

### level 1/level 2 hellos sent

Indica el número de mensajes hello de LAN que ha enviado el direccionador.

### pnt to pnt hellos rcvd

Indica el número de mensajes hello de punto a punto que ha recibido el direccionador.

### pnt to pnt hellos sent

Indica el número de mensajes hello de punto a punto que ha enviado el direccionador.

### level 1/level 2 LSPs rcvd

Indica el número de paquetes del estado de los enlaces (LSP) de L1 y L2 que el direccionador ha recibido.

### level 1/level 2 LSPs sent

Indica el número de LSP de L1 y L2 que el direccionador ha enviado.

### level 1/level 2 CSNPs rcvd

Indica el número de PDU de número de secuencia completas (CSNP) de L1 y L2 que el direccionador ha recibido.

### level 1/level 2 CSNPs sent

Indica el número de CSNP de L1 y L2 que el direccionador ha enviado.



**level 1/level 2 PSNPs rcvd**

Indica el número de PDU de número de secuencia parciales (PSNP) de L1 y L2 que el direccionador ha recibido.

**level 1/level 2 PSNPs sent**

Indica el número de PSNP de L1 y L2 que el direccionador ha enviado.

## L1-Routes

Utilice el mandato **l1-routes** para visualizar todas las rutas de nivel 1 que están en la base de datos de direccionamiento de L1.

**Sintaxis:**

l1-routes

**Ejemplo:**

**l1-routes**

Level 1 Routes	Destination System ID	Cost	Source	Next Hop
0000-9300-0047		0	LOCArea	*
AA00-0400-080C		1	ESIS	AA00-0400-0C04, Ifc 7
7777-7777-7777		0	ISIS	3455-6537-2215

**Destination System ID**

Indica el ID del sistema del sistema principal de destino.

**Cost**

Indica el coste de esta ruta.

**Source**

Indica el origen, de los tres posibles, a partir del cual el direccionador ha aprendido la ruta: LOCAREA, ESIS o ISIS.

**Next Hop**

Indica el siguiente salto que un paquete tomará en su ruta. La designación de un asterisco (\*) hace referencia al direccionador en sí como destino del paquete. Una dirección con un número de interfaz es la dirección MAC de un ES conectado directamente o la dirección de DTE si el siguiente salto es un conmutador de X.25 o un DLCI si el siguiente salto es un conmutador de Frame Relay. Un ID del sistema (34555372215) hace referencia al siguiente salto hacia el destino.

## L2-Routes

Utilice el mandato **l2-routes** para visualizar todas las rutas de nivel 2 de la base de datos de L2.

**Sintaxis:**

l2-routes

**Ejemplo:**

**l2-routes**

Level 2 Routes	Destination	Cost	Type	Next Hop
4700-0500-01		0	LOC-AREA	*
4900-02		20	AREA	0000-9310-04C9

**Destination**

Indica el ID del sistema del área de destino o dirección asequible.

**Cost**

Indica el coste de esta ruta.

## Mandatos de supervisión de OSI/DECnet V (Talk 5)

- Type** Indica los cuatro tipos de rutas: el área-LOC (local), el prefijo-LOC, el área, el prefijo/I y el prefijo/E. Un área-LOC es un área conectada directamente; un prefijo-LOC es un prefijo que este direccionador anuncia; un prefijo/I y un prefijo/E son rutas que requieren otro salto para llegar a su destino.
- Next Hop** Indica el siguiente salto que un paquete tomará en su ruta. La designación de un \*, o designación directa, hace referencia a un sistema principal conectado directamente fuera del direccionador. Un ID del sistema hace referencia al próximo direccionador por el que debe pasar el paquete para llegar a su destino.

## L1-Summary

Utilice el mandato **I1-summary** para visualizar un resumen de la base de datos de estado de los enlaces de nivel 1.

### Sintaxis:

#### I1-summary

### Ejemplo:

#### I1-summary

Link State Database Summary - Level One

LSP ID	Lifetime	Sequence #	Checksum	Flags	Cost
0000-9300-40B0-0000	0	0	0	0	1024
0000-93E0-107A-0000	384	CE	3CC9	1	0
AA00-0400-0504-0000	298	8E	40F1	B	20
AA00-0400-0504-0100	4	B8	A812	3	20

Total Checksum 25CC

**LSP ID** Representa el ID del sistema del origen de la PDU del estado de los enlaces más dos bytes adicionales. El primer byte adicional designa el tipo de actualización. 00 representa una actualización que no es de pseudonodo. 01–FF representa una actualización de pseudonodo para ese número de circuito. El segundo byte representa el número de LSP. Este número está conectado al paquete cuando los datos van contenidos en más de un paquete.

**Lifetime** Indica el período de tiempo, en segundos, durante el cual este direccionador mantendrá el LSP.

### Sequence #

Indica el número de secuencia del LSP.

### Checksum

Indica el valor de suma de comprobación del LSP.

### Flags

Indica un valor de un octeto que refleja el campo de distintivos del LSP. La división de los ocho bits es la siguiente:

**Bit 8** Indica el distintivo P. Cuando se establece (1), el IS emisor da soporte a la función opcional Reparación de partición.

**Bits 7-4** Indican el distintivo ATT. Cuando se establece (1), significa que el IS emisor se conecta a otras áreas utilizando una de las métricas siguientes: la métrica por omisión (bit 4), la métrica de retardo (bit 5), la métrica de gasto (bit 6) o la métrica de errores (bit 7).

**Bit 3** Indica el distintivo LSPDBOL. Cuando se establece (1), se ha producido una carga excesiva de la base de datos de LSP. Un LSP que tiene establecido este bit no se utiliza en el proceso de las decisiones para calcular rutas hacia otro I por medio del sistema de origen.

**Bits 2-1** Indican el distintivo de tipo de IS. Cuando se establece en los valores siguientes, designa el tipo de direccionador IS, nivel 1 ó nivel 2.

Valor	Descripción
0	No se utiliza.
1	Establecido el bit 1. IS de nivel 1.
2	No se utiliza.
3	Establecidos los bits 1 y 2. IS de nivel 2.

**Cost** Indica el coste del direccionamiento hacia ese contiguo.

## L2-Summary

Utilice el mandato **I2-summary** para visualizar un resumen de la base de datos de estado de los enlaces de nivel 2.

### Sintaxis:

I2-summary

### Ejemplo:

#### I2-summary

Link State Database Summary - Level Two

LSP ID	Lifetime	Sequence #	Checksum	Flags	Cost
0000-9310-04F0-0000	33E	12	EF19	3	0
0000-5000-FB06-0000	455	4	2BB1	3	20
0000-5000-FB06-0100	469	12	DE32	3	20

Total Checksum 0

La descripción de la salida de L2-summary es la misma que la del mandato I1-summary.

## L1-Update

Utilice el mandato **I1-update** si desea visualizar una actualización del estado de los enlaces para el IS de nivel 1 especificado.

### Sintaxis:

I1-update

### Ejemplo:

## Mandatos de supervisión de OSI/DECnet V (Talk 5)

### 11-update

LSP ID []? 0000931004F0000

Link State Update For ID 0000931004F00000

Area Addresses

470005001

Intermediate System Neighbors	Metric	Two Way
0000931004F002	20	N
0000931004F001	20	Y

End System Neighbors	Metric
00009310004F0	*

**LSP ID** Representa el ID del sistema del origen de la PDU del estado de los enlaces más dos bytes adicionales. El primer byte designa el tipo de actualización. 00 representa una actualización que no es de pseudonodo. 01–FF representa una actualización de pseudonodo. El segundo byte representa el número de LSP. Este número está conectado al paquete cuando los datos van contenidos en más de un paquete.

### Area Addresses

Indica las direcciones de área a las que este direccionador envía paquetes según la configuración.

### Intermediate System Neighbors

Indica los IS contiguos que son adyacentes.

**Metric** Indica el coste para el IS contiguo.

**Two Way** Indica si el direccionador va a recibir actualizaciones de su contiguo.

### End System Neighbors

Indica cualquier ES conectado directamente.

## L2-Update

Utilice el mandato `l2-update` si desea visualizar la actualización del estado de los enlaces para el IS de nivel 2 especificado.

### Sintaxis:

`l2-update`

### Ejemplo:

#### 12-update

LSP ID []? 0000931004F0000

Link State Update For ID 0000931004F00000

INTERMEDIATE SYSTEM NEIGHBORS	METRIC	TWO WAY
0000931004F002	20	N
0000931004F001	20	N
55002000182000	20	N

### Intermediate System Neighbors

Indica los otros IS conectados directamente.

**Metric** Indica el coste para el IS.

**Two Way** Indica si el direccionador va a recibir actualizaciones de su contiguo.

## Ping-1139

Hace que el direccionador envíe una petición con eco a un destino y espere una respuesta, según la recomendación RFC 1139. RFC 1139 la especifica como una función de OSI y no como una función de DECnet. **Ping-1139** da soporte a ecos a largo plazo y a corto plazo. Los ecos a corto plazo utilizan paquetes de datos de CLNP normales, que los hacen transparentes para los sistemas intermedios que no dan soporte a RFC1139. Los ecos a largo plazo utilizan paquetes de petición/respuesta PING.

La longitud de datos por omisión del paquete de petición con eco es de 16 bytes. Puede establecer la longitud de datos hasta un máximo de 64 bytes.

Una vez entrado el mandato **ping-1139**, se enviarán continuamente peticiones con eco hasta que pulse cualquier tecla. En ese momento, se visualizarán estadísticas mostrando el número de peticiones transmitidas y el número de respuestas recibidas.

### Sintaxis:

**ping-1139**

### Ejemplo:

```
ping-1139
Long-term/Short-term [LONG-TERM]?
Destination NSAP: []? AA0003000A14
Data Length [16]?

PINGing AA0003000A14

---- PING Statistics ----
 8 requests transmitted, 8 replies received
```

## Route

Utilice el mandato **route** para visualizar el siguiente salto que tomará un paquete hacia un destino especificado (nsapdest).

### Sintaxis:

**route nsap-dest**

### Ejemplo:

```
route 490002aa0004000e08
Destination System: 0000-9310-04C9
Destination MAC Address: AA00-0400-1408
Interface: 0
```

### Destination System

Indica el ID del sistema del IS de siguiente salto. Para un ES conectado directamente, la indicación estará en blanco.

### Destination MAC Address

Indica la dirección MAC del IS de siguiente salto o del ES conectado directamente.

**Interface** Indica la interfaz por la que pasará el paquete para llegar al IS de siguiente salto o al ES conectado directamente.

### Send (Echo Packet)

Utilice el mandato **send echo packet** para codificar un mensaje de petición con eco en el paquete de CLNP dirigido a la nsap de destino especificada. Mientras se ejecuta este mandato, el sistema no interactúa con la supervisión de OSI. Para verificar si se ha enviado la petición con eco y si se ha recibido una respuesta con eco, compruebe el ELS (Sistema de anotación cronológica de sucesos).

**Nota:** No puede enviarse un paquete con eco a sí mismo. Si lo intenta, recibirá el mensaje CLNP.004 del ELS.

#### Sintaxis:

send

#### Ejemplo:

```
send
Destination NSAP: []?
```

### Subnets

Utilice el mandato **subnets** para visualizar información sobre todas las subredes operativas. Las subredes que no están en activo o que se encuentran inhabilitadas no aparecerán en la lista.

#### Sintaxis:

subnets

#### Ejemplo:

```
subnets
      L2
Hdw  Int #  Circ  Only  ES-IS  IS-IS  L1DR  L1Pri  L2DR  L2pri  Cost  Ext
PPP/2 2      3    N    N    Y
Eth/0 0      1    N    Y    Y    Y    64    N    64    20    N
```

**Hdw** El tipo y la instancia de la red que conecta a la subred.

**Int #** El número de interfaz del direccionador que conecta a la subred.

**Circ** El ID del circuito asignado para el protocolo ISIS.

**L2 only** Indica si este direccionador es un direccionador de nivel 2 únicamente, Y (sí) o N (no).

**ES-IS** Indica si el protocolo ES-IS está habilitado en la subred, Y o N.

**IS-IS** Indica si el protocolo IS-IS está habilitado en la subred, Y o N.

**L1DR** Indica si este direccionador es el direccionador designado de nivel 1 para esta subred, Y o N.

**L1Pri** La prioridad de nivel 1 en la subred para convertirse en el direccionador designado.

**L2DR** Indica si este direccionador es el direccionador designado de nivel 2 para esta subred, Y o N.

**L2Pri** La prioridad de nivel 2 en la subred LAN para convertirse en el direccionador designado.

**Cost** El coste del circuito.

**Ext** Indica si la subred realiza operaciones fuera del dominio de direccionamiento IS-IS (externo).

## Toggle (Alias/No Alias)

Utilice el mandato **toggle alias/no alias** para habilitar o inhabilitar la función de visualización de alias de NSAP del protocolo OSI.

### Sintaxis:

**toggle**

### Ejemplo:

```
toggle
Alias substitution is ON
```

## Traceroute

Utilice el mandato **traceroute** para realizar un seguimiento de la vía de acceso que tome un paquete de OSI hacia un destino.

**Nota:** El usuario no puede ejecutar traceroute dirigido a sí mismo, pues, si lo hace, recibirá el siguiente mensaje de error:

```
Sorry, can't traceroute to this router.
```

### Sintaxis:

**traceroute** *dirección*

### Ejemplo:

```
traceroute 490002aa0004000e08
Successful trace:
```

```
TRACEROUTE 470007: 56 databytes
```

```
1          490002aa0004000e08      32ms      5ms      5ms
```

```
Destination unreachable response:
```

```
Destination unreachable
```

```
No response:
```

```
1 * * *
```

```
2 * * *
```

### TRACEROUTE

Visualiza la dirección de área de destino y el tamaño del paquete que se envía a esta dirección.

**1** El primer rastreo, que muestra la NSAP de destino y el período de tiempo que ha tardado el paquete en llegar al destino. El paquete se rastrea tres veces.

### Destination unreachable

Indica que no está disponible ninguna ruta hacia el destino.

```
1 * * *
```

**2 \* \* \*** Indica que el direccionador espera alguna forma de respuesta del destino pero el destino no responde. El direccionador esperará 32 saltos antes del tiempo de espera excedido. Acuda al ELS y active los men-

## Mandatos de supervisión de OSI/DECnet V (Talk 5)

sajes del protocolo CLNP de OSI para determinar por qué razón no responde el sistema principal.



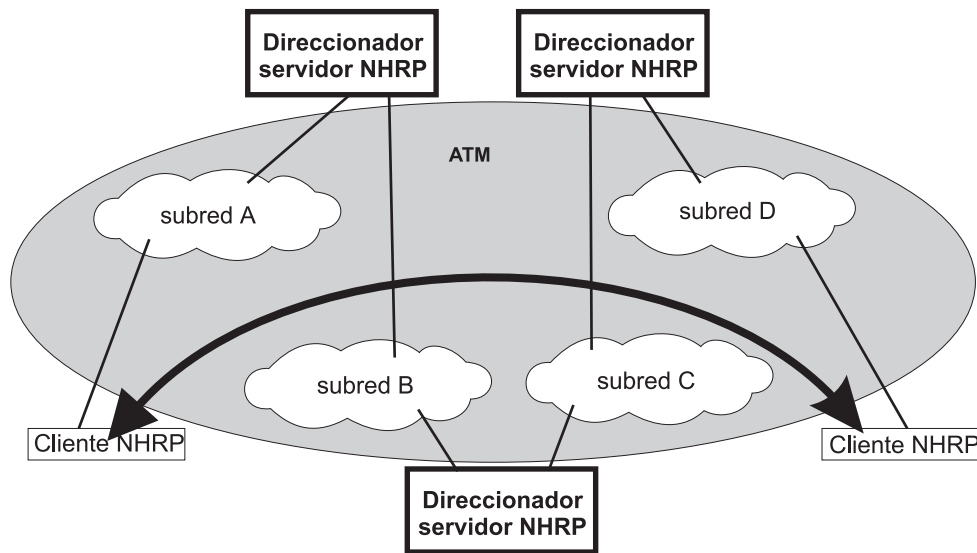
## Utilización de NHRP

Este capítulo describe cómo utilizar:

- El protocolo Next Hop Resolution Protocol (NHRP) especificado en Internet Draft Versión 13, que se ha sometido para el estado de RFC.

### Visión general de Next Hop Resolution Protocol (NHRP)

El protocolo Next Hop Resolution Protocol (NHRP) define un método para que una estación de origen determine la dirección de Acceso múltiple sin difusión (NBMA) del "siguiente salto" hacia un destino. El siguiente salto de NBMA puede ser el destino en sí o el direccionador de salida de la red de NBMA que esté "más cerca" de la estación de destino. Esta información de "siguiente salto" se denomina ruta o VC de "apertura (cut-through)" en la especificación de NHRP; para el direccionador, se utiliza el término "atajo (shortcut)" en lugar de "apertura (cut-through)". La estación de origen puede establecer entonces un circuito virtual de NBMA directamente con el destino o el direccionador de salida y reducir el número de saltos a través de la red.



VC de atajo para el tráfico cliente a cliente

Figura 26. Visión general de Next Hop Resolution Protocol (NHRP)

El 2216 puede utilizar NHRP con el fin de establecer atajos para el tráfico de IP sobre la red ATM de NBMA en las interfaces RFC 1483 y las relativas a las LAN emuladas (ELAN). El borrador de Internet no remite al uso de NHRP en un entorno de ELAN, pero el 2216 incluye mejoras para que se puedan utilizar las LAN. Estas mejoras se implementan actualmente a través de las extensiones privadas del proveedor que incluye la definición del protocolo NHRP.

El borrador sobre NHRP describe el flujo básico del protocolo del modo siguiente: los clientes NHRP registran sus direcciones de protocolo y sus direcciones de NBMA con uno o más servidores NHRP. Normalmente, los servidores son direccionadores en la vía de acceso direccionada a través de la red de NBMA hacia los clientes. Cuando un cliente desea establecer un atajo hacia un destino,

envía un paquete de petición de resolución de siguiente salto por la vía de acceso direccionada. La petición incluye la dirección de protocolo de destino. Los direccionadores (que también son servidores NHRP) de la vía de acceso direccionada comprueban en primer lugar si la dirección de protocolo de destino es una dirección que se pueda servir.

Si el direccionador puede satisfacer la petición, devuelve una respuesta de resolución de siguiente salto con la dirección de NBMA de la estación de destino. A continuación, el originador puede establecer un circuito virtual directo con el destino. Si no puede satisfacer la petición, el direccionador reenvía la petición al direccionador de siguiente salto. Este proceso de reenvíos continúa hasta que puede satisfacerse la petición o hasta que se determina que no puede accederse al destino.

Para utilizar la terminología de cliente/servidor, un dispositivo puede ser tanto un cliente como un servidor. El cliente es el dispositivo que origina peticiones de resolución de siguiente salto y el servidor es el que proporciona respuestas de resolución de siguiente salto con información sobre la dirección de NBMA. El 2216 es un dispositivo de este tipo; el cliente se "registra" conceptualmente con la función de servidor en la misma máquina, aunque no fluye ninguna petición de registro en realidad. El servidor también da soporte a registros de NHRP de clientes NHRP remotos.

La información proporcionada por los clientes a su servidor, y por los servidores a los peticionarios, debe renovarse periódicamente y puede eliminarse si lo requieren las condiciones. Los clientes y los servidores mantienen antememorias de la información de resolución que han enviado y recibido; se utilizan tiempos de mantenimiento para determinar la duración de las entradas o forzar las renovaciones.

## Ventajas de NHRP y la implementación por parte de IBM

En general, la utilización de los atajos de NHRP puede:

- Mejorar el rendimiento de final a final eliminando saltos entre direccionadores cuando el origen y el destino están en la misma red de NBMA y pueden comunicarse directamente
- Reducir la carga en direccionadores de red porque se ignoran para el tráfico que, sin NHRP, manejarían. Esto puede reducir los costes de actividad general al ser necesarios menos direccionadores o un ancho de banda menor.

La implementación de NHRP por parte de IBM proporciona estas ventajas adicionales:

- El borrador sobre NHRP no remite al uso del protocolo en un entorno de LAN emulada. No obstante la implementación de NHRP por parte de IBM incluye consideraciones acerca de estos entornos; pueden fluir paquetes de NHRP entre los direccionadores sobre conexiones ELAN y pueden establecerse VC de atajo.
- Direccionamiento de un solo salto: los dispositivos de ATM que no den soporte a NHRP pueden ser el destino de las vías de acceso de atajo, con la eliminación de otro salto de direccionador para el tráfico, al ampliarse la definición de los dispositivos que están "servidos" para que incluya los dispositivos que comparten una subred de protocolo con el servidor. Por ejemplo, todas las direcciones IP de una subred del IP clásico a la que pertenece un servidor están "servidas" por este servidor. La función de NHRP intercambia información con los componentes IP clásico 1577 y Emulación de LAN para utilizar

sus posibilidades de resolución de direcciones ATM existentes y aplicarlas a las peticiones de NHRP. Esta mejora puede utilizarse incluso para tráfico destinado a dispositivos conectados a LAN de legado que se conectan a ATM mediante conmutadores de LAN; el servidor NHRP del direccionador responde al cliente con información de sistema de dirección ATM para el conmutador de LAN, lo que permite que el cliente tome un atajo directo hacia este conmutador. Para obtener ejemplos de estos casos de “direccionamiento de un solo salto”, vea la Figura 26 en la página 439 y la Figura 27 en la página 442.

**Nota:** Un salto es una operación realizada por un direccionador tradicional al reenviar paquetes de una subred a otra. En particular, estas operaciones son (1) efectuar una búsqueda de un identificador de subred de la capa 3, (2) determinar el “siguiente salto” exterior para el paquete, (3) dismantelar y sustituir la cabecera del paquete de la capa 2: eliminar la información de enlace de entrada y añadir la información de enlace de salida. Por lo tanto, para el direccionamiento de “un solo salto”, esta operación tiene lugar una vez durante la transferencia de un paquete del origen al destino.

- La implementación por parte de IBM puede funcionar en redes en que algunos direccionadores no den soporte a NHRP. Si el direccionador de siguiente salto no puede proporcionar soporte a NHRP, pueden establecerse VC de atajo con el “último” servidor de la vía de acceso. Consulte la sección “Atajos de direccionador a direccionador anulados” en la página 451 y la sección “Listas de exclusión” en la página 449.
- El cliente puede configurar el 2216 de manera que establezca atajos únicamente cuando el tráfico dirigido a un destino sobrepase una velocidad de datos determinada. Esto puede eliminar la creación de VC para tráfico de volumen bajo o tráfico ocasional (por ejemplo, detecciones de condición de excepción de SNMP). Consulte el parámetro “data-rate” en la página 463 y el parámetro “attempt shortcuts?” en la página 462.
- El direccionador proporciona soluciones para el efecto de “dominó” que se describe en el borrador sobre NHRP. Consulte el parámetro “attempt shortcuts?” en la página 462.
- Todos los direccionadores conectados a ATM de la vía de acceso direccionada deberían dar soporte a NHRP para obtener las ventajas óptimas, aunque el 2216 también puede funcionar y proporcionar atajos en una red mixta.

## Características del rendimiento

NHRP se utiliza durante el contacto inicial de un dispositivo de origen con un destino. Una vez establecido un VC de atajo, el protocolo NHRP no está implicado en la transferencia real de datos. Las salvaguardas aseguran que no se realicen reintentos con el tráfico de NHRP para cada paquete. Además, la implementación por parte de IBM proporciona una opción para que se soliciten atajos de NHRP únicamente cuando el tráfico dirigido a un destino determinado sobrepase un umbral de velocidad de datos configurable. Con ello se puede impedir, por ejemplo, el establecimiento de circuitos virtuales que sólo se utilicen para una trama de detección de condición de excepción de SNMP generada por un sistema principal IP.

El funcionamiento de NHRP no afecta al rendimiento de la función de vía de acceso rápida del direccionador ni lo hará, de manera significativa, con respecto a la función de vía de acceso lenta. Cuando hay atajos disponibles, mejora el ren-

dimiento mediante la eliminación de saltos ajenos sobre la red ATM. Además, debe mejorar el rendimiento de los direccionadores intermedios que se ignoran debido a los atajos de NHRP porque manejan menos tráfico.

**Nota:** Si una configuración no incluye una interfaz 1577 (es decir, el direccionador sólo está configurado para las ELAN), sólo pueden establecerse VC de atajo para el direccionador desde los clientes que den soporte a las extensiones de IBM. Para evitar esta limitación, basta con definir una interfaz 1577 en el direccionador.

## Ejemplos de configuraciones de NHRP

Los párrafos siguientes ofrecen ejemplos de configuraciones de NHRP.

### NHRP en un entorno de IP clásico RFC 1577 en que todos los dispositivos tienen capacidad para NHRP

En esta representación, los clientes NHRP utilizan conexiones RFC 1577 para comunicarse con el direccionador. Utilizan el protocolo NHRP para aprender del servidor NHRP las direcciones ATM de cada cual. A continuación, establecen un circuito virtual directo entre ellos para el tráfico de IP.

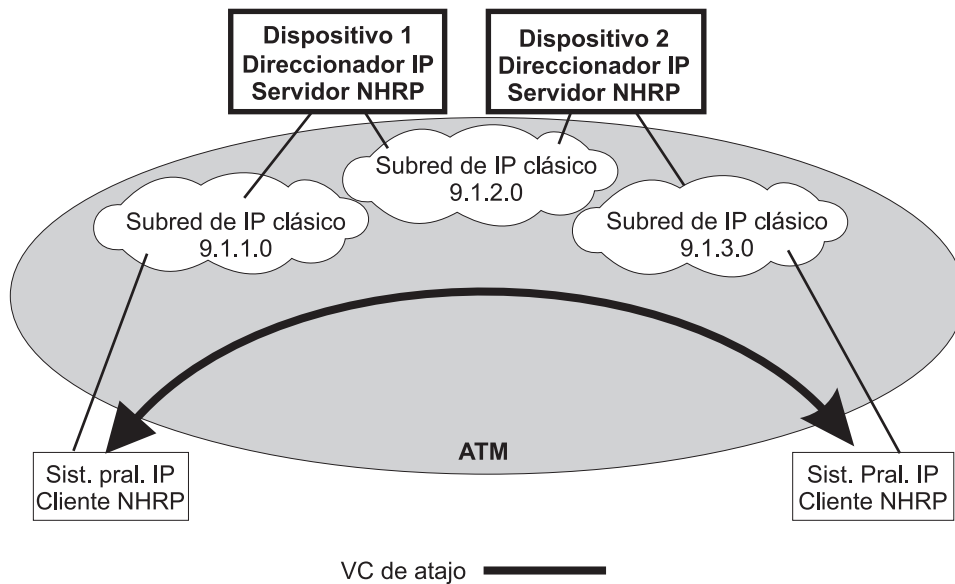


Figura 27. NHRP en un entorno de IP clásico

### NHRP en un entorno de IP clásico con dispositivo sin NHRP

Este ejemplo muestra cómo puede utilizarse NHRP entre dos dispositivos de 1577 cuando uno de ellos no da soporte a NHRP. Aquí, el Dispositivo2 proporciona al cliente NHRP la dirección ATM del dispositivo sin NHRP y el cliente puede establecer un atajo para el tráfico hacia el sistema principal sin NHRP. No obstante, cuando fluye tráfico desde el dispositivo sin NHRP, lo hace en la vía de acceso direccionada hacia el Dispositivo2; a continuación, el Dispositivo2 actúa como cliente NHRP y establece un atajo hacia el destino.

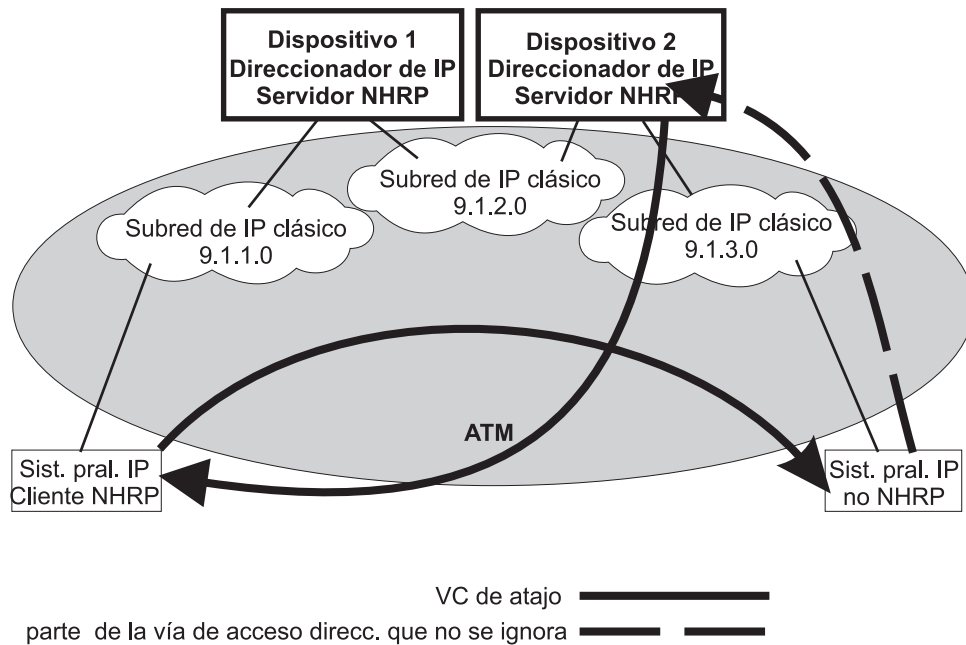


Figura 28. NHRP en un entorno de IP clásico con dispositivo sin NHRP

### NHRP en un entorno de emulación de LAN puro

En el caso de la emulación de LAN, los direccionadores utilizan las extensiones de IBM cuando proporcionan información de NBMA para los dispositivos de sus ELAN. Cuando el Dispositivo1 recibe tráfico del sistema principal A destinado al sistema principal B, origina una petición de resolución de siguiente salto y la envía por la vía de acceso direccionada. El Dispositivo2 responde a la petición con información de NBMA sobre el sistema principal B, una de las estaciones a las que sirve porque están en la misma ELAN. A continuación, el Dispositivo1 puede establecer un VCC directo de datos con el sistema principal B aunque éste no participe de los intercambios de NHRP o no les dé soporte. Tenga en cuenta que este VCC sólo se utilizará para el tráfico orientado del A al B. De forma similar, cuando el sistema principal B envía tráfico al sistema principal A, el Dispositivo2 genera una petición de resolución de siguiente salto, el Dispositivo1 responde con información de sistema de dirección sobre el sistema principal A, y el Dispositivo2 establece un VCC directo de datos con el A para el tráfico del B al A.

Los LEC de este ejemplo son dispositivos ajustados a la norma sin soporte de NHRP. Deben satisfacer los requisitos de LEC descritos en la sección "Implementación de NHRP" en la página 446).

No es necesaria una configuración especial en estos dispositivos ni en los servidores NHRP. El tráfico de NHRP fluye sobre la subred ELAN sin VC adicionales.

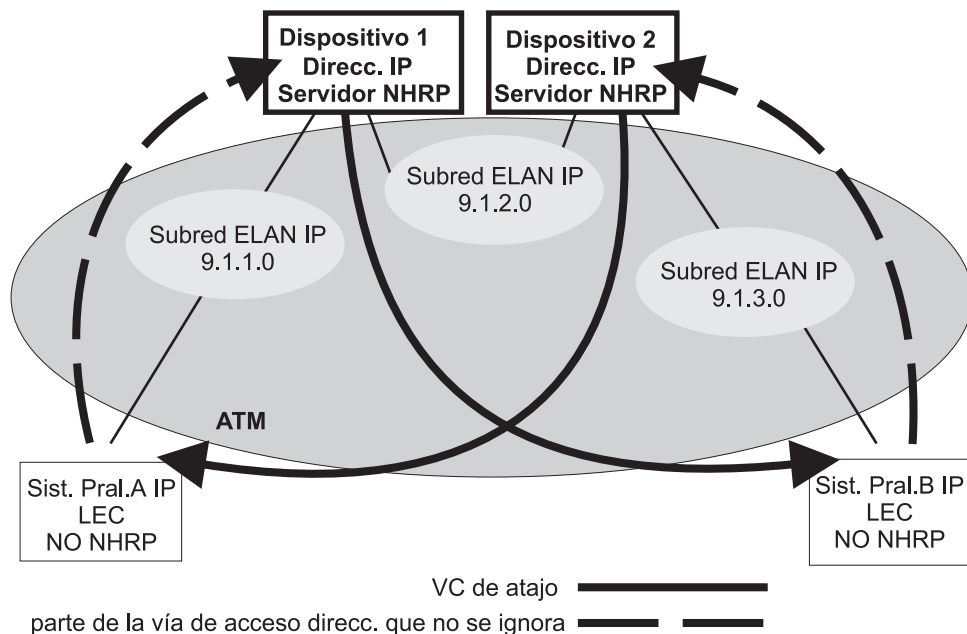


Figura 29. NHRP en un entorno de ELAN

### NHRP en un entorno de emulación de LAN con conmutadores de LAN

En este ejemplo, la estación de origen y la de destino están conectadas a LAN de legado y no se conectan a la red ATM. Los conmutadores de LAN que funcionan como clientes de emulación de LAN proporcionan la conectividad de ATM a los dispositivos de LAN de legado. Las mejoras en NHRP y las extensiones de IBM permiten el mismo tipo de "direccionamiento de un solo salto" en este entorno que el descrito en el ejemplo anterior. Con las mejoras, los servidores intercambian la información de direccionamiento y las direcciones MAC reales para los dispositivos de LAN de legado. A continuación, los 2216 pueden establecer VCC directos de datos con los conmutadores y pasar el tráfico de forma directa. Sólo hay un "salto" de direccionador en la vía de acceso, aunque el tráfico pasa por dos conmutadores de LAN.

Este ejemplo también ilustra que el entorno de ELAN puede ser de Red en Anillo, Ethernet o de cualquier mezcla de tipos de LAN.

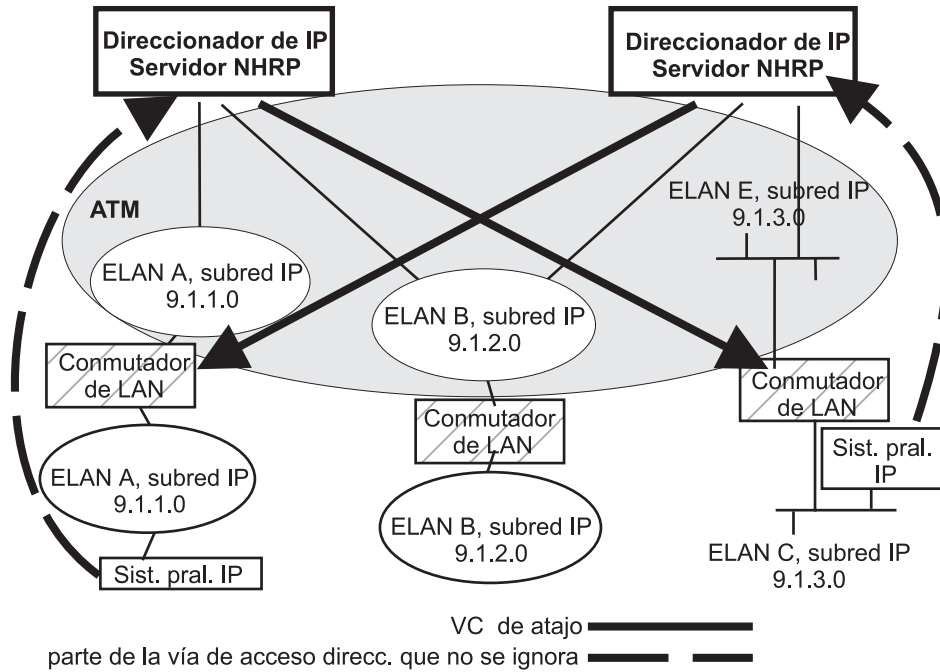


Figura 30. NHRP en un entorno de ELAN con conmutadores de LAN

### NHRP en un entorno mixto de IP clásico y ELAN

La función de NHRP del direccionador puede funcionar con las interfaces IP clásico y ELAN en la misma red. En este ejemplo, el cliente NHRP da soporte a las extensiones de IBM y puede crear un atajo directo hacia el LEC de destino para el tráfico con esta orientación.

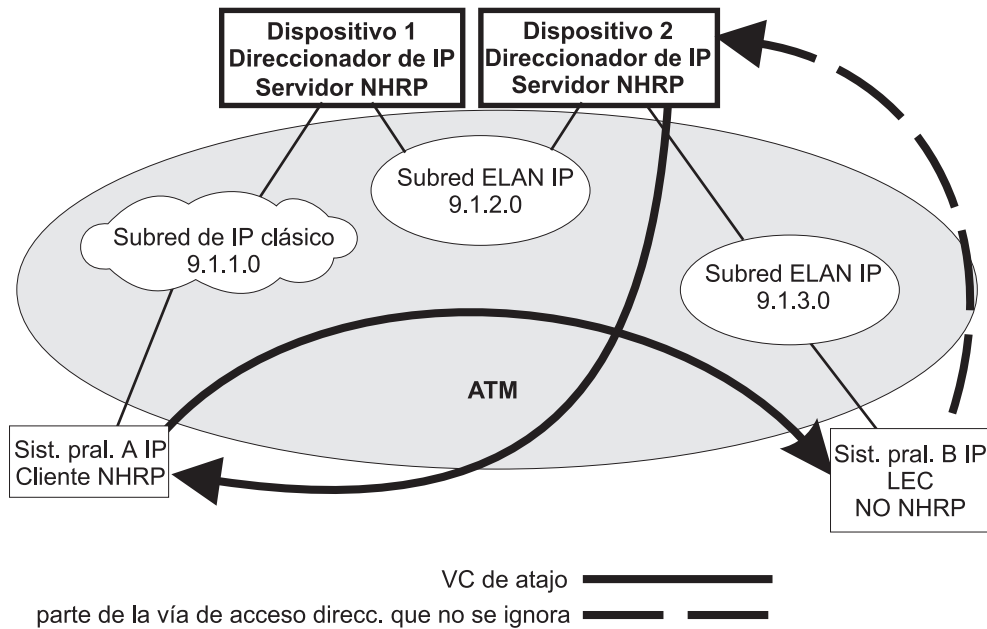


Figura 31. NHRP en un entorno mixto de IP clásico y ELAN

### NHRP para un direccionador de salida

Las estaciones de origen y/o destino del tráfico de protocolo no tienen que pertenecer a subredes servidas por participantes de NHRP. Pueden acceder a la red ATM mediante direccionadores que se comuniquen con los dispositivos de NHRP. En este caso, el 2216 proporciona atajos a través de la red ATM para eliminar el mayor número de saltos posible.

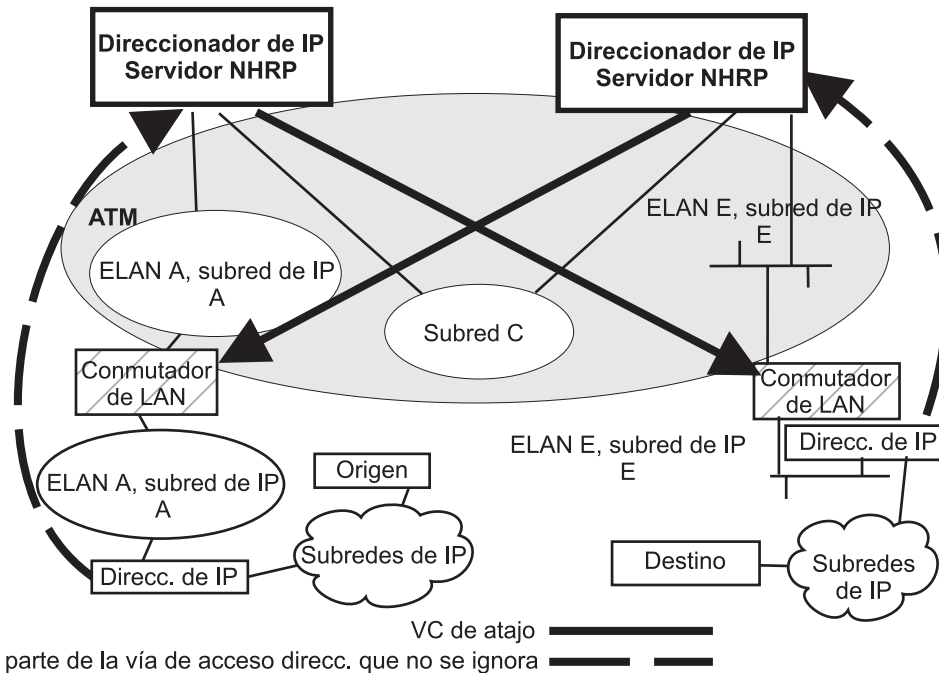


Figura 32. NHRP para un direccionador de salida

### Implementación de NHRP

NHRP interactúa con la función de direccionador del direccionador. Cuando la función de direccionador del direccionador sea reenviar paquetes por la vía de acceso direccionada y NHRP obtenga satisfactoriamente un VC de atajo, NHRP actualizará la función de direccionador de manera que envíe el paquete directamente sobre el VC de atajo.

NHRP actualiza la tabla de reenvíos de la función de direccionamiento una vez activado el VC. Esto permite que la conmutación de la vía de acceso direccionada por la vía de acceso de atajo se produzca sin la pérdida de ningún paquete.

Cuando se utiliza un atajo de NHRP, el direccionador transmite tramas a una dirección de siguiente salto de una red a la que el direccionador en sí no pertenece. Por lo tanto, la RED, o interfaz, que proporciona la vía de acceso exterior para el tráfico es una interfaz de red "virtual".

#### Virtual Network Interface (VNI)

Normalmente, el flujo de paquetes exteriores de un direccionador está restringido por lo siguiente:

- Inhabilitación para el envío directo de paquetes a direcciones de red que no estén definidas en una interfaz de red.



- Inhabilitación para el envío de paquetes a tipos de redes (por ejemplo, ELAN Red en Anillo) a menos que el tipo de red esté definido en una interfaz de red.

El manejador de red de Virtual Network Interface (VNI) elimina todas estas restricciones, lo que permite que el direccionador reenvíe paquetes directamente a siguientes saltos obtenidos mediante NHRP (rutas de atajo). Habilita el direccionamiento de un solo salto, en el que pueden crearse rutas de atajo de NHRP directamente hacia dispositivos que no dan soporte a NHRP.

VNI da soporte a las interfaces de red Red en Anillo, Ethernet V2 y Ethernet DIX ELAN y a las interfaces de red IP clásico. Cuando la vía de acceso exterior debe utilizar una interfaz IP clásico (1577), la implementación utiliza en realidad la interfaz del manejador de red 1577 existente para VNI. No obstante, cuando la vía de acceso exterior debe utilizar un atajo de LANE, se accede a una interfaz exclusiva. Ésta se denomina LANE Shortcut Interface (LSI). La interfaz LSI es diferente de una interfaz LEC tradicional porque puede proporcionar más de un tipo de encapsulación de LAN; es decir, puede establecerse un VC que utilice la encapsulación de Red en Anillo mientras otro utiliza Ethernet V2. Además, LSI proporciona conexiones con más de una LAN emulada; una interfaz LEC tradicional se conecta con una sola ELAN.

Cuando se habilita NHRP, se crea una LSI para cada adaptador de ATM. Se asigna a LSI el siguiente número de interfaz disponible, y aparecerá listada cuando invoque funciones de consola que visualicen información sobre las interfaces del direccionador.

### **LANE Shortcut Interface (LSI)**

Los atajos de LANE proporcionados por las extensiones de IBM para NHRP no son compatibles con algunas implementaciones de pilas de protocolos de estación final y Cliente de emulación de LAN (LEC). Esta sección describe cómo pueden surgir estas incompatibilidades y, en algunos casos, cómo pueden solucionarse mediante opciones de la configuración.

Los clientes LEC Paranoid son dispositivos que utilizan el Flush Protocol de Emulación de LAN para verificar si los clientes que configuran VCC directos de datos con éste son realmente miembros de su ELAN. Estos dispositivos no funcionarán con atajos de NHRP generados por interfaces LSI porque LSI no forma parte de la ELAN de destino.

**Nota:** Puede utilizarse la opción de configuración relativa a una “Lista de exclusión” para evitar atajos hacia los LEC Paranoid tal como se describe en la sección “Listas de exclusión” en la página 449.

Por omisión, LSI utilizará la dirección MAC incorporada en el adaptador de ATM asociado como la dirección MAC de origen de las tramas transmitidas sobre los VCC de atajo de LANE. Es posible, aunque improbable, que esto pueda suponer una confusión en algunas implementaciones de pilas de protocolos de estación final, ya que la dirección MAC no coincidirá con la del direccionador que la estación final utilice como pasarela para transmitir paquetes a la dirección IP asociada.

Para que esto sucediese, la estación final tendría que aprender direcciones MAC de direccionador de las tramas de IP de vertimiento único, que no es lo normal (normalmente, las correlaciones de dirección IP con dirección MAC se aprenden de los paquetes de ARP). Si llegase a suceder, la estación final podría utilizar la direc-

ción MAC aprendida como la dirección MAC de destino de las tramas que transmite al destino de IP asociado en lugar de utilizar la dirección MAC del direccionador. Estas tramas se eliminarían o se reenviarían sobre el VCC de atajo de LANE. El reenvío sólo se produciría si el LEC aprendiese la combinación de dirección MAC con dirección ATM de las tramas recibidas (que es una elección de la implementación opcional).

En cualquier caso, estas tramas no alcanzarán al destino porque LSI desecha las tramas recibidas sobre un VCC de atajo de LANE. Además, LSI libera el VCC de atajo de LANE y no se establecerán más atajos para la dirección ATM asociada. El tráfico dirigido a los destinos asociados con esa dirección ATM seguirá la vía de acceso direccionada a partir de entonces. Tenga en cuenta que los mensajes del ELS y la visualización de la consola en relación con los atajos de LANE sirven de ayuda para identificar estos destinos.

Puede configurarse LSI de manera que no utilice la dirección MAC administrada universalmente como dirección MAC de origen. Con esta opción, tiene dos elecciones para la dirección MAC de origen:

1. Puede utilizar la dirección MAC del direccionador de último salto, proporcionado en el paquete de respuesta de resolución de NHRP, como dirección MAC de origen.

Si se utiliza la dirección MAC del direccionador de último salto como dirección MAC de origen, se soluciona el problema de la confusión en las pilas de protocolos de estación final pero se genera otro problema en potencia. Puede crear confusión en los LEC que aprenden la combinación de dirección MAC con dirección ATM de las tramas recibidas, por lo que no debe utilizarse con LEC que realicen este tipo de aprendizaje. Por ejemplo, el LEC del puente ATM-LAN de 8281 de IBM realiza este tipo de aprendizaje.

2. Puede configurar la dirección MAC de origen.

Puede configurarse la dirección MAC de origen para evitar el problema de las direcciones MAC duplicadas que se ven en una ELAN a causa de atajos inter-ELAN. Debe configurarse la dirección MAC para esta red LSI cuando haya alguna entrada de atajo de LANE anulado. Consulte la sección "LANE Shortcuts" en la página 469 para obtener detalles sobre la visualización de entradas de atajo de LANE anulado.

Estas opciones de la configuración se proporcionan con el fin de maximizar la flexibilidad para conseguir una compatibilidad con el mayor conjunto de destinos posible en una instalación determinada. Consulte la sección "Configuración de LANE Shortcuts Interface (LSI)" en la página 453 para obtener más información y la sección "Change" en la página 460 para obtener una descripción del mandato **change**.

## Parámetros de configuración

Esta sección describe algunos de los parámetros de configuración relacionados con NHRP y cómo se recomienda que se utilicen. Consulte el apartado "Mandatos de configuración de NHRP" en la página 455 para conocer la sintaxis de los mandatos, los parámetros de los mandatos, los valores válidos y los valores por omisión.

## Configuración automática de NHRP

NHRP se habilita por omisión si IP está presente en el equipo. Puede inhabilitarse entrando el mandato **disable NHRP** desde el indicador `NHRP config>`. Consulte la sección “Acceso al proceso de configuración de NHRP” en la página 455 para obtener información adicional.

Cuando se utiliza un archivo de configuración existente, NHRP se habilita por omisión si no se había configurado anteriormente. El archivo de configuración se actualizará automáticamente durante la ejecución para crear interfaces de atajo de NHRP. Tiene que guardar este archivo de configuración actualizado y rearrancar para que el cliente NHRP utilice atajos de LANE.

## Listas de exclusión

La configuración le permite crear una lista de direcciones de protocolo (y las máscaras asociadas) que representen dos tipos de dispositivos:

- Direccionadores de siguiente salto que no contienen una función de servidor NHRP
- Dispositivos de destino con los que no deben permitirse VC de atajo

**Direccionadores de siguiente salto:** Puede utilizarse la lista de exclusión para identificar los direccionadores que están en la vía de acceso direccionada pero no dan soporte a la función de servidor NHRP.

El servidor responde a una petición de resolución de siguiente salto proporcionando la dirección ATM del direccionador de siguiente salto cuando es verdad todo lo siguiente:

- La dirección de siguiente salto es diferente de la dirección de destino.
- La interfaz del direccionador relativa al direccionador de siguiente salto es una subred de IP clásico de ATM o ELAN.
- La dirección de siguiente salto está en la lista de exclusión.

Al procesar la petición, el direccionador no reenvía la petición de resolución a la dirección de siguiente salto, sino que responde al cliente con información de sistema de dirección que permita al cliente establecer un VC de atajo con el direccionador de siguiente salto.

**Nota:** Si el direccionador de siguiente salto es uno de los atajos R2R anulados, el direccionador envía un mensaje NAK a la petición de resolución en lugar de una respuesta positiva.

En general, si el direccionador de siguiente salto está en la lista de exclusión, el direccionador no le envía ningún paquete de NHRP que sólo pueda manejar un servidor NHRP.

**Dispositivos de destino:** La lista de exclusión también puede utilizarse para evitar VC de atajo con una dirección de protocolo determinada (por ejemplo, un dispositivo de una red CIP o ELAN que sólo puede dar soporte a un número reducido de VC).

Al procesar una petición de resolución de siguiente salto para un dispositivo de destino, el servidor responde al cliente con información de sistema de dirección

que permita al cliente establecer un VC de atajo con el direccionador en sí cuando es verdad todo lo siguiente:

- La dirección de siguiente salto es igual que la dirección de destino.
- La interfaz del direccionador relativa al destino es una subred de IP clásico de ATM o ELAN.
- La dirección de destino está en la lista de exclusión.

### Extensiones

El protocolo NHRP incluye las **Extensiones**. Las extensiones se añaden a los paquetes de NHRP. Éstas se utilizan para solicitar funciones adicionales de los partícipes de NHRP. El uso del parámetro **extensions** le permite determinar si el direccionador enviará ciertas extensiones:

- extensiones de información de vía de acceso
- extensiones privadas del proveedor IBM

**Extensiones de información de vía de acceso:** En NHRP están definidas tres extensiones para proporcionar información de vía de acceso. Pueden utilizarse estas extensiones para ayudar a supervisar la petición en sí, para determinar la vía de acceso que ha tomado la petición y para determinar quién ha generado la respuesta así como la vía de acceso que ha tomado la respuesta. Las extensiones de información de vía de acceso son las siguientes:

- Transmisión hacia adelante - Cada servidor de siguiente salto (NHS) que reenvíe la petición por la vía debe añadir información sobre sí mismo.
- Dirección del que responde - El servidor de siguiente salto (NHS) que genere la respuesta debe añadir información sobre sí mismo.
- Transmisión invertida - Cada servidor de siguiente salto (NHS) que reenvíe la respuesta por la vía debe añadir información sobre sí mismo.

Puede configurarse el direccionador de manera que envíe cualquiera de estas extensiones, o todas ellas, en los paquetes de petición de resolución de siguiente salto que genere. La información recibida en los paquetes de respuesta se visualiza en los mensajes de NHRP del ELS del direccionador.

**Extensiones privadas del proveedor IBM:** Para dar soporte a NHRP en un entorno de LAN emulada, el servidor añade extensiones exclusivas del proveedor a los paquetes de NHRP. Estas extensiones actúan como “consultas”; el cliente NHRP las coloca en la petición de resolución de siguiente salto. Si el servidor da soporte a esta función, responde con las tres extensiones correspondientes que contienen información de sistema de dirección ELAN (dirección MAC, dirección ATM e información de direccionamiento); estas extensiones se incluyen en la respuesta de resolución de siguiente salto.

Puede configurarse el direccionador de manera que no dé soporte a las extensiones específicas de IBM. Si no se utilizan las extensiones específicas de IBM, no son posibles los atajos directos hacia dispositivos de ELAN. Utilice la opción relativa a una “Lista de exclusión” para anular de manera selectiva atajos hacia ciertos dispositivos de ELAN.

### Atajos de direccionador a direccionador anulados

El funcionamiento de NHRP puede dar como resultado el establecimiento de vías de acceso de tránsito a través de la red de NBMA entre direccionadores. No obstante, el establecimiento de un atajo de NHRP a través de una frontera donde se pierde la información utilizada en la selección de ruta puede dar como resultado un bucle de direccionamiento. Estas situaciones incluyen la pérdida de la información de vector de vía de acceso de BGP y la interacción de diversos protocolos de direccionamiento con métricas distintas. En tales circunstancias, deben anularse atajos de NHRP entre direccionadores. Puede evitarse esta situación si no hay vías de acceso de “puerta trasera” entre el direccionador de entrada y el de salida fuera de la red NBMA.

El servidor permite atajos de direccionador a direccionador (R2R) por omisión. No obstante, configurando atajos R2R anulados, puede crear una lista de direcciones de destino o de direccionador para las que el direccionador no permita atajos.

Para crear un atajo R2R anulado, debe especificar una dirección de protocolo y una máscara. La dirección de protocolo es el destino de un direccionador y la máscara permite un rango de direcciones.

Como ilustración de la manera de especificar atajos R2R anulados utilizando direcciones de protocolo y máscaras, tome en consideración el siguiente diagrama de red:

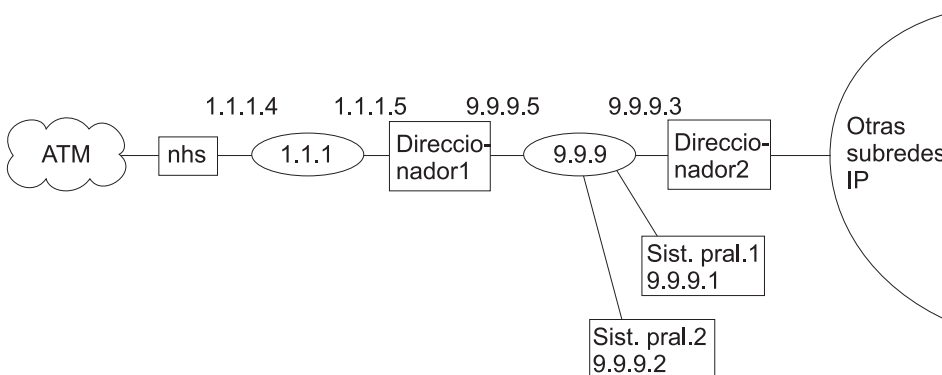


Figura 33. Utilización de atajos de direccionador a direccionador anulados

**Ejemplo 1:** Una entrada con *dirección=9.9.9.1 máscara=255.255.255.255* causará que el NHS envíe un mensaje NAK al emisor de una petición de resolución de siguiente salto con la dirección de protocolo de destino 9.9.9.1 (SISTEMA PRINCIPAL1). Puesto que el 9.9.9.1 no está conectado directamente a una de las subredes del dispositivo, pero otro direccionador puede llegar a él, el direccionador comprueba la lista de atajos R2R anulados.

**Ejemplo 2:** Una entrada con *dirección=9.9.9.0 máscara=255.255.255.0* causará que el direccionador envíe un mensaje NAK a cualquier dirección de destino de la 9.9.9.1 a la 9.9.9.255. No se ha podido llegar al SISTEMA PRINCIPAL1, al SISTEMA PRINCIPAL2 ni al DIRECCIONADOR2 utilizando atajos hacia el direccionador, pero se ha podido llegar a los dispositivos de las otras subredes que reciben servicios del DIRECCIONADOR2.

**Ejemplo 3:** Una entrada con *dirección=1.1.1.5 máscara=255.255.255.255* causará que el direccionador responda negativamente para cualquier

destino cuyo direccionador de siguiente salto sea 1.1.1.5, el DIRECCIONADOR1. El direccionador responderá negativamente para cualquier dirección de la subred 9.9.9 y para cualquier dirección de las otras subredes IP a la que se llegue mediante el direccionador 9.9.9.3 porque el siguiente salto es 1.1.1.5.

**Ejemplo 4:** Una entrada con *dirección=cualquiera máscara=0.0.0.0* inhabilitará atajos R2R para todas las direcciones.

### Utilización del control del acceso al protocolo

El parámetro relativo a este título determina si se comprobarán los controles del acceso a la capa del protocolo y, si es así, cómo se aplicarán estos controles a los paquetes de NHRP.

Si este parámetro de configuración se establece en su valor por omisión de *none*, no se comprobarán los controles del acceso a la capa del protocolo.

Con el valor de *source and destination*, cuando el peticionario NHRP no es un direccionador, se supone que la dirección IP del cliente NHRP es el origen de todos los paquetes de IP que transmitirá ese cliente por medio de la ruta de atajo de NHRP. El direccionador rechaza peticiones de atajo de NHRP de un cliente NHRP que no sea direccionador si se va a filtrar cualquier paquete de IP para ese par de direcciones de origen/destino de IP, donde el origen es la dirección del cliente NHRP.

La selección de la opción *destination only* hace que el direccionador rechace peticiones de atajo de cualquier cliente NHRP si se va a filtrar cualquier paquete de IP para la dirección de destino. Si no se debe contar con clientes NHRP, debe seleccionarse *destination only*. *destination only* puede ser la mejor opción cuando los clientes NHRP son clientes no direccionadores con diversas direcciones IP o clientes no direccionadores que transmiten paquetes que parten de otros orígenes.

Los clientes NHRP que residen en los direccionadores utilizan las rutas de atajo de NHRP para reenviar paquetes de otros orígenes: por lo tanto, si se configura *source and destination* y el direccionador recibe una petición de atajo de un direccionador, el direccionador aplicará los filtros de IP de la misma manera que cuando se selecciona *destination only*.

### Controles del acceso a NHRP

Los controles del acceso a NHRP para rechazar atajos hacia ciertas direcciones IP pueden definirse añadiendo estas direcciones tanto a la lista de exclusión como a la lista de atajos de direccionador a direccionador anulados.

### ID de red ATM

Puesto que un servidor puede tener más de un adaptador de ATM, puede conectarse a dos redes diferentes o no asociadas. Esto debe tomarse en consideración a la hora de decidir cuándo deben permitirse VC de atajo.

Puede determinar qué interfaces deben tratarse como si estuvieran conectadas a la misma red ATM física asignando a cada interfaz ATM un ID de red por medio del mandato **set** en el indicador ATM Interface Config>, tal como se describe en el capítulo "Utilización y configuración de ATM" de la publicación *Guía del usuario de software*.

Las interfaces ATM con el mismo ID de red se consideran pertenecientes a la misma red. Por omisión, todas las interfaces ATM se asignan al ID de red 0.

### Configuración de LANE Shortcuts Interface (LSI)

La interfaz para NHRP LANE Shortcut Interface (LSI) se crea automáticamente para cada adaptador de ATM cuando se habilita NHRP en el direccionador. LSI utiliza valores por omisión para los parámetros siguientes:

- El parámetro de ESI
- El de selector
- El uso del servicio Mayor Eficacia para los VCC
- La velocidad punta de célula de los VCC de datos exteriores
- La velocidad sostenida de célula de los VCC exteriores
- El uso de la dirección MAC administrada universalmente del adaptador de ATM para el origen

Los valores por omisión pueden modificarse utilizando el mandato **change** desde el indicador NHRP Advanced config>. Consulte la sección "Change" en la página 460.

### Configuración de dispositivos en una red ATM

Si tiene un cliente/servidor NHRP y su configuración necesita que el usuario proporcione la dirección ATM del servidor NHRP direccionador, debe seleccionar la dirección ATM correcta. Debe utilizar una dirección asociada con una "interfaz ATM" del dispositivo y debe asignarse una dirección IP a esta interfaz. Los dos últimos dígitos de la dirección ATM del direccionador, el selector, se asignan dinámicamente después de que el direccionador se active (y pueden cambiar si cambia la configuración del direccionador) a menos que haya configurado un selector específico.

Puede especificar la dirección ATM, incluido el selector, entrando **prot arp** en el indicador Config> de talk 6, seguido de **add atm**, proporcionando la dirección IP conveniente y, a continuación, especificando un selector. Este es el mismo procedimiento que se utiliza para definir un cliente ATMARP.

### Utilización de NHRP con Emulación de LAN

Si desea utilizar NHRP en el dispositivo, debe configurar todos los LEC con una dirección MAC administrada localmente (LAA) exclusiva. Si no configura los LEC con LAA exclusivas, la posibilidad de atajos de NHRP hacia el dispositivo o conmutador correspondiente no funcionará porque:

- El tráfico enviado sobre un VCC de atajo de NHRP LANE contendrá la dirección MAC Administrada Universalmente (administrada universalmente) como dirección MAC de origen.
- Algunos dispositivos de red aprenden la asociación entre la dirección MAC y el VCC del tráfico que ha recibido el dispositivo. Estos dispositivos utilizan, pues, el VCC de NHRP para transmitir datos.
- Si el direccionador detecta tráfico de entrada en un VCC de NHRP, supondrá que se ha producido una condición de error y concluirá este VCC para impedir que haya más atajos hacia este dispositivo de red.

**Nota:** Por omisión, el direccionador habilita las extensiones para Emulación de LAN en NHRP, por lo que el usuario debe inhabilitar las extensiones o configurar la dirección MAC administrada localmente exclusiva para cada LEC.





## Configuración y supervisión de NHRP

Este capítulo describe cómo configurar y supervisar el protocolo Next Hop Resolution Protocol (NHRP). Para obtener una descripción del mismo, consulte el apartado “Visión general de Next Hop Resolution Protocol (NHRP)” en la página 439.

Este capítulo contiene los apartados siguientes:

- “Acceso al proceso de configuración de NHRP”
- “Mandatos de configuración de NHRP”
- “Acceso al proceso de supervisión de NHRP” en la página 466
- “Mandatos de supervisión de NHRP” en la página 466
- “Rastreo de paquetes de NHRP” en la página 472
- “Soporte de la reconfiguración dinámica de servidor de NHRP” en la página 473

### Acceso al proceso de configuración de NHRP

Para acceder a la configuración de NHRP:

1. En el indicador de supervisión del operador (\*), escriba **talk 6** y pulse Intro.
2. En el indicador **config>**, escriba **protocol nhrp** y pulse Intro.
3. Se visualizará el indicador **NHRP config>**.

### Mandatos de configuración de NHRP

Este apartado explica todos los mandatos de configuración de NHRP mostrados en la Tabla 110. Entre los mandatos en el indicador **NHRP config>**.

<i>Tabla 110. Resumen de los mandatos de configuración de NHRP</i>	
Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi.
Enable NHRP	Activa NHRP para todas las interfaces que no estén definidas de forma explícita.
Disable NHRP	Desactiva NHRP para todas las interfaces que no estén definidas de forma explícita.
List	Visualiza la configuración de NHRP.
Advanced config	Le lleva al indicador <b>NHRP Advanced config&gt;</b> , desde el cual puede entrar otros mandatos, que se describen en “Mandatos de configuración avanzada de NHRP” en la página 457.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

### Enable NHRP

Utilice el mandato `enable` para habilitar NHRP en todas las interfaces no definidas de forma explícita por medio de un mandato de configuración avanzada de NHRP. Es una manera fácil de hacer que NHRP se active y ejecute con los parámetros por omisión.

**Sintaxis:**

```
enable          nhrp
```

### Disable NHRP

Utilice el mandato `disable` para inhabilitar NHRP en todas las interfaces no definidas de forma explícita por medio de un mandato de configuración avanzada de NHRP.

**Sintaxis:**

```
disable         nhrp
```

**Ejemplo:**

```
NHRP config> disable  
  Disable NHRP for the router [No]:
```

### Advanced Config

Utilice el mandato `advanced` para obtener el indicador de configuración avanzada de NHRP: `NHRP Advanced config>`. Desde este indicador, puede entrar los mandatos descritos en “Mandatos de configuración avanzada de NHRP” en la página 457.

**Sintaxis:**

```
advanced       nhrp
```

**Ejemplo:**

```
NHRP config> advanced  
  NHRP Advanced config>
```

**Nota:** La mayoría de las instalaciones no necesitarán el uso del mandato “advanced”. Basta con el mandato `enable NHRP` para habilitar NHRP con las opciones por omisión recomendadas.

### List

Utilice el mandato `list` para listar la configuración de NHRP.

**Sintaxis:**

```
list
```

**Ejemplo:**

```
NHRP config> list
Box level NHRP enabled
  Explicit interface definitions override box level setting

Interfaces explicitly defined for NHRP
-----
Interface 0: ATM
  NHRP enabled

NHRP LANE Shortcut Interface:
-----
Interface: 1  ESI: burned-in          Sel: auto
Use Best Effort: no  (Data)
Cell Rate(kbps):  Peak: 155000    Sustained: 155000
ATM adapter's burned-in MAC address is used as source address

General Parameters
-----
Holding time:                               20 minutes
Protocol Access Controls:                   Use source and destination  address
When should NHC attempt shortcuts?:         Based on datarate
Data-rate threshold:                        10 packets/second
NHS allows shortcuts to ATMARP clients?:    Yes

Cache Sizes
-----
Resolution cache:                          10000 entries
Server purge cache:                        10000 entries
Server registrations cache:                10000 entries

Extension Usage
-----
Use NHRP Forward transit NHS record client extension: No
Use NHRP Reverse transit NHS record client extension: No
Use Responder Address client extension:     No
Use LANE shortcuts extension:               Yes

List of NHRP IP exclude records
-----
# Address      Mask
1 6.6.6.6      255.255.255.255
2 5.5.5.0      255.255.255.0

Disallowed router-to-router shortcuts for IP
-----
None
```

---

## Mandatos de configuración avanzada de NHRP

Este apartado explica todos los mandatos de configuración avanzada de NHRP mostrados en la Tabla 111 en la página 458. Entre los mandatos desde el indicador NHRP Advanced config>.

Tabla 111. Resumen de los mandatos de configuración avanzada de NHRP	
Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi.
Add	Añade una interfaz NHRP, una lista de exclusión o atajos R2R anulados.
Change	Cambia una interfaz NHRP o cambia una definición de interfaz de atajo de LANE.
Delete	Suprime una interfaz NHRP, una lista de exclusión o atajos R2R anulados.
List	Visualiza la configuración de NHRP.
Set	Establece los parámetros de NHRP.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

## Add

Utilice el mandato **add** para añadir una definición explícita de interfaz, una entrada de lista de exclusión o atajos de direccionador a direccionador anulados.

### Sintaxis:

```
add          interface definition
              exclude list
              disallowed router-to-router shortcuts
```

### interface definition

Añade una definición explícita de interfaz para habilitar o inhabilitar una interfaz NHRP. Si NHRP se inhabilita en una interfaz de red en particular, no se reenviarán paquetes de NHRP a ningún direccionador al que se llegue mediante esa interfaz. Además, se desecharán las tramas de NHRP de entrada.

**Nota:** Cualquier definición explícita de interfaz altera temporalmente el valor de “habilitación/inhabilitación de NHRP” general.

**Ejemplo:** **add int**

```
Interface Number [0]?
Enable NHRP [Yes]:
```

### exclude list

Añade una entrada de lista de exclusión. Especifique una dirección de protocolo que deba excluirse de la red NHRP. Esta opción añade una entrada de lista de exclusión y realiza una solicitud para añadir la entrada de lista de exclusión a los atajos de direccionador a direccionador anulados. Consulte la sección “Controles del acceso a NHRP” en la página 452 para obtener más información.

**Valores válidos:** Una dirección IP y una máscara.

**Valor por omisión:** Vacío.

**Ejemplo:** **add exc**

```
IP Address [0.0.0.0]? 6.6.6.5
Address Mask [255.255.255.255]?
Deny Shortcuts[Yes]?
Record added to Disallowed Router-to-Router Shortcuts
Record added to Exclude List
```

### disallowed router-to-router shortcuts

Añade una dirección de protocolo de direccionador hacia la que no se permiten atajos.

Consulte la sección “Atajos de direccionador a direccionador anulados” en la página 451 para obtener más información.

#### Ejemplo: add dis

```
IP ADDRESS [0.0.0.0]? 8.8.8.1
Address Mask [255.255.255.255]?
```

**Valores válidos:** Una dirección IP y una máscara.

**Valor por omisión:** Vacío.

## Delete

Utilice el mandato **delete** para suprimir una definición de interfaz para NHRP, una entrada de lista de exclusión o atajos de direccionador a direccionador anulados.

### Sintaxis:

```
delete          interface definition for NHRP
                  exclude list
                  disallowed router-to-router shortcuts
```

### interface definition for NHRP

Suprime una definición explícita de interfaz NHRP.

#### Ejemplo: de1 int

```
Interface Number [0]?
```

### exclude list

Suprime una entrada de lista de exclusión. Esta opción suprime una entrada de lista de exclusión y realiza una solicitud para suprimir la entrada de los atajos de direccionador a direccionador anulados. Consulte la sección “Controles del acceso a NHRP” en la página 452 para obtener más información.

Debe especificar un índice que deba suprimirse. Utilice el mandato **list exclude** para determinar el índice correcto.

#### Ejemplo: de1 exc

```
Enter index of access control to be deleted [1]?
# Address      Mask
1 6.6.6.6      255.255.255.255
Are you sure this the record you want to delete [Yes]?
Record deleted from Exclude List
Delete from Disallowed Router-to-Router Shortcuts [Yes]?
Record deleted from Disallowed Router-to-Router Shortcuts
```

### disallowed router-to-router shortcuts

Suprime una entrada de los atajos de direccionador a direccionador anulados. Debe especificar un índice que deba suprimirse. Utilice el mandato **list disallowed** para determinar el índice correcto.

#### Ejemplo: de1 dis

Disallowed shortcuts index [1]?

### Change

Utilice el mandato **change** para modificar definiciones de interfaz NHRP.

#### Sintaxis:

```
change          interface definition  
                  nhrp lane shortcut interface
```

#### interface definition for NHRP

Cambie una definición explícita de interfaz para habilitar o inhabilitar una interfaz NHRP.

#### Ejemplo: ch int

```
Interface Number [0]?  
Enable NHRP [Yes]:
```

#### NHRP LANE shortcut Interface

Cambie una definición de interfaz de atajo de LANE.

#### Ejemplo: ch nhrp

```
Interface Number of NHRP LANE Shortcut Interface [0]?  
( 1) Use burned in ESI  
Select ESI [1]?  
Use internally assigned selector? [Yes]:  
Use Best Effort Service for Data VCCs? [Yes]:  
Peak Cell Rate of outbound Data VCCs (Kbps) [0]?  
Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?  
Use ATM adapter's burned-in MAC address for source?
```

#### *Interface Number of NHRP LANE Shortcut Interface*

Utilice el número de interfaz asignado a LSI. El número de interfaz puede determinarse utilizando el mandato **list interface**.

#### *( 1) Use burned in ESI*

Utilice el ESI administrado universalmente como parte de la dirección ATM. Se le pueden proporcionar otras opciones según la configuración.

#### *Select ESI*

Especifique el ESI.

#### *Use internally assigned selector*

Utilice el selector asignado internamente o asigne un selector dentro del rango del 00 al FF.

#### *Use Best Effort Service for Data VCCs*

Especifica el tipo de características de tráfico a asociar con los VCC de datos. El ancho de banda no está reservado para el tráfico de Mayor Eficacia.

#### *Peak Cell Rate of outbound Data VCCs (kbps)*

Especifica el parámetro de tráfico de velocidad punta de célula (PCR) para los VCC de datos.

#### *Sustained Cell Rate of outbound Data VCCs (Kbps)*

Especifica el parámetro de tráfico de velocidad sostenida de célula (SCR) para los VCC de datos.

*Use ATM adapter's burned-in MAC address for source?*

Puede utilizar como dirección MAC de origen para los atajos de LANE:

1. La dirección MAC administrada universalmente del adaptador
2. La dirección MAC suministrada en la respuesta de resolución de NHRP
3. La dirección MAC que ha configurado especificando una dirección MAC por medio del mandato **change nhrp**.

Consulte "ATM y Emulación de LAN" en el manual *Guía del usuario de software* para obtener más información.

**Nota:** Es recomendable que utilice los valores por omisión hasta que haya determinado las opciones de proceso específicas que necesite el entorno.

## List

Utilice el mandato **list** para visualizar la información de la configuración de NHRP.

### Sintaxis:

**list**                    all  
                          exclude list  
                          disallowed router-to-router shortcuts  
                          interface definitions  
                          cache size

**all**                    Visualiza toda la configuración de NHRP.

### Ejemplo: 1i all

La salida es la misma que la del mandato **list**. Consulte la sección "List" en la página 456.

### exclude list

Visualiza las entradas de lista de exclusión.

### Ejemplo: 1i exc

```
List of NHRP IP exclude records
-----
# Address      Mask
1 7.7.7.7      255.255.255.255
```

### disallowed router-to-router shortcuts

Visualiza los atajos de direccionador a direccionador anulados.

### Ejemplo: 1i dis

```
Disallowed router-to-router shortcuts for IP
-----
1 8.8.8.1      255.255.255.255
2 6.6.6.1      255.255.255.255
```

### interface definitions

Visualiza las definiciones de interfaz NHRP.

### Ejemplo: 1i int

## Mandatos de configuración avanzada de NHRP (Talk 6)

```
Interfaces explicitly defined for NHRP
-----
None

NHRP LANE Shortcut Interface:
-----
Interface: 3 ESI: burned-in Sel: auto
Use Best Effort: yes (Data)
Cell Rate(kbps): Peak: 0/ 0 Sustained: 1000/538764944
MAC address supplied by NHS is used as source address
```

### cache size

Visualiza los tamaños de las antememorias.

#### Ejemplo: 1i ca

```
Cache Sizes
-----
Resolution cache: 10000 entries
Server purge cache: 10000 entries
Server registrations cache: 10000 entries
```

## Set

Utilice el mandato **set** para lo siguiente:

### Sintaxis:

```
set protocol access control usage
atttempt shortcuts
holding time
data-rate threshold
extensions ...
cache size ...
shortcuts to atmarp clients
```

### protocol access control usage

Determina si se comprobarán los controles del acceso a IP y, si es así, cómo se aplicarán estos controles a los paquetes de NHRP. Consulte la sección “Utilización del control del acceso al protocolo” en la página 452 para obtener más información.

#### Ejemplo: set prot

```
Use (Destination, Source & Destination, None) [None]?
```

**Valores válidos:** None, Source and Destination, Destination

**Valor por omisión:** None

### attempt shortcuts

Determina cómo decide el cliente NHRP cuándo originar peticiones de resolución.

**Valores válidos:** Y, N, Data-rate.

**Y** Sí. Intentar siempre establecer un VC de atajo creando una petición de resolución de siguiente salto y enviándola a la estación de siguiente salto.

**N** No. No intentar nunca establecer un atajo. Si se utiliza esta opción, se inhabilita básicamente la función de cliente en el direccionador. Este valor puede utilizarse en un direccionador intermedio (uno que no es un punto de entrada en la red de NBMA para el tráfico direccionado) para eliminar el “efecto



## Mandatos de configuración avanzada de NHRP (Talk 6)

dominó”, donde el tráfico que sigue la vía de acceso direccionada desencadena peticiones de resolución de NHRP en cada direccionador de NHRP de la vía de acceso.

### Data-rate

Intentar establecer un atajo sólo después de que se alcance el umbral de velocidad de datos.

**Nota:** Este valor puede evitar la creación de VCC para tráfico “ocasional”, como, por ejemplo, detecciones de condición de excepción de SNMP que se envían a un gestor de SNMP.

**Valor por omisión:** Data-rate.

**Ejemplo:** `set attempt`

Try shortcut VCs? (Yes, No, Data-rate) [Data-rate]?

### holding time

Establece el tiempo de mantenimiento en minutos.

El parámetro de tiempo de mantenimiento se utiliza para estas funciones:

- Cuando el direccionador responde a una petición de resolución de siguiente salto con información sobre sí mismo (es decir, el direccionador va a convertirse en el atajo de siguiente salto), se envía el tiempo de mantenimiento al peticionario como el período de tiempo durante el cual puede considerarse válida la información.
- Cuando el direccionador responde a una petición de resolución de siguiente salto con información sobre otra estación de NBMA que no se ha aprendido utilizando NHRP (por ejemplo, la estación de destino es un dispositivo de ATM con una dirección IP para una de las subredes del dispositivo), se envía el tiempo de mantenimiento al peticionario como el período de tiempo durante el cual puede considerarse válida la información.

**Valores válidos:** 1 - 60 minutos.

**Valor por omisión:** 20 minutos.

**Ejemplo:** `set hold`

Holding time (in minutes) [20]?

### data-rate threshold

Establece el umbral de velocidad de datos en paquetes/segundo.

El umbral de velocidad de datos se utiliza cuando el parámetro **attempt shortcuts** está establecido en **Data-rate**.

Cuando se destina tráfico a una estación en particular y la velocidad es inferior a este umbral, el direccionador no intenta establecer atajos. (En otras palabras, no genera peticiones de resolución de siguiente salto ni las envía al siguiente salto por la vía de acceso direccionada.) Una vez que la velocidad del tráfico sobrepase el umbral, el direccionador intentará establecer un atajo. Si puede crear satisfactoriamente una vía de acceso de atajo, ésta se utilizará aunque la velocidad del tráfico esté por debajo del umbral. La vía de acceso continuará utilizándose hasta que el tráfico se detenga durante un período de tiempo. Esto se hace

## Mandatos de configuración avanzada de NHRP (Talk 6)

para evitar ir cambiando de la vía de acceso direccionada a la vía de acceso de atajo si el tráfico es esporádico.

**Valores válidos:** El mínimo es de 1 paquete/segundo. El máximo son 5120 paquetes/segundo.

**Valor por omisión:** 10 paquetes/segundo.

**Ejemplo:** `set data`

Data-rate threshold in packets/second [10]?

### extensions

Establece el uso de extensiones de NHRP seleccionadas en *yes* o *no*.

Forward transmit NHS (valor por omisión: no)

Reverse transmit NHS (valor por omisión: no)

Responder Address (valor por omisión: no)

Lane Shortcuts (valor por omisión: yes)

**Valores válidos:** yes o no

**Ejemplo:** `set ext lane`

Use LANE shortcuts extension [Yes]?

### cache size *resolution* *registration* *server purge*

Establece el número máximo de entradas de la antememoria seleccionada.

Pueden seleccionarse tamaños de antememoria para cualquiera de las opciones siguientes:

### resolution cache

Este parámetro le permite determinar el número de entradas de la antememoria para funciones de cliente. Cada entrada de antememoria contiene la correlación de dirección de protocolo con dirección de NBMA que puede utilizarse para crear VC de atajo. Hay entradas en la antememoria cuando el direccionador ha:

- Resuelto satisfactoriamente una dirección de protocolo con una dirección de NBMA enviando peticiones de resolución de siguiente salto.
- Intentado resolver una petición de protocolo con una dirección de NBMA, pero no ha recibido respuesta o bien ha recibido una respuesta negativa, y el temporizador asociado no ha caducado. Estas entradas se mantienen en la antememoria para impedir que el dispositivo genere peticiones de resolución de siguiente salto adicionales durante un período de tiempo.
- Recibido una petición de registro de un cliente y el tiempo de mantenimiento indicado en esta petición todavía no ha caducado.

Cuando se sobrepasa el tamaño de la antememoria, no se efectúan nuevos intentos para resolver direcciones de protocolo con direcciones de NBMA (en otras palabras, no se envían nuevas peticiones de resolución de siguiente salto) hasta que se eliminan las entradas existentes porque el tiempo de mantenimiento ha caducado o porque se ha recibido una petición de eliminación específica procedente de aquél que ha originado la información. Además, cuando se sobrepasa el tamaño de la antememoria, se rechazan peticiones de registro de nuevos clientes.

**Valores válidos:** De 256 a 65535 entradas.

**Valor por omisión:** 10000 entradas.

**Ejemplo:** `set cache res`

Number of cache entries [10000]?

### registration cache

Establece un límite para el número de entradas de registro de la antememoria de resolución. Cuando el servidor recibe una petición de registro, comprueba si el número de registros de cliente NHRP está por debajo de este límite antes de añadir una entrada de registro para la antememoria de resolución.

**Valores válidos:** De 256 a 16384 entradas.

**Valor por omisión:** 10000 entradas.

**Ejemplo:** `set cache reg`

Number of cache entries [10000]?

### server purge cache

Este parámetro le permite determinar el número de entradas de la antememoria de eliminación del servidor. Una entrada de esta antememoria representa una dirección de protocolo de destino y un cliente al que el servidor ha proporcionado información de NBMA autorizativa para este destino.

La dirección de destino puede representar el servidor en sí, dispositivos de redes a las que está conectado el servidor, clientes NHRP que se han registrado con el servidor o bien direccionadores para los que se ha anunciado un atajo R2R. El direccionador utiliza la información de estas entradas de antememoria para notificar a los clientes que eliminen la información de direcciones que se convierta en no válida antes de que caduque el tiempo de mantenimiento.

Cuando se sobrepasa el tamaño de la antememoria de eliminación del servidor, el servidor rechaza peticiones de resolución de siguiente salto autorizativa.

**Valores válidos:** De 256 a 65535 entradas.

**Valor por omisión:** 10000 entradas.

**Ejemplo:** `set cache serv`

Number of cache entries [10000]?

### shortcuts to ATMARP clients

Permite o anula atajos hacia clientes ATMARP.

Este parámetro puede utilizarse para permitir o dejar de permitir que el servidor proporcione atajos a clientes ATMARP nativos que no den soporte a NHRP. Puede ser necesario si estos clientes no pueden dar soporte a un gran número de VC. Utilice la opción relativa a una "Lista de exclusión" si tienen que anularse selectivamente atajos hacia determinados clientes o subredes.

**Ejemplo:** `set shortcut`

Allow shortcuts to Classical IP clients? [Yes]:

### Acceso al proceso de supervisión de NHRP

Para acceder al indicador de supervisión de NHRP:

1. En el indicador de supervisión del operador (\*), escriba **talk 5** y pulse Intro.
2. En el indicador +>, escriba **protocol nhrp** y pulse Intro.
3. Se visualizará el indicador NHRP>.

### Mandatos de supervisión de NHRP

Este apartado explica todos los mandatos de supervisión de NHRP mostrados en la Tabla 112. Entre los mandatos desde el indicador NHRP>.

Tabla 112. Resumen de los mandatos de supervisión de NHRP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxxi.
Box Status	Visualiza el estado de habilitación/inhabilitación de NHRP.
Interface Status	Visualiza el estado de las interfaces NHRP.
Statistics	Visualiza estadísticas de las interfaces NHRP.
Cache	Visualiza las entradas de la antememoria de resolución de NHRP.
Server_purge_cache	Visualiza las entradas de la antememoria de eliminación del servidor de NHRP.
MIB	Visualiza información de la MIB.
LANE Shortcuts	Visualiza las entradas de atajo de LANE.
CONFIG Parameters	Visualiza, cambia o restablece información de la configuración de NHRP.
Reset	Reconfigura dinámicamente el protocolo o las interfaces NHRP.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxi.

### Box Status

Utilice el mandato **box status** para visualizar el estado de NHRP tal como se ha configurado en general (por ejemplo, todas las interfaces no definidas explícitamente).

#### Sintaxis:

**box-status**

#### Ejemplo:

```
box status
Box level NHRP is ON by config
```

## Interface Status

Utilice el mandato **interface status** para visualizar el estado de NHRP en las interfaces.

### Sintaxis:

**interface-status**

### Ejemplo:

```
interface status
Interface 0: UP (NHRP enabled)
Interface 1: UP (NHRP disabled)
Interface 2: DOWN
Interface 3: UP (NHRP LANE Shortcut Interface)
```

## Statistics

Utilice el mandato **statistics** si desea visualizar estadísticas de NHRP para todas las interfaces o para una interfaz específica.

### Sintaxis:

```
statistics      all
                  interface
```

**all** Lista estadísticas de NHRP sobre todas las interfaces.

### Ejemplo: statistics all

La salida es como la del mandato **statistics interface** mostrado en el ejemplo siguiente.

**interface** Lista estadísticas de NHRP sobre una interfaz específica.

### Ejemplo: statistics interface

```
Interface number [0]? 0

Statistics for Interface 0
-----
Field Description                               Value
-----
Inbound Requests                               5
Outbound Requests                             3
Inbound Replies                               3
Outbound Replies                             5
Inbound Registers                             0
Outbound Registers                           0
Inbound Error Packets                         0
Inbound Error Indication Packets             0
Outbound Error Indication Packets            0
Reply Forwards                                0
Unrecognized Options                          0
Registration Overflows                        0
ProtocolErrors                               0
Negative Outbound Replies                     0
Inbound Packets on NHRP disabled interface  0
'Send_to_me' Outbound Replies                0
Inbound Purges                                0
Outbound Purges                              2
```

### Cache

Utilice el mandato **cache** para visualizar todas las entradas de la antememoria de resolución de NHRP o una entrada de antememoria específica identificada por una dirección de destino.

#### Sintaxis:

```
cache          list  
                entry
```

**list** Lista las entradas de la antememoria de NHRP.

**entry** Lista una entrada de antememoria de NHRP específica.

#### Ejemplos:

```
cache list  
Total Client Cache Entries = 3  
  
NHRP Client Cache Entries  
=====
```

Dest Address	NextHop Address	State	Htime	MTU	Net
5.5.5.1	5.5.5.1	Act	1121	4490	1
5.5.5.2	5.5.5.2	Inact	1185	4490	1
6.6.6.1	6.6.6.1	Act	602	9180	0

```
cache entry  
Enter destination address [0.0.0.0]? 6.6.6.1  
Destination: 6.6.6.1  
NextHop: 6.6.6.1  
ATM Address: 39840F00000000000000000000410005A00DEADCA  
State: Act  
Net: 0  
HoldingTime: 433 seconds  
MTU size: 9180  
Flags: 0x00420000
```

### Server\_purge\_cache

Utilice el mandato **server\_purge\_cache** para listar todas las entradas de la antememoria de eliminación del servidor de NHRP.

#### Sintaxis:

```
server_purge_cache
```

### MIB

Utilice el mandato **MIB** para visualizar información relacionada con la MIB NHRP.

#### Sintaxis:

```
mib          list ...  
                entry ...
```

**list** Lista entradas de la MIB NHRP para:

- Server table
- Client table
- Next-Hop Server (NHS) statistics table

- Next-Hop Client (NHC) statistics table
- Resolution cache table

**Ejemplo: mib list server table**

```
MIB Server Table List
=====
Index Server Address State ATM Addr
-----
0 6.6.6.2 UP 39840F0000000000000000000000000210005A00DEADC8
```

**entry** Lista una entrada específica de la MIB NHRP de una de estas opciones:

- Server table
- Client table
- Next-Hop Server (NHS) statistics table
- Next-Hop Client (NHC) statistics table
- Resolution cache table

**Ejemplo: mib entry serv**

```
Index [0]? 0
Index      : 0
Protocol   : 1x0800
Protocol Address: 6.6.6.2
ATM Address type: 0x0 (NSAP)
ATM Address : 39840F000....
SubnetworkId : 0
Authentication : 1
Current Clients : 0
Max Clients   : 512
State        : 1
Net          : 1
```

## LANE Shortcuts

Utilice el mandato **lane shortcuts** para visualizar todas las entradas que utilizan atajos de LANE o entradas específicas. También puede visualizar las direcciones ATM hacia las que están anulados atajos de LANE debido a problemas operativos.

**Sintaxis:**

```
lane-shortcuts  all
                  entry
                  disallowed
```

**all** Visualiza todos los atajos de LANE.

**Ejemplo: lane all**

```
LANE Shortcut Interface #: 1, ATM Network Interface #: 0
=====
Next Hop Prot @   Dest Mac @           VPI/VCI
-----
5.5.5.1           04-AA-AA-AA-AA-01   0/34

Current MTU being used: 4490
```

**entry** Visualiza una entrada de atajo de LANE.

**Ejemplo: lane entry**

## Mandatos de supervisión de NHRP (Talk 5)

```
LANE Shortcut Interface number [0]? 1
Enter IP address of next hop [0.0.0.0]? 5.5.5.1
Next Hop Addr: 5.5.5.1
Dest Mac Addr: 04-AA-AA-AA-AA-01
ATM Address: 39840F0000000000000000000310005A00DEAD02
Media type: Token Ring
VPI/VCI: 0/34
Holding Time: 20 minutes
MTU size: 4490
RI Field:064001020203
```

### disallowed

Visualiza todas las entradas de atajo de LANE anuladas.

Cualquier dirección ATM listada en esta visualización significa que la interfaz de NHRP LANE Shortcut Interface ha recibido datos de esta dirección ATM. Esto no está permitido porque todos los VCC de la interfaz de NHRP LANE Shortcut Interface se utilizarán únicamente para transmitir datos a un LEC del otro extremo. Si el LEC intenta enviar datos sobre un VCC configurado por la interfaz de NHRP LANE Shortcut Interface, el VCC se desactivará y no se configurarán más atajos de LANE hacia este LEC.

Una vez corregida la condición que ha causado que la interfaz de NHRP LANE Shortcut Interface reciba datos, el dispositivo debe reiniciarse con el fin de permitir que esa dirección ATM se utilice de nuevo para atajos de NHRP en LANE.

### Ejemplo: 1an dis

```
LAN Shortcut Interface #: 2, ATM Network Interface #: 0
=====
Atm Address
-----
39840F0000000000000000000310005A00DEAD02
```

## CONFIG Parameters

Utilice el mandato **config parameters** si desea acceder a los menús de los mandatos para los parámetros de configuración de NHRP **display**, **change** o **reset**.

Tabla 113. Resumen de los parámetros de configuración de NHRP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxxi.
Display	Visualiza los parámetros de configuración actuales de NHRP y Route-switching.
Change	Permite cambiar dinámicamente parámetros de configuración de NHRP sin que ello afecte a la configuración estática.
Reset	Lee el parámetro de configuración en la configuración estática y lo utiliza durante la ejecución del direccionador.

### Display

Utilice el mandato **display** para visualizar los parámetros de configuración actuales de NHRP y Route-Switching.

### Sintaxis:

**display**                    nhrp



**nhrp** Visualiza los parámetros de configuración de NHRP, incluidos los parámetros generales, los tamaños de las antememorias, el uso de las extensiones, la lista de exclusión y los atajos de direccionador a direccionador anulados.

### Change

Utilice el mandato **change** para cambiar los parámetros de configuración actuales de NHRP. Consulte la sección “Set” en la página 462 para obtener una descripción de estos parámetros de configuración.

#### Sintaxis:

```
change          protocol_access_control_usage
                  attempt_shortcuts
                  holding_time
                  data-rate_threshold
                  cache_size
                  extensions
                  shortcuts_to_atmarp_clients
```

### Reset

Utilice el mandato **reset** para restablecer el valor de un parámetro de la configuración dinámica en el valor de la configuración estática. Consulte la sección “Set” en la página 462 para obtener una descripción de estos parámetros de configuración.

#### Sintaxis:

```
reset           protocol_access_control_usage
                  attempt_shortcuts
                  holding_time
                  data-rate_threshold
                  cache_size
                  extensions
                  shortcuts_to_atmarp_clients
                  exclude_list
                  disallowed_router-to-router
```

## Reset

Utilice el mandato **reset** para reconfigurar dinámicamente el protocolo o una interfaz NHRP. Una acción de reset hace que se utilicen los valores aplicables de la configuración estática.

#### Sintaxis:

```
reset          interface
                  nhrp
```

## Rastreo de paquetes de NHRP

- nhrp** Restablece las estadísticas, las interfaces y los parámetros de configuración de NHRP en los valores de la configuración estática. Esto es equivalente a un arranque en frío de NHRP.
- interface** Desactiva la interfaz NHRP y, a continuación, activa la interfaz con los nuevos valores de interfaz de la configuración estática.

---

## Rastreo de paquetes de NHRP

Pueden activarse rastreos de paquetes de NHRP desde el Sistema de anotación cronológica de sucesos (ELS), que es una parte integral del sistema operativo del direccionador. Consulte “Utilización y configuración del Sistema de anotación cronológica de sucesos” y “Supervisión del Sistema de anotación cronológica de sucesos” en el manual *Guía del usuario de software*.

El mecanismo de rastreo de paquetes de NHRP da soporte a la opción “set trace decode on”. Esta opción permite que pueda interpretarse para la visualización la salida del rastreo de paquetes de NHRP. También pueden rastrearse las tramas de control sobre LSI aparte de los paquetes del protocolo NHRP. Para obtener detalles sobre cómo utilizar el recurso del rastreo, vea la descripción del mandato **trace** de “Supervisión del Sistema de anotación cronológica de sucesos” en el manual *Guía del usuario de software*.

Los paquetes del protocolo NHRP se identifican mediante el suceso 19 y los paquetes de control de LSI se identifican mediante el suceso 113.

### Salida de rastreo de muestra núm. 1:

```
Dir:OUTGOING Time:0.0.48.88 Trap:6035
Comp:NHRP Type:UNKNOWN Port:1 Circuit:0x000000 Size:160
-----
** NHRP/MPOA Frame **
AddressFamily:ATM_NSAP ProtocolType:IPv4 HopCount:64 PacketSize:160
Checksum:0x03F4 ExtensionOffset:0x0038 Version:1 PktType:ResolutionRequest
SrcAddrTL:20 SrcSubAddrTL:0 SrcProtoLen:4 DstProtoLen:4
Flags:requester is a router Flags:want authoritative only Flags:want unique
only ReqID:1
Src NBMA:39840F0000000000000000000000000610005A019600C9
Src Protocol Addr: 6.6.6.1 Dest Protocol Addr: 3.3.3.2
0038: 00 08 00 1C 08 00 5A 00 00 01 00 0A 00 00 00 00 | .....Z..... |
0048: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ..... |
0058: 00 08 00 34 08 00 5A 00 00 01 00 0C 00 00 00 00 | ...4..Z..... |
0068: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ..... |
0078: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ..... |
0088: 00 00 00 00 00 00 00 00 00 08 00 08 08 00 5A 00 | .....Z. |
0098: 00 01 00 06 80 00 00 00 00 00 00 00 00 00 00 00 | ..... |
```

### Salida de rastreo de muestra núm. 2:

```

Dir:INCOMING Time:0.0.50.69 Trap:6035
Comp:NHRP Type:UNKNOWN Port:1 Circuit:0x000000 Size:202
-----
** NHRP/MPOA Frame **
AddressFamily:ATM_NSAP ProtocolType:IPv4 HopCount:63 PacketSize:202
Checksum:0xEC88 ExtensionOffset:0x005C Version:1 PktType:ResolutionReply
SrcAddrTL:20 SrcSubAddrTL:0 SrcProtoLen:4 DstProtoLen:4
Flags:requester is a router Flags:authoritative info Flags:requested info
unique ReqID:1
Src NBMA:39840F0000000000000000000610005A019600C9
Src Protocol Addr: 6.6.6.1 Dest Protocol Addr: 3.3.3.2
1483 VCC Shortcut Information (CIE) follows:
  CIE Code:0 Prefix:32 MTU:4376 Htime:180 Preference:254
  CIE NBMA:39840F0000000000000000000310005A01950103
  CIE Protocol Addr: 3.3.3.1
005C: 00 08 00 1C 08 00 5A 00 00 01 00 0B 00 00 00 01 | .....Z..... |
006C: 97 00 01 04 03 03 03 02 11 18 90 00 5A 01 94 00 | .....Z... |
007C: 00 08 00 34 08 00 5A 00 00 01 00 0D 00 B4 14 00 | ...4..Z..... |
008C: 39 84 0F 00 00 00 00 00 00 00 00 00 03 10 00 5A | 9.....Z |
009C: 01 95 01 03 00 00 00 00 00 00 00 00 00 00 00 00 | .....Z. |
00AC: 00 00 00 00 00 00 00 00 00 08 00 0E 08 00 5A 00 | .....Z. |
00BC: 00 01 00 07 06 A0 00 80 00 20 80 00 00 00 00 00 | .....Z. |

```

---

## Soporte de la reconfiguración dinámica de servidor de NHRP

Este apartado describe la reconfiguración dinámica (DR) tal como afecta a los mandatos Talk 6 y Talk 5.

### Mandato Delete Interface de CONFIG (Talk 6)

El servidor de NHRP da soporte al mandato de CONFIG (Talk 6) **delete interface** con la consideración siguiente:

- La interfaz de NHRP LANE Shortcut Interface no puede suprimirse con el mandato **delete interface**. Utilice la opción de configuración **disable nhrp** para suprimir la interfaz de NHRP LANE Shortcut Interface.

### Mandato Activate Interface de GWCON (Talk 5)

El servidor de NHRP da soporte al mandato de GWCON (Talk 5) **activate interface** con la consideración siguiente:

- La interfaz de NHRP LSI (LANE Shortcut Interface) asociada con cada interfaz física ATM se activa automáticamente después de que se active la interfaz física ATM asociada.

Todos los mandatos específicos de interfaz de servidor de NHRP reciben soporte del mandato de GWCON (Talk 5) **activate interface**.

### Mandato Reset Interface de GWCON (Talk 5)

El servidor de NHRP da soporte al mandato de GWCON (Talk 5) **reset interface** con la consideración siguiente:

- No se puede restablecer el tipo de interfaz de NHRP LANE Shortcut Interface sin un reinicio.

Todos los mandatos específicos de interfaz de servidor de NHRP reciben soporte del mandato de GWCON (Talk 5) **reset interface**.



---

## Utilización de IP Versión 6 (IPv6)

Este capítulo describe cómo utilizar IPv6.

---

### Visión general de IPv6

IP Versión 6 (IPv6) es una nueva versión del protocolo Internet Protocol. Se ha diseñado como sucesor de IP Versión 4 (IPv4). La lista siguiente identifica algunas de las ventajas proporcionadas por IPv6:

- Gran espacio de direcciones

IPv6 utiliza una dirección de 128 bits.

- Direccionamiento

Al utilizar el gran tamaño de dirección, IPv6 proporciona un esquema de direcciones jerárquico que permite al usuario crear una jerarquía flexible en el direccionamiento.

- Facilidad de la configuración

NDP proporciona la configuración automática del sistema principal.

- Seguridad

IPv6 hace que la Seguridad de IP sea necesaria.

- Soporte para el tráfico multimedia

La cabecera de IPv6 tiene los campos de etiqueta de prioridad y flujo para facilitar la integración de la Calidad de los servicios.

- Simplificación

La cabecera de IPv6 es fija y está simplificada. Ya no es necesario que el direccionador realice la fragmentación, con lo cual se ha simplificado el proceso de los paquetes. Además, se implementan datos con tipos de opciones en las cabeceras de la extensión que sólo procesa el nodo de destino.

---

### Comparación de IPv6 con IPv4

IPv6 incluye muchos cambios respecto a IPv4. Los más significativos son:

- Dirección
- Formato de cabecera
- Tamaño mínimo de MTU
- Necesidad del protocolo Path MTU Discovery
- Necesidad de la Seguridad de IP
- Neighbor Discovery Protocol (NDP)

---

### Sistema de dirección IPv6

El sistema de dirección IPv6 aumenta la dirección de 32 bits a 128 bits. Este aumento permite más grados de la jerarquización que en las capas básicas de red, subred y sistema principal.

Las direcciones IPv6 pertenecen a una de estas tres categorías:

- Vertimiento único. Un paquete se entrega a la interfaz identificada por la dirección.
- Vertimiento múltiple. Un paquete se envía a todos los miembros del grupo de vertimiento múltiple identificado por la dirección.
- Vertimiento en cualquiera. Un paquete sólo se envía al miembro más cercano del grupo identificado por la dirección.

Se ha sustituido el sistema de dirección de difusión por el sistema de dirección de vertimiento múltiple en IPv6.

### Formato de dirección IPv6

La dirección IPv6 está compuesta por 128 bits. Estos bits se escriben como ocho enteros de 16 bits separados por el signo de dos puntos.

**Ejemplo:**

**ABCD:1234:0000:1234:5555:FFEE:7777:0123**

Puede utilizar las siguientes normas de simplificación:

- Sáltese los ceros iniciales.

**Ejemplo:**

**ABCD:1234:0:1234:0:FFEE:7777:123**

- Dentro de una dirección, puede sustituirse un conjunto de números de 16 bits nulos y consecutivos por dos signos de dos puntos.

**Ejemplo:**

**ABCD:1234::1234:5555:FFEE:7777:123**

**1234::7899**

El signo de dos puntos doble sólo puede utilizarse una vez dentro de la dirección.

- Cuando trabaje con un entorno mixto de nodos IPv4 y IPv6, puede utilizar el formato **x:x:x:x:x:d.d.d.d**

donde las x son los valores hexadecimales de las seis partes de 16 bits más a la izquierda de la dirección, y las d son los valores decimales de las cuatro partes de 8 bits más a la derecha de la dirección en la representación estándar de IPv4.

**Ejemplo:**

**ABCD:1234::1234:5555:FFEE:1.2.3.4**

**::1.2.3.4**

## Representación textual de los prefijos de dirección

Un prefijo de dirección IPv6 se representa mediante la notación:

### **dirección-IPv6/longitud-prefijo**

La dirección IPv6 puede utilizar cualquiera de las notaciones listadas en la sección “Formato de dirección IPv6” en la página 476 y la longitud de prefijo es un valor decimal que especifica el número de bits contiguos más a la izquierda de la dirección que abarca el prefijo.

### **Ejemplo:**

**ABCD:1234::1234:5555:FFEE:1.2.3.4/64**

---

## Formato de cabecera de IPv6

La cabecera de IPv6 tiene un total de 8 campos, con la eliminación de algunos campos de IPv4, como, por ejemplo, el de suma de comprobación y el de fragmentación.

---

## Tamaño mínimo de MTU en IPv6

El tamaño mínimo de MTU para IPv6 es de 1280 bytes. No puede habilitar IPv6 en una interfaz con una MTU que tenga menos de 1280 bytes.

---

## Necesidad de Path MTU Discovery en IPv6

Path MTU Discovery es un protocolo que permite que un sistema principal determine el tamaño máximo de los paquetes que pasarán por una vía de acceso satisfactoriamente hasta un destino sin fragmentación. Puesto que los paquetes se generan y envían desde el sistema principal, está disponible la MTU de la interfaz de salida determinada a la que se transmitirá el paquete.

Si el paquete se ajusta a la interfaz de salida, en su totalidad o en fragmentos, se transmite. Si un direccionador de la vía de acceso tiene que reenviar este paquete a una red con una MTU más pequeña que el tamaño del paquete, éste se eliminará y se enviará un mensaje de ICMP al que ha originado el paquete indicando el tamaño de paquete que es necesario para que se ajuste a la red de salida del direccionador intermedio. El sistema principal que reciba este mensaje ajustará el tamaño de los paquetes subsiguientes remitidos por la vía de acceso. Este proceso puede producirse varias veces antes de que el paquete llegue a su destino final. Una vez que el paquete haya llegado a su destino, no deben eliminarse paquetes subsiguientes porque su tamaño de paquete sea demasiado extenso.

Puesto que la ruta puede cambiar dinámicamente, la MTU de la vía de acceso puede aumentar y necesitará ajuste en el nodo sistema principal. Las MTU de la vía de acceso aprendidas tienen una duración y el proceso de Path MTU Discovery vuelve a producirse. Esto permite que el tamaño del paquete transmitido reaccione ante la naturaleza dinámica de las rutas a través de la red.

Path MTU Discovery es necesario porque no está permitida la fragmentación en los direccionadores de tránsito.

Si el dispositivo actúa como direccionador de tránsito, no reenviará paquetes cuyo tamaño sea superior al de la MTU de la red de salida. Generará un mensaje de ICMP que exprese que el paquete es demasiado grande y lo enviará al origen del paquete.

Puede utilizarse el mandato **enable path-mtu-discovery** en el indicador IPv6 Config> para habilitar o inhabilitar el descubrimiento de la MTU de la vía de acceso. El descubrimiento de la MTU de la vía de acceso está habilitado por omisión.

Utilice el mandato **set path-mtu-aging-timer** en el indicador IPv6 Config> para especificar el tiempo de duración de las MTU de la vía de acceso que se han determinado.

---

## Necesidad de la Seguridad en IPv6

Un nodo IPv6 debe dar soporte a la seguridad de IP. La seguridad de IP puede habilitarse o inhabilitarse. Consulte “Using IP Security” y “Configuring and Monitoring IP Security” en la publicación *Utilización y configuración de las características* para obtener información adicional sobre la seguridad de IP.

1. Utilice el mandato **add packet** en el indicador IPv6 Config> para añadir un filtro de paquete.
2. Utilice el mandato **update packet** en el indicador IPv6 Config> para actualizar el filtro de paquete.
3. Utilice el mandato **add access** en el indicador Packet-filter 'nombre\_filtro' Config> para añadir controles del acceso.
4. Utilice el mandato **set acc on** en el indicador IPv6 Config> para habilitar el control del acceso.

---

## Neighbor Discovery Protocol (NDP) en IPv6

IPv6 utiliza NDP para realizar la configuración automática. NDP permite que los nodos IPv6 del mismo enlace descubran la presencia de unos y otros, determinen las direcciones de capa de enlace de unos y otros, encuentren direccionadores y mantengan información sobre la asequibilidad relativa a las vías de acceso hacia contiguos activos.

## Descubrimiento de direccionadores y prefijos

Los sistemas principales utilizan Router Discovery para descubrir los direccionadores que residen en un enlace. Cada direccionador vierte periódicamente y de manera múltiple un paquete de anuncio de direccionador, si está configurado, para advertir de su disponibilidad. Los anuncios de direccionador contienen una lista de prefijos que se utilizan para la determinación 'en enlace' y para la configuración de direcciones autónoma. Los sistemas principales pueden utilizar los prefijos 'en enlace' anunciados para determinar cuándo se encuentra en el enlace o más allá de un direccionador el destino de un paquete.



## Configuración automática de direcciones

Los anuncios de direccionador permiten que los direccionadores informen al sistema principal de cómo realizar la configuración automática de direcciones. Los direccionadores pueden especificar si los sistemas principales utilizarán la configuración de direcciones con estado o autónoma (sin estado).

## Resolución de direcciones

Los direccionadores llevan a cabo una resolución de direcciones mediante el vertimiento múltiple de un mensaje de solicitud a contiguo que pide al nodo de destino que devuelva su dirección de capa de enlace. La dirección de capa de enlace se devuelve en un anuncio de contiguo con vertimiento único. Incluyendo su dirección de capa de enlace en el mensaje de solicitud a contiguo y con un solo par de mensajes de petición-respuesta, el iniciador del mensaje y el destino pueden determinar las direcciones de capa de enlace de cada cual.

## Detección de inasequibilidad de contiguo

NDP puede detectar la anomalía de un contiguo o la anomalía de la vía de acceso hacia adelante para el contiguo. Cuando no se ha recibido una confirmación positiva de un contiguo durante un intervalo de tiempo, el nodo prueba el contiguo utilizando mensajes de solicitud a contiguo con vertimiento único para verificar si la vía de acceso hacia adelante todavía funciona.

## Redireccionamiento

Si la dirección de origen del paquete y el siguiente salto están en la misma red, un direccionador puede enviar un mensaje de redireccionamiento para informar al emisor de que el siguiente salto es un contiguo.

Utilice el mandato **p ndp** en el indicador `Config>` para configurar los parámetros de NDP.

---

## Función de túnel de IPv6 sobre IPv4

La función de túnel de IPv6 sobre IPv4 le permite migrar de redes IPv4 a redes IPv6 sin necesidad de actualizar simultáneamente todo el equipo para el soporte de IPv6. La función de túnel de IPv6 sobre IPv4 permite que tramas de IPv6 atraviesen una red IPv4 y lleguen a un destino de IPv6. La trama de IPv6 se encapsula en una trama de IPv4 y esta trama encapsulada se reenvía por la red IPv4 hacia un destino específico de IPv4, denominado punto final del túnel. En este punto final, se desencapsula el paquete y se reenvía al destino final de IPv6.

La adición de un túnel configurado hace que se añada una interfaz virtual. Ésta recibe el tratamiento de interfaz normal en IPv6 y RIP puede utilizarla para el establecimiento de rutas.

Utilice el mandato **add tunnel** en el indicador `IPv6 Config>` para añadir un túnel de IPv6 sobre IPv4.

---

## Protocol Independent Multicast (PIM)

Consulte el apartado “Utilización de PIM” en la página 525 para obtener información sobre cómo utilizar el protocolo PIM.

---

## Configuración y supervisión de IPv6

Este capítulo describe cómo utilizar los mandatos de configuración y funcionamiento de IPv6 e incluye los apartados siguientes:

- “Acceso al entorno de configuración de IPv6”
- “Mandatos de configuración de IPv6”
- “Acceso al entorno de supervisión de IPv6” en la página 502
- “Mandatos de supervisión de IPv6” en la página 502
- “Soporte de la reconfiguración dinámica de IPv6” en la página 510

---

### Acceso al entorno de configuración de IPv6

Utilice el procedimiento siguiente para acceder al proceso de configuración de IPv6.

1. En el indicador de OPCON, entre **talk 6**. (Para obtener información más detallada sobre este mandato, consulte *El proceso y los mandatos de OPCON* en la publicación Nways Multiprotocol Access Services Guía del usuario de software.) Por ejemplo:

```
* talk 6
Config>
```

Después de entrar el mandato **talk 6**, se visualizará el indicador CONFIG (Config>) en el terminal. Si no aparece el indicador la primera vez que entre la configuración, pulse **Intro** de nuevo.

2. En el indicador CONFIG, entre el mandato **p ipv6** para obtener el indicador IPv6 Config>.

---

### Mandatos de configuración de IPv6

Para configurar IPv6, entre los mandatos en el indicador IPv6 Config>.

## Mandatos de configuración de IPv6 (Talk 6)

Tabla 114. Resumen de los mandatos de configuración de IPv6	
Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi.
add	Añade una dirección, rutas de escape, un filtro de paquete, una ruta o un túnel.
change	Cambia una dirección, rutas de escape, un filtro de paquete, una ruta o un túnel.
delete	Suprime una dirección, rutas de escape, un filtro de paquete, una ruta o un túnel.
disable	Inhabilita los redireccionamientos de icmp, un filtro de paquete o el descubrimiento de la MTU de la vía de acceso.
enable	Inhabilita los redireccionamientos de ICMP, los filtros de paquetes o el descubrimiento de la MTU de la vía de acceso.
list	Lista la configuración.
move	Desplaza el control del acceso.
set	Establece los valores de la configuración asociados con los túneles automáticos, el tamaño de almacenamiento intermedio de antememoria de vía de acceso de reenvío rápido, la pasarela por omisión, MLD, el temporizador de duración de la MTU de la vía de acceso, el tamaño de almacenamiento intermedio de reensamblaje de paquetes, el tamaño de tabla de direccionamiento, el ID de direccionador y el período de duración del direccionador.
update	Actualiza el filtro de paquete.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

## Add

Utilice el mandato **add** para añadir una dirección IPv6, rutas de escape, filtros de paquetes, rutas o túneles de IPv6 sobre IPv4.

```

add          access-control
               address red dirección prefijo
               leaked-routes destino
               packet-filter nombre interfaz
               route destino máscara pasarela coste ...
               tunnel destino prefijo direcciónr direcciónlocal coste ttl fragmen-
               tación
    
```

### Ejemplo:

```
IPv6 config>add address
Which net is this address for [0]? 5
New address []? 1::2
Prefix length must between 8 and 128 [128]?
```

```
IPv6 config>add leaked
IPv4 destination []? 1.2.3.4
Address mask [255.0.0.0]? 255.255.255.255
```

```
IPv6 config>add packet-filter
Packet-filter name []? pktf01
Filter incoming or outgoing traffic [IN]
Which interface is this filter for [0]? 3
```

```
IPv6 config>add route
IPv6 destination []? 8::9
Prefix length must between 8 and 128 [8]? 128
Via gateway 1 at []? 1::2
Cost [1]?
Via gateway 2 at []? 2::3
Cost [1]? 1000
Via gateway 3 at []? 3::4
Cost [1]? 10000
Via gateway 4 at []? 4::5
Cost [1]? 10
```

```
IPv6 config>add tunnel
Add a static route through this tunnel? [Yes[:
IPv6 destination network []? 3::4
Prefix length must between 0 and 128 [64]? 128
IPv4 tunnel remote address []? 1.2.3.4
IPv4 tunnel local address []? 2.3.40.0
Cost [1]?
TTL value [64]?
Allow fragmentation in tunnel?(Yes or [No]):
```

### access-control

Añade el control del acceso.

#### access control type

Indica lo que se hace con los paquetes que coinciden con los parámetros de normas del control del acceso.

- |   |  |
|---|--|
| E | Exclusivo; se desechan los paquetes coincidentes.                                      |
| I | Inclusivo; el direccionador realiza un proceso adicional de los paquetes coincidentes. |

#### Internet source

Dirección Internet de origen.

**Valores válidos:** Cualquier dirección Internet válida

**Valores por omisión:** Ninguno

#### Source Prefix length

Especifica la longitud de prefijo para la dirección de origen Internet.

**Valores válidos:** 0 - 128

**Valores por omisión:** 128

### Internet destination

Dirección Internet de destino.

**Valores válidos:** Cualquier dirección Internet válida

**Valor por omisión:** Ninguno

### Destination Prefix length

Especifica la longitud de prefijo para la dirección de destino Internet.

**Valores válidos:** 0 - 128

**Valores por omisión:** 128

### Starting protocol number

Especifica el número de protocolo de inicio para un rango de números de protocolo. Entre un valor de 0 para seleccionar todos los protocolos.

Algunos números de protocolo frecuentes son:

- 1 para ICMP
- 6 para TCP
- 17 para UDP
- 89 para OSPF
- 50 para ESP-Encryption
- 51 para AH-Encryption

**Valores válidos:** Del 0 al 255

**Valores por omisión:** 0

### Ending protocol number

Especifica el número de protocolo final para un rango de números de protocolo. Entre un valor de 0 para seleccionar todos los protocolos.

Algunos números de protocolo frecuentes son:

- 1 para ICMP
- 6 para TCP
- 17 para UDP
- 89 para OSPF
- 50 para ESP-Encryption
- 51 para AH-Encryption

**Valores válidos:** Del 0 al 255

**Valores por omisión:** El valor especificado en **starting protocol number**

### Starting destination port number

Especifica el número de puerto de inicio para un rango de números de puerto de destino TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye el 6 (para TCP) o el 17 (para UDP). Estos parámetros se ignoran para los paquetes en que el número de protocolo no sea el 6 ó el 17.

Algunos números de puerto que se utilizan normalmente son:

- 21 para FTP
- 23 para Telnet

25 para SMTP  
513 para rlogin  
520 para RIP para IPv4  
521 para RIP6 para IPv6

**Valores válidos:** 0 - 65535

**Valor por omisión:** 0

### Ending destination port number

Especifica el número de puerto final para un rango de números de puerto de destino TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye el 6 (para TCP) o el 17 (para UDP). Estos parámetros se ignoran para los paquetes en que el número de protocolo no sea el 6 ó el 17.

Algunos números de puerto que se utilizan normalmente son:

21 para FTP  
23 para Telnet  
25 para SMTP  
513 para rlogin  
520 para RIP para IPv4  
521 para RIP6 para IPv6

**Valores válidos:** 0 - 65535

**Valor por omisión:** El valor especificado en **starting destination port number**

### Starting source port number

Especifica el número de puerto de inicio para un rango de números de puerto de origen TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye el 6 (para TCP) o el 17 (para UDP). Estos parámetros se ignoran para los paquetes en que el número de protocolo no sea el 6 ó el 17. Consulte la descripción de **starting destination port number** para ver la lista de los números de puerto TCP/UDP que se utilizan normalmente.

**Valores válidos:** 0 - 65535

**Valor por omisión:** 0

### Ending source port number

Especifica el número de puerto final para un rango de números de puerto de origen TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye el 6 (para TCP) o el 17 (para UDP). Estos parámetros se ignoran para los paquetes en que el número de protocolo no sea el 6 ó el 17. Consulte la descripción de **starting destination port number** para ver la lista de los números de puerto TCP/UDP que se utilizan normalmente.

**Valores válidos:** 0 - 65535

**Valor por omisión:** El valor especificado en **starting source port number**

**address** Añade una dirección IPv6.

## Mandatos de configuración de IPv6 (Talk 6)

### Which net is this address for

Especifica la red a la que debe añadirse la dirección IPv6.

**Valores válidos:** Un valor numérico que identifique a una interfaz de red

**Valor por omisión:** 0

### New address

Especifica la nueva dirección IPv6 a añadir.

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

### Prefix length

Valor decimal que especifica el número de bits contiguos más a la izquierda de la dirección que abarca el prefijo.

**Valores válidos:** 8 - 128

**Valor por omisión:** 128

### leaked-routes

Añade una ruta de escape.

#### IPV4 destination

Especifica la dirección IPv6 del destino de la ruta de escape.

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

### packet-filter

Añade un filtro de paquete.

#### packet-filter name

Especifica un nombre alfanumérico utilizado para identificar al filtro de paquete.

**Valores válidos:** Cualquier serie de caracteres alfanuméricos con un máximo de 16 caracteres de longitud

**Valor por omisión:** Ninguno

#### Filter incoming or outgoing traffic?

Especifica si desea filtrar el tráfico de entrada o el de salida.

**Valores válidos:** OUT o IN

**Valor por omisión:** IN

#### which interface is this filter for

Especifica el número de interfaz de red al que este filtro de paquete va a añadirse.

**Valores válidos:** Un valor numérico que identifique a cualquier interfaz para la que IPv6 sea un protocolo válido, o "a", que especifica que este filtro es para el túnel automático.

**Valor por omisión:** 0

**route**      Añade una ruta.



### IPv6 destination

Especifica la dirección IPv6 del destino de la ruta.

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

### Prefix length

Especifica la máscara que se va a aplicar a la dirección de destino.

**Valores válidos:** 8 - 128 (0 se permite si el destino de IPv6 es 0::0)

**Valor por omisión:** 8

### Via gateway 1

Especifica la dirección IPv6 de la pasarela 1.

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

### Cost

Especifica el coste de esta ruta.

**Valores válidos:** Un valor numérico

**Valor por omisión:** 1

### Via gateway 2

Especifica la dirección IPv6 de la pasarela 2.

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

### Cost

Especifica el coste de esta ruta.

**Valores válidos:** Un valor numérico

**Valor por omisión:** 1

### Via gateway 3

Especifica la dirección IPv6 de la pasarela 3.

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

### Cost

Especifica el coste de esta ruta.

**Valores válidos:** Un valor numérico

**Valor por omisión:** 1

### Via gateway 4

Especifica la dirección IPv6 de la pasarela 4.

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

### Cost

Especifica el coste de esta ruta.

**Valores válidos:** Un valor numérico

**Valor por omisión:** 1

**tunnel** Añade un túnel.

### Add a static route through this tunnel?

Especifica si el túnel tendrá definida una ruta estática o no.

**Valores válidos:** Yes o No

**Valor por omisión:** Yes

### IPv6 destination network

Especifica la dirección IPv6 de la red de destino a la que llegará el túnel.

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

### Prefix length

Valor decimal que especifica el número de bits contiguos más a la izquierda de la dirección IPv6 que abarca el prefijo.

**Valores válidos:** 8 - 128

**Valor por omisión:** 64

### IPv4 tunnel remote address

Especifica la dirección IPv4 de las tramas de IPv6 que pasen por el túnel.

**Valores válidos:** Cualquier dirección IP válida (32 bits)

**Valor por omisión:** Ninguno

### IPv4 tunnel local address

Especifica la dirección de origen IPv4 de las tramas de IPv6 que pasen por el túnel.

**Valores válidos:** Cualquier dirección IP válida (32 bits)

**Valor por omisión:** Ninguno

### Cost

Especifica el coste asociado con el túnel que se utilizará durante las búsquedas de rutas para encontrar la mejor ruta hacia el destino.

**Valores válidos:** 1 - 255

**Valor por omisión:** 1

### TTL value

Especifica el valor de período de duración utilizado en las tramas encapsuladas para este túnel

**Valores válidos:** Cualquier valor numérico dentro del rango del 1 al 255

**Valor por omisión:** 64

### Allow fragmentation in the tunnel?

Especifica si se permitirá la fragmentación en el túnel. Si se especifica yes, se permite la fragmentación en el túnel en el caso de que la red IPv4 que utilice el túnel no proporcione suficiente información como para permitir que el dispositivo devuelva un mensaje indicando que hay un "paquete demasiado grande" al sistema principal IPv6.

**Valores válidos:** yes o no

Valor por omisión: no

## Change

Utilice el mandato **change** para añadir un registro de control del acceso, una dirección IPv6, rutas de escape, filtros de paquetes, rutas o túneles.

### Sintaxis:

**change**            *access-control índice*  
                       *address red dirección prefijo*  
                       *leaked-routes destino*  
                       *packet-filter nombre interfaz*  
                       *route destino máscara pasarela coste ...*  
                       *tunnel destino prefijo direcciónr direcciónlocal coste ttl fragmen-*  
                           *tación*

### **access-control**

Cambia la configuración del control del acceso.

**address**    Cambia una dirección.

### **leaked-routes**

Cambia la configuración de una ruta de escape.

### **packet-filter**

Cambia la configuración de un filtro de paquete.

**route**        Cambia la configuración de una ruta.

**tunnel**      Cambia la configuración de un túnel.

Consulte la sección "Add" en la página 482 para obtener una descripción de los parámetros asociados con el mandato **change**.

## Delete

Utilice el mandato **delete** para eliminar un registro de control del acceso, una dirección, rutas de escape, un filtro de paquete, una ruta o un túnel.

### Sintaxis:

**delete**            *access-control índice*  
                       *address dirección*  
                       *leaked-routes destino*  
                       *packet-filter nombre*  
                       *route destino máscara pasarela*  
                       *tunnel túnelnúm.*

## Disable

Utilice el mandato **disable** para inhabilitar el redireccionamiento de ICMP, los filtros de paquetes y el descubrimiento de la MTU de la vía de acceso.

### Sintaxis:

**disable**            *icmp-redirect dirección*  
                       *packet-filter nombre-filtro-paquete*  
                       *path-mtu-discovery*

## Mandatos de configuración de IPv6 (Talk 6)

### **icmp-redirect**

Inhabilita los redireccionamientos de ICMP.

### **packet-filter**

Inhabilita un filtro de paquete.

#### **packet-filter name**

Especifica el nombre del filtro de paquete a inhabilitar.

**Valores válidos:** Cualquier filtro de paquete configurado

**Valor por omisión:** Ninguno

### **path-mtu-discovery**

Inhabilita el protocolo Path MTU Discovery.

## Enable

Utilice el mandato **enable** para habilitar los redireccionamientos de ICMP, los filtros de paquetes o el descubrimiento de la MTU de la vía de acceso.

### **Sintaxis:**

**enable**            *icmp-redirect dirección*  
                      *packet-filter nombre-filtro-paquete*  
                      *path-mtu-discovery*

### **icmp-redirect**

Habilita los redireccionamientos de ICMP.

#### **interface address**

Especifica la dirección de interfaz.

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Nulo (especifica todas las direcciones)

### **packet-filter**

Habilita un filtro de paquete.

#### **packet-filter name**

Especifica el nombre del filtro de paquete a habilitar. Este nombre se configura utilizando el mandato **add packet-filter**.

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

### **path-mtu-discovery**

Habilita Path MTU Discovery, un protocolo que permite que un nodo sistema principal determine el tamaño máximo de los paquetes que pasarán por una vía de acceso hacia un destino sin fragmentación.

## List

Utilice el mandato **list** para visualizar la configuración de IPv6.

### **Sintaxis:**

**list**                *all*  
                      *access-control*  
                      *addresses*  
                      *icmp-redirect*  
                      *leaked-routes*

mld  
packet-filter  
routes  
sizes  
tunnels

**Ejemplo:**

```

IPv6 config>list all
Interface addresses
IPv6 addresses for each interface:
  intf 0          IP disabled on this interface
  intf 1          IP disabled on this interface
  intf 2          IP disabled on this interface
  intf 3          IP disabled on this interface
  intf 4          IP disabled on this interface
  intf 5  1234:1234:1234:1234:5234:6234:7234:8234/128
             1223::7:1234/8
Router-ID: 1::9
Internal IP address: 1::8

Routing

route to: 1234::1223/128
  via: 1234:0:9::8          cost: 100
  via: 1234:0:9:8:8:7:6:8   cost: 232
  via: 1:2:3:4:5:6:7:8      cost: 1
  via: 8:7:6:5:4:3:2:1      cost: 1
route to: ::/0
  via: 1::8                 cost: 100
route to: 2::8:9/8
  via: 1::8                 cost: 1

Path MTU Discovery: disabled
Path MTU Aging Timer: 10 minutes

Access Control is: enabled
  
```

## Mandatos de configuración de IPv6 (Talk 6)

IPv6 config>**list addresses**

IPv6 addresses for each interface:

```
intf 0          IP disabled on this interface
intf 1          IP disabled on this interface
intf 2          IP disabled on this interface
intf 3          IP disabled on this interface
intf 4          IP disabled on this interface
intf 5  1234:1234:1234:1234:5234:6234:7234:8234/128
            1223::7:1234/8
```

Router-ID: 1::9

Internal IP address: 1::8

IPv6 config>**list icmp-redirect**

ICMP Redirect generation for IP interface:

```
intf 0          IP disabled on this interface
intf 1          IP disabled on this interface
intf 2          IP disabled on this interface
intf 3          IP disabled on this interface
intf 4          IP disabled on this interface
intf 5  1234:1234:1234:1234:5234:6234:7234:8234/128 ICMP Redirect enabled
            1223::7:1234/8 ICMP Redirect enabled
intf 6          IP disabled on this interface
intf 7          IP disabled on this interface
```

IPv6 config>**list leaked-routes**

# IPv4 Address Mask

IPv6 config>**list mld**

Net	Query Interval (secs)	Response Interval (secs)	Leave Query Interval (secs)
---	-----	-----	-----
5	125	10	1

IPv6 config>**list packet-filter**

List of packet-filter records:

Name	Interface	State
packet01	0	On
pack01	5	On

Access Control is: enabled

IPv6 config>**list routes**

```
route to: 1234::1223/128
  via: 1234:0:9::8          cost: 100
  via: 1234:0:9:8:8:7:6:8   cost: 232
  via: 1:2:3:4:5:6:7:8     cost: 1
  via: 8:7:6:5:4:3:2:1     cost: 1
route to: ::/0
  via: 1::8                cost: 100
route to: 2::8:9/8
  via: 1::8                cost: 1
```

IPv6 config>**list sizes**

Routing table size: 768 nets (79872 bytes)

Reassembly buffer size: 12000 bytes

Routing cache size: 64 entries

Time to live: 64

Path MTU aging timer: 10

IPv6 config>**list tunnel**

Tun#	Remote Endpoint	Local Endpoint	Frag Allowed	TTL	Cost	Net#	IPv6 Address/Prefix
1	1.2.3.4	2.3.4.5	No	100	100	7	1:2:3:4:5:6:7:8/128

IPv6 config>

## Move

Utilice el mandato **move** para cambiar el orden de los registros de control del acceso configurados.

### Sintaxis:

move                    access-control

### Index of control to move

Seleccione el número de índice del registro de control del acceso que desee desplazar.

### Move record AFTER record number

Seleccione el número de índice del registro de control del acceso al que desea que siga este registro.

### Are you sure that this is what you want to do

Le permite confirmar si es correcta la instrucción del desplazamiento.

## Set

Utilice el mandato **set** para establecer los parámetros de configuración.

### Sintaxis:

set                    access-control  
automatic-tunnel-parameters *ttl fragmentación cuentasaltos*  
cache-size *núm.entradas*  
default ...  
internal-ip-address  
mld ...  
path-mtu-aging-timer  
reassembly-size  
router-id  
routing *núm.redes*  
ttl

### Ejemplo:

## Mandatos de configuración de IPv6 (Talk 6)

```
IPv6 config>set au
TTL value [64]?
Allow fragmentation in tunnel?(Yes or [No]):
```

```
IPv6 config>set ca
number of cache entries [64]?
```

```
IPv6 config>set mld query-interval
Network interface [0]? 5
New Query Interval (in secs) [125]?
```

```
IPv6 config>set mld response-interval
Network interface [0]? 5
New Response Interval (in secs) [10]?
```

```
IPv6 config>set mld robust
Network interface [0]? 5
New Robustness Variable [2]?
IPv6 config>set mld leave
Network interface [0]?
New Leave Interval (in secs) [1]?
IPv6 config>?
```

### **access-control**

Especifica si el control del acceso se habilita o inhabilita.

**Valores válidos:** on/off

**Valor por omisión:** off

### **automatic-tunnel-parameters**

Especifica los valores de los parámetros de túnel para los túneles automáticos que fluyen por el direccionador.

**ttl value** Especifica el valor de tiempo de duración para las tramas encapsuladas para el túnel.

**Valores válidos:**

**Valor por omisión:** 64

### **allow fragmentation in tunnel?**

Especifica si se permitirá la fragmentación en el túnel. Si se especifica *yes*, se permite la fragmentación en el túnel en el caso de que la red IPv4 que utilice el túnel no proporcione suficiente información como para permitir que el dispositivo devuelva un mensaje indicando que hay un "paquete demasiado grande" al sistema principal IPv6.

**Valores válidos:** yes o no

**Valor por omisión:** no

### **hop count**

Especifica la cuenta de saltos a utilizar en los paquetes de túnel automático.

**Valores válidos:** 1 - 255

**Valor por omisión:** 64

### **cache-size**

Especifica el tamaño de almacenamiento intermedio para la antememoria de vía de acceso de reenvío rápido.



### **number of cache entries**

Especifica el número de entradas de la antememoria de vía de acceso de reenvío rápido.

**Valores válidos:** 64 - 10 000

**Valor por omisión:** 64

### **default network-gateway**

#### **default gateway**

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

#### **gateway's cost**

Especifica el coste asociado con esta pasarela.

**Valores válidos:** 1 - 255

**Valor por omisión:** 1

### **default subnet-gateway**

#### **for which subnetted network**

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

#### **default gateway**

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

#### **gateway's cost**

Especifica el coste asociado con esta pasarela.

**Valores válidos:** 1 - 255

**Valor por omisión:** 1

### **internal-ip-address**

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

### **mld**

#### **query-interval**

#### **network interface**

**Valores válidos:** Cualquier número de interfaz de red válido

**Valor por omisión:** 0

## Mandatos de configuración de IPv6 (Talk 6)

### new query interval (in secs)

**Valores válidos:** 1 - 3600

**Valor por omisión:** 125

### response-interval

#### network interface

**Valores válidos:** Cualquier número de interfaz de red válido

**Valor por omisión:** 0

#### new response interval (in secs)

**Valores válidos:** 1 - 60

**Valor por omisión:** 10

### robustness-variable

#### network interface

**Valores válidos:** Cualquier número de interfaz de red válido

**Valor por omisión:** 0

#### new robustness variable

**Valores válidos:** 2 - 10

**Valor por omisión:** 2

### leave-interval

#### network interface

**Valores válidos:** Cualquier número de interfaz de red válido

**Valor por omisión:** 0

#### new leave interval (in secs)

**Valores válidos:** 1 - 60

**Valor por omisión:** 1

### path-mtu-aging-timer

Especifica el período de tiempo en minutos para las MTU de vía de acceso que se han determinado por medio del descubrimiento de la MTU de la vía de acceso.

**Valores válidos:** De 10 a 60 minutos, donde 0 = inhabilitación

**Valor por omisión:** 10

**reassembly-size**

Especifica el tamaño de los almacenamientos intermedios de reensamblaje utilizados para procesar la cabecera de fragmento.

**Valores válidos:** 2048 - 65536

**Valor por omisión:** 12000

**router-id** Especifica la dirección IPv6 del direccionador.

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

**routing table-size**

**number of nets**

**Valores válidos:** 64 - 65535

**Valor por omisión:** 768

**ttl** Especifica el valor de período de duración de IPv6.

**Valores válidos:**

**Valor por omisión:** 64

## Update

Utilice el mandato **update** para actualizar el filtro de paquete.

**Sintaxis:**

**update** packet-filter

**packet-filter**

Utilice este mandato para acceder al indicador de mandatos `Packet-filter 'xx' Config>`, desde el cual puede configurar los filtros de paquetes.

## Mandatos de Update Packet-filter

<i>Tabla 115. Resumen de los mandatos de configuración de Update Packet-filter</i>	
Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi.
Add	Añade el control del acceso.
Change	Cambia el control del acceso.
Delete	Suprime el control del acceso.
Move	Reordena la lista de controles del acceso aplicada al filtro de paquete.
List	
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

### Add

Utilice el mandato **update packet-filter add** para añadir una lista de controles del acceso.

### Sintaxis:

**add** *access-control tipo dirorigen preforigen dirdest predest*

#### access-control

Añade un elemento de control del acceso a la lista de controles del acceso.

**Type** Especifica si el control del acceso es inclusivo o exclusivo.

**Valores válidos:** I o E

**Valor por omisión:** I

#### Internet source

Especifica la dirección IPv6 del origen del paquete.

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

#### Prefix length

Valor decimal que especifica el número de bits contiguos más a la izquierda de la dirección IPv6 que abarca el prefijo.

**Valores válidos:** 0- 128

**Valor por omisión:** 128

#### Internet destination

Especifica la dirección IPv6 del destino del paquete.

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

#### Prefix length

Valor decimal que especifica el número de bits contiguos más a la izquierda de la dirección IPv6 que abarca el prefijo.

**Valores válidos:** 0- 128

**Valor por omisión:** 128

#### Starting protocol number

Especifica el número de protocolo de inicio para un rango de números de protocolo. Entre un valor de 0 para seleccionar todos los protocolos.

Algunos números de protocolo frecuentes son:

1 para ICMP

6 para TCP

17 para UDP

89 para OSPF

50 para ESP-Encryption

51 para AH-Encryption

**Valores válidos:** Del 0 al 255

**Valores por omisión:** 0

### Ending protocol number

Especifica el número de protocolo final para un rango de números de protocolo. Entre un valor de 0 para seleccionar todos los protocolos.

Algunos números de protocolo frecuentes son:

- 1 para ICMP
- 6 para TCP
- 17 para UDP
- 89 para OSPF
- 50 para ESP-Encryption
- 51 para AH-Encryption

**Valores válidos:** Del 0 al 255

**Valores por omisión:** El valor especificado en **starting protocol number**

### Starting destination port number

Especifica el número de puerto de inicio para un rango de números de puerto de destino TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye el 6 (para TCP) o el 17 (para UDP). Estos parámetros se ignoran para los paquetes en que el número de protocolo no sea el 6 ó el 17.

Algunos números de puerto que se utilizan normalmente son:

- 21 para FTP
- 23 para Telnet
- 25 para SMTP
- 513 para rlogin
- 520 para RIP

**Valores válidos:** 0 - 65535

**Valor por omisión:** 0

### Ending destination port number

Especifica el número de puerto final para un rango de números de puerto de destino TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye el 6 (para TCP) o el 17 (para UDP). Estos parámetros se ignoran para los paquetes en que el número de protocolo no sea el 6 ó el 17.

Algunos números de puerto que se utilizan normalmente son:

- 21 para FTP
- 23 para Telnet
- 25 para SMTP
- 513 para rlogin
- 520 para RIP

**Valores válidos:** 0 - 65535

**Valor por omisión:** El valor especificado en **starting destination port number**

### Starting source port number

Especifica el número de puerto de inicio para un rango de números de puerto de origen TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye el 6 (para TCP) o el 17 (para UDP). Estos parámetros se ignoran para los paquetes en que el número de protocolo no sea el 6 ó el 17. Consulte la descripción de **starting destination port number** para ver la lista de los números de puerto TCP/UDP que se utilizan normalmente.

**Valores válidos:** 0 - 65535

**Valor por omisión:** 0

### Ending source port number

Especifica el número de puerto final para un rango de números de puerto de origen TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye el 6 (para TCP) o el 17 (para UDP). Estos parámetros se ignoran para los paquetes en que el número de protocolo no sea el 6 ó el 17. Consulte la descripción de **starting destination port number** para ver la lista de los números de puerto TCP/UDP que se utilizan normalmente.

**Valores válidos:** 0 - 65535

**Valor por omisión:** El valor especificado en **starting source port number**

## Change

Utilice el mandato **update packet-filter change** para cambiar un control del acceso.

### Sintaxis:

**change** *access-control tipo dirorigen preforigen dirdest prefdest*

### access-control

Cambia un elemento de control del acceso.

**Type** Especifica si el elemento de control del acceso es inclusivo o si se utilizará para identificar paquetes que deban asegurarse.

**Valores válidos:** I o S

**Valor por omisión:** I

### Internet source

Especifica la dirección IPv6 del origen del paquete.

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

### Prefix length

Valor decimal que especifica el número de bits contiguos más a la izquierda de la dirección IPv6 que abarca el prefijo.

**Valores válidos:** 0- 128

**Valor por omisión:** 128

### Internet destination

Especifica la dirección IPv6 del destino del paquete.

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

### Prefix length

Valor decimal que especifica el número de bits contiguos más a la izquierda de la dirección IPv6 que abarca el prefijo.

**Valores válidos:** 0- 128

**Valor por omisión:** 128

### Delete

Utilice el mandato **update packet-filter delete** para eliminar un elemento de control del acceso de la lista de controles del acceso.

#### Sintaxis:

delete                    *access-control índicenúm.*

#### access-control

Suprime un control del acceso.

#### index of access control to be deleted

Especifica el índice de la configuración de control del acceso a eliminar.

**Valores válidos:** Del 1 al número de registros de control del acceso definidos para este filtro de paquete

**Valor por omisión:** 1

### Move

Utilice el mandato **update packet-filter move** para reordenar la lista de controles del acceso aplicada al filtro de paquete.

#### Sintaxis:

move                    *access-control índicenúm. número a seguir*

#### access-control

#### index of control to move

**Valores válidos:** Del 1 al número de registros de control del acceso definidos para este filtro de paquete

**Valor por omisión:** 1

#### Move record after record number

Especifica la ubicación de destino dentro de la lista de controles del acceso. Se le solicitará que verifique si ésta es la acción que desea configurar.

**Valores válidos:** Del 1 al número de registros de control del acceso definidos para este filtro de paquete

**Valor por omisión:** 0

## Mandatos de supervisión de IPv6 (Talk 5)

### List

Utilice el mandato **update packet-filter list** para visualizar la configuración de la lista de controles del acceso.

### Sintaxis:

```
list          access-controls
```

### Ejemplo:

```
Packet-filter 'x' Config> li acc
Access control is : enabled
List of access control records:

1  Type=IS  Source=2001:1::6101/128
    Dest= 2001:1::86/128
    Tid=3

2  Type=I   Source=::/0
    Dest=::/0

Packet-filter 'x' Config>
```

---

## Acceso al entorno de supervisión de IPv6

Utilice el procedimiento siguiente para acceder a los mandatos de supervisión de IPv6. Este proceso le proporciona acceso al proceso de supervisión de IPv6.

1. En el indicador de OPCON, entre **talk 5**. (Para obtener información más detallada sobre este mandato, consulte el capítulo titulado “El proceso y los mandatos de OPCON” en la publicación *Nways Multiprotocol Access Services Guía del usuario de software*.) Por ejemplo:

```
* talk 5
+
```

Después de que se entre el mandato **talk 5**, se visualizará el indicador de GWCON (+) en el terminal. Si no aparece el indicador la primera vez que entre la configuración, pulse **Intro** de nuevo.

2. En el indicador +, entre el mandato **p ipv6** para obtener el indicador ipv6>.

### Ejemplo:

```
+ p ipv6
ipv6>
```

---

## Mandatos de supervisión de IPv6

Este apartado describe los mandatos de supervisión de IPv6.



Tabla 116. Resumen de los mandatos de supervisión de IPv6

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi.
access-control	Visualiza los registros de control del acceso.
cache	Visualiza las entradas de antememoria.
counters	Visualiza los contadores.
dump routing tables	Vuelca las tablas de direccionamiento configuradas.
interface addresses	Visualiza las direcciones definidas en la interfaz.
internal address	Visualiza la dirección interna especificada.
mcast	Visualiza una lista de las direcciones de vertimiento múltiple registradas.
mld	Visualiza los contadores o parámetros de MLD.
reset	Restablece la interfaz IPv6.
route	
sizes	Visualiza los tamaños de antememoria.
sniffer	Establece diversas opciones de rastreo.
static routes	Visualiza las rutas estáticas.
packet-filter	Visualiza los filtros de paquetes configurados.
path-mtu	
ping6	Activa Ping.
traceroute6	Efectúa el rastreo de una ruta dinámicamente.
tunnels	Visualiza los túneles configurados.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

## Access-control

Utilice el mandato **access-control** para supervisar los registros de control del acceso configurados.

### Sintaxis:

**access-control**

### Cache

Utilice el mandato **cache** para visualizar

**Sintaxis:**

cache

**Ejemplo:**

```
IPv6>cache
Destination                               Usage           Next hop
```

### Counters

Utilice el mandato **counters** para visualizar el estado de los contadores.

**Sintaxis:**

counters

**Ejemplo:**

```
IPv6>counters
Routing errors
Count  Type
    0   Routing table overflow
    0   Net unreachable
    0   Bad subnet number
    0   Bad net number
    0   Unhandled broadcast
    0   Unhandled anycast
    0   Unhandled directed broadcast
    0   Attempted forward of LL broadcast
    0
    0   None

Packets discarded through filter  0
IP multicasts accepted:           0

IP input packet overflows
  Net  Count
  ATM/0  0
  NHRPL/0  0
    TKR/0  0
    TKR/1  0
    FR/0  0
    PPP/0  0
  FDDI/0  0
  IP64/0  0
```

### Dump routing tables

Utilice el mandato **dump** para visualizar las tablas de direccionamiento configuradas.

**Sintaxis:**

dump

**Ejemplo:**

```
IPv6>dump
Type  Dest net/Prefix          Cost   Age   Next hop(s)

Stat* 1:2:3:4:5:6:7:8/128      100   30    IP64/0

IPv6 Routing table size: 768 nets (79872 bytes), 1 nets known
                        0 nets hidden, 0 nets deleted, 0 nets inactive
                        0 routes used internally, 767 routes free
```

### Interface addresses

Utilice el mandato **interface** para visualizar las direcciones configuradas en la interfaz.

#### Sintaxis:

interface

#### Ejemplo:

```
IPv6>interface
```

Interface	Net:Status	IPV6 State	IPV6 MTU	ICMP redir	IPV6 Address/Prefixlen
Eth/0	0 : DWN	DWN	1500	Enabled	2003:6:14:1::610/64
Eth/1	1 : DWN	DWN	1500	Enabled	2003:7:6:1::610/64
IP64/0	3 : UP	UP	2048	Enabled	FE80::14FF:FE80:3/64

### Internal address

Utilice el mandato **internal** para visualizar la dirección interna especificada.

#### Sintaxis:

internal

### Mcast

Utilice el mandato **mcast** para visualizar las direcciones de vertimiento múltiple configuradas.

#### Sintaxis:

mcast

#### Ejemplo:

```
IPv6>mcast
List of IPV6 registered multicast addresses
```

```
Interface: Eth/0:
```

```
Address/Ref_Cnt
FF02::1/1
FF02::2/1
FF02::1:FF00:610/1
FF02::1:FF02:6200/1
FF02::9/1
```

## Mandatos de supervisión de IPv6 (Talk 5)

### Mld

Utilice el mandato **mld** para visualizar los contadores y parámetros de mld configurados.

#### Sintaxis:

```
mld          counters
              parameters
```

#### Ejemplo:

```
IPv6>mld counters
Net      Querier      Polls Sent      Polls Rcvd      Reports Rcvd
---      -
IPv6>mld parameters
Net      Robustness  Query Interval  Response Interval  Leave Query Interval
      Variable      (secs)          (secs)              (secs)
---      -
IPv6>
```

### Reset

Utilice el mandato **reset** para restablecer dinámicamente la interfaz IPv6.

#### Sintaxis:

```
reset          ipv6
```

#### Ejemplo:

```
IPv6>reset ipv6
```

### Route

Utilice el mandato **route** para mostrar la ruta hacia la dirección IPv6.

#### Sintaxis:

```
route          dirección
```

#### Ejemplo:

```
IPv6>route 6::9
IPv6>
```

### Sizes

Utilice el mandato **sizes** para visualizar los tamaños de almacenamiento intermedio configurados.

#### Sintaxis:

```
sizes
```

#### Ejemplo:

```
IPv6>sizes
  Routing table size:          768
  Table entries used:         3
  Reassembly buffer size:    12000
  Largest reassembled pkt:   0
  Size of routing cache:     64
  # cache entries in use:    0
```

```
IPv6>
```

## Sniffer

Utilice el mandato **sniffer** para establecer diversas opciones de rastreo.

### Sintaxis:

```
sniffer          mandato de rastreo
```

Elija el **mandato de rastreo** a partir de esta lista:

- 1 List current traces
- 2 Trace source address
- 3 Trace destination address
- 4 Trace protocol
- 5 Trace TCP source port
- 6 Trace TCP destination port
- 7 Trace UDP source port
- 8 Trace UDP destination port
- 9 Clear trace
- 10 Exit

## Static routes

Utilice el mandato **static** para visualizar las rutas estáticas configuradas.

### Sintaxis:

```
static
```

### Ejemplo:

```
IPv6>static
Net/Mask_len      Cost Next hop
1234::1223/128    100  1234:0:9::8 PPP/0
                  232  1234:0:9:8:8:7:6:8 PPP/0
8::9              128  N/A  filter
```

```
IPv6>
```

## Packet-filter

Utilice el mandato **packet-filter** para visualizar un resumen de los filtros de paquetes configurados.

### Sintaxis:

```
packet-filter
```

## Mandatos de supervisión de IPv6 (Talk 5)

### Ejemplo:

```
IPv6>pac
Name          Dir  Intf  State  #Access-Controls
packet01      Out  0     On     0
pack01        Out  5     On     2
IPv6>
```

## Path-mtu

Utilice el mandato **path-mtu** para mostrar las vías de acceso que se han identificado como vías que contienen una MTU cuyo tamaño es inferior al de un paquete enviado por esa vía de acceso.

### Sintaxis:

path-mtu

### Ejemplo:

## Ping6

Utilice el mandato **ping6** para realizar una acción de ping con una dirección IPv6.

### Sintaxis:

ping6

### Ejemplo:

```
IPv6>ping
Destination IPv6 address [::]? 8::9
Source IPv6 Address [1::8]?
Ping data size in bytes [56]?
Ping TTL [64]?
Ping rate in seconds [1]?
PING6 1::8 -> 8::9: 56 data bytes, ttl=64, every 1 sec.
```

```
----8::9 PING6 Statistics----
36 packets transmitted, 36 packets received
```

### Destination IPv6 address

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

### Source IPv6 address

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

### Ping data size in bytes

**Valores válidos:** Del 0 al tamaño del almacenamiento intermedio global

**Valor por omisión:** 56

**Ping ttl** Especifica el período de duración para el ping.

**Valores válidos:** 1 - 255

**Valor por omisión:** 64

**Ping rate in seconds**

Especifica la frecuencia de los ping.

**Valores válidos:** 1 - 60

**Valor por omisión:** 1

## Traceroute6

Utilice el mandato **traceroute6** para realizar el rastreo de una ruta dinámicamente.

**Sintaxis:**

**traceroute6 ...**

**Ejemplo:**

```
IPv6>traceroute6
Destination IPv6 address []? 7::8
Source IPv6 address []? 6::9
Data size in bytes [56]?
Number of probes per hop [3]?
Wait time between retries in seconds [3]?
Maximum TTL [32]?
TRACEROUTE6 7::8: 56 data bytes
 1 * * * *
IPv6>
```

**Destination IPv6 address**

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

**Source IPv6 address**

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

**Data size in bytes**

**Valores válidos:** Del 0 al tamaño del almacenamiento intermedio global

**Valor por omisión:** 56

**Number of probes per hop**

**Valores válidos:** 1 - 10

**Valor por omisión:** 3

**Wait time between retries in seconds**

**Valores válidos:** 1 - 60

**Valor por omisión:** 3

## Maximum ttl

**Valores válidos:** 1 - 255

**Valor por omisión:** 32

## Tunnels

Utilice el mandato **tunnels** para visualizar los túneles configurados.

### Sintaxis:

**tunnels**

### Ejemplo:

IPv6>**tunnels**

```

                                Configured Tunnels
Tun# Remote Endpoint Local Endpoint Frag Allowed TTL MTU Net# IPv6 Address/Prefix
  1   1.2.3.4         2.3.4.5           No         100  2048  7   1:2:3:4:5:6:7:8/128

                                Automatic Tunnels
Tun# Remote Endpoint Frag Allowed TTL MTU
IPv6>
```

---

## Soporte de la reconfiguración dinámica de IPv6

Este apartado describe la reconfiguración dinámica (DR) tal como afecta a los mandatos Talk 6 y Talk 5.

### Mandato Delete Interface de CONFIG (Talk 6)

IP Versión 6 (IPv6) da soporte al mandato de CONFIG (Talk 6) **delete interface** sin restricciones.

### Mandato Activate Interface de GWCON (Talk 5)

IPv6 da soporte al mandato de GWCON (Talk 5) **activate interface** con la consideración siguiente:

Si antes no se ha configurado IPv6, es necesario rearrancar.

El mandato de GWCON (Talk 5) **activate interface** da soporte a todos los mandatos específicos de interfaz IPv6.

### Mandato Reset Interface de GWCON (Talk 5)

IPv6 da soporte al mandato de GWCON (Talk 5) **reset interface** con las consideraciones siguientes:

- Si antes no se ha configurado IPv6, es necesario rearrancar.
- Si falla la asignación de memoria, es necesario rearrancar.

El mandato de GWCON (Talk 5) **reset interface** da soporte a todos los mandatos específicos de interfaz IPv6.



## Mandatos Reset de GWCON (Talk 5) del componente

IPv6 da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos de IPv6:

### Mandato Reset IPv6 de GWCON, Protocolo IPv6

**Descripción:** Vuelve a leer la SRAM y vuelve a inicializar IPv6. También restablece RIP6, NDP6 y PIM6.

**Efecto en la red:** Ninguno.

**Limitaciones:** Ninguna.

Se activan automáticamente todos los cambios de la configuración de IPv6 excepto los siguientes:

Mandatos cuyos cambios no se activan mediante el mandato reset ipv6 de GWCON, protocolo ipv6
CONFIG, protocolo ipv6, set routing table-size
CONFIG, protocolo ipv6, set reassembly-size
CONFIG, protocolo ipv6, set cache-size

## Mandatos de CONFIG (Talk 6) de cambio inmediato

IPv6 da soporte a los siguientes mandatos de CONFIG que cambian inmediatamente el estado operativo del dispositivo. Estos cambios se guardan y se conservan si se vuelve a cargar o a iniciar el dispositivo o si se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
CONFIG, protocolo ipv6, add route
CONFIG, protocolo ipv6, delete route
CONFIG, protocolo ipv6, change route
CONFIG, protocolo ipv6, enable icmp-redirect
CONFIG, protocolo ipv6, disable icmp-redirect
CONFIG, protocolo ipv6, set access-control
CONFIG, protocolo ipv6, set ttl
CONFIG, protocolo ipv6, set path-mtu-aging-timer



---

## Configuración y supervisión de Neighbor Discovery Protocol (NDP)

La configuración de NDP se realiza para cada interfaz. Este capítulo describe cómo utilizar los mandatos de configuración y funcionamiento de NDP e incluye los apartados siguientes:

- “Acceso al entorno de configuración de NDP”
- “Mandatos de configuración de NDP”
- “Acceso al entorno de supervisión de NDP” en la página 520
- “Mandatos de supervisión de NDP” en la página 520
- “Soporte de la reconfiguración dinámica de NDP6” en la página 521

---

### Acceso al entorno de configuración de NDP

Utilice el procedimiento siguiente para acceder al proceso de configuración de NDP.

1. En el indicador de OPCON, entre **talk 6**. (Para obtener información más detallada sobre este mandato, consulte *El proceso y los mandatos de OPCON* en la publicación Nways Multiprotocol Access Services Guía del usuario de software.) Por ejemplo:

```
* talk 6
Config>
```

Después de entrar el mandato **talk 6**, se visualizará el indicador CONFIG (Config>) en el terminal. Si no aparece el indicador la primera vez que entre la configuración, pulse **Intro** de nuevo.

2. En el indicador CONFIG, entre el mandato **p ndp** para obtener el indicador NDP6 Config>.

---

### Mandatos de configuración de NDP

Para configurar NDP, entre los mandatos en el indicador NDP6 Config>.

Tabla 117. Resumen de los mandatos de configuración de NDP	
Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi.
add	Añade un anuncio o parámetros de direccionador.
change	Cambia un anuncio o parámetros de direccionador.
delete	Suprime un anuncio o parámetros de direccionador.
disable	Inhabilita el anuncio de direccionador.
enable	Habilita el anuncio de direccionador.
list	Lista la configuración.
set	Establece la cuenta de saltos de DHCP.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

## Add

Utilice el mandato **add** para añadir un anuncio de direccionador.

```
add          ra ...
                _dhcp-server
```

**ra** Añade un anuncio de direccionador.

### **add router advertisement on which interface**

Especifica la interfaz a la que se añadirá el anuncio de direccionador.

**Valores válidos:** Un valor numérico que identifique a una interfaz de red

**Valor por omisión:** 0

### **Managed address configuration (stateful)**

Especifica si los sistemas principales utilizarán el protocolo administrado para la configuración automática de direcciones además de direcciones configuradas automáticamente mediante la configuración automática sin estado.

**Valores válidos:** yes o no

**Valor por omisión:** n

Si especifica *yes*, el agente de relay de DHCPv6 permitirá que los sistemas principales utilicen direcciones de enlace local al configurar las direcciones aunque el servidor DHCPv6 no esté en el mismo enlace.

### **Other stateful configuration**

Especifica si los sistemas principales utilizarán el protocolo administrado para la configuración automática de otra información (no direcciones).

**Valores válidos:** yes o no

**Valor por omisión:** no

### **Include link layer address with router advertisement**

Especifica si se va a incluir la dirección de capa de enlace en el anuncio de direccionador. Un direccionador puede omitir esta dirección en el anuncio con el fin de habilitar el compartimiento de la carga interior entre diversas direcciones de capa de enlace.

**Valores válidos:** yes o no

**Valor por omisión:** yes

**Hop limit** Especifica el valor por omisión a colocar en el campo de límite de saltos en los mensajes de anuncio de direccionador enviados por el direccionador. Este valor se utiliza en el campo de cuenta de saltos de la cabecera de IP para los paquetes de IP de salida.

**Valores válidos:** 0 - 255, donde 0 significa no especificado por este direccionador

**Valor por omisión:** 0

### **Maximum router advertisement interval**

Especifica el período de tiempo máximo, en segundos, permitido entre los envíos de anuncios de direccionador no solicitados con vertimiento múltiple desde la interfaz.

**Valores válidos:** De 4 a 1800 segundos

**Valor por omisión:** 600

### **Minimum router advertisement interval**

Especifica el período de tiempo mínimo, en segundos, permitido entre los envíos de anuncios de direccionador no solicitados con vertimiento múltiple desde la interfaz.

**Valores válidos:** 3 -  $(0,75 * \text{Maximum router advertisement interval})$

**Valor por omisión:**  $\text{Maximum router advertisement interval}/3$

### **Router lifetime**

Especifica el período, en segundos, durante el cual el direccionador va a utilizarse como direccionador por omisión.

**Valores válidos:** 0 ó de 4 a 9000 segundos, donde 0 indica que el direccionador no va a utilizarse como direccionador por omisión

**Valor por omisión:**  $(3 * \text{Maximum router advertisement interval})$

### **Reachable Time**

Especifica el período, en segundos, durante el cual un nodo supone que un contiguo es asequible después de haber recibido una confirmación de asequibilidad.

**Valores válidos:** De 0 a 3600 segundos, donde 0 indica no especificado por este direccionador

**Valor por omisión:** 0

## Mandatos de configuración de NDP (Talk 6)

### Retransmit timer

Especifica el período, en segundos, entre los mensajes de solicitud a contiguo retransmitidos.

**Valores válidos:** De 0 a 3600 segundos, donde 0 indica no especificado por este direccionador

**Valor por omisión:** 0

**link-mtu** Especifica el valor a colocar en las opciones de MTU enviadas por el direccionador. Este valor debe enviarse sobre los enlaces que tienen una MTU variable y puede enviarse sobre otros enlaces.

**Valores válidos:** Un entero sin signo de 32 bits, donde 0 indica que no se envían opciones de MTU

**Valor por omisión:** 0

### dhcp-server

Añade un servidor DHCP.

#### server addresses

Especifica una lista de direcciones de servidor IPv6 de vertimiento único a utilizar para reenviar el mensaje de solicitud a DHCPv6 inicial. Si no se especifica ninguna dirección, el agente de relay de DHCPv6 envía el paquete a la dirección de vertimiento múltiple de los servidores DHCP.

**Nota:** Si utiliza la dirección de vertimiento múltiple de los servidores, debe habilitar el direccionamiento con vertimiento múltiple en general por medio de la habilitación y configuración de Protocol Independent Multicast (PIM). Consulte “Configuración y supervisión del protocolo de direccionamiento Protocol Independent Multicast (PIM)” en la página 525 para obtener información.

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

## Change

Utilice el mandato **change** para cambiar un anuncio o prefijo de ruta.

### Sintaxis:

**change**                   ...prefix ...  
ra

**prefix** Cambia un prefijo configurado. Los prefijos se añaden o se suprimen cuando se modifica la configuración de las direcciones IPv6. Consulte “Add” en la página 482 para obtener más información sobre cómo añadir direcciones IPv6.

Para añadir un prefijo:

```
Config> p IPv6
IPv6 user configuration
IPv6 config> add addr
Which net is this address for [0]? 5
New address []? 2002:9::6204
Prefix length must be between 8 and 128 [128]? 64
IPv6 config> exit
```

Para cambiar un prefijo:

```
Config> p ndp6
Neighbor Discovery for IPv6 user configuration
NDP6 Config> change prefix
Change Prefix Information option for which Prefix address []? 2002:2::
Use this prefix for on-link determination? [Yes]:
Use this prefix for autonomous address configuration? [Yes]: n
Valid lifetime for Prefix [2592000]? ffffffff
Decrement the Valid Lifetime in real time? [No]:
Preferred Lifetime for Prefix [604800]? ffffffff
Decrement the Preferred Lifetime in real time? [No]:
```

### Change prefix information options for which prefix address?

Especifica el prefijo de dirección IPv6 que se va a colocar en la opción de información de prefijo de los anuncios de direccionador enviados desde la interfaz.

**Valores válidos:** Cualquier dirección IPv6 válida

**Valor por omisión:** Ninguno

### Use this prefix for on-link determination?

Especifica el valor que se va a colocar en el distintivo de tipo 'en enlace' de la opción de información de prefijo. Cuando se establece en *yes*, el prefijo puede utilizarse para la determinación 'en enlace'. Cuando se establece en *no*, el anuncio no realizará ninguna declaración de las propiedades 'en enlace' o 'fuera de enlace' del prefijo.

**Valores válidos:** yes o no

**Valor por omisión:** yes

### Use this prefix for autonomous address configuration?

Especifica el valor que se va a colocar en el distintivo de configuración de direcciones autónoma de la opción de información de prefijo. Cuando se establece en *yes*, el prefijo puede utilizarse para la configuración de direcciones autónoma.

**Valores válidos:** yes o no

**Valor por omisión:** yes

### Valid Lifetime for Prefix?

Especifica el período de tiempo, en segundos, que se va a colocar en la duración válida de la opción de información de prefijo. Este valor representa el período de tiempo, respecto al momento en que se envía el paquete, durante el cual el prefijo es válido para la determinación 'en enlace'.

**Valores válidos:** Un entero sin signo de 32 bits, donde X'FFFFFFFF' representa una duración ilimitada

**Valor por omisión:** 259200 (que son 30 días)

## Mandatos de configuración de NDP (Talk 6)

### Decrement the Valid Lifetime in real time?

Especifica si el valor de Valid Lifetime disminuye en tiempo real, lo que dará como resultado una duración de cero en el tiempo especificado en un futuro, O BIEN es fijo (permanecerá igual en los anuncios consecutivos de direccionador).

**Valores válidos:** yes o no

**Valor por omisión:** no

### Preferred lifetime for prefix

Especifica el período de tiempo, en segundos, que se va a colocar en la duración preferente de la opción de información de prefijo. Este valor representa el período de tiempo, respecto al momento en que se envía el paquete, durante el cual permanecerán como preferentes las direcciones generadas a partir del prefijo mediante la configuración automática de direcciones sin estado.

**Valores válidos:** Un entero sin signo de 32 bits, donde X'FFFFFFFF' representa una duración ilimitada

**Valor por omisión:** 604800

### Decrement the Preferred Lifetime in real time?

Especifica si el valor de Preferred Lifetime disminuye en tiempo real, lo que dará como resultado una duración de cero en el tiempo especificado en un futuro, O BIEN es fijo (permanecerá igual en los anuncios consecutivos de direccionador).

**Valores válidos:** yes o no

**Valor por omisión:** no

**ra** Cambia un anuncio de ruta configurado. Consulte "Add" en la página 514 para obtener una descripción de los parámetros asociados con el mandato **change ra**.

## Delete

Utilice el mandato **delete** para eliminar un anuncio de ruta configurado.

### Sintaxis:

```
delete          dhcp-server  
                ra
```

## Disable

Utilice el mandato **disable** para inhabilitar el anuncio de ruta.

### Sintaxis:

```
disable        dhcp-relay  
                ra
```

### dhcp-relay

Inhabilita el agente de relay de DHCPv6.

**ra** Inhabilita el anuncio de ruta.



## Enable

Utilice el mandato **enable** para habilitar el anuncio de ruta.

### Sintaxis:

```
enable          dhcp-relay
                  ra
```

### **dhcp-relay**

Habilita el agente de relay de DHCPv6.

**ra** Habilita el anuncio de ruta.

## List

Utilice el mandato **list** para visualizar la configuración de NDP.

### Sintaxis:

```
list           dhcp
                  ndp6 configuration
                  prefix
                  ra
```

### Ejemplo:

```
NDP>list dhcp

DHCPv6 Relay Agent
-----
State           Hopcount
DISABLED        4
NDP>

NDP config>list ndp6

NDP config>list ra

NDP config>list prefix
NDP config>
```

## Set

Utilice el mandato **set** para establecer la cuenta de saltos de DHCP.

### Sintaxis:

```
set           dhcp-hopcount
```

### **dhcp-hopcount**

Especifica el número de saltos que se van a utilizar al retransmitir paquetes de DHCPv6.

**Valores válidos:**

**Valor por omisión:** 4

### Ejemplo:

```
NDP6 Config>set dhcp-hopcount
Hop Count [4]?
NDP6 Config>
```

### Acceso al entorno de supervisión de NDP

Utilice el procedimiento siguiente para acceder a los mandatos de supervisión de NDP. Este proceso le proporciona acceso al proceso de supervisión de NDP.

1. En el indicador de OPCON, entre **talk 5**. (Para obtener información más detallada sobre este mandato, consulte “El proceso y los mandatos de OPCON” en la publicación *Nways Multiprotocol Access Services Guía del usuario de software*.) Por ejemplo:

```
* talk 5
+
```

Después de que se entre el mandato **talk 5**, se visualizará el indicador de GWCON (+) en el terminal. Si no aparece el indicador la primera vez que entre la configuración, pulse **Intro** de nuevo.

2. En el indicador +, entre el mandato **p ndp** para obtener el indicador NDP>.

#### Ejemplo:

```
+ p ndp
NDP>
```

### Mandatos de supervisión de NDP

Este apartado describe los mandatos de supervisión de NDP.

Tabla 118. Resumen de los mandatos de supervisión de NDP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi.
dhcpv6-relay	Establece los contadores y parámetros de DHCPv6-relay.
dump	Visualiza las tablas de direccionamiento.
list	Visualiza la configuración.
ping6	Realiza una acción de ping con una dirección IPv6 dinámicamente.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

### DHCPv6-Relay

Utilice el mandato **dhcpv6-relay** para establecer los contadores y parámetros de DHCPv6-Relay.

#### Sintaxis:

```
dhcpv6-relay    counters
                  parameters
```

**counters**

**parameters**

#### Ejemplo:

## Dump

Consulte la sección “Dump routing tables” en la página 533 para conseguir información sobre el mandato **dump**.

## List

Utilice el mandato **list** para visualizar la configuración. Sólo se visualizan las interfaces que tienen configurado un RA aunque pueda haber un prefijo en la lista de prefijos de las otras interfaces como resultado de la configuración de las direcciones IPv6.

### Sintaxis:

```
list           dhcpv6-relay
                dump routing tables
                ndp6 parameters
                ping6
```

### Ejemplo:

```
NDP>list dhcp
```

```
DHCPv6 Relay Agent
```

```
-----
State           Hopcount
DISABLED        4
```

```
NDP>
```

```
NDP>list ndp6
```

```
Router Advertisement for Interface 0 (PPP/0):
```

State	M	O	LLA	Hop Limit	RA Interval Min - Max	Rtr Lifetime	Reach Time	Retrans Timer	MTU
ENABLED	N	N	Y	0	200 - 600	1800	0	0	0

```
Advertised Prefixes:
```

```
Prefix/Length                               On-Link Auto Valid/Preferred Life
```

## Ping6

Consulte la sección “Ping6” en la página 508 para obtener información detallada sobre el mandato **ping6**.

---

## Soporte de la reconfiguración dinámica de NDP6

Este apartado describe la reconfiguración dinámica (DR) tal como afecta a los mandatos Talk 6 y Talk 5.

## Mandato Delete Interface de CONFIG (Talk 6)

Neighbor Discovery Protocol para IPv6 (NDP6) da soporte al mandato de CONFIG (Talk 6) **delete interface** sin restricciones.

## Mandato Activate Interface de GWCON (Talk 5)

NDP6 da soporte al mandato de GWCON (Talk 5) **activate interface** sin restricciones.

La tabla siguiente resume los cambios de la configuración de NDP6 que se activan cuando se invoca el mandato de GWCON (Talk 5) **activate interface**:

Mandatos cuyos cambios se activan mediante el mandato de GWCON (Talk 5) activate interface
CONFIG, protocol NDP6, add ra
CONFIG, protocol NDP6, change prefix
CONFIG, protocol NDP6, change ra
CONFIG, protocol NDP6, delete ra
CONFIG, protocol NDP6, disable ra
CONFIG, protocol NDP6, enable ra

## Mandato Reset Interface de GWCON (Talk 5)

NDP6 da soporte al mandato de GWCON (Talk 5) **reset interface** sin restricciones.

La tabla siguiente resume los cambios de la configuración de NDP6 que se activan cuando se invoca el mandato de GWCON (Talk 5) **reset interface**:

Mandatos cuyos cambios se activan mediante el mandato de GWCON (Talk 5) reset interface
CONFIG, protocol NDP6, add ra
CONFIG, protocol NDP6, change prefix
CONFIG, protocol NDP6, change ra
CONFIG, protocol NDP6, delete ra
CONFIG, protocol NDP6, disable ra
CONFIG, protocol NDP6, enable ra

## Mandatos Reset de GWCON (Talk 5) del componente

NDP6 da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos de NDP6:

### Mandato Reset IPV6 de GWCON, Protocol IPV6

**Descripción:** Restablece dinámicamente todos los parámetros de configuración de NDP6. Consulte la descripción del mandato en IPv6 para obtener información detallada al completo sobre este mandato.

**Efecto en la red:** No se produce ninguna interrupción de la red relativa a NDP6.

**Limitaciones:** Ninguna.

La tabla siguiente resume los cambios de la configuración de NDP6 que se activan cuando se invoca el mandato de **GWCON, protocol ipv6, reset ipv6**:

<b>Mandatos cuyos cambios se activan mediante el mandato reset ipv6 de GWCON, protocolo ipv6</b>
CONFIG, protocolo NDP6, add ra
CONFIG, protocolo NDP6, change prefix
CONFIG, protocolo NDP6, change ra
CONFIG, protocolo NDP6, delete ra
CONFIG, protocolo NDP6, disable ra
CONFIG, protocolo NDP6, enable ra



---

# Configuración y supervisión del protocolo de direccionamiento Protocol Independent Multicast (PIM)

La configuración de PIM se realiza para cada interfaz. Este capítulo describe cómo utilizar los mandatos de configuración y funcionamiento de PIM e incluye los apartados siguientes:

- “Utilización de PIM”
- “Acceso al entorno de configuración de PIM” en la página 526
- “Mandatos de configuración de PIM” en la página 527
- “Acceso al entorno de supervisión de PIM” en la página 532
- “Mandatos de supervisión de PIM” en la página 532
- “Soporte de la reconfiguración dinámica de PIM” en la página 541
- “Soporte de la reconfiguración dinámica de PIM para IPv6” en la página 542
- “Soporte de la reconfiguración dinámica de Multicast Forwarding Cache” en la página 543
- “Soporte de la reconfiguración dinámica de Multicast Forwarding Cache V6” en la página 544

---

## Utilización de PIM

Protocol Independent Multicast Dense Mode (PIM-DM) es un protocolo de vertimiento múltiple con poda y difusión utilizado por IP. Da soporte tanto a IPv4 como a IPv6 y los mandatos y sintaxis son idénticos para ambas versiones. Funciona bien en redes de campus, donde el ancho de banda está repleto y los usuarios están estrechamente agrupados, no dispersos por un área amplia de redes. PIM utiliza una aproximación de poda y difusión para el reenvío con vertimiento múltiple de datagramas y se utiliza cuando los grupos de vertimiento múltiple están densamente distribuidos a través de la Internet. Supone que todos los sistemas de sentido directo desean recibir datagramas con vertimiento múltiple y poda las ramas de los sistemas que no lo desean.

PIM-DM es un protocolo de estado transitorio. Esto significa que los estados de poda, si no los elimina alguna otra actividad (como, por ejemplo, injertos o uniones), se eliminan después de un período de tiempo (configurable) y los datos de vertimiento múltiple se difunden una vez más a todos los sistemas de sentido directo, donde se produce la poda una vez más.

PIM-DM establece adyacencias con direccionadores de PIM contiguos intercambiando mensajes Hello con todos los contiguos. Mantiene activa la adyacencia hasta que sobrepasa el tiempo de espera excedido. Mientras los direccionadores contiguos están activos y en ejecución, se envían nuevos mensajes Hello para renovar el estado de Hello y evitar que la adyacencia sobrepase el tiempo de espera excedido. La frecuencia con la que se envían mensajes Hello es configurable.

PIM-DM utiliza la tabla de direccionamiento con vertimiento único, sin tener en cuenta qué protocolo de vertimiento único posee una entrada, para llevar a cabo el cálculo de reenvío por vía de acceso invertida sobre un datagrama con vertimiento múltiple recibido. El reenvío por vía de acceso invertida (RPF) se utiliza para validar si el datagrama con vertimiento múltiple recibido ha llegado por una interfaz que será válida para el reenvío a la dirección de origen contenida en el datagrama

con vertimiento múltiple. Si es una interfaz incorrecta, el datagrama se desecha o, si no, se crea una nueva entrada de vertimiento múltiple y el datagrama con vertimiento múltiple se reenvía sobre todas las otras interfaces (aquellas con PIM-DM activo, miembros de sistema principal locales y cualquier interfaz adicional añadida por otros protocolos de vertimiento múltiple). El uso de rutas de vertimiento único para llevar a cabo el RPF con miras a la validación de interfaz de entrada requiere que el direccionamiento con vertimiento único sea simétrico.

También se da soporte a los injertos para permitir que los sistemas principales se unan a un grupo dinámicamente. Esto injerta una rama a un árbol de vertimiento múltiple ya existente y elimina todos los estados de poda donde sea necesario para asegurar que los sistemas principales que se han unido reciban los datagramas solicitados con vertimiento múltiple en grupo.

Debido a la naturaleza independiente de PIM con respecto a los protocolos de direccionamiento con vertimiento único y a la naturaleza de difusión de PIM-DM, pueden aparecer vías de acceso paralelas a partir del origen y pueden reenviarse datos duplicados con vertimiento múltiple. PIM-DM utiliza un procedimiento de afirmación para elegir el direccionador de reenvío adecuado cuando se produce esta situación. Pueden configurarse las preferencias en direccionadores que ejecuten protocolos de direccionamiento con vertimiento único diferentes para resolver qué direccionador conviene que tenga prioridad. Cuando el direccionamiento con vertimiento único es el mismo, se utilizan costes de métrica de vertimiento único respecto al origen para determinar la ruta mejor. Y, cuando todos los demás son iguales, se elige el direccionador con la dirección de interfaz IP mayor como el reenviador adecuado.

Utilice el mandato **p pim** en el indicador `Config>` para configurar los parámetros de PIM.

---

## Acceso al entorno de configuración de PIM

Utilice el procedimiento siguiente para acceder al proceso de configuración de PIM.

1. En el indicador de OPCODE, entre **talk 6**. (Para obtener información más detallada sobre este mandato, consulte “El proceso y los mandatos de OPCODE” en la publicación *Nways Multiprotocol Access Services Guía del usuario de software*.) Por ejemplo:

```
* talk 6
Config>
```

Después de entrar el mandato **talk 6**, se visualizará el indicador CONFIG (Config>) en el terminal. Si no aparece el indicador la primera vez que entre la configuración, pulse **Intro** de nuevo.

2. Si se trata de IPv4, en el indicador CONFIG entre el mandato **p pim** para obtener el indicador PIM Config>. Si se trata de IPv6, entre el mandato **p pim6** para obtener el indicador PIM6 Config>.



## Mandatos de configuración de PIM

Si desea configurar PIM para IPv4, entre los mandatos en el indicador PIM Config>. Si se trata de IPv6, entre los mandatos en el indicador PIM6 Config>.

Tabla 119. Resumen de los mandatos de configuración de PIM

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi.
delete	Suprime una interfaz PIM.
disable	Inhabilita PIM en el dispositivo.
enable	Habilita PIM en el dispositivo y establece los valores de configuración globales por omisión de PIM.
list	Lista la configuración.
set	Establece los valores de los parámetros de configuración de PIM.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

### Delete

Utilice el mandato **delete** para eliminar una interfaz PIM configurada.

#### Sintaxis:

**delete** *dirinterfaz*

#### Interface address

#### Ejemplo:

```
PIM Config> delete
Interface address []?
```

### Disable

Utilice el mandato **disable** para inhabilitar PIM en el dispositivo.

#### Sintaxis:

**disable**

### Enable

Utilice el mandato **enable** para habilitar PIM en el dispositivo y establecer los valores de configuración globales por omisión de PIM.

#### Sintaxis:

**enable**

### List

Utilice el mandato **list** para visualizar la configuración de PIM.

#### Sintaxis:

```
list          all  
                interface  
                preference  
                variables
```

**all** Visualiza toda la información de la configuración de PIM.

**interface** Visualiza la información de la configuración de PIM sobre las interfaces que actualmente están configuradas.

#### Ejemplo:

```
PIM Config>list i
```

Type	IP Address	Hello Interval	State Holdtime
Physical	9.37.2.1	30	210

**Type** Identifica el tipo de la interfaz que se ha configurado.

#### IP address

Identifica la dirección IP asignada a esta interfaz.

#### Hello Interval

Identifica el intervalo, en segundos, entre los mensajes hello enviados sobre esta interfaz.

#### State holdtime

Identifica el número de segundos que se indicará a otros dispositivos de sentido inverso durante los cuales se debe mantener el estado de PIM para este dispositivo. En PIM, es el período de tiempo para que los dispositivos de sentido inverso mantengan las podas en activo.

**variables** Visualiza la información de la configuración sobre las variables globales de PIM.

#### Ejemplo:

```
PIM Config>list v
```

```
PIM Global Configuration Values
```

```
PIM: on
```

```
Graft Timeout:      3 seconds  
Assert Timeout:    210 seconds
```

```
PIM Config>
```

#### PIM: on/off

Identifica si PIM está habilitado o inhabilitado actualmente.

#### Graft timeout

Identifica el número de segundos para retransmitir injertos si no se ha recibido ningún acuse de recibo de injerto.

#### Assert timeout

Identifica el número de segundos durante los cuales se retiene la información de afirmación aprendida por medio de

los dispositivos de sentido inverso antes de volver a la información de direccionamiento local.

### preference

Visualiza las preferencias de métrica de los tipos de direccionamiento que están actualmente configuradas.

#### Ejemplo: (sólo IPv4)

```
PIM Config>list p
```

```
Direct    0
Static    1
OSPF      110
RIP       120
BGP       200
```

```
PIM Config>
```

### Un tipo de ruta

Identifica el tipo de ruta soportado y lista un valor hexadecimal que visualiza la preferencia de métrica configurada actualmente.

## Set

Utilice el mandato **set** para cambiar los valores de los parámetros de configuración de PIM. Puede utilizar este mandato para añadir una nueva interfaz física.

### Sintaxis:

```
set          interface direccióninterfaz períodohello tiempo  
mantenpodaunión  
preference tiporuta valorpreferencia  
variables
```

### interface

#### Ejemplo:

```
PIM Config>set interface  
Interface address []?  
Hello period [30]?  
Join Prune Hold Time [210]?
```

#### Interface address

**Valores válidos:** Cualquier dirección IP válida

**Valor por omisión:** Ninguno

#### Hello period

Especifica el número de segundos entre los mensajes Hello. En las interfaces punto a punto, este valor se ignora. Una vez establecida una adyacencia por el 2216, se silencian los mensajes Hello.

**Valores válidos:** 1 - 65535

**Valor por omisión:** 30

#### Join prune hold time

Controla los mensajes que informan al dispositivo receptor del período de tiempo (en segundos) durante el cual debe mantenerse el estado activado por el mensaje. Las podas

## Mandatos de configuración de PIM (Talk 6)

enviadas al dispositivo permanecen activas durante este número de segundos.

**Valores válidos:** 1 - 65535

**Valor por omisión:** 210

### **preference** *tiporuta*

Es una preferencia de métrica configurada que se va a utilizar en el proceso de afirmación. Permite que el usuario elija de forma selectiva qué tipos de rutas con vertimiento único de las tablas de reenvío con vertimiento único tienen preferencia sobre otros tipos de rutas. Sólo tiene un significado local, lo que quiere decir que se utiliza para este dispositivo y todas sus interfaces PIM conectadas activas. Puede utilizarse si este direccionador se sirve de varios protocolos de direccionamiento con vertimiento único, si los direccionadores adyacentes ejecutan protocolos de direccionamiento diferentes o si son más convenientes que las rutas aprendidas tipos de rutas como, por ejemplo, las rutas por omisión.

*Tiporuta* puede especificar los siguientes tipos de rutas:

- direct
- static
- ospf (sólo IPv4)
- rip (sólo IPv4)
- bgp

### **Ejemplo:**

```
PIM Config> set preference rip
RIP Metric Preference [120]?
```

### **Metric Preference**

Este valor se envía a los otros direccionadores en el proceso de afirmación durante la detección de reenvío duplicado con vertimiento múltiple y se utiliza con los costes de métrica de ruta para determinar qué direccionador debe ser el direccionador de reenvío. Todas las preferencias de métrica se establecen inicialmente en 0.

**Rango:** 0 - 65535

**Valores por omisión:**

<b>direct</b>	0
<b>static</b>	1
<b>ospf</b>	110
<b>rip</b>	120
<b>bgp</b>	200

### **variables** *cache\_life*

### **Ejemplo:**

```
PIM Config>set v cache_life
Mcfwd cache Holdtime [60]
```

### Mcfwd cache holdtime

Especifica el período de tiempo en segundos durante el cual se permitirá que una entrada de reenvío con vertimiento múltiple que no se ha utilizado para reenviar ningún datagrama con vertimiento múltiple exista en la antememoria de reenvío con vertimiento múltiple antes de que se elimine.

**Valores válidos:** Un valor numérico superior a 0

**Valor por omisión:** 60

### variables assert\_tout

#### Ejemplo:

```
PIM Config>set v assert_tout
PIM Assert Time Out [210]
```

#### Assert time out

El período de tiempo en segundos durante el cual los direccionadores de sentido directo guardarán información de afirmación de dos o más direccionadores de sentido inverso que afirman. La información de afirmación se utiliza para asegurarse de que los direccionadores de sentido directo entiendan cuál es el direccionador de sentido inverso correcto, o direccionador de reenvío, y de este modo los mensajes de PIM puedan enviarse al direccionador correcto. Si no se reciben más afirmaciones antes de que caduque el tiempo de afirmación, la información de afirmación se desecha y el direccionador utiliza la información local de las tablas de direccionamiento con vertimiento único para determinar el direccionador de reenvío de sentido inverso correcto.

**Valores válidos:** 1 - 65535

**Valor por omisión:** 210

### variables graft\_tout

#### Ejemplo:

```
PIM Config>set v graft_tout
PIM Graft Time Out [3]
```

#### Graft time out

Especifica el número de segundos durante los cuales el dispositivo que ha enviado un mensaje de injerto, sin recibir acuse de recibo, esperará antes de enviar otro mensaje.

**Valores válidos:** 1 - 65535

**Valor por omisión:** 3

---

### Acceso al entorno de supervisión de PIM

Utilice el procedimiento siguiente para acceder a los mandatos de supervisión de PIM. Este proceso le proporciona acceso al proceso de supervisión de PIM.

1. En el indicador de OPCON, entre **talk 5**. (Para obtener información más detallada sobre este mandato, consulte *El proceso y los mandatos de OPCON* en la publicación Nways Multiprotocol Access Services Guía del usuario de software.) Por ejemplo:

```
* talk 5
+
```

Después de que se entre el mandato **talk 5**, se visualizará el indicador de GWCON (+) en el terminal. Si no aparece el indicador la primera vez que entre la configuración, pulse **Intro** de nuevo.

2. Si se trata de IPv4, en el indicador + entre el mandato **p pim** para obtener el indicador PIM>. Si se trata de IPv6, en el indicador + entre el mandato **p pim6** para obtener el indicador PIM6>.

#### Ejemplo:

```
+ p pim
PIM>
```

---

### Mandatos de supervisión de PIM

Este apartado describe los mandatos de supervisión de PIM.

Tabla 120. Resumen de los mandatos de supervisión de PIM

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi.
dump	Visualiza las tablas de direccionamiento.
clear	Borra la tabla de reenvío con vertimiento múltiple.
interface	Visualiza el estado de la interfaz.
join	Une un grupo de vertimiento múltiple.
leave	Deja un grupo de vertimiento múltiple.
mcache	Visualiza las entradas de antememoria de tabla de reenvío con vertimiento múltiple que están activas actualmente.
mgroups	Visualiza la pertenencia a grupo de las interfaces conectadas del dispositivo.
mstats	Visualiza diversas estadísticas de direccionamiento con vertimiento múltiple.
neighbor	Visualiza información sobre las adyacencias actuales.
pim	Visualiza la base de datos de estados de PIM.
summary pim	Visualiza un resumen de la base de datos de estados de PIM.
ping	Realiza una acción de ping con una dirección IPv6 dinámicamente.
reset	Restablece PIM dinámicamente.
traceroute	Efectúa el rastreo de una ruta dinámicamente.
variables	Visualiza los valores de configuración para las variables de PIM.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

## Dump routing tables

Utilice el mandato **dump** para visualizar las tablas de direccionamiento configuradas.

### Sintaxis:

#### dump

Para obtener un ejemplo de la salida de este mandato, consulte la descripción del mandato **dump routing table** en el apartado Mandatos de supervisión de IP de la publicación *Consulta de configuración y supervisión de protocolos Volumen 1*.

### Clear

Utilice el mandato **clear** para restablecer la antememoria.

#### Sintaxis:

**clear**

#### Ejemplo:

```
PIM>clear
```

```
Mfwd Cache has been cleared!
```

```
PIM>
```

### Interface

Utilice el mandato **interface** para visualizar un resumen de las estadísticas y los parámetros relativos a la interfaz.

#### Sintaxis:

**interface**

#### Ejemplo:

```
PIM>interface
```

```
PIM Interface Table
```

IP Address	Hello Interval	State Holdtime	Status	Type
9.32.45.1	30	210	up	TKR/0
9.10.32,23	30	210	up	TKR/1

```
PIM>
```

#### IP address

Especifica la dirección IP de la interfaz.

#### Hello interval

Especifica el número de segundos entre los mensajes hello en esta interfaz.

#### State holdtime

Especifica el número de segundos notificado a los dispositivos de sentido inverso para mantener la información de estado antes de desecharla. Para PIM, es el número de segundos durante los cuales una poda está activa en sentido inverso.

#### Status

Especifica el estado actual de la interfaz.

**up** La interfaz está activa y es totalmente operativa, pero no genera las consultas de mld.

**disabled** La interfaz es operativa pero está inhabilitada y PIM no está activo.

**down** La interfaz no es operativa.



## Join

Utilice el mandato **join** para unirse a un grupo de vertimiento múltiple.

**Sintaxis:**

**join**

**Ejemplo:**

```
PIM>join 224.12.2.2
```

## Leave

Utilice el mandato **leave** para dejar un grupo de vertimiento múltiple. Esto evita que el dispositivo responda a los ping y consultas de SNMP que se envíen a la dirección de grupo.

**Sintaxis:**

**leave**

**Ejemplo:**

```
PIM>leave 224.12.2.2
```

## Mcache

Utilice el mandato **mcache** para visualizar una lista de las entradas de antememoria de vertimiento múltiple que están activas actualmente. Las entradas de antememoria de vertimiento múltiple se crean a petición siempre que se recibe el primer datagrama con vertimiento múltiple coincidente. Existe una entrada de antememoria por separado (y, por consiguiente, una ruta por separado) para cada combinación de red de origen de datagrama y grupo de destino.

**Sintaxis:**

**mcache**

**Ejemplo:**

```
PIM>mcache
```

```

0: TKR/0          1: TKR/1          2: TKR/2
3: IPPN/0         4: BDG/0          5: Internal

                Prot   Count   Upstr   Downstream
Source          Destination Owner   Count   Upst    Downstream
9.10.12.3       224.12.2.2     PIM    124     0       1, 2
*10.23.55.2    224.32.4.5     PIM     3       1       1
PIM>
```

**Prot** Especifica el protocolo propietario de la entrada de tabla de reenvío con vertimiento múltiple.

**Count** Visualiza el número de paquetes con vertimiento múltiple recibidos para esta entrada de tabla de reenvío con vertimiento múltiple.

**Upstr** Visualiza la red o el direccionador contiguos de los que debe recibirse el datagrama para reenviarlo.

## Mandatos de supervisión de PIM (Talk 5)

### Downstream

Visualiza el número total de interfaces o contiguos de sentido directo a los que se reenviará el datagrama.

## Mgroups

Utilice el mandato **mgroups** para visualizar la pertenencia a grupo de las interfaces conectadas del dispositivo. Sólo se visualizan las pertenencias a grupo de aquellas interfaces en las que el direccionador es un direccionador designado o un direccionador designado de reserva.

### Sintaxis:

**mgroups**

### Ejemplo:

```
PIM>mgroups
```

Group	Local Group Database Interface	Lifetime (secs)
224.12.2.2	9.32.4.5 (TKR/0)	176
224.5.5.5	Internal	1

```
PIM>
```

**Group** Visualiza la dirección de grupo notificada (mediante MLD) de una interfaz en particular.

**Interface** Visualiza la dirección de interfaz a la que se ha notificado la dirección de grupo (mediante MLD). La pertenencia a grupo interna del direccionador se indica con el valor de *internal*. Para estas entradas, el campo Lifetime (ver a continuación) indica el número de las aplicaciones que han solicitado pertenencia dentro del grupo en particular.

**Lifetime** Visualiza el número de segundos que durará la entrada si cesan de oírse informes de pertenencia en la interfaz para el grupo determinado.

## Mstats

Utilice el mandato **mstats** para visualizar varias estadísticas de direccionamiento con vertimiento múltiple. El mandato indica si está habilitado el direccionamiento con vertimiento múltiple y si el direccionador es un reenviador de vertimiento múltiple interáreas y/o inter-AS.

### Sintaxis:

**mstats**

### Ejemplo:

PIM>mstats

```

MOSPF forwarding:      Disabled
Inter-area forwarding: Disabled
DVMRP forwarding:     Enabled
PIM forwarding:        Disabled

```

```

Datagrams received:      10143  Datagrams fwd (multicast): 10219
Datagrams fwd (unicast): 0      Locally delivered:         0
Unreachable source:     0      Unallocated cache entries: 0
Off multicast tree:     0      Unexpected DL multicast:   0
Buffer alloc failure:   0      TTL scoping:               0
Administrative filtering: 235

# DVMRP routing entries: 5      # DVMRP entries freed:     0
# fwd cache alloc:      1      # fwd cache freed:         0
# fwd cache GC:         0      # local group DB alloc:    0
# local group DB free:  0

```

PIM>

### Datagrams received

Visualiza el número de datagramas con vertimiento múltiple recibidos por el direccionador.

### Datagrams fwd (multicast)

Visualiza el número de datagramas que se han reenviado como vertimientos múltiples en enlace de datos (esto incluye las réplicas de paquetes, cuando son necesarias, por lo cual es perfectamente posible que esta cuenta supere el número de los recibidos).

### Datagrams fwd (unicast)

Visualiza el número de datagramas que se han reenviado como vertimientos únicos en enlace de datos.

### Locally delivered

Visualiza el número de datagramas que se han reenviado a aplicaciones internas.

### Unreachable source

Visualiza una cuenta de aquellos datagramas cuya dirección de origen era inasequible.

### Unallocated cache entries

Visualiza una cuenta de aquellos datagramas cuyas entradas de antememoria no han podido crearse debido a escaseces de recursos.

### Off multicast tree

Visualiza una cuenta de aquellos datagramas que no se han reenviado porque no había ningún contiguo de sentido inverso ni ningún/ninguna contiguo/interfaz de sentido directo en la entrada de antememoria coincidente.

### Unexpected DL multicast

Visualiza una cuenta de aquellos datagramas que se han recibido como vertimientos múltiples en enlace de datos sobre las interfaces que se han configurado para el vertimiento único en enlace de datos.

### Buffer alloc failure

Visualiza una cuenta de aquellos datagramas que no han podido replicarse debido a la escasez de almacenamientos intermedios.

## Mandatos de supervisión de PIM (Talk 5)

### TTL scoping

Indica aquellos datagramas que no se han reenviado porque su TTL indicaba que nunca podrían llegar a un miembro del grupo.

### Administrative filtering

Visualiza el número de datagramas desechados a causa de la filtración de salida.

### #fwd cache alloc

Indica el número de entradas de antememoria asignadas. El tamaño de antememoria de reenvío actual es el número de entradas asignadas (**# fwd cache alloc**) menos el número de entradas de antememoria liberadas (**# fwd cache freed**).

### #fwd cache freed

Indica el número de entradas de antememoria liberadas. El tamaño de antememoria de reenvío actual es el número de entradas asignadas (**# fwd cache alloc**) menos el número de entradas de antememoria liberadas (**# fwd cache freed**).

### #fwd cache GC

Indica el número de entradas de antememoria que se han borrado porque no se utilizaban recientemente y la antememoria se desbordó.

### #local group DB alloc

Indica el número de entradas de base de datos de grupos locales asignadas. El número de entradas asignadas (**# local group DB alloc**) menos el número de entradas liberadas (**# local group DB free**) equivale al tamaño actual de la base de datos de grupos locales.

### #local group DB free

Indica el número de entradas de base de datos de grupos locales liberadas. El número de entradas asignadas (**# local group DB alloc**) menos el número de entradas liberadas (**# local group DB free**) equivale al tamaño actual de la base de datos de grupos locales.

## Neighbor

Utilice el mandato **neighbor** para visualizar información sobre los dispositivos de PIM contiguos y el estado de su adyacencia.

### Sintaxis:

nneighbor

### Ejemplo:

```
PIM>neighbor
PIM Neighbor Listing
```

Neighbor Addr	DR	Last Heard	First Heard	Ifc
9.12.2.2	NO	21	6139	TKR/0
9.25.3.111	YES	29	6204	TKR/1

```
PIM>
```

### Neighbor Addr

Identifica si este direccionador ha identificado al contiguo como direccionador designado.

**DR** Identifica si este direccionador ha identificado al contiguo como direccionador designado.

**Last Heard**

El número de segundos desde la última vez que se ha tenido noticia del contiguo.

**First Heard**

El número total de segundos desde que se ha establecido la adyacencia con este contiguo por primera vez.

**lfc** La interfaz en la que se ha descubierto el contiguo.

## PIM

Utilice el mandato **pim** para visualizar la base de datos de estados de PIM.

**Sintaxis:**

pim

**Ejemplo:**

PIM>pim

```

                                PIM State Database
                                -----
Interface  Group          Source          Lifetime (sec)
1  PRUNE  224.12.2.2      9.32.4.128     205
1  PRUNE  224.23.121.4   9.124.23.1     155

```

PIM>

**Group** La dirección de grupo de destino asociada con la entrada.

**Source** La dirección de origen del que ha originado el datagrama con vertimiento múltiple.

**Interface** El número de interfaz PIM y el tipo de estado de PIM en la base de datos.

**Lifetime** La duración total, en segundos, del estado que se ha recibido obtenida del mensaje de control de PIM que ha configurado el estado.

## Summary PIM

Utilice el mandato **summary pim** para visualizar información de resumen de la base de datos de estados de PIM.

**Sintaxis:**

summary pim

**Ejemplo:**

PIM>s

```

                                Summary PIM State Database
                                -----
0)   Group: 224.0.1.42
0)   Source: 9.37.179.1
0)   States: 1-P 2-P

```

PIM>

**Group** La dirección de grupo de destino asociada con la entrada.

## Mandatos de supervisión de PIM (Talk 5)

- Source** La dirección de origen del que ha originado el datagrama con ver-timiento múltiple.
- States** Visualiza las interfaces y los estados asociados con el par origen-grupo. P identifica un estado de poda.

## Ping

Utilice el mandato **ping** para realizar dinámicamente una acción de ping con otra dirección IPv6 de destino.

### Sintaxis:

ping

Para obtener un ejemplo de la salida de este mandato, consulte la descripción del mandato **ping** en el apartado Mandatos de supervisión de IP de la publicación *Consulta de configuración y supervisión de protocolos Volumen 1*.

Consulte la sección “Ping6” en la página 508 para ver una descripción de los parámetros.

## Reset

Utilice el mandato **reset** para restablecer PIM y volver a cargar la configuración.

### Sintaxis:

reset

### Ejemplo:

```
PIM>reset
```

## Traceroute

Utilice el mandato **traceroute** para realizar el rastreo de una ruta dinámicamente.

### Sintaxis:

traceroute

Para obtener un ejemplo de la salida de este mandato, consulte la descripción del mandato **traceroute** en el apartado Mandatos de supervisión de IP de la publicación *Consulta de configuración y supervisión de protocolos Volumen 1*. Consulte la sección “Traceroute6” en la página 509 para ver una descripción de los parámetros.

## Variables

Utilice el mandato **variables** para visualizar información sobre las variables de configuración de PIM.

### Sintaxis:

variables

### Ejemplo:

PIM>**variables**

PIM: on

Graft Timeout: 3 seconds  
Assert Timeout: 210 seconds

PIM Unicast Metric Preferences

Direct 0  
Static 1  
OSPF 110  
RIP 120  
BGP 200

PIM>

### **PIM: on/off**

Indica si PIM-DM está habilitado o inhabilitado actualmente.

### **Graft Timeout**

El número de segundos para retransmitir injertos si no se ha recibido ningún acuse de recibo de injerto.

### **Assert Timeout**

El número de segundos durante los cuales se retiene la información de afirmación aprendida por medio de los direccionadores de sentido inverso antes de volver a la información de direccionamiento local.

### **PIM Unicast Metric Preferences**

Visualiza las preferencias de métrica de los tipos de direccionamiento que están actualmente configuradas. Cada tipo de ruta soportado se lista con un valor decimal que visualiza la preferencia de métrica configurada actualmente.

---

## **Soporte de la reconfiguración dinámica de PIM**

Este apartado describe la reconfiguración dinámica (DR) tal como afecta a los mandatos Talk 6 y Talk 5.

### **Mandato Delete Interface de CONFIG (Talk 6)**

Protocol Independent Multicast (PIM) da soporte al mandato de CONFIG (Talk 6) **delete interface** sin restricciones.

### **Mandato Activate Interface de GWCON (Talk 5)**

PIM da soporte al mandato de GWCON (Talk 5) **activate interface** con la consideración siguiente:

PIM debe habilitarse globalmente para que pueda activarse en una interfaz de red.

El mandato de GWCON (Talk 5) **activate interface** da soporte a todos los mandatos específicos de interfaz PIM.

## Mandato Reset Interface de GWCON (Talk 5)

PIM da soporte al mandato de GWCON (Talk 5) **reset interface** con la consideración siguiente:

PIM debe habilitarse globalmente para que pueda activarse en una interfaz de red.

El mandato de GWCON (Talk 5) **reset interface** da soporte a todos los mandatos específicos de interfaz PIM.

## Mandatos Reset de GWCON (Talk 5) del componente

PIM da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos de PIM:

### Mandato Reset de GWCON, Protocol PIM

**Descripción:** Restablece dinámicamente las interfaces y los valores de variable de PIM.

**Efecto en la red:** Pérdida de adyacencia de contiguo de PIM en todas las interfaces en que se ejecute PIM. Esto puede afectar al reenvío con vertimiento múltiple de IP, aunque la información se corrige después de un período de tiempo durante el cual se establece una vez más la adyacencia de contiguo.

**Limitaciones:** Ninguna.

El mandato de **GWCON, protocol pim, reset** da soporte a todos los mandatos de PIM.

---

## Soporte de la reconfiguración dinámica de PIM para IPv6

Este apartado describe la reconfiguración dinámica (DR) tal como afecta a los mandatos Talk 6 y Talk 5.

## Mandato Delete Interface de CONFIG (Talk 6)

Protocol Independent Multicast para IPv6 (PIM6) da soporte al mandato de CONFIG (Talk 6) **delete interface** sin restricciones.

## Mandato Activate Interface de GWCON (Talk 5)

PIM6 da soporte al mandato de GWCON (Talk 5) **activate interface** con la consideración siguiente:

PIM6 debe habilitarse globalmente para que pueda activarse en una interfaz de red.

El mandato de GWCON (Talk 5) **activate interface** da soporte a todos los mandatos específicos de interfaz PIM6.



## Mandato Reset Interface de GWCON (Talk 5)

PIM6 da soporte al mandato de GWCON (Talk 5) **reset interface** con la consideración siguiente:

PIM6 debe habilitarse globalmente para que pueda activarse en una interfaz de red.

El mandato de GWCON (Talk 5) **reset interface** da soporte a todos los mandatos específicos de interfaz PIM6.

## Mandatos Reset de GWCON (Talk 5) del componente

PIM6 da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos de PIM6:

### Mandato Reset de GWCON, Protocol PIM

**Descripción:** Restablece dinámicamente las interfaces y los valores de variable de PIM6.

**Efecto en la red:** Pérdida de adyacencia de contiguo de PIM6 en todas las interfaces en que se ejecute PIM6. Esto puede afectar al reenvío con vertimiento múltiple de IPv6, aunque la información se corrige después de un período de tiempo durante el cual se establece una vez más la adyacencia de contiguo.

**Limitaciones:** Ninguna.

El mandato de **GWCON, protocol pim, reset** da soporte a todos los mandatos de PIM.

---

## Soporte de la reconfiguración dinámica de Multicast Forwarding Cache

**Nota:** Los mandatos siguientes son comunes a MOSPF, DVMRP y PIM, y tienen la consideración de mandatos de MFC para IPv4:

- **join**
- **leave**
- **mcache**
- **mgroups**
- **mstats**

Consulte “Configuración y supervisión de OSPF” si desea más información sobre MOSPF y consulte “Configuración y supervisión de DVMRP” si desea más información sobre DVMRP. Ambos capítulos se encuentran en la publicación *Consulta de configuración y supervisión de protocolos Volumen 1*.

Este apartado describe la reconfiguración dinámica (DR) tal como afecta a los mandatos Talk 6 y Talk 5.

## Mandato Delete Interface de CONFIG (Talk 6)

Multicast Forwarding Cache (MFC) da soporte al mandato de CONFIG (Talk 6) **delete interface** con la consideración siguiente:

IP debe notificar a MFC la actualización de la dirección.

## Mandato Activate Interface de GWCON (Talk 5)

MFC da soporte al mandato de GWCON (Talk 5) **activate interface** con la consideración siguiente:

IP debe notificar a MFC la actualización de la dirección.

El mandato de GWCON (Talk 5) **activate interface** da soporte a todos los mandatos específicos de interfaz MFC.

## Mandato Reset Interface de GWCON (Talk 5)

MFC da soporte al mandato de GWCON (Talk 5) **reset interface** con la consideración siguiente:

IP debe notificar a MFC la actualización de la dirección.

El mandato de GWCON (Talk 5) **reset interface** da soporte a todos los mandatos específicos de interfaz MFC.

## Mandatos no reconfigurables dinámicamente

Todos los parámetros de configuración de MFC pueden cambiarse dinámicamente.

---

## Soporte de la reconfiguración dinámica de Multicast Forwarding Cache V6

**Nota:** Los siguientes mandatos de PIM tienen la consideración de mandatos de Multicast Forwarding Cache para IPv6 (MFC6):

- **join**
- **leave**
- **mcache**
- **mgroups**
- **mstats**

Este apartado describe la reconfiguración dinámica (DR) tal como afecta a los mandatos Talk 6 y Talk 5.

## Mandato Delete Interface de CONFIG (Talk 6)

Multicast Forwarding Cache V6 (MFC6) da soporte al mandato de CONFIG (Talk 6) **delete interface** con la consideración siguiente:

IPv6 debe notificar a MFC6 la actualización de la dirección.

## Mandato Activate Interface de GWCON (Talk 5)

Multicast Forwarding Cache V6 (MFC6) da soporte al mandato de GWCON (Talk 5) **activate interface** con la consideración siguiente:

IPv6 debe notificar a MFC6 la actualización de la dirección.

El mandato de GWCON (Talk 5) **activate interface** da soporte a todos los mandatos específicos de interfaz MFC6 (Multicast Forwarding Cache V6).

## **Mandato Reset Interface de GWCON (Talk 5)**

Multicast Forwarding Cache V6 (MFC6) da soporte al mandato de GWCON (Talk 5) **reset interface** con la consideración siguiente:

IPv6 debe notificar a MFC6 la actualización de la dirección.

El mandato de GWCON (Talk 5) **reset interface** da soporte a todos los mandatos específicos de interfaz MFC6 (Multicast Forwarding Cache V6).

## **Mandatos no reconfigurables dinámicamente**

Todos los parámetros de configuración de Multicast Forwarding Cache V6 (MFC6) pueden cambiarse dinámicamente.



---

## Configuración y supervisión de Routing Information Protocol (RIP6)

RIP6 es un protocolo de direccionamiento de vector de distancia. La configuración de RIP6 se realiza para cada interfaz. Este capítulo describe cómo utilizar los mandatos de configuración y funcionamiento de RIP6 e incluye los apartados siguientes:

- “Acceso al entorno de configuración de RIP6”
- “Mandatos de configuración de RIP6”
- “Acceso al entorno de supervisión de RIP6” en la página 557
- “Mandatos de supervisión de RIP6” en la página 558
- “Soporte de la reconfiguración dinámica de RIP6” en la página 559

---

### Acceso al entorno de configuración de RIP6

Utilice el procedimiento siguiente para acceder al proceso de configuración de RIP6.

1. En el indicador de OPCON, entre **talk 6**. (Para obtener información más detallada sobre este mandato, consulte “El proceso y los mandatos de OPCON” en la publicación *Nways Multiprotocol Access Services Guía del usuario de software*.) Por ejemplo:

```
* talk 6
Config>
```

Después de entrar el mandato **talk 6**, se visualizará el indicador CONFIG (Config>) en el terminal. Si no aparece el indicador la primera vez que entre la configuración, pulse **Intro** de nuevo.

2. En el indicador CONFIG, entre el mandato **p rip6** para obtener el indicador RIP66 Config>.

---

### Mandatos de configuración de RIP6

Para configurar RIP6, entre los mandatos en el indicador RIP66 Config>.

## Mandatos de configuración de RIP6 (Talk 6)

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi.
add	Añade RIP6 sobre una interfaz.
change	Cambia los valores de configuración de métrica de RIP6 o el valor por omisión de origen.
delete	Elimina RIP6 de una interfaz.
disable	Inhabilita RIP6 en una interfaz.
enable	Habilita RIP6 en una interfaz.
list	Lista la configuración.
set	Establece los valores de métrica de RIP6.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

### Add

Utilice el mandato **add** para añadir RIP6 sobre una interfaz.

#### Sintaxis:

**add** *interfaznúm.*

#### **interfaznúm.**

Especifica la interfaz a la que se añadirá el protocolo RIP6.

**Nota:** Esta interfaz debe tener configurada una dirección IPv6 o debe ser la interfaz virtual de un túnel de IPv6 sobre IPv4.

**Valores válidos:** Cualquier número de interfaz válido

**Valor por omisión:** Ninguno

### Change

Utilice el mandato **change** para cambiar una métrica de RIP6.

#### Sintaxis:

**change** originating-default  
rip6-in-metric  
rip6-out-metric

#### **originating-default**

Los siguientes parámetros de configuración le permiten cambiar el direccionador por omisión de origen.

#### **Always originate default route**

Si habilita este parámetro, permitirá que RIP6 anuncie el direccionador como direccionador por omisión (denominado “originador de la ruta por omisión”). El direccionador por omisión realiza el direccionamiento para otros direccionadores interredes que tienen paquetes dirigidos a un destino de red desconocido.

**Valores válidos:** Yes o No

**Valor por omisión:** No

### **Originate default dependent on BGP route availability**

Este campo permite al usuario habilitar o inhabilitar un direccionador que ejecuta EGP/BGP para que se anuncie a sí mismo como direccionador por omisión mediante su IGP (RIP6 en este caso).

**Valores válidos:** Yes o No

**Valor por omisión:** No

### **From AS number**

Si desea configurar RIP6 de manera que origine una ruta por omisión cuando estén disponibles rutas de EGP, también puede configurarlo de manera que sólo origine el valor por omisión cuando las rutas de EGP se reciban de un AS en particular. Por ejemplo, si desea que sólo se genere una ruta por omisión cuando se reciba una ruta de EGP del AS número 12, establecerá este parámetro en 12. El establecimiento del número de AS en 0 significa “de cualquier AS”.

**Valores válidos:** 0 - 65535

**Valor por omisión:** Ninguno

### **Destination prefix (or network number)**

Si desea originar una ruta por omisión cuando estén disponibles rutas de EGP, también puede elegir que sólo se origine el valor por omisión cuando se reciba una ruta determinada mediante EGP. Por ejemplo, si desea que sólo se genere una ruta por omisión cuando se reciba una ruta hacia la red N, establecerá este parámetro en N. El establecimiento del número de red en :: (cero) significa “cualquier ruta recibida”.

**Valores válidos:** Cualquier dirección IPv6 de vertimiento único, ninguna dirección de vertimiento múltiple, ninguna dirección de bucle de retorno, ninguna dirección de enlace local, ninguna dirección de sitio local, ninguna dirección correlacionada con IPv4

**Valor por omisión:** Ninguno

### **Prefix length**

La longitud del prefijo. Debe configurarse este parámetro si **originate default if BGP routes available** es yes.

**Valores válidos:** 8 - 128

**Valor por omisión:**

### **Originate default if OSPF6 routes available**

Puede configurar un direccionador que ejecuta OSPF6 de manera que se anuncie a sí mismo como direccionador por omisión (se trata del originador de la ruta por omisión) mediante RIP6. Cuando está habilitado este parámetro, el direccionador se anuncia a sí mismo como direccionador por

## Mandatos de configuración de RIP6 (Talk 6)

omisión mediante RIP6 si tiene rutas derivadas de OSPF6 en la tabla de direccionamiento. El direccionador por omisión realiza el direccionamiento para otros direccionadores interredes que tienen paquetes dirigidos a un destino de red desconocido.

**Valores válidos:** Yes o No

**Valor por omisión:** No

### Originated default cost

Este parámetro especifica el coste que RIP anunciará con la ruta por omisión que origine. El coste se utiliza para determinar la vía de acceso más corta de la ruta por omisión hacia el direccionador contiguo.

**Valores válidos:** 1 - 16

**Valor por omisión:** 1

### Ejemplo:

```
RIP6 config>set originating
Always originate default route? [No]: Yes
Enter Originated default cost: between 1 and 15 [1]? 1
Update RIP6 default origination dynamically: OK
RIP6 config>
```

### Ejemplo:

```
RIP6 config>set originating
Always originate default route? [Yes]: no
Originate default dependent on BGP6 route availability? [No]: yes
From AS number [0]? 10
Dest. prefix (or network number) [::]? 1234::0
Prefix length must between 8 and 128 [64]? 64
Enter Originated default cost: between 1 and 15 [1]? 1
Update RIP6 default origination dynamically: OK
RIP6 config>
```

### rip6-in-metric

Cambia el valor de la métrica de RIP6 para las actualizaciones de RIP6 de entrada.

**Change RIPng metric on which interface?** Especifica el número de interfaz en que se va a cambiar la métrica de entrada de RIP6.

**Nota:** La interfaz debe tener configurado RIP6.

**Valores válidos:** Cualquier número de interfaz válido

**Valor por omisión:** 0

**RIP6 input Metric** Cambia el valor de la métrica de RIP6 en las actualizaciones de RIP6 de entrada.

**Valores válidos:** 1 - 15

**Valor por omisión:** 1

### rip6-out-metric

Cambia la métrica de RIP6 en las actualizaciones de RIP6 de salida.

**Change RIPng metric on which interface?** Especifica el número de interfaz en que se va a cambiar la métrica de salida de RIP6.

**Nota:** La interfaz debe tener configurado RIP6.



**Valores válidos:** Cualquier número de interfaz válido

**Valor por omisión:** 0

**RIP6 output Metric** Especifica el valor de la métrica de RIP6 en las actualizaciones de RIP6 de salida.

**Valores válidos:** 0 - 15

**Valor por omisión:** 0

## Delete

Utilice el mandato **delete** para eliminar RIP6 de la interfaz especificada.

**Sintaxis:**

**delete** *interfaznúm.*

**interfaznúm.**

Especifica la interfaz de la que se eliminará el protocolo RIP6.

**Nota:** La interfaz debe tener configurado RIP6.

**Valores válidos:** Cualquier número de interfaz válido

**Valor por omisión:** Ninguno

## Disable

Utilice el mandato **disable** para inhabilitar RIP6.

**Sintaxis:**

**disable** *override ...  
rip6  
sending ...*

**override ...**

**static-routes** Altera temporalmente las rutas estáticas de RIP6 en una interfaz.

**Modify RIP6 flags on which interface?** Especifica el número de interfaz en que se va a inhabilitar RIP6.

**Nota:** La interfaz debe tener configurado RIP6.

**Valores válidos:** Cualquier número de interfaz válido

**Valor por omisión:** 0

**default** Altera temporalmente las rutas por omisión de RIP6 en una interfaz.

**Modify RIP6 flags on which interface?** Especifica el número de interfaz en que se va a inhabilitar RIP6.

**Nota:** La interfaz debe tener configurado RIP6.

## Mandatos de configuración de RIP6 (Talk 6)

**Valores válidos:** Cualquier número de interfaz válido

**Valor por omisión:** 0

**rip6** Inhabilita RIP6 en la interfaz especificada.

**Valores válidos:** Yes o No

**Valor por omisión:** Yes

**Modify RIP6 flags on which interface?** Especifica el número de interfaz en que se va a inhabilitar RIP6.

**Nota:** La interfaz debe tener configurado RIP6.

**Valores válidos:** Cualquier número de interfaz válido

**Valor por omisión:** 0

**sending ...**

**Modify RIP6 flags on which interface?**

Especifica el número de interfaz en que se va a inhabilitar RIP6.

**Nota:** La interfaz debe tener configurado RIP6.

**Valores válidos:** Cualquier número de interfaz válido

**Valor por omisión:** 0

**all-routes**

Inhabilita el anuncio de todas las rutas de RIP6 en una interfaz.

**Valores válidos:** Yes o No

**Valor por omisión:** Yes

**default-routes**

Inhabilita el anuncio de las rutas por omisión de RIP6 en una interfaz.

**Valores válidos:** Yes o No

**Valor por omisión:** Yes

**static-routes**

Inhabilita el anuncio de las rutas estáticas de RIP6 en una interfaz.

**Valores válidos:** Yes o No

**Valor por omisión:** Yes

**poisoned-reverse-routes**

Inhabilita la inversión en el envío de actualizaciones de RIP6 sobre una interfaz.

**Valores válidos:** Yes o No

**Valor por omisión:** Yes

## Enable

Utilice el mandato **enable** para habilitar RIP6.

### Sintaxis:

```
enable          override ...
                  rip6
                  sending ...
```

**override ...**

**static-routes** Altera temporalmente las rutas estáticas de RIP6 en una interfaz.

**Modify RIP6 flags on which interface?** Especifica el número de interfaz en que se va a habilitar RIP6.

**Nota:** La interfaz debe tener configurado RIP6.

**Valores válidos:** Cualquier número de interfaz válido

**Valor por omisión:** 0

**default** Altera temporalmente las rutas por omisión de RIP6 en una interfaz.

**Modify RIP6 flags on which interface?** Especifica el número de interfaz en que se va a habilitar RIP6.

**Nota:** La interfaz debe tener configurado RIP6.

**Valores válidos:** Cualquier número de interfaz válido

**Valor por omisión:** 0

**rip6** Habilita RIP6 en la interfaz especificada.

**Valores válidos:** Yes o No

**Valor por omisión:** Yes

**Modify RIP6 flags on which interface?** Especifica el número de interfaz en que se va a habilitar RIP6.

**Nota:** La interfaz debe tener configurado RIP6.

**Valores válidos:** Cualquier número de interfaz válido

**Valor por omisión:** 0

**sending ...**

**Modify RIP6 flags on which interface?**

Especifica el número de interfaz en que se va a habilitar RIP6.

**Nota:** La interfaz debe tener configurado RIP6.

**Valores válidos:** Cualquier número de interfaz válido

**Valor por omisión:** 0

## Mandatos de configuración de RIP6 (Talk 6)

### **all-routes**

Habilita el anuncio de todas las rutas de RIP6 en una interfaz.

**Valores válidos:** Yes o No

**Valor por omisión:** Yes

### **default-routes**

Habilita el anuncio de las rutas por omisión de RIP6 en una interfaz.

**Valores válidos:** Yes o No

**Valor por omisión:** Yes

### **static-routes**

Habilita el anuncio de las rutas estáticas de RIP6 en una interfaz.

**Valores válidos:** Yes o No

**Valor por omisión:** Yes

### **poisoned-reverse-routes**

Habilita la inversión en el envío de actualizaciones de RIP6 sobre una interfaz.

**Valores válidos:** Yes o No

**Valor por omisión:** Yes

## List

Utilice el mandato **list** para visualizar la configuración de RIP6.

### **Sintaxis:**

**list** all

### **Ejemplo:**

```
RIP6>list all
RIP6
  Nets: - 0      RIP6: ENABLED
                Send: static routes
                Poison reverse enabled.
                Receive: Not override default and static routes
                RIP interface input metric: 1
                RIP interface output metric: 0

RIP6 default origination: BGP6(AS=10, net/prefix_len=1234::/64), cost = 1

Import BGP6 routes: enabled - AUTOTAG: enabled
```

## Set

Utilice el mandato **set** para establecer los parámetros de configuración de RIP6.

### **Sintaxis:**

**set** import bgp6 routes  
originating default  
rip6-in-metric  
rip6-out-metric

### **import bgp6 routes**

Este parámetro especifica que se importarán rutas aprendidas por BGP6 a la red de direccionamiento de RIP6. Sólo se importarán las rutas que aparezcan en las tablas de intercambio de entrada de BGP6. Todas las rutas se importan con un coste igual que el coste existente en la tabla de direccionamiento.

**Valores válidos:** Yes o No

**Valor por omisión:** Yes

Si se importan las rutas aprendidas por BGP6 a la red de direccionamiento de RIP6, puede configurarse el parámetro siguiente:

**Enable autotag** Este parámetro permite que RIP6 genere automáticamente identificadores para las rutas de BGP6. El valor de identificador es el número de AS a partir del cual se aprende la ruta.

**Valores válidos:** Yes o No

**Valor por omisión:** Yes

### **Ejemplo:**

```
RIP6 config>set import
Import BGP6 routes?? [Yes]:
Enable AUTOTAG? [Yes]:
AUTOTAG is updated dynamically
```

### **originating default**

Los siguientes parámetros de configuración le permiten establecer RIP6 de manera que anuncie el direccionador como direccionador por omisión.

#### **Always originate default route**

Si habilita este parámetro, permitirá que RIP6 anuncie el direccionador como direccionador por omisión (se trata del originador de la ruta por omisión). El direccionador por omisión realiza el direccionamiento para otros direccionadores interredes que tienen paquetes dirigidos a un destino de red desconocido.

**Valores válidos:** Yes o No

**Valor por omisión:** No

#### **Originate default dependent on BGP route availability**

Este campo permite al usuario habilitar o inhabilitar un direccionador que ejecuta EGP/BGP para que se anuncie a sí mismo como direccionador por omisión mediante su IGP (RIP6 en este caso).

**Valores válidos:** Yes o No

**Valor por omisión:** No

#### **From AS number**

Si desea configurar RIP6 de manera que origine una ruta por omisión cuando estén disponibles rutas de EGP, también puede configurarlo de manera que sólo origine el valor por omisión cuando las rutas de EGP se reciban de un AS en particular. Por ejemplo, si desea que sólo se genere una ruta

## Mandatos de configuración de RIP6 (Talk 6)

por omisión cuando se reciba una ruta de EGP del AS número 12, establecerá este parámetro en 12. El establecimiento del número de AS en 0 significa “de cualquier AS”.

**Valores válidos:** 0 - 65535

**Valor por omisión:** Ninguno

### **Destination prefix (or network number)**

Si desea originar una ruta por omisión cuando estén disponibles rutas de EGP, también puede elegir que sólo se origine el valor por omisión cuando se reciba una ruta determinada mediante EGP. Por ejemplo, si desea que sólo se genere una ruta por omisión cuando se reciba una ruta hacia la red N, establecerá este parámetro en N. El establecimiento del número de red en :: (cero) significa “cualquier ruta recibida”.

**Valores válidos:** Cualquier dirección IPv6 de vertimiento único, ninguna dirección de vertimiento múltiple, ninguna dirección de bucle de retorno, ninguna dirección de enlace local, ninguna dirección de sitio local, ninguna dirección correlacionada con IPv4

**Valor por omisión:** Ninguno

### **Prefix length**

La longitud del prefijo. Debe configurarse este parámetro si **originate default if BGP routes available** es *yes*.

**Valores válidos:** 8 - 128

**Valor por omisión:**

### **Originate default if OSPF6 routes available**

Puede configurar un direccionador que ejecuta OSPF6 de manera que se anuncie a sí mismo como direccionador por omisión (se trata del originador de la ruta por omisión) mediante RIP6. Cuando está habilitado este parámetro, el direccionador se anuncia a sí mismo como direccionador por omisión mediante RIP6 si tiene rutas derivadas de OSPF6 en la tabla de direccionamiento. El direccionador por omisión realiza el direccionamiento para otros direccionadores interredes que tienen paquetes dirigidos a un destino de red desconocido.

**Valores válidos:** Yes o No

**Valor por omisión:** No

### **Originated default cost**

Este parámetro especifica el coste que RIP anunciará con la ruta por omisión que origine. El coste se utiliza para determinar la vía de acceso más corta de la ruta por omisión hacia el direccionador contiguo.

**Valores válidos:** 1 - 16

**Valor por omisión:** 1

### **Ejemplo:**

```
RIP6 config>set originating
Always originate default route? [No]: Yes
Enter Originated default cost: between 1 and 15 [1]? 1
Update RIP6 default origination dynamically: OK
RIP6 config>
```

### Ejemplo:

```
RIP6 config>set originating
Always originate default route? [Yes]: no
Originate default dependent on BGP6 route availability? [No]: yes
From AS number [0]? 10
Dest. prefix (or network number) [::]? 1234::0
Prefix length must between 8 and 128 [64]? 64
Enter Originated default cost: between 1 and 15 [1]? 1
Update RIP6 default origination dynamically: OK
RIP6 config>
```

### rip6-in-metric

Establece la métrica de RIP6 en las actualizaciones de RIP6 de entrada.

**Change RIPng metric on which interface?** Especifica el número de interfaz en que se va a establecer la métrica de entrada de RIP6.

**Valores válidos:** Cualquier número de interfaz válido

**Valor por omisión:** 0

**RIP6 input Metric** Especifica el valor de la métrica de RIP6 utilizada en las actualizaciones de RIP6 de entrada.

**Valores válidos:** 1 - 15

**Valor por omisión:** 1

### rip6-out-metric

Establece la métrica de RIP6 utilizada en las actualizaciones de RIP6 de salida.

**Change RIPng metric on which interface?** Especifica el número de interfaz en que se va a establecer la métrica de salida de RIP6.

**Valores válidos:** Cualquier número de interfaz válido

**Valor por omisión:** 0

**RIP6 output Metric** Especifica el valor de la métrica de RIP6 utilizada en las actualizaciones de RIP6 de salida.

**Valores válidos:** 0 - 15

**Valor por omisión:** 0

---

## Acceso al entorno de supervisión de RIP6

Utilice el procedimiento siguiente para acceder a los mandatos de supervisión de RIP6. Este proceso le proporciona acceso al proceso de supervisión de RIP6.

1. En el indicador de OPCON, entre **talk 5**. (Para obtener información más detallada sobre este mandato, consulte “El proceso de OPCON” en la publicación *Nways Multiprotocol Access Services Guía del usuario de software*.) Por ejemplo:

## Mandatos de supervisión de RIP6 (Talk 5)

```
* talk 5  
+
```

Después de que se entre el mandato **talk 5**, se visualizará el indicador de GWCON (+) en el terminal. Si no aparece el indicador la primera vez que entre la configuración, pulse **Intro** de nuevo.

2. En el indicador +, entre el mandato **p rip6** para obtener el indicador RIP6>.

### Ejemplo:

```
+ p rip6  
RIP6>
```

---

## Mandatos de supervisión de RIP6

Este apartado describe los mandatos de supervisión de RIP6.

*Tabla 122. Resumen de los mandatos de supervisión de RIP6*

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi.
dump	Visualiza las tablas de direccionamiento.
list	Visualiza la configuración.
ping6	Realiza una acción de ping con una dirección IPv6 dinámicamente.
reset	Restablece RIP6 dinámicamente.
traceroute6	Efectúa el rastreo de una ruta dinámicamente.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

## Dump

Consulte la sección “Dump routing tables” en la página 533 para conseguir información sobre el mandato **dump**.

## List

Utilice el mandato **list** para visualizar la configuración.

### Sintaxis:

**list**

### Ejemplo:



```
RIP6>list
```

RIP6 Intf	State	In Metric	Out Metric	Send-Flags	Receive-Flags
0	Enabled /UP	1	0	St,P	

```
Send Flags: St=Static D=Default P=PoisonReverse  
Recv Flags: OSt=Override-Static OD=Override-Default
```

```
RIP originates default with cost 1 under these conditions:  
  BGP6 or OSPF6 External route 1234::/64 from AS 10 available  
  Default origination conditions not satisfied  
Import BGP6 routes: enabled - AUTOTAG: enabled
```

## Ping6

Consulte la sección “Ping6” en la página 508 para obtener información detallada sobre el mandato **ping6**.

## Reset

**Sintaxis:**

```
reset
```

**Ejemplo:**

```
RIP6>reset
```

## Traceroute6

Consulte la sección “Traceroute6” en la página 509 para obtener información detallada sobre el mandato **traceroute6**.

---

## Soporte de la reconfiguración dinámica de RIP6

Este apartado describe la reconfiguración dinámica (DR) tal como afecta a los mandatos Talk 6 y Talk 5.

### Mandato Delete Interface de CONFIG (Talk 6)

Routing Information Protocol para IPV6 (RIP6) da soporte al mandato de CONFIG (Talk 6) **delete interface** con la consideración siguiente:

También se suprimen todas las configuraciones de RIP6 efectuadas en relación con esta interfaz.

### Mandato Activate Interface de GWCON (Talk 5)

RIP6 da soporte al mandato de GWCON (Talk 5) **activate interface** con la consideración siguiente:

Debe configurarse IPv6 para esta interfaz.

El mandato de GWCON (Talk 5) **activate interface** da soporte a todos los mandatos específicos de interfaz RIP6.

## Mandato Reset Interface de GWCON (Talk 5)

RIP6 da soporte al mandato de GWCON (Talk 5) **reset interface** con la consideración siguiente:

Todas las configuraciones de RIP6 relativas a una interfaz cambian dinámicamente si hay una dirección IPv6 configurada para esta interfaz.

El mandato de GWCON (Talk 5) **reset interface** da soporte a todos los mandatos específicos de interfaz RIP6.

## Mandatos Reset de GWCON (Talk 5) del componente

Routing Information Protocol para IPv6 (RIP6) da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos de RIP6:

### Mandato Reset Interface (o All Interfaces) de GWCON, Protocol RIP6

**Descripción:** Cambia dinámicamente las políticas o los parámetros de una interfaz RIP6 (todas las interfaces RIP6).

**Efecto en la red:** Según los cambios de la configuración, modificará las políticas de envío o recepción de las rutas de RIP6 en una interfaz.

**Limitaciones:** Ninguna.

El mandato de **GWCON, protocolo RIP6, reset interface (o all interfaces)** da soporte a todos los mandatos de RIP6.

## Mandatos de CONFIG (Talk 6) de cambio inmediato

RIP6 da soporte a los siguientes mandatos de CONFIG que cambian inmediatamente el estado operativo del dispositivo. Estos cambios se guardan y se conservan si se vuelve a cargar o a iniciar el dispositivo o si se ejecuta un mandato reconfigurable dinámicamente.

Todos los mandatos de Talk 6 de RIP6 son dinámicos.

## Mandatos no reconfigurables dinámicamente

Todos los parámetros de configuración de RIP6 pueden cambiarse dinámicamente.

---

## Configuración y supervisión de BGP6

El protocolo BGP4 con la adición de RFC 2283, *Multiprotocol Extensions for BGP4 (BGP4+)*, da soporte a la información de direccionamiento de IPv6.

Este capítulo describe los mandatos de configuración y supervisión de BGP6 e incluye los apartados siguientes:

- “Mandatos de configuración de BGP6”
- “Acceso al entorno de configuración de BGP6”
- “Acceso al entorno de supervisión de BGP6” en la página 579
- “Mandatos de supervisión de BGP6” en la página 579
- “Soporte de la reconfiguración dinámica de BGP6” en la página 589

---

### Acceso al entorno de configuración de BGP6

Para acceder al entorno de configuración de BGP6, entre el mandato siguiente en el indicador Config>:

```
Config> protocol bgp6  
BGP6 Config>
```

---

### Mandatos de configuración de BGP6

Este apartado describe los mandatos de configuración de BGP6. Estos mandatos le permiten modificar el comportamiento del protocolo BGP6 para que cumpla los requisitos específicos. Es necesaria una cierta cantidad de configuración para conseguir un direccionador de BGP6 completamente funcional. Entre los mandatos de configuración de BGP6 en el indicador BGP6 Config>.

## Mandatos de configuración de BGP6 (Talk 6)

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxxi.
Add	Añade contiguos y políticas a BGP6.
Attach	Conecta una lista de políticas de envío y una de políticas de recepción con un contiguo en particular.
Change	Modifica la información entrada originalmente con el mandato <b>add</b> .
Delete	Suprime la información de configuración de BGP6 entrada con el mandato <b>add</b> .
Disable	Inhabilita determinadas funciones de BGP6 que se han activado mediante el mandato <b>enable</b> .
Enable	Habilita altavoces de BGP6 y contiguos de BGP6.
List	Visualiza los elementos de la configuración de BGP6.
Move	Cambia el orden en el que se han definido las políticas y los agregados.
Set	Establece el temporizador de exploración de tabla de rutas de IPv6.
Update	Manipula una política de un nombre de lista de políticas configurado mediante los mandatos de submenú <b>add</b> , <b>delete</b> , <b>change</b> y <b>move</b> .
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxi.

### Add

Utilice el mandato **add** para añadir información de BGP6 a la configuración.

#### Sintaxis:

```
add                aggregate . . .  
                    neighbor . . .  
                    no-receive númas . . .  
                    originate-policy . . .  
                    policy-list . . .  
                    receive-policy . . .  
                    send-policy . . .
```

#### **aggregate** *prefijo de red longitud de prefijo*

El mandato **add aggregate** hace que el altavoz de BGP6 agregue un bloque de direcciones y anuncie una sola ruta a sus contiguos de

BGP6. Debe especificar el prefijo de red común a todas las rutas que se agregarán y la longitud de prefijo. El ejemplo que aparecerá a continuación ilustra cómo agregar un bloque de direcciones.

1. El **prefijo de red** especifica las direcciones afectadas. El prefijo es la primera dirección de un rango de direcciones especificadas en una política de BGP6.

**Valores válidos:** una dirección IPv6 de vertimiento único válida o una dirección IPv4 compatible válida, excepto las siguientes:

- direcciones de enlace de tipo local (FE80::)
- direcciones de sitio de tipo local (FEC0::)
- dirección de bucle de retorno (::1)
- direcciones IPv6 correlacionadas con IPv4 (::FFFF:<dirección IPv4>)

**Valor por omisión:** ninguno

2. La **longitud de prefijo** se aplica a la dirección especificada para el prefijo de red con el fin de generar una dirección utilizada en una política de BGP6.

**Valores válidos:** 8 - 128

**Valor por omisión:** 64

**Ejemplo:** `add aggregate`

```
Network Prefix []? 2000::  
Prefix Length [64]? 16
```

Cuando añade una definición de agregado, recuerde que debe definir una política para bloquear la exportación de las rutas agregadas. Si no lo hace, el direccionador anunciará tanto las rutas individuales como los agregados que haya definido. Esto no es aplicable cuando se agregan las rutas, que se originan a partir de su tabla de direccionamiento de IGP.

**neighbor** *dirección de contiguo* *númAS* *temporizador de inicial*. *temporizador de conexión* *temporizador de mantenim*. *temporizador de keep alive* *tamaño de segmento de tcp*

Utilice el mandato **add neighbor** para definir un contiguo de BGP6. El contiguo puede ser externo o interno con respecto al AS del altavoz de BGP6. Para activar este contiguo dinámicamente, utilice el mandato **reset neighbor** de la supervisión de BGP6.

### dirección de contiguo

La **dirección de contiguo** es la dirección IPv6 del contiguo con el que desea mantener una relación de igual. Puede estar dentro del propio sistema autónomo o en otro sistema autónomo. Si es un contiguo externo, ambos altavoces de BGP6 deben compartir la misma red. Para los contiguos internos, no existe esta restricción.

**Valores válidos:** una dirección IPv6 de vertimiento único válida o una dirección IPv4 compatible válida, excepto las siguientes:

- direcciones de enlace de tipo local (FE80::)

- direcciones de sitio de tipo local (FEC0::)
- dirección de bucle de retorno (::1)
- direcciones IPv6 correlacionadas con IPv4 (::FFFF:<dirección IPv4>)
- dirección cero (::0)

**Valor por omisión:** ninguno

**númAS** El **númAS** es el el número del propio sistema autónomo para el contiguo interno o el número de sistema autónomo del contiguo. El número de AS del contiguo tiene:

**Valores válidos:** un entero dentro del rango del 1 al 65535

**Valor por omisión:** 1

### temporizador de inicialización

El **temporizador de inicialización** especifica el período de tiempo que el altavoz de BGP6 espera para inicializar los recursos y reiniciar la conexión de transporte con el contiguo en el caso de que el altavoz haya pasado anteriormente al estado de desocupado debido a un error. Si persiste el error, este temporizador experimenta un aumento exponencial.

**Valores válidos:** de 0 a 65535 segundos

**Valor por omisión:** 12 segundos

### temporizador de conexión

El **temporizador de conexión** especifica el período de tiempo que espera el altavoz de BGP6 para reiniciar la conexión de transporte con el contiguo si la conexión TCP falla mientras se encuentra en el estado activo o de conexión. Mientras, el altavoz de BGP6 continúa escuchando cualquier conexión que pueda iniciar el contiguo.

**Valores válidos:** de 0 a 65535 segundos

**Valor por omisión:** 120 segundos

### temporizador de mantenimiento

Entre el **temporizador de mantenimiento** para especificar el período de tiempo que el altavoz de BGP6 espera antes de suponer que el contiguo no es asequible. Ambos contiguos intercambian la información configurada en el mensaje OPEN y eligen el menor de los dos temporizadores como valor de temporizador de mantenimiento negociado.

Una vez que los contiguos han establecido la conexión BGP6, intercambian mensajes Keepalive a intervalos frecuentes para asegurarse de que la conexión continúa y de que los contiguos son asequibles. El intervalo del temporizador de Keep-Alive se calcula como un tercio del valor de temporizador de mantenimiento negociado. Por consiguiente, el valor de temporizador de mantenimiento debe ser cero o un mínimo de tres segundos.

Tenga en cuenta que, en las líneas conmutadas, es posible que desee utilizar el valor de cero del temporizador de man-

tenimiento para guardar el ancho de banda no enviando mensajes Keepalive a intervalos frecuentes.

**Valores válidos:** de 0 a 65535 segundos

**Valor por omisión:** 90 segundos

### tamaño de segmento de TCP

El **tamaño de segmento de TCP** especifica el tamaño de datos máximo que puede intercambiarse en la conexión TCP con un contiguo. Este valor se utiliza para la conexión TCP activa con el contiguo.

**Valores válidos:** de 1 a 65535 bytes.

**Valor por omisión:** 1220 bytes

### Ejemplo: add neighbor

```
Neighbor address []? 2002:9::6205
AS [1]? 2002
Init timer [12]?
Connect timer [120]?
Hold timer [90]?
TCP segment size [1220]?
```

### no-receive númAS

Utilice **add no-receive númAS** para excluir vías de acceso de AS si aparece el número de AS determinado en alguna parte de la lista de vías de acceso de AS.

El **númAS** tiene:

**Valores válidos:** del 1 al 65535

**Valor por omisión:** 1

### Ejemplo: add no-receive

```
Enter AS: [1]? 2003
```

### originate-policy (*exclusive/ inclusive*) *prefijo de red longitud de prefijo coincidencia de dirección (Exact/Range) identificador*

Utilice el mandato **add originate-policy** con el fin de especificar el valor a utilizar en la selección de rutas para el anuncio.

*Exclusive* Las políticas exclusivas impiden que se incluya información de ruta en la tabla de direccionamiento del altavoz de BGP6.

*Inclusive* Las políticas inclusivas aseguran que se incluyan rutas específicas en la tabla de direccionamiento del altavoz de BGP6.

*prefijo de red* Este parámetro especifica la dirección de red afectada por esta política.

**Valores válidos:** una dirección IPv6 de vertimiento único válida o una dirección IPv4 compatible válida, excepto las siguientes:

- direcciones de enlace de tipo local (FE80::)
- direcciones de sitio de tipo local (FEC0::)

## Mandatos de configuración de BGP6 (Talk 6)

- dirección de bucle de retorno (::1)
- direcciones IPv6 correlacionadas con IPv4 (::FFFF:<dirección IPv4>)

**Valor por omisión:** ninguno

*longitud de prefijo* La **longitud de prefijo** se aplica a la dirección especificada para el prefijo de red con el fin de generar una dirección utilizada en una política de BGP6.

**Valores válidos:** 0 - 128

**Valor por omisión:** 0

*coincidencia de dirección* La dirección o rango de direcciones afectadas por la sentencia de la política.

**Valores válidos:** Exact o Range

**Valor por omisión:** Range

*identificador* El valor de identificador representa el número de AS a partir del cual se aprende la ruta. El valor de identificador se utiliza para la interacción con un IGP, como por ejemplo RIP6. Consulte "Set" en la página 554 para obtener información sobre cómo importar rutas de BGP6 y generar automáticamente identificadores para BGP6.

**Valores válidos:** 0 - 65535

**Valor por omisión:** 0

El ejemplo siguiente incluye todas las rutas en la tabla de direccionamiento de IGP del altavoz de BGP6 para el anuncio.

**Ejemplo: add originate-policy inclusive**

```
Network Prefix [::]?  
Prefix length[0]?  
Address Match (Exact/Range) [Range]?  
Tag [0]?
```

### policy-list

Utilice el mandato **add policy-list** para configurar un grupo de políticas, que puede conectarse con un contiguo específico mediante el mandato **attach policy-to-neighbor**.

**Name** Especifica el nombre a utilizar para identificar el grupo de políticas.

**Valores válidos:** una serie de 1 a 15 caracteres ASCII

**Valor por omisión:** ninguno

**Ejemplo: add policy-list**

```
Name[]? nbr1-rcv  
Policy Type(Receive/Send) [Receive]?Receive
```

**Ejemplo: add policy-list**

```
Name[]? nbr1-snd  
Policy Type(Receive/Send) [Receive]?Send
```

**receive-policy** (*exclusive/ inclusive*) *prefijo de red* *longitud de prefijo* *coincidencia de dirección* *númAS de origen* *númAS adyacente* *métricaigp* (*sólo inclusivas*)



Utilice el mandato **add receive-policy** para determinar qué rutas se importarán a la tabla de direccionamiento del altavoz de BGP6.

Las políticas exclusivas impiden que se incluya información de ruta en la tabla de direccionamiento del altavoz de BGP6.

Las políticas inclusivas aseguran que se incluyan rutas específicas en la tabla de direccionamiento del altavoz de BGP6.

### prefijo de red

Especifica las direcciones afectadas.

**Valores válidos:** una dirección IPv6 de vertimiento único válida o una dirección IPv4 compatible válida, excepto las siguientes:

- direcciones de enlace de tipo local (FE80::)
- direcciones de sitio de tipo local (FEC0::)
- dirección de bucle de retorno (::1)
- direcciones IPv6 correlacionadas con IPv4 (::FFFF:<dirección IPv4>)

**Valor por omisión:** ninguno

### longitud de prefijo

La **longitud de prefijo** se aplica a la dirección especificada para el **prefijo de red** con el fin de generar una dirección utilizada en una política de BGP6.

**Valores válidos:** 0 - 128

**Valor por omisión:** 0

### coincidencia de dirección

La **coincidencia de dirección** es un rango de direcciones o una dirección exacta.

**Valores válidos:** Exact o Range

**Valor por omisión:** Range

### númAS de origen

Un **númAS de origen** tiene:

**Valores válidos:** del 0 al 65535

**Valor por omisión:** 0

### númAS adyacente

El **númAS adyacente** especifica el número de AS de contigüidad.

**Valores válidos:** del 0 al 65535

**Valor por omisión:** 0

### métrica de IGP

La **métrica de IGP** (sólo para políticas de recepción inclusivas) especifica el valor de métrica con el que las rutas aceptadas se importan a la tabla de direccionamiento de IGP del altavoz. Si la métrica de IGP es -1, estas rutas no se importarán a la tabla de IGP; por lo tanto, estas rutas no podrán volver a anunciarse.

**Valores válidos:** del -1 al 65535

**Valor por omisión:** 0

**Ejemplo:** `add receive-policy exclusive`

```
Network Prefix [::]? 2003::  
Prefix length[0]? 16  
Address Match (Exact/Range) [Range]?  
Originating AS# [0]? 168  
Adjacent AS# [0]? 165
```

**Ejemplo:** `add receive-policy inclusive`

```
Network Prefix [::]? 2000:: Prefix Length [0]? 64  
Address Match (Exact/Range) [Range]?  
Originating AS# [0]?  
Adjacent AS# [0]?  
IGP-metric [0]?
```

**send-policy** (*exclusive/ inclusive*) *prefijo de red longitud de prefijo coincidencia de dirección identificador númAS adyacente*

Utilice el mandato **add send-policy** para crear políticas que determinen cuál de las rutas aprendidas del altavoz de BGP6 volverá a anunciarse. Estas rutas pueden ser internas o externas con respecto al AS del altavoz de BGP6.

Las políticas exclusivas impiden que se anuncie a contiguos de BGP6 información de ruta de la tabla de direccionamiento del altavoz de BGP6.

Las políticas inclusivas aseguran que se anuncien a contiguos de BGP6 rutas específicas de la tabla de direccionamiento del altavoz de BGP6.

### **prefijo de red**

El **prefijo de red** hace referencia a las direcciones afectadas.

**Valores válidos:** una dirección IPv6 de vertimiento único válida o una dirección IPv4 compatible válida, excepto las siguientes:

- direcciones de enlace de tipo local (FE80::)
- direcciones de sitio de tipo local (FEC0::)
- dirección de bucle de retorno (::1)
- direcciones IPv6 correlacionadas con IPv4 (::FFFF:<dirección IPv4>)

**Valor por omisión:** ninguno

### **longitud de prefijo**

La **longitud de prefijo** se aplica a la dirección especificada para el prefijo de red con el fin de generar una dirección utilizada en una política de BGP6.

**Valores válidos:** 0 - 128

**Valor por omisión:** 0

### **coincidencia de dirección**

La **coincidencia de dirección** es un rango de direcciones o una dirección exacta.

**Valores válidos:** Exact o Range

**Valor por omisión:** Range

**identificador**

El valor de identificador representa el número de AS a partir del cual se aprende la ruta. El valor de identificador se utiliza para la interacción con un IGP, como por ejemplo RIP6. Consulte “Set” en la página 554 para obtener información sobre cómo importar rutas de BGP6 y generar automáticamente identificadores para BGP6.

**Valores válidos:** del 0 al 65535

**Valor por omisión:** 0

**númAS adyacente**

El **númAS adyacente** especifica el número de AS de contigüidad.

**Valores válidos:** del 0 al 65535

**Valor por omisión:** 0

**Ejemplo: add send exclusive**

```
Network Prefix []? 2003::
Prefix length[0]? 16
Address Match (Exact/Range) [Range]?
Tag [0]?
Adjacent AS# [0]?
```

**Attach**

Utilice el mandato **attach policy-to-neighbor** para conectar un nombre de lista de políticas configurado con un contiguo específico. Puede conectar hasta tres nombres de lista de políticas de recepción y tres nombres de lista de políticas de envío.

**Sintaxis:**

```
attach                policy-to-neighbor
```

**Ejemplo: attach policy-to-neighbor**

```
Neighbor address [::]? 2003::
First receive policy list name (none for global AS based policy)[]? nbr1-rcv
Second receive policy list name (none for exit)[]?
First send policy list name (none for global AS based policy)[]? nbr1-snd
Second send policy list name (none for exit)[]?
```

**Change**

Utilice el mandato **change** para cambiar un elemento de la configuración de BGP6 instalado anteriormente por el mandato add.

**Sintaxis:**

```
change                aggregate . . .
                        neighbor . . .
                        originate-policy . . .
                        policy-to-neighbor
                        receive-policy . . .
                        send-policy . . .
```

## Mandatos de configuración de BGP6 (Talk 6)

**aggregate** *númíndice prefijo de red longitud de prefijo*  
Este ejemplo cambia el agregado actual (agregado 1).

**Ejemplo:** **change aggregate 1**

```
Network Prefix [2000::]? 2001::  
Prefix Length [16]?
```

**neighbor** *dirección IPv6 de contiguo númAS temporizador de inicial.  
temporizador de conexión temporizador de mantenim. temporizador  
de keep alive tamaño de segmento de tcp*  
Utilice este mandato para cambiar los valores de los parámetros de configuración relativos a un contiguo existente. Es posible que no se utilice para cambiar la dirección de un contiguo existente.

Para volver a activar el contiguo dinámicamente, utilice el mandato **reset neighbor** de la supervisión de BGP6.

La **dirección de contiguo** a modificar tiene:

**Valores válidos:** cualquier dirección de contiguo configurada actualmente

**Valor por omisión:** ninguno

El ejemplo siguiente cambia el valor del temporizador de mantenimiento por cero para el contiguo 2002:0::6205.

**Ejemplo:** **change neighbor 2002:0::6205**

```
AS [2002]?  
Init timer [12]?  
Connect timer [60]?  
Hold timer [12]? 0  
TCP segment size [1220]?
```

**originate-policy** *númíndice (exclusive/ inclusive) prefijo de red  
longitud de prefijo coincidencia de dirección identificador*  
Utilice el mandato **change originate-policy** para modificar una definición de política de origen existente.

Este ejemplo modifica la política de origen del altavoz de BGP6.

**Ejemplo:** **change originate-policy**

```
Enter index of originate-policy to be modified [1]?  
Policy Type (Inclusive/Exclusive) [Exclusive]? inclusive  
Network Prefix [2003::]? 2004::  
Prefix Length [16]? 16  
Address Match (Exact/Range) [Range]?  
Tag [0]?
```

**policy-to-neighbor**

Utilice el mandato **change policy-to-neighbor** para cambiar una conexión de lista de políticas con un contiguo en particular.

**Ejemplo:** **change policy-to-neighbor**

```
Neighbor address [0::0]? 2003::  
First receive policy list name to be changed[nbr1-rcv]?  
Second receive policy list name to be changed[]?  
Third receive policy list name to be changed[]?  
First send policy list name to be changed[nbr1-snd]?  
Second send policy list name to be changed[]?  
Third send policy list name to be changed[]?
```

**receive-policy** *númíndice (exclusive/inclusive) prefijo de red longitud de prefijo  
coincidencia de dirección númAS de origen númAS adyacente  
métricaigp (sólo inclusivas)*

Utilice el mandato **change receive-policy** para modificar una definición de política de recepción existente.

Este ejemplo añade una restricción a la política de recepción del altavoz de BGP6. En lugar de hacer que se importe información de ruta de cada igual BGP6 a la tabla de direccionamiento de IGP, ahora impedirá que se importen rutas del AS 165.

**Ejemplo: change receive-policy**

```
Enter index of receive-policy to be modified [1]?
Policy Type (Inclusive/Exclusive) [Inclusive]? exclusive
Network Prefix [2003::]?
Prefix Length [16]?
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Adjacent AS# [0]? 165
```

**send-policy** *númíndice (exclusive/ inclusive) prefijo de red longitud de prefijo coincidencia de dirección identificador númAS adyacente*

Utilice el mandato **change send-policy** para modificar una política de envío existente de manera que sea más inclusiva o más exclusiva.

Este ejemplo añade una restricción a la política de envío del altavoz de BGP6.

**Ejemplo: change send-policy**

```
Enter index of send-policy to be modified [1]?
Policy Type (Inclusive/Exclusive) [Inclusive]? exclusive
Network Prefix [0::0]? 2004:6::6205
Prefix Length [16]? 16
Address Match (Exact/Range) [Range]?
Tag [0]?
Adjacent AS# [0]? 165
```

## Delete

Utilice el mandato **delete** para suprimir un elemento de la configuración de BGP6 instalado anteriormente por el mandato **add**.

**Sintaxis:**

```
delete          aggregate . . .
                  neighbor . . .
                  no-receive . . .
                  originate-policy . . .
                  policy-list . . .
                  policy-to-neighbor
                  receive-policy . . .
                  send-policy. . .
```

**aggregate** *númíndice*

Debe especificar el número de índice del agregado que desea suprimir.

**Ejemplo: delete aggregate 1**

**neighbor** *dirección IPv6 de contiguo*

Utilice este mandato para suprimir un contiguo de BGP6. Debe especificar la dirección de red del contiguo.

La **dirección de red del contiguo a suprimir** tiene:

**Valores válidos:** cualquier dirección de contiguo configurada actualmente

## Mandatos de configuración de BGP6 (Talk 6)

**Valor por omisión:** ninguno

Para desactivar este contiguo dinámicamente, utilice el mandato **reset neighbor** de la supervisión de BGP6.

**Ejemplo:** `delete neighbor 2002:9::6024`

**no-receive** *númAS*

Utilice este mandato para suprimir la política de no recepción configurada para un AS en particular. Debe especificar el número de AS.

El **númAS** tiene:

**Valores válidos:** del 1 al 65535

**Valor por omisión:** ninguno

**Ejemplo:** `delete no-receive 168`

**originate-policy** *númíndice*

Utilice este mandato para suprimir una política de origen específica. Debe especificar el número de índice asociado con la política.

**Ejemplo:** `delete originate-policy 2`

**policy-list**

Utilice el mandato **delete policy-list** para suprimir una lista de políticas.

**Ejemplo:** `delete policy-list`

```
Name of policy-list to delete []? nbr1-rcv
All policies defined for 'nbr1-rcv' will be deleted.
Are you sure you want to delete (Yes or [No])? Yes
Policy-list 'nbr1-rcv' is deleted.
```

The policy-to-neighbor attachment will be adjusted accordingly.

**policy-to-neighbor**

Utilice el mandato **delete policy-to-neighbor** para suprimir una conexión de nombre de lista de políticas existente con un contiguo en particular.

**Ejemplo:** `delete policy-to-neighbor`

```
Neighbor address []? 2009:9::6205
Remove first receive policy-list name [nbr1-rcv]
Are you sure you want to remove (Yes or [No])? yes
Remove first send policy-list name [nbr1-snd]
Are you sure you want to remove (Yes or [No])? yes
```

**receive-policy** *númíndice*

Utilice este mandato para suprimir una política de recepción específica. Debe especificar el número de índice asociado con la política.

**Ejemplo:** `delete receive-policy`

```
Enter index of receive-policy to be deleted [1]?
```

**send-policy** *númíndice#*

Utilice este mandato para suprimir una política de envío específica. Debe especificar el número de índice asociado con la política.

**Ejemplo:** `delete send-policy 4`

## Disable

Utilice el mandato **disable** para inhabilitar un altavoz o contiguo de BGP6 anteriormente habilitado. Tenga en cuenta que los contiguos se habilitan implícitamente al añadirse mediante el mandato **add**.

### Sintaxis:

```
disable          BGP6 speaker
                  compare-med-from-diff-AS
                  neighbor . . .
```

### BGP6 speaker

Utilice el mandato **disable BGP6 speaker** para inhabilitar el protocolo BGP6.

**Ejemplo: disable BGP6 speaker**

### compare-med-from-diff-AS

Utilice este mandato para inhabilitar una comparación de MED entre diferentes AS.

**Ejemplo: disable compare-med-from-diff-AS**

### neighbor *dirección IPv6 de contiguo*

Utilice este mandato para inhabilitar un contiguo actualmente configurado. La **dirección de contiguo** tiene:

**Valores válidos:** cualquier dirección IPv6 válida

**Valor por omisión:** ninguno

**Ejemplo: disable neighbor 2002:9::6205**

## Enable

Utilice el mandato **enable** para activar las funciones, posibilidades e información de BGP6 que haya añadido a la configuración de BGP6.

### Sintaxis:

```
enable          BGP6 speaker
                  compare-med-from-diff-AS
                  neighbor . . .
```

### BGP6 speaker *númAS tamaño de segmento de tcp*

Utilice el mandato **enable BGP6 speaker** para habilitar el protocolo BGP6.

1. El **númAS** está asociado con este conjunto de direccionadores y nodos.

**Valores válidos:** del 1 al 65535

**Valor por omisión:** 1

2. Entre el **tamaño de segmento de TCP** para especificar el tamaño de segmento máximo que BGP6 debe utilizar para las conexiones TCP pasivas.

**Valores válidos:** de 1 a 65535 bytes.

**Valor por omisión:** 1220 bytes

## Mandatos de configuración de BGP6 (Talk 6)

**Ejemplo:** `enable BGP6 speaker`

AS [0]? 165  
TCP segment size [1220]?

### **compare-med-from-diff-AS**

Utilice este mandato para habilitar una comparación de MED entre diferentes AS.

**Ejemplo:** `enable compare-med-from-diff-AS`

### **neighbor** *dirección IPv6 de contiguo*

Utilice este mandato para habilitar un contiguo de BGP6.

La **dirección de contiguo** tiene:

**Valores válidos:** cualquier dirección de contiguo configurada actualmente

**Valor por omisión:** ninguno

**Ejemplo:** `enable neighbor 2002:9::6205`

## List

Utilice el mandato **list** para visualizar varias partes de los datos de configuración de BGP6 de acuerdo con el submandato determinado que se invoque.

### **Sintaxis:**

**list**                    aggregate  
                          all  
                          BGP6 speaker  
                          neighbor  
                          no-receive  
                          originate-policy  
                          policy-list . . .  
                          policy-to-neighbor  
                          receive-policy  
                          send-policy

### **aggregate**

Utilice el mandato **list aggregate** para listar todas las rutas agregadas que se han definido con el mandato **add aggregate**.

**Ejemplo:** `list aggregate`

```
Aggregation:
Index  Prefix/Prefix length
1      2000::/16
```

### **all**

Utilice el mandato **list all** para listar los contiguos, políticas, rutas agregadas y registros de as sin recepción de BGP6 existentes en la configuración actual de BGP6.

**Ejemplo:** `list all`



## Mandatos de configuración de BGP6 (Talk 6)

```
BGP6 Protocol:      Enabled
AS:                 710
TCP-Segment Size:  1220
```

Neighbors and their AS:

Address	State	AS	Init Timer	Conn Timer	Hold Timer	TCPSEG Size
2003:7:8:2::820	ENABLD	820	12	120	90	1220
2002:9::6205	ENABLD	2002	12	120	90	1220

Receive-Policies:

Index	Type	Prefix/Prefix length	Match Range	OrgAS	AdjAS	IGPmet
1	INCL	::/0	0	0	0	
2	EXCL	2003::/16	0	0		

Send-Policies:

Index	Type	Prefix/Prefix length	Match Range	Tag	AdjAS
1	INCL	::/0	0		0
2	EXCL	2003::/16	0		0

Originate-Policies:

Index	Type	Prefix/Prefix Length	Match Range	Tag
1	INCL	::/0	0	
2	EXCL	2003::/16	0	

Aggregation:

Index	Prefix/Prefix Length
1	2000::/16

AS-PATH with following ASs will be discarded:  
AS 2003  
compare-med-from-diff-as is enabled.  
IPv6-route-table-scan-timer value is 2 seconds.

### BGP6 speaker

Utilice el mandato **list BGP6 speaker** para hacer que aparezca información sobre el altavoz de BGP6. Se proporciona la información siguiente:

**Ejemplo:** `list BGP6 speaker`

```
BGP6 Protocol:      Enabled
AS:                 165
TCP-Segment Size:  1220
```

**neighbor** Utilice el mandato **list neighbor** para hacer que aparezca información sobre los contiguos de BGP6.

**Ejemplo:** `list neighbor`

Neighbors and their AS along with attached policy-list name(s):

Address	State	AS	Init Timer	Conn Timer	Hold Timer	TCPSEG Size
2003:7:8:2::820	ENABLD	820	12	120	90	1220
2002:9::6205	ENABLD	2002	12	120	90	1220

### no-receive

Utilice el mandato **list no-receive** para hacer que aparezca información sobre las definiciones de AS sin recepción que se han añadido a la configuración de BGP6.

**Ejemplo:** `list no-receive`

```
AS-PATH with following autonomous systems will be discarded:
AS 178
AS 165
```

## Mandatos de configuración de BGP6 (Talk 6)

### **originate-policy** *all índice prefijo*

Utilice el mandato **list originate-policy** para hacer que aparezca información sobre las políticas de origen que se han añadido a la configuración de BGP6.

#### **Ejemplo: list originate-policy**

```
Originate-Policies:
Index  Type  Prefix/Prefix Length      Match  Tag
1      INCL  ::/0                      Range  0
2      EXCL  2003::/16                 Range  0
```

### **policy-list**

Utilice el mandato **list policy-list** para listar los nombres de lista de políticas que se han configurado.

#### **Ejemplo: list policy-list**

```
BGP6 Config>li policy list
Policy list:
nbr1-rcv  Receive
nbr1-snd  Send
```

### **policy-to-neighbor**

Utilice el mandato **list policy-to-neighbor** para listar las políticas conectadas con contiguos.

#### **Ejemplo: list policy-to-neighbor**

```
Neighbor address      Receive      Send
2002:9::6205          rec1         send1
```

### **receive-policy número-as-adyacente** *all o índice o prefijo*

Utilice el mandato **list receive-policy** para hacer que aparezca información sobre las políticas de recepción que se han añadido a la configuración de BGP6. Puede visualizar todas las políticas de recepción definidas para un AS o bien visualizar las políticas relativas a un número de prefijo o índice.

#### **Ejemplo: list receive-policy**

```
Receive-Policies:
Index  Type  Prefix/Prefix Length      Match  OrgAS  AdjAS  IGPmet
1      INCL  ::/0                      Range  0      0      0
2      EXCL  2003::/16                 Range  0      0
```

### **send-policy número-as-adyacente** *all o índice o prefijo*

Utilice el mandato **list send-policy** con el fin de visualizar información sobre las políticas de envío definidas para los sistemas autónomos especificados. Puede visualizar todas las políticas de envío definidas para un AS o bien visualizar las políticas relativas a un número de prefijo o índice.

#### **Ejemplo: list send-policy**

```
Send-Policies:
Index  Type  Prefix/Prefix length      Match  Tag  AdjAS
1      INCL  ::/0                      Range  0      0
2      EXCL  2003::/16                 Range  0      0
```

## Move

Utilice el mandato **move** para cambiar el orden en que se han definido las políticas y los agregados. Así se cambia el orden en que el direccionador aplica las políticas existentes a la información de ruta. Antes de utilizar este mandato, es aconsejable que utilice el mandato **list** para ver qué políticas se han definido.

**Sintaxis:**

**move**                    **aggregate** u **originate-policy** o **receive-policy** o **send-policy**

**Ejemplo:**

```
move originate-policy
Enter index of originate-policy to move [1]? 3
Move record AFTER record number [0]?
```

**Set**

Utilice el mandato **set** para establecer el temporizador de exploración de tabla de rutas de IPv6. El valor de este temporizador se utiliza con el fin de establecer el intervalo de tiempo de exploración de tabla de reenvío de IPv6 para las actualizaciones de BGP6.

**Sintaxis:**

**set**                    ipv6-route-table-scan-timer

**Valores válidos:** del 1 al 10  
**Valor por omisión:** 1

**Ejemplo:**

```
set ipv6-route-table-scan-timer
Timer Value in seconds [1]? 2
```

**Update**

Utilice el mandato **update** y sus submandatos para manipular políticas.

**Sintaxis:**

**update**                *policy-list*

**Ejemplo para las políticas de recepción:**

```
update policy-list
Name[]? nbr1-rcv
```

**Add**

Utilice el mandato **Add** para añadir políticas de recepción o envío dentro del mandato **update**.

**Ejemplo:** Adición de una política de recepción

## Mandatos de configuración de BGP6 (Talk 6)

```
BGP6 Config>add POLICY-LIST
Policy-list name []? rec1
Policy Type (Receive/Send) [Receive]?
BGP6 Config>UPDATE POLICY-LIST
Policy-list name []? rec1
Policy-list rec1:Receive Config>add
Policy Type (Inclusive/Exclusive) [Exclusive]?
Network Prefix [::]? 1234::
Prefix Length [0]? 16
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
Policy-list rec1:Receive Config>list
Receive Policy list for rec1:
Idx T Prefix/Length/Match          OrgAS AnyAS MED   Weight
LP   IGPm
1   E 1234::/16/R                   0     0

```

```
Policy-list rec1:Receive Config>add
Policy Type (Inclusive/Exclusive) [Exclusive]? inc
Network Prefix [::]? 5678::
Prefix Length [0]? 16
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
MED [0]?
Local-pref [0]?
Weight [0]?
IGP-metric [0]?
Policy-list rec1:Receive Config>list
Receive Policy list for rec1:
Idx T Prefix/Length/Match          OrgAS AnyAS MED   Weight
LP   IGPm
1   E 1234::/16/R                   0     0
2   I 5678::/16/R                   0     0     0     0

```

### Ejemplo: Adición de una política de envío

```
BGP6 Config>add POLICY-LIST
Policy-list name []? send1
Policy Type (Receive/Send)
[Receive]? send
BGP6 Config>UPDATE POLICY-LIST
Policy-list name []? send1
Policy-list send1:Send Config>add
Policy Type (Inclusive/Exclusive) [Exclusive]? i
Network Prefix [::]? 1234::
Prefix Length [0]? 16
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
Tag [0]?
MED [0]?
# of AS padding [0]?
Policy-list send1:Send Config>list
Send Policy list for send1:
Idx T Prefix/Length/Match          OrgAS AnyAS Tag   MED
ASpad
1   I 1234::/16/R                   0     0     0     0

```

### Notas:

1. No habrá solicitudes para los parámetros de valor de *MED*, *prefijo-local*, *peso* y *métrica-IGP* en la política de recepción exclusiva. Se utilizarán valores de *MED* y *prefijo-local* a partir del anuncio recibido si están configurados como '0'. El valor '0' del parámetro de *peso* indica que debe ignorarse el valor de peso en el proceso de selección de rutas.

2. La solicitud de los valores de parámetro de *MED* y *número de rellenos de AS* sólo aparece en las políticas de envío inclusivas.

### Change

Utilice el mandato **change** para cambiar políticas dentro del mandato **update**.

#### Ejemplo:

Enter index of receive-policy to be modified [1]?

### Delete

Utilice el mandato **delete** para suprimir políticas dentro del mandato **update**.

#### Ejemplo:

Enter index of receive-policy to be deleted [1]?

### Move

Utilice el mandato **move** para trasladar políticas dentro del mandato **update**.

#### Ejemplo:

Enter index of receive-policy to move [1]?  
Move record after record number [0]?

### List

Utilice el mandato **list policy-list** para listar las políticas de recepción dentro del mandato **update**.

#### Ejemplo: list policy-list

```
Receive Policy list for rec1:
Idx T Prefix/Length/Match          OrgAS AnyAS MED  Weight
LP  IGPm
1  E 1234::/16/R                    0    0
2  I 5678::/16/R                    0    0    0    0
```

#### Ejemplo para las políticas de envío:

```
update policy-list
Name[]? nbr1-rcv
```

---

## Acceso al entorno de supervisión de BGP6

Para acceder al entorno de supervisión de BGP6, entre el mandato siguiente en el indicador +:

```
+ protocol bgp6
BGP6>
```

---

## Mandatos de supervisión de BGP6

Este apartado describe los mandatos de supervisión de BGP6. Estos mandatos le permiten modificar el comportamiento del protocolo BGP6 para que cumpla los requisitos específicos. Es necesaria una cierta cantidad de configuración para conseguir un direccionador de BGP6 completamente funcional. Entre los mandatos de supervisión de BGP6 en el indicador de supervisión BGP6>.

Tabla 124. Resumen de los mandatos de supervisión de BGP6	
Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi.
Disable neighbor	Inhabilita un contiguo determinado o todos los contiguos.
Dump routing tables	Lista el contenido de la tabla de direccionamiento de IPv6.
List	Lista todas las entradas de la tabla de direccionamiento de BGP.
Enable neighbor	Habilita un contiguo determinado o todos los contiguos.
Neighbors	Visualiza los contiguos que actualmente están activos.
Parameter	Visualiza los globales de BGP6 instalados del sistema BGP6.
Paths	Visualiza todas las vías de acceso disponibles de la base de datos.
Ping6	Envía peticiones con eco relativas a ICMP para otro sistema principal una vez por segundo y observa si hay respuesta. Este mandato puede utilizarse para identificar problemas en un entorno de interredes.
Policy-list	Visualiza la política instalada actualmente para un contiguo específico y estadísticas de la utilización de cada política.
Reset neighbor	Restablece un contiguo en particular.
Traceroute6	Visualiza la vía de acceso al completo (salto a salto) hacia un destino en particular.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

### Disable Neighbor

Utilice el mandato **disable neighbor** para inhabilitar un contiguo en particular o todos los contiguos que se han habilitado. Este mandato desactiva la sesión de BGP6 y elimina las rutas aprendidas a partir de ese contiguo.

#### Sintaxis:

**disable neighbor** *dirección IPv6 de contiguo*

**Ejemplo:**           **disable neighbor**

```
Enter a Neighbor address or :: for all neighbors []? ::
neighbor 2003:1::6105 disabled
```

## Dump Routing Tables

Para obtener una explicación completa del mandato **dump routing tables**, consulte el mandato **Dump Routing Tables** en la sección “Dump routing tables” en la página 504.

### Ejemplo:

Type	Dest net/Prefix	Cost	Age	Next hop(s)/Net
BGPR	2001:6::/64	0	193	IP64/0
BGPR	2001:7::/64	0	187	IP64/0
BGPR	2001:9::/64	0	200	IP64/0
BGPR	2001:17::/64	0	200	IP64/0
Dir*	2002:2::/64	1	7889	Eth/1
RIP6	2002:5::/64	3	10	FE80::220:35FF:FE45:2488
	Eth/1			
RIP6	2002:6::/64	2	10	FE80::220:35FF:FE45:2488
	Eth/1			
RIP6	2002:9::/64	2	10	FE80::220:35FF:FE45:2488
	Eth/1			
RIP6	2002:99::/64	3	10	FE80::220:35FF:FE45:2488
	Eth/1			
RIP6	2002:1111::/64	3	10	FE80::220:35FF:FE45:2488
	Eth/1			
Dir*	2003:1::/64	1	7889	IP64/0

IPv6 Routing table size: 768 nets (79872 bytes), 11 nets known  
 0 nets hidden, 0 nets deleted, 1 nets inactive  
 0 routes used internally, 756 routes free

## Enable Neighbor

Utilice el mandato **enable neighbor** para habilitar un contiguo en particular o habilitar todos los contiguos que se han inhabilitado. Este mandato empieza la sesión de BGP6 con un contiguo.

### Sintaxis:

**enable neighbor** *dirección IPv6 de contiguo*

### Ejemplo:

```
Enter a Neighbor address or :: for all neighbors []? ::
neighbor 2003:1::6105 enabled
```

## List

Utilice el mandato **list** para volcar todas las entradas de tabla de direccionamiento de BGP6 o bien para visualizar información sobre las rutas anunciadas a las direcciones BGP6 de contiguo especificadas (destinos) o las rutas recibidas de éstas.

### Sintaxis:

```
list all
      dst_network dirección de red
      rt_rcved_from_nbr dirección de red
      rt_sent_to_nbr dirección de red
```

**all**

### Ejemplo:

## Mandatos de supervisión de BGP6 (Talk 5)

```
BGP6> list all

MED   Weight LPref AAG AGRAS ORG AS-Path

0     0     0     No 0     IGP seq[2001]
Network/Prefixlen: 2001:6::/64
Next Hop:          2003:1::6105
Next Hop LLA:      FE80::3030:30FF:FE30:B

0     0     0     No 0     IGP seq[2001]
Network/Prefixlen: 2001:7::/64
Next Hop:          2003:1::6105
Next Hop LLA:      FE80::3030:30FF:FE30:B

0     0     0     No 0     IGP seq[2001]
Network/Prefixlen: 2001:9::/64
Next Hop:          2003:1::6105
Next Hop LLA:      FE80::3030:30FF:FE30:B

0     0     0     No 0     IGP seq[2001]
Network/Prefixlen: 2001:17::/64
Next Hop:          2003:1::6105
Next Hop LLA:      FE80::3030:30FF:FE30:B

0     0     0     No 0     IGP
Network/Prefixlen: 2002:2::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::

0     0     0     No 0     IGP
Network/Prefixlen: 2002:5::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::

0     0     0     No 0     IGP
Network/Prefixlen: 2002:6::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::

0     0     0     No 0     IGP
Network/Prefixlen: 2002:9::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::

0     0     0     No 0     IGP
Network/Prefixlen: 2002:99::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::

0     0     0     No 0     IGP
Network/Prefixlen: 2002:1111::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::
```

### **dst\_network** *dirección de red*

Visualiza información detallada sobre la red de destino o ruta especificada. El mandato muestra cómo se ha aprendido una ruta específica, la vía de acceso mejor hacia un destino específico, la métrica asociada con la ruta y otro tipo de información.

### **Ejemplo:**



```

BGP6>list dst_network
Destination network prefix []? 2002:1111::
Do you want specify prefix len? [No]: y
Prefix len (0-128) [64]?

Destination: 2002:1111::/64
          Age:30, Upd#:4, LastSent: 0002:10:17

Eligible paths: 1
PathID: 0 - (Best Path)
ASpath:
Origin: IGP, Pref: 0, LocalPref: 0
Metric: 0, Weight: 0, MED: 0
NextHop: 2002:2::6202
NextHop LLA: ::
Neighbor: 2002:2::6202
AtomicAggr: No

```

- ASpath** Enumeración de los sistemas autónomos de la vía de acceso.
- seq: Secuencia ordenada de los sistemas autónomos de la vía de acceso
  - set: Conjunto de sistemas autónomos de la vía de acceso
- Origin** El originador del destino. Es EGP, IGP o Incomplete (originado por algún otro medio desconocido).
- LocalPref** El grado de preferencia respecto al destino en el direccionador de origen.
- Metric** La métrica de vía de acceso con la que se importa la ruta.
- Weight** El peso de vía de acceso.
- MED** Un valor de discriminador de diversas salidas que se utiliza con el fin de efectuar una discriminación entre diversos puntos de entrada/salida respecto al mismo AS.
- NextHop** La dirección del direccionador a utilizar como dirección de reenvío para los destinos accesibles mediante la vía de acceso determinada.
- AtomicAggr** Indica si el direccionador que anuncia la vía de acceso ha incluido la vía de acceso en un agregado atómico.

**rt\_rcved\_from\_nbr** *dirección de red*  
 Lista todas las rutas recibidas del contiguo de BGP especificado.

**Ejemplo:**

## Mandatos de supervisión de BGP6 (Talk 5)

```
BGP6>list rt_rcved_from_nbr
BGP6 neighbor address []? 2003:1::6105

Destinations obtained from BGP6 neighbor 2003:1::6105

MED  Weight LPref AAG AGRAS ORG AS-Path

0 0 0 No 0 IGP seq[2001]
Network/Prefixlen: 2001:9::/64
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B

0 0 0 No 0 IGP seq[2001]
Network/Prefixlen: 2001:7::/64
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B

0 0 0 No 0 IGP seq[2001]
Network/Prefixlen: 2001:17::/64
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B

0 0 0 No 0 IGP seq[2001]
Network/Prefixlen: 2001:6::/64
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B
```

### **rt\_sent\_to\_nbr** *dirección de red*

Lista todas las rutas anunciadas al contiguo de BGP especificado.

#### **Ejemplo:**

```
BGP6>list rt_sent_to_nbr
BGP6 neighbor address []? 2003:1::6105

Destinations advertised to BGP6 neighbor 2003:1::6105

MED  Weight LPref AAG AGRAS ORG AS-Path

0 0 0 No 0 IGP
Network/Prefixlen: 2002:9::/64
Next Hop: 2002:2::6202
Next Hop LLA: ::

0 0 0 No 0 IGP
Network/Prefixlen: 2002:5::/64
Next Hop: 2002:2::6202
Next Hop LLA: ::

0 0 0 No 0 IGP
Network/Prefixlen: 2002:99::/64
Next Hop: 2002:2::6202
Next Hop LLA: ::

0 0 0 No 0 IGP
Network/Prefixlen: 2002:1111::/64
Next Hop: 2002:2::6202
Next Hop LLA: ::

0 0 0 No 0 IGP
Network/Prefixlen: 2002:6::/64
Next Hop: 2002:2::6202
Next Hop LLA: ::
```

## Neighbors

Utilice el mandato **neighbors** para visualizar información sobre todos los contiguos de BGP6 activos.

#### **Sintaxis:**

**neighbors** *dirección IPv6 de contiguo*

#### **Ejemplo:**

BGP6>neighbors

Address:	Status	State	DAY-HH:MM:SS	AS	Upd#
2003:1::6105	ENABLD	Established	000-00:03:42	2001	11
bgp6-ID: 20.1.7.5					

### IPv6-Address

Especifica la dirección IPv6 del contiguo de BGP6.

**State** Especifica el estado de la conexión. Los valores posibles son:

**Connect** En espera de que se complete la conexión TCP con el contiguo.

**Active** En el caso de anomalía de conexión TCP, el estado pasa a Active y continúa el intento de acceso al contiguo.

**OpenSent** En este estado, se ha enviado OPEN y BGP6 espera un mensaje OPEN del contiguo.

**OpenConfirm** En este estado, se ha enviado un mensaje KEEPALIVE como respuesta al mensaje OPEN del contiguo y se espera un mensaje KEEPALIVE/NOTIFICATION del contiguo.

**Established** Se ha establecido satisfactoriamente una conexión BGP6 y ahora puede empezar el intercambio de mensajes UPDATE.

**BGP-ID** Especifica el número de identificación de BGP6 del contiguo.

**AS** Especifica el número de AS del contiguo.

**Upd#** Especifica el número de secuencia del último mensaje UPDATE enviado al contiguo.

### dirección IPv6 de contiguo

Utilice el mandato **neighbor** para visualizar información detallada sobre un contiguo de BGP6 en particular.

**Ejemplo:**

## Mandatos de supervisión de BGP6 (Talk 5)

```
BGP6>neighbors 2000::662:0
Active Conn: None
Passve Conn: Sprt:179 Dprt:1026 State: Established KeepAlive/Hold Time: 30/90
TCP connection errors: 1 TCP state transitions: 1

BGP6 Messages: Sent Received Update: Sent Received
Open: 2 2 2 2
Notification: 1 0 KeepAlive: 2 2
Total Messages: 7 6

Msg Header Errs: Sent Received Bad msg length: Sent Received
Conn sync err: 0 0
Bad msg type: 0 0

Open Msg Errs: Sent Received Unsupp auth code: Sent Received
Unsupp versions: 0 0
Bad peer AS ident: 0 0 Auth failure: 0 0
Bad BGP ident: 0 0 Bad hold time: 0 0

Update Msg Errs: Sent Received AS routing loop: Sent Received
Bad attr list: 0 0
Bad wlkn attr: 0 0 Bad NEXT_HOP atr: 0 0
Mssng wlkn attr: 0 0 Optional atr err: 0 0
Attr flags err: 0 0 Bad netwrk field: 0 0
Attr length err: 0 0 Bad AS_PATH attr: 0 0
Bad ORIGIN attr: 0 0

Total Errors: Sent Received Hold Timer Exprd: Sent Received
Msg Header Errs: 0 0
Open Msg Errs: 0 0 FSM Errs: 0 0
Update Msg Errs: 0 0 Cease: 1 0
```

## Parameter

Utilice el mandato **parameter** de BGP6 para visualizar los globales de BGP6 instalados del sistema BGP6.

### Sintaxis:

**parameter**

### Ejemplo:

```
compare-med-from-diff-as is disabled.
IPv6-route-table-scan-timer value is 1 seconds.
```

## Paths

Utilice el mandato **paths** de BGP6 para visualizar las vías de acceso almacenadas en la base de datos de descripción de vías de acceso.

### Sintaxis:

**paths**

### Ejemplo:

```
paths
PathId MED AAG AGRAS RefCnt ORG AS_PATH

0 0 No 0 6 IGP
Next Hop: 2002:2::6202
Next Hop LLA: ::

1 0 No 0 2 IGP seq[2001]
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B

2 0 No 0 2 IGP seq[2001]
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B
```

<b>PathId</b>	Identificador de vía de acceso.
<b>NextHop</b>	La dirección del direccionador a utilizar como dirección de reenvío para los destinos accesibles mediante la vía de acceso determinada.
<b>MED</b>	El discriminador de diversas salidas que se utiliza con el fin de efectuar una discriminación entre diversos puntos de entrada/salida respecto al mismo AS.
<b>AAG</b>	Indica si se ha incluido la vía de acceso en un agregado atómico, es decir, si el direccionador que anuncia la vía de acceso determinada ha seleccionado una ruta menos específica antes que la más específica cuando se le han presentado rutas con solapa.
<b>AGRAS</b>	Indica el número de AS del altavoz de BGP6 que ha agregado las rutas.
<b>RefCnt</b>	Indica el número de entidades de vía de acceso referentes al descriptor.
<b>ORG</b>	Especifica el originador de los destinos anunciados de la vía de acceso determinada: EGP, IGP o Incomplete (originados por algún otro medio desconocido).
<b>AS Path</b>	Enumeración de los sistemas autónomos de la vía de acceso.
<b>seq:</b>	Secuencia ordenada de los sistemas autónomos de la vía de acceso.
<b>set:</b>	Conjunto de sistemas autónomos de la vía de acceso.

## Ping6

Para encontrar una explicación del mandato **ping6**, consulte “Ping6” en la página 508.

## Policy-List

Utilice el mandato **policy-list** para visualizar la política instalada actualmente para un contiguo específico y estadísticas de la utilización de cada política.

### Ejemplo:

```
BGP6>policy-list
Destination network prefix []? 2003:1::6105
Policy Type (Receive/Send/Origin) [All]?

Receive policy list for all neighbors:
Idx T Match OrgAS AdjAS IGPmet Usage Prefix
1 I Range 0 0 0 5 2001::/16

AS-PATH with following ASs will be discarded:

Send policy list for all neighbor:
Idx T Match TAG AdjAS Usage Prefix
1 I Range 0 0 11 2002::/16

Origin policy list for all neighbor:
Idx T Match Tag Usage Prefix
1 I Range 0 6 2002::/16
```

## Mandatos de supervisión de BGP6 (Talk 5)

```
BGP6>policy-list
Neighbor address []? 2000::1
Policy Type (Receive/Send/Origin) [All]? r

Receive policy list for neighbor '2000::1' :
Idx T Match OrgAS AnyAS MED Weight LPref IGPmet Usage Prefix
1 I Range 0 0 10 0 100 0 0 ::/0

BGP6>policy-list
Neighbor address []? 2000::1
Policy Type (Receive/Send/Origin) [All]? s

Send policy list for neighbor '2000::1' :
Idx T Match OrgAS AnyAS Tag MED ASpad Usage Prefix
1 I Range 0 0 0 30 0 0 ::/0

BGP6>policy-list
Neighbor address []? 2000::1
Policy Type (Receive/Send/Origin) [All]? o

Origin policy list for all neighbor:
Idx T Match Tag Usage Prefix
1 I Range 0 2 ::/0
```

## Reset Neighbor

Utilice el mandato **reset neighbor** para que, basándose en los parámetros de configuración de contiguo almacenados en la memoria de la configuración, restablezca el contiguo de BGP6 especificado.

### Sintaxis:

**reset neighbor** *dirección IPv6 de contiguo*

**Ejemplo:** **reset neighbor**

```
Enter a Neighbor address: []? 2003:1::6105
resetting neighbor 2003:1::6105
```

## Sizes

Utilice el mandato **sizes** de BGP6 para visualizar el número de entradas almacenadas en las diversas bases de datos.

### Sintaxis:

**sizes**

**Ejemplo:** **sizes**

```
# Paths: 10
# Path descriptors: 3
Update sequence#: 11
# Routing tbl entries (allocated): 10
# Current tbl entries (not imported): 0
# Current tbl entries (imported to IGP): 4
```

**Paths** El número total de vías de acceso elegibles para todas las rutas de la tabla de direccionamiento de BGP6.

### Path descriptors

El número total de descriptores de vía de acceso de la base de datos cuya finalidad es la de contener información de vía de acceso común.

**Update sequence#**

Indica el número de secuencia de actualización actual.

**Routing tbl entries (allocated)**

Indica el número de entradas de la tabla de direccionamiento de BGP6.

**Current tbl entries (not imported)**

Indica el número de rutas de BGP6 no importadas a IGP.

**Current tbl entries(imported to IGP)**

Indica el número de rutas de BGP6 importadas a IGP.

## Traceroute6

Para encontrar una explicación del mandato **traceroute6**, consulte “Traceroute6” en la página 509.

---

## Soporte de la reconfiguración dinámica de BGP6

Este apartado describe la reconfiguración dinámica (DR) tal como afecta a los mandatos Talk 6 y Talk 5.

### Mandato Delete Interface de CONFIG (Talk 6)

Border Gateway Protocol para IPv6 (BGP6) da soporte al mandato de CONFIG (Talk 6) **delete interface** con la consideración siguiente:

Suprime contiguos externos de BGP6 configurados si la dirección de contiguo tiene un prefijo de IPv6 común con una dirección IPv6 suprimida en esta interfaz.

### Mandato Activate Interface de GWCON (Talk 5)

El mandato de GWCON (Talk 5) **activate interface** no es aplicable en BGP6. BGP6 no tiene registros de SRAM asociados con una interfaz.

### Mandato Reset Interface de GWCON (Talk 5)

El mandato de GWCON (Talk 5) **reset interface** no es aplicable en BGP6. BGP6 no tiene registros de SRAM asociados con una interfaz.

### Mandatos Reset de GWCON (Talk 5) del componente

BGP6 da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos de BGP6:

**Mandato Reset Neighbor de GWCON, Protocol Bgp6**

**Descripción:** Añade o suprime un contiguo de BGP6. Cambia parámetros y políticas de contiguo.

**Efecto en la red:** La conexión de contiguo de BGP6 y las rutas aprendidas se actualizan basándose en el cambio de la configuración.

**Limitaciones:** Ninguna.

La tabla siguiente resume los cambios de la configuración de BGP6 que se activan cuando se invoca el mandato de **GWCON, protocol bgp6, reset neighbor**:

<b>Mandatos cuyos cambios se activan mediante el mandato reset neighbor de GWCON, protocolo bgp6</b>
CONFIG, protocolo BGP6, add neighbor
CONFIG, protocolo BGP6, change neighbor
CONFIG, protocolo BGP6, delete neighbor
CONFIG, protocolo BGP6, attach policy-to-neighbor
CONFIG, protocolo BGP6, change policy-to-neighbor
CONFIG, protocolo BGP6, delete policy-to-neighbor
CONFIG, protocolo BGP6, add policy-list
CONFIG, protocolo BGP6, update policy-list

## Mandatos de GWCON (Talk 5) de cambio temporal

BGP6 da soporte a los siguientes mandatos de GWCON que cambian temporalmente el estado operativo del dispositivo. Estos cambios se pierden siempre que se vuelve a cargar o a iniciar el dispositivo o siempre que se ejecuta un mandato reconfigurable dinámicamente.

<b>Mandatos</b>
GWCON, protocolo BGP6, enable neighbor
GWCON, protocolo BGP6, disable neighbor

## Mandatos no reconfigurables dinámicamente

La tabla siguiente describe los mandatos de configuración de BGP6 que no pueden cambiarse dinámicamente. Para activar estos mandatos, tiene que volver a cargar o a iniciar el dispositivo.

<b>Mandatos</b>
CONFIG, protocolo BGP6, enable bgp6
CONFIG, protocolo BGP6, disable bgp6
CONFIG, protocolo BGP6, add no-receive
CONFIG, protocolo BGP6, delete no-receive
CONFIG, protocolo BGP6, add/change/delete/move aggregate
CONFIG, protocolo BGP6, add/change/delete/move originate-policy
CONFIG, protocolo BGP6, add/change/delete/move receive-policy
CONFIG, protocolo BGP6, add/change/delete/move send-policy
CONFIG, protocolo BGP6, enable compare-med-from-diff-as
CONFIG, protocolo BGP6, set ipv6-route-table-scan-timer



---

## Apéndice A. Tamaños de los paquetes

Este apéndice define los tamaños de los paquetes para las diversas redes y protocolos soportados. Incluye los apartados siguientes:

- Datos generales
- Límites de tamaño específicos de las redes
- Límites de tamaño específicos de los protocolos
- Cómo cambiar los tamaños máximos de los paquetes

---

### Datos generales

Remitiéndonos al propósito de este tema, los paquetes que manejan los direccionadores están compuestos por datos de usuario e información de cabecera.

La cantidad de datos de usuario que puede contener un paquete está limitada por la cantidad de información de cabecera del paquete. La cantidad de información de cabecera depende de lo siguiente (como mínimo):

- Los tipos de redes por donde debe pasar el paquete.
- Los protocolos que se utilizan en estas redes.

Los factores siguientes afectan al tamaño del contenido del paquete:

- La longitud de la información de cabecera de enlace de datos que el tipo e interfaz de red actuales requieren que tenga el paquete.
- La longitud de la información de cola (si la hay) que el tipo e interfaz de red actuales requieren que tenga el paquete.

En cualquier red, la suma del tamaño máximo de datos más el tamaño de la cabecera y el de la cola será equivalente al tamaño máximo de paquete de la red. Cuando se direcciona entre redes con tamaños máximos de paquete diferentes, puede producirse la fragmentación del paquete.

---

### Límites de tamaño específicos de las redes

Dada la información del apartado anterior, puede determinarse la cantidad máxima de datos de capa de red soportada por cada capa de enlace de datos (interfaz de red). La Tabla 125 en la página 592 lista los tamaños máximos de paquete por omisión de los tipos de interfaces más comunes.

Tabla 125. Tamaño máximo por omisión de paquete específico de la red

Tipo de red (enlace de datos)	Tamaño máx. de paquete de capa de red (bytes)	Longitud de la cabecera de red	Información de la cola
Red en Anillo 4 Mbps	2052	22	0
Red en Anillo 16 Mbps	2052	22	0
Ethernet	1500	18	4
PPP	2046	2	0
Frame Relay	2048 (vea las notas)	variable	2

**Nota:** Para las interfaces Frame Relay, se configura el tamaño máximo de trama y no el tamaño máximo de paquete de capa de red. Si desea determinar el tamaño máximo de paquete de capa de red para un protocolo, consulte la descripción del mandato **set frame-size** en el capítulo titulado Configuración y supervisión de las interfaces Frame Relay dentro de la publicación *Nways Multiprotocol Access Services Guía del usuario de software*.

**Nota:** Puede cambiar el tamaño máximo de paquete de las interfaces que no sean Ethernet. Utilice el mandato **network** desde el indicador Config> para acceder a los mandatos de configuración de la interfaz.

El tamaño máximo de paquete es la cantidad máxima de datos que el reenviador del protocolo puede pasar al dispositivo.

**Nota:** Estos números corresponden a las MTU de UNIX de BSD 4.2.

En un paquete de IP se incluyen la cabecera de IP, la cabecera de UDP o TCP y todos los datos.

El tamaño de paquete en uso se visualiza cuando se utiliza el mandato memory del direccionador en GWCON. El tamaño de "Pkt" es el tamaño de paquete de capa de red. Los tamaños de Hdr (cabecera) y Tlr (cola) dependen de las redes y sus interfaces de red.

---

## Límites de tamaño específicos de los protocolos

Este apartado explica los límites de tamaño específicos de los protocolos.

### Longitudes de paquete de IP

Las especificaciones del protocolo IP no requieren que una implementación de IP de sistema principal acepte paquetes de IP de más de 576 octetos; no obstante, las implementaciones de IP de direccionador deben incluir paquetes de IP de cualquier longitud hasta los límites impuestos por los paquetes específicos de las redes en uso.

Además, el protocolo IP de direccionador realiza la fragmentación transparente y el reensamblaje de paquetes que, de lo contrario, sobrepasarían las restricciones de longitud específicas de las redes, tal como requiere la especificación de IP.

Las discrepancias entre los tamaños de los paquetes no causan problemas de conectividad. No obstante, el reensamblaje de los fragmentos impone una carga en el rendimiento, por lo que debe evitarse la fragmentación siempre que sea posible.

---

### Cómo cambiar los tamaños máximos de los paquetes

Normalmente, el direccionador establece de manera automática el tamaño máximo de paquete de capa de red en el tamaño del paquete más grande posible de todas las redes conectadas. A continuación, añade las cabeceras y colas requeridas por las redes para determinar el tamaño de almacenamiento intermedio interno, que es superior al tamaño de capa de red.

Algunas redes (Red en Anillo 4 Mbps y Red en Anillo 16 Mbps) permiten que el usuario configure tamaños máximos de paquete. La configuración de tamaños máximos de paquete afecta al tamaño de los almacenamientos intermedios utilizados en el direccionador, lo que, a su vez, afecta al número de almacenamientos intermedios disponibles para un tamaño de memoria determinado. Los direccionadores determinan de manera automática qué tamaño de almacenamiento intermedio se va a necesitar. El usuario puede cambiar el tamaño máximo de paquete de capa de red que maneja el direccionador por medio del mandato `set packet-size`; no obstante, no utilice este mandato a menos que se lo indique específicamente el Servicio al cliente.

## Tamaños de los paquetes

---

## Apéndice B. Lista de Abreviaturas

<b>AARP</b>	AppleTalk Address Resolution Protocol
<b>ABR</b>	Direccionador de frontera de área
<b>ack</b>	Acuse de recibo
<b>AIX</b>	Advanced Interactive Executive
<b>AMA</b>	Direccionamiento del MAC arbitrario
<b>AMP</b>	Supervisor presente activo
<b>ANSI</b>	American National Standards Institute
<b>AP2</b>	AppleTalk Phase 2
<b>APPN</b>	Advanced Peer-to-Peer Networking
<b>ARE</b>	Explorador de todas las rutas
<b>ARI</b>	Interfaz ATM real
<b>ARI/FCI</b>	Indicador de dirección reconocida/indicador de trama copiada
<b>ARP</b>	Address Resolution Protocol
<b>AS</b>	Sistema autónomo
<b>ASBR</b>	Direccionador de frontera de sistema autónomo
<b>ASCII</b>	American National Standard Code for Information Interchange
<b>ASN.1</b>	Notación de sintaxis de abstracción 1
<b>ASRT</b>	Direccionamiento transparente de origen adaptable
<b>ASYNC</b>	Asíncrono
<b>ATCP</b>	AppleTalk Control Protocol
<b>ATP</b>	AppleTalk Transaction Protocol
<b>AUI</b>	Interfaz de unidad de conexión
<b>AVI</b>	Interfaz ATM virtual
<b>ayt</b>	¿Hay alguien ahí?
<b>BAN</b>	Boundary Access Node
<b>BBCM</b>	Bridging Broadcast Manager
<b>BECN</b>	Notificación de congestión explícita hacia atrás
<b>BGP</b>	Border Gateway Protocol
<b>BNC</b>	Bayonet Niell-Concelman
<b>BNCP</b>	Bridging Network Control Protocol
<b>BOOTP</b>	Protocolo BOOT
<b>BPDU</b>	Unidad de datos de protocolo de puente
<b>bps</b>	Bits por segundo
<b>BR</b>	Función de puente/direccionamiento

<b>BRS</b>	Reserva de ancho de banda
<b>BSD</b>	Distribución de software de Berkeley
<b>BTP</b>	Agente de relay de BOOTP
<b>BTU</b>	Unidad básica de transmisión
<b>CAM</b>	Memoria dirigible a través del contenido
<b>CCITT</b>	Comisión Consultiva de la Telefonía y Telegrafía Internacionales
<b>CD</b>	Detección de colisión
<b>CGWCON</b>	Consola de pasarela
<b>CIDR</b>	Direccionamiento entre dominios sin clase
<b>CIP</b>	IP clásico
<b>CIR</b>	Velocidad de información comprometida
<b>CLNP</b>	Connectionless-Mode Network Protocol
<b>CPU</b>	Unidad central de proceso
<b>CRC</b>	Comprobación de redundancia cíclica
<b>CRS</b>	Servidor de informes de configuración
<b>CTS</b>	Preparado para transmitir
<b>CUD</b>	Datos de usuario de llamada
<b>DAF</b>	Filtración de direcciones de destino
<b>DB</b>	Base de datos
<b>DBsum</b>	Resumen de la base de datos
<b>DCD</b>	Detector de señal de línea recibida de canal de datos
<b>DCE</b>	Equipo de terminación de circuito de datos
<b>DCS</b>	Servidor conectado directamente
<b>DDLC</b>	Controlador de enlace de datos dual
<b>DDN</b>	Defense Data Network
<b>DDP</b>	Datagram Delivery Protocol
<b>DDT</b>	Dynamic Debugging Tool
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>dir</b>	Conectado directamente
<b>DL</b>	Enlace de datos
<b>DLC</b>	Control de enlace de datos
<b>DLCI</b>	Identificador de conexión de enlace de datos
<b>DLS</b>	Conmutación del enlace de datos
<b>DLSw</b>	Conmutación del enlace de datos
<b>DMA</b>	Acceso de memoria directo
<b>DNA</b>	Digital Network Architecture
<b>DNCP</b>	DECnet Protocol Control Protocol

<b>DNIC</b>	Código de identificador de red de datos
<b>DdD</b>	Departamento de Defensa
<b>DOS</b>	Disk Operating System
<b>DR</b>	Direccionador designado
<b>DRAM</b>	Memoria de acceso aleatorio dinámica
<b>DSAP</b>	Punto de acceso a servicios de destino
<b>DSE</b>	Equipo de conmutación de datos
<b>DSE</b>	Intercambio de conmutaciones de datos
<b>DSR</b>	Aparato de datos preparado
<b>DSU</b>	Unidad de servicio de datos
<b>DTE</b>	Equipo terminal de datos
<b>DTR</b>	Terminal de datos preparado
<b>Dtype</b>	Tipo de destino
<b>DVMRP</b>	Distance Vector Multicast Routing Protocol
<b>E&amp;M</b>	Ear & Mouth
<b>E1</b>	Velocidad de transmisión de 2,048 Mbps
<b>EDEL</b>	Delimitador de final
<b>EDI</b>	Indicador de errores detectados
<b>EGP</b>	Exterior Gateway Protocol
<b>EIA</b>	Electronics Industries Association
<b>ELAN</b>	LAN emulada
<b>ELAP</b>	EtherTalk Link Access Protocol
<b>ELS</b>	Sistema de anotación cronológica de sucesos
<b>ELSCon</b>	Consola secundaria de ELS
<b>ESI</b>	Identificador de sistema final
<b>EST</b>	Horario Estándar del Este de los EE.UU
<b>Eth</b>	Ethernet
<b>fa-ga</b>	Dirección funcional-dirección de grupo
<b>FCS</b>	Secuencia de comprobación de trama
<b>FECN</b>	Notificación de congestión explícita hacia adelante
<b>FIFO</b>	Primero en entrar, primero en salir
<b>FLT</b>	Biblioteca de filtros
<b>FR</b>	Frame Relay
<b>FRL</b>	Frame Relay
<b>FTP</b>	File Transfer Protocol
<b>FXO</b>	Oficina de Divisas
<b>FXS</b>	Estación de Divisas

<b>GMT</b>	Hora Media de Greenwich
<b>GOSIP</b>	Perfil de Interconexión de Sistemas Abiertos del Gobierno
<b>GTE</b>	Compañía Telefónica General
<b>GWCON</b>	Consola de pasarela
<b>HDLC</b>	Control de enlace de datos de alto nivel
<b>HEX</b>	Hexadecimal
<b>HPR</b>	Direccionamiento de alto rendimiento
<b>HST</b>	Servicios de sistema principal de TCP/IP
<b>HTF</b>	Formato de tabla de sistema principal
<b>IBD</b>	Dispositivo de arranque integrado
<b>ICMP</b>	Internet Control Message Protocol
<b>ICP</b>	Internet Control Protocol
<b>ID</b>	Identificación
<b>IDP</b>	Parte de dominio inicial
<b>IDP</b>	Internet Datagram Protocol
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>Ifc#</b>	Número de interfaz
<b>IGP</b>	Interior Gateway Protocol
<b>InARP</b>	Inverse Address Resolution Protocol
<b>IP</b>	Internet Protocol
<b>IPCP</b>	IP Control Protocol
<b>IPPN</b>	IP Protocol Network
<b>IPX</b>	Internetwork Packet Exchange
<b>IPXCP</b>	IPX Control Protocol
<b>RDSI</b>	Red digital de servicios integrados
<b>ISO</b>	Organización Internacional para la Normalización
<b>Kbps</b>	Kilobits por segundo
<b>LAC</b>	Concentrador del acceso a la red L2TP
<b>LAN</b>	Red de área local
<b>LAPB</b>	Protocolo de acceso a enlace equilibrado
<b>LAT</b>	Transporte de área local
<b>LCS</b>	Estación de canal de LAN
<b>LCP</b>	Link Control Protocol
<b>LED</b>	Diodo emisor de luz
<b>LF</b>	Trama mayor; salto de línea
<b>LIS</b>	Subred IP lógica
<b>LLC</b>	Control de enlace lógico



<b>LLC2</b>	Control de enlace lógico 2
<b>LMI</b>	Interfaz de gestión local
<b>LNS</b>	Servidor de red L2TP
<b>LRM</b>	Mecanismo de información de LAN
<b>LS</b>	Estado de los enlaces
<b>LSA</b>	Notificación del estado de los enlaces
<b>LSA</b>	Link Services Architecture
<b>LSB</b>	Bit menos significativo
<b>LSI</b>	Interfaz de métodos abreviados de LAN
<b>LSreq</b>	Petición del estado de los enlaces
<b>LSrxl</b>	Lista de retransmisiones del estado de los enlaces
<b>LU</b>	Unidad lógica
<b>MAC</b>	Control del acceso al medio
<b>Mb</b>	Megabit
<b>MB</b>	Megabyte
<b>Mbps</b>	Megabits por segundo
<b>MBps</b>	Megabytes por segundo
<b>MC</b>	Vertimiento múltiple
<b>MCF</b>	Filtración del MAC
<b>MIB</b>	Base de la información de gestión
<b>MIB II</b>	Base de la información de gestión II
<b>MILNET</b>	Red militar
<b>MOS</b>	Micro Operating System
<b>MOSDBG</b>	Micro Operating System Debugging Tool
<b>MOSPF</b>	Open Shortest Path First con extensiones de vertimiento múltiple
<b>MPC</b>	Canal de diversas vías de acceso
<b>MPC+</b>	Canal de diversas vías de acceso de transferencia de datos de alto rendimiento (HPDT)
<b>MSB</b>	Bit más significativo
<b>MSDU</b>	Unidad de datos de servicio MAC
<b>MRU</b>	Unidad máxima de recepción
<b>MTU</b>	Unidad máxima de transmisión
<b>nak</b>	Sin acuse de recibo
<b>NAS</b>	Estación Nways Switch Administration
<b>NBMA</b>	Acceso múltiple sin difusión
<b>NBP</b>	Name Binding Protocol
<b>NBR</b>	Direccionador contiguo

<b>NCP</b>	Network Control Protocol
<b>NCP</b>	Network Core Protocol
<b>NDPS</b>	Conmutación de vías de acceso sin interrupciones
<b>NetBIOS</b>	Network Basic Input/Output System
<b>NHRP</b>	Next Hop Resolution Protocol
<b>NIST</b>	National Institute of Standards and Technology
<b>NPDU</b>	Unidad de datos de protocolo de red
<b>NRZ</b>	Sin vuelta a cero
<b>NRZI</b>	Sin vuelta a cero invertido
<b>NSAP</b>	Punto de acceso a servicios de red
<b>NSF</b>	National Science Foundation
<b>NSFNET</b>	National Science Foundation NETwork
<b>NVCNFG</b>	Configuración permanente
<b>OOS</b>	Fuera de servicio
<b>OPCON</b>	Consola del operador
<b>OSI</b>	Interconexión de sistemas abiertos
<b>OSICP</b>	OSI Control Protocol
<b>OSPF</b>	Open Shortest Path First
<b>OUI</b>	Identificador exclusivo de organización
<b>PC</b>	Personal Computer
<b>PCA</b>	Adaptador de canal paralelo
<b>PCR</b>	Velocidad punta de célula
<b>PDN</b>	Red de datos pública
<b>PING</b>	Sonda de paquetes InterNet
<b>PDU</b>	Unidad de datos de protocolo
<b>PID</b>	Identificación de proceso
<b>P-P</b>	Punto a punto
<b>PPP</b>	Point-to-Point Protocol
<b>PROM</b>	Memoria de sólo lectura programable
<b>PU</b>	Unidad física
<b>PVC</b>	Circuito virtual permanente
<b>RAM</b>	Memoria de acceso aleatorio
<b>RD</b>	Descriptor de ruta
<b>REM</b>	Supervisor de errores de anillo
<b>REV</b>	Recepción
<b>RFC</b>	Request for Comments
<b>RI</b>	Indicador de llamada; información de direccionamiento

<b>RIF</b>	Campo de información de direccionamiento
<b>RII</b>	Indicador de información de direccionamiento
<b>RIP</b>	Routing Information Protocol
<b>RISC</b>	Sistema de juego reducido de instrucciones
<b>RNR</b>	Recepción no preparada
<b>ROM</b>	Memoria de sólo lectura
<b>ROpcon</b>	Consola del operador remota
<b>RPS</b>	Servidor de parámetros de anillo
<b>RTMP</b>	Routing Table Maintenance Protocol
<b>RTP</b>	RouTing update Protocol
<b>RTS</b>	Petición de emisión
<b>Rtype</b>	Tipo de ruta
<b>rxmits</b>	Retransmisiones
<b>rxmt</b>	Retransmisión
<b>s</b>	Segundo
<b>SAF</b>	Filtración de direcciones de origen
<b>SAP</b>	Punto de acceso a servicios
<b>SAP</b>	Service Advertising Protocol
<b>SCR</b>	Velocidad sostenida de célula
<b>SCSP</b>	Server Cache Synchronization Protocol
<b>sdel</b>	Delimitador de inicio
<b>SDLC</b>	Relay de SDLC, control síncrono de enlace de datos
<b>seqno</b>	Número de secuencia
<b>SGID</b>	Identificación de grupo de servidores
<b>SGMP</b>	Simple Gateway Monitoring Protocol
<b>SL</b>	Línea serie
<b>SMP</b>	Supervisor presente en espera
<b>SMTP</b>	Simple Mail Transfer Protocol
<b>SNA</b>	Systems Network Architecture
<b>SNAP</b>	Subnetwork Access Protocol
<b>SNMP</b>	Simple Network Management Protocol
<b>SNPA</b>	Punto de conexión de subred
<b>SPF</b>	Ruta intraárea OSPF
<b>SPE1</b>	Tipo 1 de ruta externa OSPF
<b>SPE2</b>	Tipo 2 de ruta externa OSPF
<b>SPIA</b>	Tipo de ruta interárea OSPF
<b>SPID</b>	Identificación de perfil de servicio

<b>SPX</b>	Sequenced Packet Exchange
<b>SQE</b>	Error en calidad de señal
<b>SRAM</b>	Memoria de acceso aleatorio estática
<b>SRB</b>	Puente de direccionamiento de origen
<b>SRF</b>	Trama específicamente direccionada
<b>SRLY</b>	Relay de SDLC
<b>SRT</b>	Direccionamiento transparente de origen
<b>SR-TB</b>	Puente de direccionamiento transparente de origen
<b>STA</b>	Estático
<b>STB</b>	Puente de árbol de expansión
<b>STE</b>	Explorador de árbol de expansión
<b>STP</b>	Par trenzado y apantallado; protocolo de árbol de expansión
<b>SVC</b>	Circuito virtual conmutado
<b>TB</b>	Puente transparente
<b>TCN</b>	Notificación de cambio de topología
<b>TCP</b>	Transmission Control Protocol
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol
<b>TEI</b>	Identificador de punto de terminal
<b>TFTP</b>	Trivial File Transfer Protocol
<b>TKR</b>	Red en Anillo
<b>TMO</b>	Tiempo de espera excedido
<b>TOS</b>	Tipo de servicio
<b>TSF</b>	Tramas de expansión transparentes
<b>TTL</b>	Período de duración
<b>TTY</b>	Teletipo
<b>TX</b>	Transmisión
<b>UA</b>	Acuse de recibo sin número
<b>UDP</b>	User Datagram Protocol
<b>UI</b>	Información sin número
<b>UTP</b>	Par trenzado y no apantallado
<b>VCC</b>	Conexión de canal virtual
<b>VINES</b>	Virtual NETworking System
<b>VIR</b>	Velocidad de información variable
<b>VL</b>	Enlace virtual
<b>VNI</b>	Virtual Network Interface
<b>VoFR</b>	Voz sobre Frame Relay
<b>VR</b>	Ruta virtual

<b>WAN</b>	Red de área amplia
<b>WRS</b>	Redireccionamiento/restauración de WAN
<b>X.25</b>	Redes de paquetes conmutados
<b>X.251</b>	Capa física de X.25
<b>X.252</b>	Capa de trama de X.25
<b>X.253</b>	Capa de paquetes de X.25
<b>XID</b>	Identificación de intercambio
<b>XNS</b>	Xerox Network Systems
<b>XSUM</b>	Suma de comprobación
<b>ZIP</b>	AppleTalk Zone Information Protocol
<b>ZIP2</b>	AppleTalk Zone Information Protocol 2
<b>ZIT</b>	Tabla de información de zonas



---

## Glosario

Este glosario incluye términos y definiciones de la documentación siguiente:

- El *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 del American National Standards Institute (ANSI). Los ejemplares pueden adquirirse en el American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Las definiciones se identifican mediante el símbolo (A) que aparece después de la definición.
- La *Fiber Optic Terminology*, norma ANSI/EIA 440-A. Los ejemplares pueden adquirirse en la Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006. Las definiciones se identifican mediante el símbolo (E) que aparece después de la definición.
- El *Information Technology Vocabulary* desarrollado por la Subcomisión 1, Comisión Técnica Mixta 1, de la Organización Internacional para la Normalización y la Comisión Electrotécnica Internacional (JTC1/SC1 de la ISO/IEC). Las definiciones de las secciones publicadas de este vocabulario se identifican mediante el símbolo (I) que aparece después de la definición; las definiciones de los borradores de normas internacionales, borradores de comisiones y documentos de trabajo que está desarrollando la JTC1/SC1 de la ISO/IEC se identifican mediante el símbolo (T) que aparece después de la definición, símbolo que indica que las Corporaciones Nacionales de la SC1 participantes todavía no han llegado a un acuerdo definitivo.
- El *IBM Dictionary of Computing*, New York: McGraw-Hill, 1994.
- Internet Request for Comments: 1208, *Glossary of Networking Terms*
- Internet Request for Comments: 1392, *Internet Users' Glossary*
- El *Object-Oriented Interface Design: IBM Common User Access Guidelines*, Carmel, Indiana: Que, 1992.

En este glosario, se utilizan las siguientes referencias cruzadas:

**Compárese con:** Se refiere a un término que tiene un significado opuesto o esencialmente distinto.

**Sinónimo de:** Indica que el término tiene el mismo significado que un término preferente, el cual está definido en el lugar que le corresponde dentro del glosario.

**Sinónimo con:** Es una referencia hacia atrás de un término definido a los otros términos que tienen el mismo significado.

**Véase:** Remite al lector a términos de diversas palabras que tienen la misma palabra al principio.

**Véase también:** Remite al lector a términos que tienen un significado relacionado, pero no sinónimo.

## A

**AAL-5.** Capa de adaptación de ATM 5, una de las diversas AAL estándares. AAL-5 se ha diseñado para las comunicaciones de datos, y la utilizan la Emulación de LAN y el IP clásico.

**AAL.** Capa de adaptación de ATM, que es la que adapta los datos de usuario a/de la red ATM añadiendo/eliminando cabeceras y segmentando/volviendo a ensamblar los datos en/a partir de células.

**acceso de memoria directo (DMA).** Recurso del sistema que permite que un dispositivo del bus Micro Channel obtenga acceso directo a la memoria del sistema o a la memoria del bus sin la intervención del procesador del sistema.

**acceso múltiple con detección de portadora y detección de colisión (CSMA/CD).** Protocolo que necesita detección de portadora y en el que una estación de datos transmisora que detecta otra señal mientras transmite detiene la emisión, envía una señal de atasco y luego espera durante un período variable antes de volver a intentar la acción. (T) (A)

**ACCESS.** En el protocolo Simple Network Management Protocol (SNMP), cláusula de un módulo de la Base de la información de gestión (MIB) que define el nivel mínimo de soporte que proporciona un nodo gestionado para un objeto.

**activo.** (1) Operativo. (2) Perteneciente a un nodo o dispositivo que está conectado o está disponible para la conexión con otro nodo o dispositivo.

**actualización de base de datos de topología (TDU).** Mensaje sobre un nodo o enlace nuevo o modificado que se difunde entre los nodos de red APPN para mantener la base de datos de topología de red, que está reproducida en su totalidad en cada nodo de red. Una TDU contiene información para identificar lo siguiente:

- El nodo emisor.
- Las características de nodo y enlace de diversos recursos de la red.
- El número de secuencia de la actualización más reciente para cada uno de los recursos descritos.

**acuse de recibo.** (1) Transmisión, por parte de un receptor, de caracteres de acuse de recibo como respuesta afirmativa a un remitente. (T) (2) Indicación de que se ha recibido un elemento enviado.

**Address Resolution Protocol (ARP).** (1) En el conjunto de protocolos de Internet, protocolo que correlaciona dinámicamente una dirección IP con una dirección utilizada por una red de área metropolitana o local de soporte, como, por ejemplo, Ethernet o Red en Anillo. (2) Véase también *Reverse Address Resolution Protocol (RARP)*.

**Advanced Peer-to-Peer Networking (APPN).** Extensión de SNA que ofrece (a) un control superior de las redes distribuidas que evita las dependencias jerárquicas críticas y, por lo tanto, aísla los efectos de puntos anómalos individuales; (b) intercambio dinámico de información de topología de red para facilitar la conexión, reconfiguración y selección de rutas adaptables; (c) definición dinámica de recursos de red; y (d) automatización en el registro de recursos y la búsqueda en directorios. APPN hace extensiva la orientación de igual de la LU 6.2 para los servicios de usuario final al control de redes y da soporte a diversos tipos de LU, incluidas la LU 2, la LU 3 y la LU 6.2.

**agencia operativa privada reconocida (RPOA).** Cualquier individuo, empresa o corporación (que no sea un departamento o servicio del gobierno) que realiza operaciones en un servicio de telecomunicaciones y está sujeta a las obligaciones definidas en el Convenio de la Unión de Telecomunicaciones Internacionales y en la legislación; por ejemplo, una empresa de telecomunicación.

**agente.** Sistema que asume un papel de agente.

**alerta.** Mensaje enviado a un punto focal de servicios de gestión de una red para identificar un problema o un problema inminente.

**American National Standards Institute (ANSI).** Organización compuesta por productores, clientes y grupos con intereses generales que establece los procedimientos mediante los cuales organizaciones acreditadas crean y mantienen normas voluntarias de la industria en los Estados Unidos. (A)

**analógico.** (1) Perteneciente a datos compuestos por cantidades físicas continuamente variables. (A)  
(2) Compárese con *digital*.

**ancho de banda.** El ancho de banda de un enlace óptico designa la capacidad de contener información del enlace y está relacionado con la máxima velocidad en bits a la que puede dar soporte un enlace de fibra.

**anillo.** Véase *red de tipo anillo*.

**anomalía en la autenticación.** En el protocolo Simple Network Management Protocol (SNMP), detección (de condición de excepción) que una entidad de autenticación puede haber generado cuando un cliente petionario no es miembro de la comunidad de SNMP.

**antememoria.** (1) Almacenamiento intermedio de fines especiales más pequeño y rápido que el almacenamiento principal; se utiliza para que contenga una copia de instrucciones y datos obtenidos del almacenamiento principal y que probablemente necesitará a continuación el procesador. (T) (2) Almacenamiento intermedio que contiene instrucciones y datos a los que se accede frecuentemente; se utiliza para reducir el tiempo del acceso. (3) Parte opcional de la base de datos de directorios existente en los nodos de red donde puede almacenarse información de directorios de uso frecuente para acelerar las búsquedas en directorios. (4) Colocar, ocultar o almacenar en antememoria.

**aparato de datos preparado (DSR).** Sinónimo de *DCE preparado*.

**AppleTalk.** Protocolo de red desarrollado por Apple Computer, Inc. Este protocolo se utiliza para la interconexión de dispositivos de red, que pueden ser una mezcla de productos Apple y productos que no son Apple.

**AppleTalk Address Resolution Protocol (AARP).** En redes AppleTalk, protocolo que (a) convierte las direcciones de nodo AppleTalk en direcciones de hardware y (b) soluciona las discrepancias de direccionamiento en las redes que dan soporte a más de un conjunto de protocolos.

**AppleTalk Transaction Protocol (ATP).** En redes AppleTalk, protocolo que proporciona funciones de petición y respuesta de cliente/servidor a los sistemas principales que acceden al protocolo Zone Information Protocol (ZIP) para la información de zonas.

**árbol de expansión.** En contextos de LAN, método mediante el cual los puentes desarrollan automáticamente una tabla de direccionamiento y actualizan esta tabla en respuesta a un cambio de la topología para asegurarse de la existencia de una sola ruta entre dos LAN cualesquiera en la red con puentes. Este método evita bucles de paquetes, donde un paquete vuelve en una ruta de circuito al direccionador emisor.

**archivo de configuración.** Archivo que especifica las características de un dispositivo del sistema o una red.

**área.** En los protocolos de direccionamiento de Internet y DECnet, subconjunto de una red o pasarela que se ha agrupado por definición del administrador de red. Cada área es independiente; la información sobre la topología de un área permanece oculta respecto a las otras áreas.



**arquitectura de red.** Estructura lógica y principios operativos de una red de sistema. (T)

**Nota:** Los principios operativos de una red incluyen los principios de los servicios, funciones y protocolos.

**arquitectura Interconexión de Sistemas Abiertos (OSI).** Arquitectura de red que se ajusta al conjunto particular de normas ISO relacionado con Interconexión de Sistemas Abiertos. (T)

**arreglo temporal del programa (PTF).** Solución o ajuste temporal de un problema diagnosticado por IBM del release actual no modificado del programa.

**asequibilidad.** Capacidad de un nodo o recurso para comunicarse con otro nodo o recurso.

**asíncrono (ASYN).** Perteneciente a dos o más procesos que no dependen de la aparición de sucesos específicos, como, por ejemplo, señales comunes de temporización. (T)

**ATM.** Asynchronous Transfer Mode, tecnología de red de gran velocidad orientada a las conexiones que se basa en la conmutación de células.

**ATMARP.** ARP en el IP clásico.

## B

**base de datos de configuración (CDB).** Base de datos que almacena los parámetros de configuración de uno o diversos dispositivos. Se prepara y actualiza utilizando el programa de configuración.

**Base de la información de gestión (MIB).** (1) Conjunto de objetos a los que se puede acceder por medio de un protocolo de gestión de red. (2) Definición de información de gestión que especifica la información disponible de un sistema principal o una pasarela y las operaciones permitidas. (3) En OSI, depósito conceptual de información de gestión dentro de un sistema abierto.

**baudio.** En la transmisión asíncrona, unidad de velocidad de modulación correspondiente al intervalo de una unidad por segundo; es decir, si la duración del intervalo de la unidad es de 20 milisegundos, la velocidad de modulación es de 50 baudios. (A)

**bit D.** Bit de confirmación de entrega. En comunicaciones X.25, bit de un paquete de datos o paquete de petición de llamada que se establece en 1 si el destinatario necesita acuse de recibo (confirmación de entrega) de extremo a extremo.

**Border Gateway Protocol (BGP).** Protocolo de direccionamiento de Internet Protocol (IP) utilizado entre dominios y sistemas autónomos.

**bucle de direccionamiento.** Situación que ocurre cuando los direccionadores hacen circular información entre ellos hasta que se produce la convergencia o hasta que se consideran inasequibles las redes implicadas.

## C

**cabecera.** (1) Información de control definida por el sistema que precede a los datos de usuario. (2) Parte de un mensaje que contiene información de control para el mismo, como, por ejemplo, uno o más campos de destino, el nombre de la estación de origen, el número de secuencia de entrada, una serie de caracteres que indica el tipo de mensaje y el nivel de prioridad del mensaje.

**cabecera de transmisión (TH).** Información de control, seguida opcionalmente de una unidad básica de información (BIU) o de un segmento de BIU, que crea y utiliza el control de la vía de acceso para direccionar unidades de mensajes y controlar su flujo dentro de la red. Véase también *unidad de información de vía de acceso*.

**canal.** (1) Vía de acceso por la que pueden enviarse señales, como, por ejemplo, canal de datos, canal de salida. (A) (2) Unidad funcional, controlada por el procesador, que maneja la transferencia de datos entre el almacenamiento del procesador y el equipo de periféricos local.

**canal de diversas vías de acceso (MPC).** Protocolo de canal que utiliza diversos subcanales unidireccionales para la comunicación bidireccional de VTAM a VTAM.

**canal de entrada/salida.** En un sistema de proceso de datos, unidad funcional que maneja la transferencia de datos entre el equipo interno y el equipo de periféricos. (I) (A)

**canalización.** Proceso consistente en romper el ancho de banda de una línea de comunicaciones en varios canales, posiblemente de diferentes tamaños. También se denomina *multiplexación de la división del tiempo* (TDM).

**canal lógico.** En el funcionamiento en modalidad de paquete, canal de emisión y canal de recepción que se utilizan conjuntamente para enviar y recibir datos sobre un enlace de datos al mismo tiempo. Pueden establecerse varios canales lógicos en el mismo enlace de datos si se intercala la transmisión de paquetes.

**capa.** (1) En una arquitectura de red, grupo de servicios que está completo desde un punto de vista conceptual, que es uno de los grupos de un conjunto de grupos ordenados jerárquicamente y que se extiende

por todos los sistemas que se ajustan a la arquitectura de red. (T) (2) En el modelo de referencia Interconexión de Sistemas Abiertos, uno de los siete grupos de servicios, funciones y protocolos ordenados jerárquicamente y completos conceptualmente que se extienden por todos los sistemas abiertos. (T) (3) En SNA, agrupación de funciones relacionadas que están separadas lógicamente de las funciones de otros grupos. La implementación de las funciones de una capa puede cambiar sin que ello afecte a las funciones de otras capas.

**capa de control de enlace de datos (DLC).** En SNA, capa que está compuesta por las estaciones de enlace que planifican la transferencia de datos sobre un enlace entre dos nodos y realizan un control de errores para el enlace. Ejemplos de control de enlace de datos son: el SDLC para la conexión de enlaces serie por bit y el control de enlace de datos para el canal de System/370.

**Nota:** Normalmente, la capa de DLC es independiente del mecanismo de transporte físico y asegura la integridad de los datos que alcanzan las capas superiores.

**capa de enlace de datos.** En el modelo de referencia Interconexión de Sistemas Abiertos, capa que proporciona servicios para la transferencia de datos entre las entidades de la capa de red sobre un enlace de comunicaciones. La capa de enlace de datos detecta los errores que puedan producirse en la capa física y posiblemente los corrige. (T)

**capa de red.** En la arquitectura Interconexión de Sistemas Abiertos (OSI), capa que es responsable del direccionamiento, de la conmutación y del acceso a la capa de enlace a lo largo del entorno de OSI.

**capa de transporte.** En el modelo de referencia Interconexión de Sistemas Abiertos, capa que proporciona un servicio fiable de transferencia de datos de extremo a extremo. Puede haber sistemas abiertos del tipo Relay en la vía de acceso. (T) Véase también *modelo de referencia Interconexión de Sistemas Abiertos*.

**capa física.** En el modelo de referencia Interconexión de Sistemas Abiertos, capa que proporciona los medios mecánicos, eléctricos, funcionales y de procedimiento para establecer, mantener y liberar conexiones físicas sobre el medio de transmisión. (T)

**carácter comodín.** Sinónimo de *carácter de coincidencia con el patrón*.

**carácter de coincidencia con el patrón.** Carácter especial, como, por ejemplo, un asterisco (\*) o un signo de interrogación (?), que puede utilizarse para representar uno o más caracteres. Cualquier carácter o conjunto de caracteres puede sustituir a un carácter de

coincidencia con el patrón. Sinónimo con *carácter global* y *carácter comodín*.

**CCITT.** Comisión Consultiva de la Telefonía y Telegrafía Internacionales. Era una organización de la Unión de Telecomunicaciones Internacionales (ITU). El 1 de marzo de 1993 se reorganizó la ITU y las responsabilidades de la normalización recayeron en una organización subordinada que se denomina Sector de Normalización de Telecomunicaciones de la Unión de Telecomunicaciones (ITU-TS). La "CCITT" sigue funcionando para las recomendaciones que se aprobaron antes de la reorganización.

**central privada (PBX).** Central telefónica privada para la transmisión de llamadas desde y hacia la red telefónica pública.

**centro de información de la red (NIC).** En comunicaciones de Internet, grupos locales, regionales y nacionales de todo el mundo que proporcionan ayuda, documentación, formación y otros servicios a los usuarios.

**circuito de datos.** (1) Par de canales de transmisión y recepción asociados que proporcionan un medio de comunicación de datos de dos direcciones. (I) (2) En SNA, sinónimo de *conexión de enlace*. (3) Véase también *circuito físico* y *circuito virtual*.

**Notas:**

1. Entre los intercambios de conmutaciones de datos, el circuito de datos puede incluir un equipo de terminación de circuito de datos (DCE) de acuerdo con el tipo de interfaz que se utilice en el intercambio de conmutaciones de datos.
2. Entre una estación de datos y un intercambio de conmutaciones de datos o concentrador de datos, el circuito de datos incluye el equipo de terminación de circuito de datos en el extremo de la estación de datos y puede incluir un equipo similar a un DCE en el intercambio de conmutaciones de datos o en la ubicación del concentrador de datos.

**circuito físico.** Circuito establecido sin multiplexación. Véase también *circuito de datos*. Compárese con *circuito virtual*.

**circuito huérfano.** Circuito no configurado cuya disponibilidad se aprende dinámicamente.

**circuito virtual.** (1) En la conmutación de paquetes, recursos proporcionados por una red que ofrecen el aspecto de una conexión real ante el usuario. (T) Véase también *circuito de datos*. Compárese con *circuito físico*. (2) Conexión lógica establecida entre dos DTE.

**circuito virtual conmutado (SVC).** Circuito X.25 que se establece dinámicamente cuando es necesario. El

equivalente, en X.25, de una línea conmutada. Compárese con *circuito virtual permanente (PVC)*.

**circuito virtual permanente (PVC).** En comunicaciones de X.25 y Frame-Relay, circuito virtual que tiene un canal lógico asignado permanentemente al mismo en cada equipo terminal de datos (DTE). No son necesarios protocolos de establecimiento de llamada. Compárese con *circuito virtual conmutado (SVC)*.

**clase de productividad.** En la conmutación de paquetes, velocidad a la que circulan los paquetes de un equipo terminal de datos (DTE) por la red de conmutación de paquetes.

**clase de servicio (COS).** Conjunto de características (como, por ejemplo, seguridad de ruta, prioridad de transmisión y ancho de banda) utilizadas para crear una ruta entre los asociados a una sesión. La clase de servicio deriva de un nombre de modalidad especificado por el iniciador de una sesión.

**cliente.** (1) Unidad funcional que recibe servicios compartidos de un servidor. (T) (2) Usuario.

**cliente de emulación de LAN (LEC).** Componente de la emulación de LAN que representa a los usuarios de la LAN emulada.

**cliente/servidor.** En comunicaciones, modelo de interacción en el proceso de datos distribuidos en el que un programa de un sitio envía una petición a un programa de otro sitio y espera una respuesta. El programa peticionario se denomina cliente; el programa que responde se denomina servidor.

**codificar.** Convertir datos mediante el uso de un código de manera que sea posible la reconversión al formato original. (T)

**colisión.** Condición no deseada que deriva de la existencia de transmisiones simultáneas en un canal. (T)

**compresión.** (1) Proceso consistente en eliminar claros, campos vacíos, redundancias y datos innecesarios para disminuir la longitud de los registros o los bloques. (2) Cualquier codificación destinada a reducir el número de bits utilizados para representar un mensaje o un registro determinado.

**comunidad.** En el protocolo Simple Network Management Protocol (SNMP), relación administrativa entre las entidades.

**Concentrador del acceso a L2TP (LAC).** Dispositivo conectado a una o más líneas RDSI o de red telefónica de servicios públicos (PSTN) con posibilidades de manejar el funcionamiento de PPP y el del protocolo L2TP. El LAC implementa el medio sobre el que funciona L2TP. L2TP pasa el tráfico a uno o más Ser-

vidores de red L2TP (LNS). L2TP puede proporcionar la función de túnel para cualquier protocolo que conlleve la red PPP.

**concentrador (inteligente).** Concentrador de cableado, como, por ejemplo, el IBM 8260, que proporciona funciones de puente y direccionamiento a las LAN con diferentes cables y protocolos.

**conectable en caliente.** Se refiere a un componente de hardware que puede instalarse o eliminarse sin estorbar el funcionamiento de otros recursos que no están conectados a este componente o no dependen del mismo.

**conectado mediante enlace.** (1) Perteneciente a dispositivos que están conectados a una unidad de control por medio de un enlace de datos. (2) Compárese con *conectado mediante canal*. (3) Sinónimo con *remoto*.

**conexión.** En la comunicación de datos, asociación establecida entre unidades funcionales para comunicar información. (I) (A)

**conexión de enlace.** (1) Equipo físico que proporciona comunicación en dos direcciones entre una estación de enlace y otra u otras estaciones de enlace; por ejemplo, un equipo de terminación de circuito de datos (DCE) y una línea de telecomunicaciones. (2) En SNA, sinonimia con *circuito de datos*.

**conexión Rapid Transport Protocol (RTP).** En el direccionamiento de alto rendimiento (HPR), conexión establecida entre los puntos finales de la ruta para transportar tráfico de sesión.

**conexión virtual.** En Frame Relay, vía de acceso de vuelta de una conexión potencial.

**configuración.** (1) Manera en que están organizados e interconectados el hardware y el software de un sistema de proceso de información. (T) (2) Dispositivos y programas que componen un sistema, un subsistema o una red.

**configuración del sistema.** Proceso que especifica los dispositivos y programas que componen un sistema de proceso de datos determinado.

**congestión.** Véase *congestión de la red*.

**congestión de la red.** Condición no deseada de carga excesiva causada por la presencia de más tráfico del que puede manejar una red.

**conmutación de la línea.** Sinónimo de *conmutación del circuito*.

**conmutación del circuito.** (1) Proceso que, a petición, conecta dos o más equipos terminales de datos (DTE) y permite el uso exclusivo de un circuito de datos

entre ellos hasta que se libera la conexión. (1) (A)  
(2) Sinónimo con *conmutación de la línea*.

**conmutación del enlace de datos (DLSw).** Método de los protocolos de red de transporte que utilizan el tipo 2 de control de enlace lógico (LLC) de IEEE 802.2. SNA y NetBIOS son ejemplos de protocolos que utilizan el tipo 2 de LLC. Véase también *encapsulación y simulación*.

**conmutación de paquetes.** (1) Proceso consistente en direccionar y transferir datos por medio de paquetes dirigidos de manera que un canal esté ocupado durante la transmisión de un paquete solamente. Cuando se completa la transmisión, el canal queda disponible para la transferencia de otros paquetes. (1) (2) Sinónimo con *funcionamiento en modalidad de paquete*. Véase también *conmutación del circuito*.

**consola remota.** Estación que ejecuta OS/2, TCP/IP y el programa Nways Switch Resource Control remoto. Puede conectarse con cualquier estación de soporte de red para realizar operaciones en Nways Switch y darle servicio técnico remotamente.

La conexión puede ser mediante:

- Una línea conmutada que utilice un módem

Cualquier estación de soporte de red puede utilizarse como consola remota de otra estación de soporte de red.

**contigua activa de donde proceden los datos (NAUN).** En la Red en Anillo de IBM, estación que envía datos directamente a una estación determinada del anillo.

**control de enlace de datos de alto nivel (HDLC).** En la comunicación de datos, utilización de una serie de bits especificada para controlar enlaces de datos de acuerdo con las normas internacionales respecto al HDLC: la estructura de trama de ISO 3309 y los elementos de procedimientos de ISO 4335.

**control de enlace de datos (DLC).** Conjunto de normas utilizado por los nodos de un enlace de datos (como, por ejemplo, un enlace de SDLC o una Red en Anillo) para efectuar un intercambio de información ordenado.

**control de enlace lógico (LLC).** Subcapa de LAN de control de enlace de datos (DLC) que proporciona dos tipos de operaciones de DLC para el intercambio ordenado de información. El primer tipo es el servicio sin conexiones, que permite enviar y recibir información sin establecer un enlace. La subcapa de LLC no efectúa recuperación de errores ni control del flujo para el servicio sin conexiones. El segundo tipo es el servicio orientado a las conexiones, que requiere el establecimiento de un enlace antes del intercambio de información. El servicio orientado a las conexiones

proporciona transferencia de información en secuencia, control del flujo y recuperación de errores.

**control del acceso al medio (MAC).** En las LAN, subcapa de la capa de control de enlace de datos que da soporte a funciones dependientes del medio y utiliza los servicios de la capa física para proporcionar servicios a la subcapa de control de enlace lógico (LLC). La subcapa del MAC incluye el método para determinar cuándo un dispositivo tiene acceso al medio de transmisión.

**control de la vía de acceso (PC).** Función que direcciona unidades de mensajes entre las unidades de red accesibles de la red y proporciona las vías de acceso entre éstas. Convierte las unidades básicas de información (BIU) del control de transmisión (posiblemente segmentándolas) en unidades de información de vía de acceso (PIU) e intercambia unidades básicas de transmisión que contienen una o más PIU con el control de enlace de datos. El control de la vía de acceso difiere según el tipo de nodo: algunos nodos (los nodos APPN, por ejemplo) utilizan identificadores de sesión generados localmente para el direccionamiento y otros (los nodos de subárea) utilizan direcciones de red para el direccionamiento.

**control del flujo.** (1) En SNA, proceso consistente en gestionar la velocidad a la que pasa el tráfico de datos entre los componentes de la red. La finalidad del control del flujo es optimizar la velocidad del flujo de unidades de mensajes con la congestión mínima de la red; es decir, ni desbordar los almacenamientos intermedios del receptor o de nodos de direccionamiento intermedio ni dejar al receptor esperando más unidades de mensajes. (2) Véase también *ritmo*.

**Control síncrono de enlace de datos (SDLC).**  
(1) Disciplina que se ajusta a los subconjuntos de los Advanced Data Communication Control Procedures (ADCCP) del American National Standards Institute (ANSI) y del Control de enlace de datos de alto nivel (HDLC) de la Organización Internacional para la Normalización, y está destinada a la gestión de la transferencia síncrona de información serie por bit de código transparente sobre una conexión de enlace. Los intercambios de transmisiones pueden ser dúplex o semi-dúplex sobre enlaces conmutados o no conmutados. La configuración de la conexión de enlace puede ser de punto a punto, de multipunto o de bucle. (1)  
(2) Compárese con *comunicación síncrona en binario (BSC)*.

**correlación.** Proceso consistente en convertir datos que el emisor transmite con un formato determinado en el formato de datos que puede aceptar el receptor.

**corriente de datos general (GDS).** Corriente de datos utilizada para las conversaciones en sesiones de LU 6.2.

**coste de la vía de acceso.** En los protocolos de direccionamiento de estado de los enlaces, suma de los costes de enlace a lo largo de la vía de acceso entre dos nodos o redes.

**cronometraje.** (1) En la comunicación síncrona en binario, utilización de pulsaciones de reloj para controlar la sincronización de los datos y caracteres de control. (2) Método para controlar el número de bits de datos enviados en una línea de telecomunicaciones en un momento determinado.

**cuenta de saltos.** (1) Métrica o medida de distancia entre dos puntos. (2) En comunicaciones de Internet, número de direccionadores por los que pasa un datagrama cuando se dirige a su destino. (3) En SNA, medida consistente en el número de enlaces por los que se debe pasar en la vía de acceso a un destino.

## D

**daemon.** Programa que se ejecuta desatendido para realizar un servicio estándar. Algunos daemon se desencadenan de manera automática para realizar su tarea; otros realizan las operaciones periódicamente.

**datagrama.** (1) En la conmutación de paquetes, paquete individual e independiente de otros paquetes que contiene información suficiente para el direccionamiento desde el equipo terminal de datos (DTE) de origen al DTE de destino sin apoyarse en intercambios anteriores entre los DTE y la red. (1) (2) En TCP/IP, unidad básica de información que pasa a través del entorno de Internet. Un datagrama contiene direcciones de origen y de destino junto con los datos. Un datagrama de Internet Protocol (IP) está compuesto por una cabecera de IP seguida de los datos de capa de transporte. (3) Véase también *paquete* y *segmento*.

**datagrama de IP.** En el conjunto de protocolos de Internet, unidad básica de información transmitida a través de una internet. Contiene direcciones de origen y de destino, datos de usuario e información de control, como, por ejemplo, la longitud del datagrama, la suma de comprobación de cabecera y distintivos que indican si el datagrama puede fragmentarse o si se ha fragmentado.

**Datagram Delivery Protocol (DDP).** En redes AppleTalk, protocolo que proporciona conectividad de red por medio de un servicio de entrega de socket a socket sin conexiones de la capa de internet.

**DCE preparado.** En la norma EIA 232, señal que indica al equipo terminal de datos (DTE) que el equipo de terminación de circuito de datos (DCE) local está conectado al canal de comunicaciones y se encuentra preparado para enviar datos. Sinónimo con *aparato de datos preparado (DSR)*.

**DECnet.** Arquitectura de red que define el funcionamiento de una familia de módulos de software, bases de datos y componentes de hardware que se utilizan normalmente con el fin de conectar entre sí sistemas Digital Equipment Corporation para el compartimiento de recursos, cálculo distribuido o configuración de sistemas remotos. Las implementaciones de la red DECnet siguen el modelo Digital Network Architecture (DNA).

**detección de colisión.** En el acceso múltiple con detección de portadora y detección de colisión (CSMA/CD), señal que indica que dos o más estaciones están transmitiendo simultáneamente.

**detección (de condición de excepción).** En Simple Network Management Protocol (SNMP), mensaje enviado por un nodo gestionado (la función de agente) a una estación de gestión para informarle de una condición de excepción.

**detección de portadora.** En una red de área local, actividad continua de una estación de datos para detectar si otra estación está transmitiendo. (T)

**detector de portadora.** Sinónimo de *detector de señal de línea recibida (RLSD)*.

**detector de portadora de datos (DCD).** Sinónimo de *detector de señal de línea recibida (RLSD)*.

**detector de señal de línea recibida (RLSD).** En la norma EIA 232, señal que indica al equipo terminal de datos (DTE) que está recibiendo una señal del equipo de terminación de circuito de datos (DCE) remoto. Sinónimo con *detector de portadora* y *detector de portadora de datos (DCD)*.

**determinación de problemas.** Proceso consistente en determinar el origen de un problema; por ejemplo, un componente de un programa, una anomalía en una máquina, recursos de telecomunicaciones, programas o equipos instalados por el contratista o por el usuario, una anomalía del entorno, como, por ejemplo, pérdida de alimentación, o un error del usuario.

**difusión.** (1) Transmisión de los mismos datos a todos los destinos. (T) (2) Transmisión simultánea de datos a más de un destino. (3) Compárese con *ver-timiento múltiple*.

**digital.** (1) Perteneciente a datos compuestos por dígitos. (T) (2) Perteneciente a datos con formato de dígitos. (A) (3) Compárese con *analógico*.

**Digital Network Architecture (DNA).** Modelo para todas las implementaciones de hardware y software DECnet.

**dirección.** En la comunicación de datos, código exclusivo asignado a cada dispositivo, estación de trabajo o usuario conectado a una red.

**dirección administrada localmente.** En una red de área local, dirección de adaptador que el usuario puede asignar para alterar temporalmente la dirección administrada universalmente. Compárese con *dirección administrada universalmente*.

**dirección administrada universalmente.** En una red de área local, dirección codificada de forma permanente en un adaptador en el momento de la fabricación. Todas las direcciones administradas universalmente son exclusivas. Compárese con *dirección administrada localmente*.

**direccionador.** (1) Sistema que determina la vía de acceso del flujo de tráfico de red. La selección de vía de acceso se realiza entre diversas vías de acceso sobre la base de la información obtenida a partir de protocolos específicos, algoritmos que intentan identificar la vía de acceso mejor o la más corta, y otros criterios, como, por ejemplo, direcciones de destino específicas de los protocolos o la métrica. (2) Dispositivo de conexión que conecta dos segmentos de LAN, los cuales utilizan arquitecturas similares o diferentes, en la capa de red del modelo de referencia. (3) En terminología de OSI, función que determina una vía de acceso mediante la cual puede accederse a una entidad. (4) En TCP/IP, sinonimia con *pasarela*. (5) Compárese con *puente*.

**direccionador contiguo.** Direccionador de una subred común designado por un administrador de red para recibir información de direccionamiento.

**direccionador de frontera.** En comunicaciones de Internet, direccionador que está posicionado al borde de un sistema autónomo y se comunica con un direccionador que está posicionado al borde de un sistema autónomo diferente.

**direccionador de germinación.** En redes AppleTalk, direccionador que mantiene datos de configuración (números de red de rango y listas de zonas, por ejemplo) para la red. Cada red debe tener, como mínimo, un direccionador de germinación. El direccionador de germinación debe configurarse inicialmente por medio de la herramienta configuradora. Compárese con *direccionador sin germinación*.

**direccionador de IP.** Dispositivo de una internet IP que tiene la responsabilidad de tomar decisiones acerca de las vías de acceso por las que fluirá tráfico de red. Los protocolos de direccionamiento se utilizan para obtener información sobre la red y para determinar la mejor ruta por la que debe reenviarse el datagrama hacia el destino final. Los datagramas se direccionan sobre la base de direcciones de destino IP.

**direccionador designado.** Direccionador que informa a los nodos finales de la existencia y la identidad de los otros direccionadores. La selección del direccionador designado se basa en el direccionador con la prioridad superior. Cuando diversos direccionadores comparten la prioridad superior, se selecciona el direccionador con la dirección de estación superior.

**direccionador sin germinación.** En redes AppleTalk, direccionador que obtiene información del rango de números de red y de la lista de zonas de un direccionador de germinación conectado a la misma red.

**direccionador troncal.** (1) Direccionador utilizado para transmitir datos entre áreas. (2) Direccionador de una serie que se utiliza para interconectar redes de manera que formen una internet mayor.

**direccionamiento.** En la comunicación de datos, manera que tiene una estación de seleccionar la estación a la que va a enviar datos.

**direccionamiento.** (1) Asignación de la vía de acceso mediante la cual un mensaje va a alcanzar su destino. (2) En SNA, reenvío de una unidad de mensaje por una vía de acceso determinada a través de una red tal como lo determinan los parámetros contenidos en la unidad de mensaje, como, por ejemplo, la dirección de red de destino de una cabecera de transmisión.

**direccionamiento de alto rendimiento (HPR).** Adición para la arquitectura Advanced Peer-to-Peer Networking (APPN) que mejora el rendimiento y la fiabilidad del direccionamiento de datos, especialmente en la utilización de enlaces de gran velocidad.

**direccionamiento del MAC arbitrario (AMA).** En la arquitectura DECnet, esquema de direccionamiento utilizado por DECnet Phase IV-Prime que da soporte a direcciones administradas universalmente y direcciones administradas localmente.

**direccionamiento de origen.** En las LAN, método mediante el cual la estación emisora determina la ruta que la trama seguirá e incluye la información de direccionamiento en la trama. A continuación, los puentes leen la información de direccionamiento para determinar si deben reenviar la trama.

**direccionamiento de sesiones intermedias (ISR).** Tipo de función de direccionamiento de un nodo de red APPN que proporciona información de indisponibilidad y control del flujo de nivel de sesión para todas las sesiones que pasan por el nodo pero cuyos puntos finales están en otra parte.

**direccionamiento dinámico.** Direccionar utilizando rutas aprendidas en lugar de las rutas configuradas estáticamente durante la inicialización.

**direccionamiento intraárea.** En comunicaciones de Internet, direccionamiento de datos dentro de un área.

**dirección canónica.** En las LAN, formato de IEEE 802.1 de la transmisión de direcciones del control del acceso al medio (MAC) para adaptadores de Red en Anillo y Ethernet. En el formato canónico, el bit menos significativo (situado más a la derecha) de cada byte de dirección se transmite en primer lugar. Compárese con *dirección no canónica*.

**dirección de difusión.** En comunicaciones, dirección de estación (ocho números 1) reservada como dirección común a todas las estaciones de un enlace. Sinónimo con *dirección de todas las estaciones*.

**dirección de dispositivo.** Dirección de unidad transmitida por la vía de acceso de canal para seleccionar un dispositivo 2216. También se denomina número de subcanal en la arquitectura de E/S S/370. Este valor está definido en el IOCP del sistema principal mediante la sentencia UNITADD de la instrucción de macro CNTLUNIT para el dispositivo real.

**Dirección de enlace.** Para el 2216 con un Adaptador de Canal ESCON, número de puerto determinado de la manera siguiente: si hay un ESCD en la vía de acceso de comunicaciones, es el número de puerto del Director de ESCON (ESCD) conectado al sistema principal. Si hay dos ESCD en la vía de acceso, es el número de puerto de la parte del sistema principal del ESCD definido con la conexión dinámica. Cuando no hay ningún ESCD en la vía de acceso de comunicaciones, este valor debe establecerse en X'01'.

**dirección de red.** Según ISO 7498-3, nombre que no es ambiguo en el entorno de OSI y que identifica a un conjunto de puntos de acceso a servicios de red.

**dirección de subred.** En comunicaciones de Internet, extensión del esquema básico de direccionamiento de IP donde una parte de la dirección de sistema principal se interpreta como dirección de red local.

**dirección de todas las estaciones.** En comunicaciones, sinónimo de *dirección de difusión*.

**dirección de usuario de red (NUA).** En comunicaciones de X.25, dirección X.121 que contiene hasta 15 dígitos en código binario.

**dirección Internet.** Véase *dirección IP*.

**dirección IP.** Dirección de 32 bits definida por Internet Protocol, norma 5, Request for Comments (RFC) 791. Normalmente, se representa mediante formato decimal con puntos.

**Dirección lógica de CU.** Dirección de unidad de control definida en el sistema principal para el 2216.

Este valor está definido en el programa de configuración de la entrada/salida (IOCP) del sistema principal mediante la sentencia CUADD de la instrucción de macro CNTLUNIT. La Dirección de unidad de control debe ser exclusiva para cada partición lógica definida en el mismo sistema principal.

**dirección no canónica.** En las LAN, formato de la transmisión de direcciones del control del acceso al medio (MAC) para adaptadores de Red en Anillo. En el formato no canónico, el bit más significativo (situado más a la izquierda) de cada byte de dirección se transmite en primer lugar. Compárese con *dirección canónica*.

**directorío.** Tabla de identificadores y referencias para los elementos de datos correspondientes. (I) (A)

**dispositivo.** Aparato mecánico, eléctrico o electrónico con un fin específico.

**dominio.** (1) Parte de una red de sistema en la que los recursos de proceso de datos están bajo un control común. (T) (2) En Interconexión de Sistemas Abiertos (OSI), parte de un sistema distribuido o conjunto de objetos gestionados a los que se aplica una política común. (3) Véase *Dominio administrativo y nombre de dominio*.

**Dominio administrativo.** Conjunto de sistemas principales y direccionadores, y las redes de interconexión, que gestiona una sola autoridad administrativa.

**dominio de direccionamiento.** En comunicaciones de Internet, grupo de sistemas intermedios que utilizan un protocolo de direccionamiento para que la representación de la red en un conjunto sea la misma en cada sistema intermedio. Los dominios de direccionamiento se conectan entre sí mediante enlaces exteriores.

## E

**eco.** En la comunicación de datos, señal de un canal de comunicaciones reflejada. Por ejemplo, en un terminal de comunicaciones, cada señal se visualiza dos veces, una cuando entra en el terminal local y otra cuando vuelve sobre el enlace de comunicaciones. Esto permite comprobar la exactitud de las señales.

**EIA 232.** En la comunicación de datos, especificación de la Electronic Industries Association (EIA) que define la interfaz entre el equipo terminal de datos (DTE) y el equipo de terminación de circuito de datos (DCE), que utiliza el intercambio de datos binarios serie.

**Electronic Industries Association (EIA).** Organización de fabricantes del campo de la electrónica que anticipa el crecimiento tecnológico de la industria, representa los puntos de vista de sus miembros y desarrolla normas para la industria.

**Emulación de LAN (LE).** Norma del ATM Forum que da soporte a aplicaciones de legado de LAN sobre redes ATM.

**encapsulación.** (1) En comunicaciones, técnica utilizada por protocolos de capa mediante la cual una capa añade a la unidad de datos de protocolo (PDU) información de control de la capa a la que da soporte. A este respecto, la capa encapsula los datos de la capa soportada. En el conjunto de protocolos de Internet, por ejemplo, un paquete contendrá información de control de la capa física, a continuación información de control de la capa de red y a continuación los datos de protocolo de la aplicación. (2) Véase también *conmutación del enlace de datos*.

**enlace.** Combinación de la conexión de enlace (el medio de transmisión) y dos estaciones de enlace, una a cada extremo de la conexión de enlace. Una conexión de enlace puede estar compartida entre diversos enlaces en una configuración de multipunto o Red en Anillo.

**enlace lógico.** Par de estaciones de enlace, una en cada uno de dos nodos adyacentes, y su conexión de enlace subyacente que proporcionan una sola conexión de capa de enlace entre los dos nodos. Pueden distinguirse diversos enlaces lógicos mientras comparten el uso del mismo medio físico de conexión de dos nodos. Ejemplos son los enlaces lógicos de 802.2 utilizados en recursos de red de área local (LAN) y los enlaces lógicos de LAP E del mismo enlace físico punto a punto entre dos nodos. El término enlace lógico también incluye los diversos canales lógicos de X.25 que comparten el uso del enlace de acceso de un DTE con una red X.25.

**enlace virtual.** En Open Shortest Path First (OSPF), interfaz punto a punto que conecta direccionadores de frontera separados por un área de tránsito no troncal. Puesto que los direccionadores de área forman parte del troncal OSPF, el enlace virtual conecta el troncal. Los enlaces virtuales aseguran que el troncal OSPF no se vuelva discontinuo.

**equipo de terminación de circuito de datos (DCE).** En una estación de datos, equipo que proporciona la conversión de señal y la codificación entre el equipo terminal de datos (DTE) y la línea. (I)

**Notas:**

1. El DCE puede ser un equipo independiente o parte integral del DTE o del equipo intermedio.
2. Un DCE puede realizar otras funciones que normalmente se llevan a cabo al final de red de la línea.

**equipo terminal de datos (DTE).** Parte de una estación de datos que funciona como origen y/o destino de datos. (I) (A)

**esfera de control (SOC).** Conjunto de dominios de punto de control servidos por un solo punto focal de servicios de gestión.

**estación.** Punto de entrada o salida de un sistema que utiliza recursos de telecomunicaciones; por ejemplo, uno o más sistemas, terminales, dispositivos y programas asociados de una ubicación determinada que pueden enviar o recibir datos sobre una línea de telecomunicaciones.

**estación de configuración Nways Switch.** Estación de OS/2 dedicada que ejecuta una versión autónoma de la herramienta Nways Switch Configuration Tool (NCT). Se utiliza para generar una base de datos de configuración de red y debe instalarse como consola remota.

**estación de enlace.** (1) Componentes de hardware y software de un nodo que representan una conexión con un nodo adyacente sobre un enlace específico. Por ejemplo, si el nodo A es el extremo primario de una línea multipunto que se conecta con tres nodos adyacentes, el nodo A tendrá tres estaciones de enlace que representarán las conexiones con los nodos adyacentes. (2) Véase también *estación de enlace adyacente (ALS)*.

**estación de gestión.** En comunicaciones de Internet, sistema responsable de la gestión de toda una red o de parte de la misma. La estación de gestión se comunica con agentes de gestión de red que residen en el nodo gestionado por medio de un protocolo de gestión de red, como, por ejemplo, Simple Network Management Protocol (SNMP).

**estación de gestión de red.** En el protocolo Simple Network Management Protocol (SNMP), estación que ejecuta programas de aplicación de gestión que supervisan y controlan elementos de red.

**estación de soporte de red.** Procesador utilizado para realizar operaciones en Nways Switch y darle servicio técnico localmente. Lo utilizan el administrador o el personal de servicio encargados de Nways Switch.

**estado de los enlaces.** En los protocolos de direccionamiento, información anunciada sobre las interfaces utilizables y los direccionadores contiguos a un direccionador o una red asequibles. La base de datos topológica del protocolo se forma a partir de los anuncios reunidos sobre el estado de los enlaces.

**Estructura de la información de gestión (SMI).**

(1) En el protocolo Simple Network Management Protocol (SNMP), normas utilizadas para definir los objetos a los que puede accederse por medio de un protocolo de gestión de red. (2) En OSI, conjunto de normas relativas a la información de gestión. El con-



junto incluye el *Management Information Model* y las *Guidelines for the Definition of Managed Objects*.

**Ethernet.** Red de área local de banda base de 10 Mbps que permite que diversas estaciones accedan al medio de transmisión a voluntad sin coordinación previa, evita la contención utilizando la detección y deferencia de portadora y resuelve la contención utilizando la detección de colisión y la retransmisión retardada. Ethernet utiliza el acceso múltiple con detección de portadora y detección de colisión (CSMA/CD).

**excepción.** Condición anormal, como, por ejemplo, un error de E/S encontrado durante el proceso de un conjunto de datos o archivo.

**extensión de ruta (REX).** En SNA, componentes de red de control de la vía de acceso, incluido un enlace periférico, que componen la parte de una vía de acceso que está entre un nodo de subárea y una unidad de red dirigible (NAU) de un nodo periférico adyacente. Véase también *ruta explícita (ER)*, *vía de acceso y ruta virtual (VR)*.

**Exterior Gateway Protocol (EGP).** En el conjunto de protocolos de Internet, protocolo utilizado entre dominios y sistemas autónomos que permite anunciar e intercambiar información sobre la asequibilidad de la red. Las direcciones de red IP de un sistema autónomo se anuncian en otro sistema autónomo por medio de direccionadores que participan de EGP. Un ejemplo de EGP es Border Gateway Protocol (BGP). Compárese con Interior Gateway Protocol (IGP).

## F

**fax.** Copia impresa que se recibe de una máquina de facsímil. Sinónimo con *telecopia*.

**File Transfer Protocol (FTP).** En el conjunto de protocolos de Internet, protocolo de capa de aplicación que utiliza servicios de TCP y Telnet para transferir archivos de datos generales entre máquinas o sistemas principales.

**fluctuación.** (1) Variaciones no acumulativas a corto plazo de los instantes significativos de una señal digital respecto a sus posiciones ideales en el tiempo. (2) Variaciones no deseadas de una señal digital transmitida. (3) Variaciones en el retardo de la red.

**formato decimal con puntos.** Representación sintáctica de un entero de 32 bits que consta de cuatro números de 8 bits escritos en base 10 con puntos que los separan. Se utiliza para representar direcciones IP.

**fragmentación.** (1) Proceso consistente en dividir un datagrama en partes más pequeñas, o fragmentos, para que se ajuste a las posibilidades del medio físico

por el que se va a transmitir. (2) Véase también *segmentación*.

**fragmento.** Véase *fragmentación*.

**Frame Relay.** (1) Norma de interfaz que describe el límite entre el equipo de un usuario y una red de paquetes rápidos. En los sistemas Frame-Relay, se eliminan las tramas defectuosas; la recuperación se produce de extremo a extremo en lugar de efectuarse salto a salto. (2) Técnica derivada de la norma de canal D de red digital de servicios integrados (RDSI). Supone que las conexiones son fiables y prescinde de la actividad general de control y detección de errores en la red.

**funcionamiento en modalidad de paquete.** Sinónimo de *conmutación de paquetes*.

**función de puente.** En las LAN, el reenvío de una trama de un segmento de LAN a otro. El destino está especificado mediante la dirección de subcapa del control del acceso al medio (MAC) codificada en el campo de dirección de destino de la cabecera de la trama.

**función de puente de ruta de origen.** En las LAN, método de función de puente que utiliza el campo de información de direccionamiento de la cabecera del control del acceso al medio (MAC) de IEEE 802.5 de una trama para determinar los anillos o segmentos de Red en Anillo que debe recorrer la trama. El nodo de origen inserta el campo de información de direccionamiento en la cabecera del MAC. La información del campo de información de direccionamiento deriva de los paquetes exploradores generados por el sistema principal de origen.

**función de puente local.** Función de un programa de puente que permite que un solo puente conecte diversos segmentos de LAN sin la utilización de un enlace de telecomunicaciones. Compárese con *función de puente remota*.

**función de puente remota.** Función de un puente que permite que dos puentes conecten diversas LAN utilizando un enlace de telecomunicaciones. Compárese con *función de puente local*.

**función de puente transparente.** En las LAN, método para relacionar redes de área local individuales entre sí en el nivel del control del acceso al medio (MAC). Un puente transparente almacena las tablas que contienen direcciones MAC para que las tramas que ve el puente puedan reenviarse a otra LAN si las tablas lo indican así.

**función de túnel.** Trata a una red de transporte como si fuera una sola LAN o un solo enlace de comunicaciones. Véase también *encapsulación*.

## G

**gestión de red.** Proceso consistente en planificar, organizar y controlar un proceso de datos o sistema de información orientado a las comunicaciones.

**gestor de red.** Programa o grupo de programas que se utiliza para supervisar y gestionar una red así como para diagnosticar los problemas de la misma.

**grupo de transmisión (TG).** (1) Conexión entre nodos adyacentes que se identifica mediante un número de grupo de transmisión. (2) En una red de subárea, enlace o grupo de enlaces entre nodos adyacentes. Cuando un grupo de transmisión está compuesto por un grupo de enlaces, los enlaces se ven como un solo enlace lógico y el grupo de transmisión se denomina *grupo de transmisión multienlace (MLTG)*. Un *grupo de transmisión multienlace de mezcla de medios (MMMLTG)* contiene enlaces de diferentes tipos de medios (por ejemplo, Red en Anillo, SDLC conmutado, SDLC no conmutado y enlaces Frame-Relay). (3) En una red APPN, enlace entre nodos adyacentes. (4) Véase también *grupos de transmisión paralelo*.

**grupos de transmisión paralelo.** Diversos grupos de transmisión entre nodos adyacentes, teniendo cada grupo un número de grupo de transmisión distinto.

## H

**Hello.** Protocolo utilizado por un grupo de direccionadores que cooperan y se apoyan entre sí para poder descubrir rutas de retardo mínimo.

**heurístico.** Perteneciente a métodos exploratorios para la resolución de problemas en los que se descubren soluciones mediante una evaluación del progreso realizada respecto al resultado final.

**histéresis.** Cantidad que indica cuánto debe cambiar la temperatura una vez pasado el umbral del establecimiento de alerta y antes de que se elimine la condición de alerta.

**horizonte dividido.** Técnica destinada a minimizar el tiempo para conseguir la convergencia en la red. Un direccionador registra la interfaz sobre la que ha recibido una ruta en particular y no propaga su información sobre la ruta otra vez sobre la misma interfaz.

## I

**identificación de intercambio (XID).** Tipo específico de unidad básica de enlace que se utiliza para la comunicación de características de nodo y enlace entre nodos adyacentes. Los XID se intercambian entre estaciones de enlace antes de la activación del enlace

y durante la misma para establecer y negociar las características de enlace y nodo, y después de la activación del enlace para comunicar los cambios de estas características.

**identificador de conexión de enlace de datos (DLCI).** Identificador numérico de un subpuerto Frame-Relay o segmento de PVC en una red Frame-Relay. Cada subpuerto de un puerto Frame-Relay individual tiene un DLCI exclusivo. La tabla siguiente, extraída de la norma T1.618 del American National Standards Institute (ANSI) y la norma Q.922 de la Comisión Consultiva de la Telefonía y Telegrafía Internacionales (ITU-T/CCITT), indica las funciones asociadas con determinados valores de DLCI:

Valores de DLCI	Función
0	Señalización de canal de entrada
1–15	Se reserva
16–991	Se asigna utilizando procedimientos de conexión de Frame-Relay
992–1007	Gestión de capa 2 de servicio portador de Frame-Relay
1008–1022	Se reserva
1023	Gestión de capa de canal de entrada

**identificador de puente.** Campo de 8 bytes que se utiliza en un protocolo de árbol de expansión y está compuesto por la dirección MAC del puerto con el identificador de puerto más bajo y un valor definido por el usuario.

**identificador de red.** (1) En TCP/IP, parte de la dirección IP que define a una red. La longitud del identificador de red depende del tipo de la clase de red (A, B o C). (2) Nombre de 1 a 8 bytes seleccionado por el cliente o nombre de 8 bytes registrado por IBM que identifica de manera exclusiva a una subred específica.

**inhabilitado.** (1) Perteneciente a un estado de una unidad de proceso que evita la aparición de determinados tipos de interrupciones. (2) Perteneciente al estado en el cual una unidad de control de transmisión o unidad de respuestas audibles no puede aceptar llamadas de entrada de una línea.

**inhabilitar.** Convertir en no funcional.

**Integrated Digital Network Exchange (IDNX).** Procesador que integra aplicaciones a base de voz, datos e imágenes. También gestiona los recursos de transmisión y se conecta a multiplexores y sistemas de soporte de gestión de redes. Permite la integración de equipos de diferentes proveedores.

**intercalación.** (1) Alternancia de dos o más operaciones o funciones a través del uso solapado de un recurso del sistema. (2) En la transmisión de datos,

alternancia de paquetes de una corriente de datos con paquetes de otra.

**intercambio de conmutaciones de datos (DSE).**

Equipo instalado en una ubicación individual para proporcionar funciones de conmutación, como, por ejemplo, conmutación del circuito, conmutación de mensajes y conmutación de paquetes. (I)

**Interconexión de Sistemas Abiertos (OSI).**

(1) Interconexión de sistemas abiertos que sigue las normas de la Organización Internacional para la Normatización (ISO) para el intercambio de información. (T) (A) (2) Utilización de procedimientos normalizados para permitir la interconexión de sistemas de proceso de datos.

**Nota:** La arquitectura OSI establece una infraestructura para coordinar el desarrollo de normas actuales y futuras de cara a la interconexión de sistemas. Las funciones de red se dividen en siete capas. Cada capa representa un grupo de funciones relacionadas de proceso de datos y comunicación que pueden llevarse a cabo de una manera estándar para dar soporte a diferentes aplicaciones.

**interfaz.** (1) Límite compartido entre dos unidades funcionales en cuya definición entran características funcionales, características de señalización u otras características según lo que corresponda. El concepto incluye la especificación de la conexión de dos dispositivos que tienen funciones diferentes. (T) (2) Hardware y/o software para el enlace de sistemas, programas o dispositivos.

**interfaz de gestión local (LMI).** Véase *protocolo de interfaz de gestión local (LMI)*.

**interfaz de unidad de conexión (AUI).** En una red de área local, interfaz entre la unidad de conexión al medio y el equipo terminal de datos de una estación de datos. (I) (A)

**Interior Gateway Protocol (IGP).** En el conjunto de protocolos de Internet, protocolo utilizado para propagar información sobre la asequibilidad y direccionamiento de la red dentro de un sistema autónomo. Ejemplos de IGP son Routing Information Protocol (RIP) y Open Shortest Path First (OSPF).

**Internet.** Red internet administrada por la Internet Architecture Board (IAB) y compuesta por grandes redes troncales nacionales así como por muchas redes regionales y de campus en todo el mundo. Internet utiliza el conjunto de protocolos de Internet.

**internet.** Conjunto de redes interconectadas por una serie de direccionadores que les permiten funcionar como una sola red grande. Véase también *Internet*.

**Internet Architecture Board (IAB).** Corporación técnica que supervisa el desarrollo del conjunto de protocolos de Internet conocidos como TCP/IP.

**Internet Control Message Protocol (ICMP).** Protocolo utilizado para manejar mensajes de control y errores en la capa de Internet Protocol (IP). Los informes sobre problemas y destinos incorrectos de datagramas se devuelven al origen del datagrama. ICMP forma parte de Internet Protocol.

**Internet Control Protocol (ICP).** Protocolo de Virtual NETworking System (VINES) que proporciona notificaciones de excepciones, notificaciones sobre métrica y el soporte del programa PING. Véase también *RouTing update Protocol (RTP)*.

**Internet Engineering Task Force (IETF).** Grupo de operaciones de la Internet Architecture Board (IAB) que es responsable de la resolución de las necesidades técnicas de la Internet a corto plazo.

**Internet Protocol (IP).** Protocolo sin conexiones que direcciona datos a través de una red o redes interconectadas. IP actúa como intermediario entre las capas de protocolos superiores y la red física. No obstante, este protocolo no proporciona recuperación de errores ni control del flujo ni garantiza la fiabilidad de la red física.

**Internetwork Packet Exchange (IPX).** (1) Protocolo de red utilizado para conectar servidores Novell, o cualquier estación de trabajo o direccionador que implemente IPX, con otras estaciones de trabajo. Aunque es similar a Internet Protocol (IP), IPX utiliza unos formatos de paquete y una terminología diferentes. (2) Véase también *Xerox Network Systems (XNS)*.

**interoperatividad.** Posibilidad de comunicarse, ejecutar programas o transferir datos entre diversas unidades funcionales de tal forma que el usuario necesite tener poco conocimiento, o ninguno, de las características exclusivas de estas unidades. (T)

**Inverse Address Resolution Protocol (InARP).** En el conjunto de protocolos de Internet, protocolo utilizado para ubicar una dirección de protocolo mediante la dirección de hardware conocida. En un contexto de Frame-Relay, identificador de conexión de enlace de datos (DLCI) es sinónimo con dirección de hardware conocida.

**IPPN.** Interfaz que otros protocolos pueden utilizar para transportar datos sobre IP.

**IPXWAN.** Protocolo de Novell que se utiliza para intercambiar información de direccionador a direccionador antes de intercambiar información de direccionamiento

de Internetwork Packet Exchange (IPX) estándar y tráfico sobre redes de área amplia (WAN).

## J

## L

**LAN Network Manager (LNM).** Programa bajo licencia de IBM que permite que un usuario gestione y supervise recursos de LAN desde una estación de trabajo central.

**LE.** Emulación de LAN. Norma del ATM Forum que da soporte a aplicaciones de legado de LAN sobre redes ATM.

**LEC.** Cliente de emulación de LAN. Componente de la emulación de LAN que representa a los usuarios de la LAN emulada.

**LECS.** Servidor de configuración de emulación de LAN. Componente de LAN Emulation Service que centraliza y difunde datos de configuración.

**LES.** Servidor de emulación de LAN. Componente de LAN Emulation Service que resuelve destinos de LAN en direcciones ATM.

**línea tronco.** Línea de gran velocidad que conecta dos Nways Switch. Puede ser un cable coaxial, un cable de fibra u ondas de radio, por ejemplo, y puede alquilarse en empresas de telecomunicación.

**local.** (1) Perteneciente a un dispositivo al que se accede directamente sin utilizar una línea de telecomunicaciones. (2) Compárese con *remoto*. (3) Sinónimo de *conectado mediante canal*.

**LP.** partición lógica

**LPAR.** lógicamente particionada

## M

**mandato ping.** Mandato que envía un paquete de petición con eco de Internet Control Message Protocol (ICMP) a una pasarela, direccionador o sistema principal esperando recibir una respuesta.

**máscara.** (1) Patrón de caracteres utilizado para controlar la retención o eliminación de partes de otro patrón de caracteres. (I) (A) (2) Utilizar un patrón de caracteres para controlar la retención o eliminación de partes de otro patrón de caracteres. (I) (A)

**máscara de dirección.** Respecto a las subredes de internet, máscara de 32 bits utilizada para identificar los

bits de dirección de subred de la parte del sistema principal de una dirección IP. Sinónimo con *máscara de subred* y *máscara de subred (grupo de nodos)*.

**máscara de subred.** Sinónimo de *máscara de dirección*.

**máscara de subred (grupo de nodos).** Sinónimo de *máscara de dirección*.

**memoria de almacenamiento dinámico.** Cantidad de RAM utilizada para asignar estructuras de datos dinámicamente.

**memoria de sólo lectura (ROM).** Memoria en la que el usuario no puede modificar los datos almacenados salvo en condiciones especiales.

**memoria instantánea.** Dispositivo de almacenamiento de datos que puede programarse y borrarse y que no necesita alimentación continua. La ventaja principal de la memoria instantánea sobre otros dispositivos de almacenamiento de datos que pueden programarse y borrarse es que puede volver a programarse sin quitarla de la placa de circuitos.

**mensaje hello.** (1) Mensaje enviado periódicamente para establecer y probar la asequibilidad entre direccionadores o entre direccionadores y sistemas principales. (2) En el conjunto de protocolos de Internet, mensaje definido por el protocolo Hello como Interior Gateway Protocol (IGP).

**métrica.** En comunicaciones de Internet, valor asociado con una ruta que se utiliza para establecer diferencias entre los múltiples puntos de entrada o salida respecto al mismo sistema autónomo. Se prefiere la ruta con la métrica inferior.

**MIB.** (1) Módulo de la MIB. (2) Base de la información de gestión.

**MIB estándar.** En el protocolo Simple Network Management Protocol (SNMP), módulo de la MIB que se ubica bajo la rama de gestión de la Estructura de la información de gestión (SMI) y que se considera una norma en Internet Engineering Task Force (IETF).

**MILNET.** Red militar que formaba parte de ARPANET en un principio. Quedó separada de ARPANET en 1984. MILNET proporciona un servicio de red fiable para las instalaciones militares.

**modalidad lógicamente particionada (LPAR).** Función de algunos procesadores principales en que el proceso se divide en particiones lógicas (LP) para parecer diversos procesadores. En modalidad LPAR, el adaptador de ESCON puede compartir una conexión de fibra física con diversas particiones de sistema principal.

**modalidad LPAR.** Modalidad lógicamente particionada (LPAR).

**modelo de referencia Interconexión de Sistemas Abiertos (OSI).** Modelo que describe los principios generales de Interconexión de Sistemas Abiertos así como la finalidad y la ordenación jerárquica de sus siete capas. (T)

**módem (modulador/demodulador).** (1) Unidad funcional que modula y demodula señales. Una de las funciones de un módem es permitir que los datos digitales se transmitan sobre recursos de transmisión analógicos. (T) (A) (2) Dispositivo que convierte los datos digitales de un sistema en una señal analógica que pueda transmitirse en una línea de telecomunicaciones, y convierte la señal analógica recibida en datos para el sistema.

**modulación en código de pulsaciones (PCM).** Norma adoptada para la digitalización de una señal de voz analógica. En la PCM, se realiza un muestreo de la voz a una velocidad de ocho kHz y cada muestra se codifica en una trama de 8 bits.

**módulo.** En Nways Switch, unidad de hardware funcional empaquetada que contiene tarjetas lógicas, conectores y luces. Los módulos se utilizan para empaquetar adaptadores, acopladores de interfaz de línea, extensiones de servidor de voz y otros componentes. Todos los módulos pueden **conectarse en caliente** en los subastidores lógicos.

**módulo.** (1) Perteneciente a un módulo matemático; por ejemplo, 9 equivale a 4 módulo 5. (2) Véase también *módulo (diferencia)*.

**módulo (diferencia).** Número, como por ejemplo un entero positivo, de una relación que divide la diferencia entre dos números relacionados sin dejar un resto; por ejemplo, 9 y 4 tienen un módulo de 5 ( $9 - 4 = 5$ ;  $4 - 9 = -5$ ; y 5 divide tanto 5 como -5 sin dejar un resto).

**multiplexación de la división del tiempo (TDM).** Véase *canalización*.

## N

**Name Binding Protocol (NBP).** En redes AppleTalk, protocolo que proporciona la función de conversión de nombre a partir del nombre (serie de caracteres) de una entidad (recurso) AppleTalk en una dirección IP AppleTalk (número de 16 bits) en la capa de transporte.

**NetBIOS.** Network Basic Input/Output System. Interfaz estándar para redes, IBM PC (Personal Computer) y PC compatibles que se utiliza en las LAN para proporcionar funciones de mensajes, de servidor de impresión y de servidor de archivos. Los programas de aplicación

que utilizan NetBIOS no necesitan manejar los detalles de protocolos de control de enlace de datos (DLC) de la LAN.

**nivel de enlace.** (1) Parte de la recomendación X.25 que define el protocolo de enlace utilizado para entrar datos en la red y sacarlos de la misma a través del enlace dúplex que conecta la máquina del abonado con el nodo de red. LAP y LAPB son los protocolos de acceso de enlace recomendados por la CCITT. (2) Véase *nivel de enlace de datos*.

**nivel de enlace de datos.** (1) En la estructura jerárquica de una estación de datos, nivel conceptual de control o lógica de proceso entre la lógica de alto nivel y el enlace de datos que mantiene el control del enlace de datos. El nivel de enlace de datos realiza funciones tales como la inserción de bits de transmisión y supresión de bits de recepción; interpretación de campos de dirección y control; generación, transmisión e interpretación de mandatos y respuestas; y cálculo e interpretación de secuencias de comprobación de trama. Véase también *nivel de paquete* y *nivel físico*. (2) En comunicaciones de X.25, sinónimo de *nivel de trama*.

**nivel de trama.** Sinónimo con *nivel de enlace de datos*. Véase *nivel de enlace*.

**nodo.** (1) En una red, punto donde una o más unidades funcionales conectan canales o circuitos de datos. (I) (2) Cualquier dispositivo conectado a una red que transmite y recibe datos.

**nodo Advanced Peer-to-Peer Networking (APPN).** Nodo de red APPN o nodo final APPN.

**nodo de destino.** Nodo al que se envían datos o una petición.

**nodo de esfera de control (SOC).** Nodo que está incluido directamente en la esfera de control de un punto focal. Un nodo de SOC ha intercambiado elementos de habilitación de los servicios de gestión con su punto focal. Un nodo final APPN puede ser un nodo de SOC si da soporte a la función de intercambio de elementos de habilitación de los servicios de gestión.

**nodo de red Advanced Peer-to-Peer Networking (APPN).** Nodo que ofrece un amplio rango de servicios de usuario final y que puede proporcionar lo siguiente:

- servicios de directorios distribuidos, incluido el registro de los recursos del dominio con un servidor de directorios central
- Intercambios de bases de datos de topología con otros nodos de red APPN, lo que permite que los nodos de red de la red seleccionen las rutas óptimas para sesiones de LU-LU basándose en las clases de servicio solicitadas

- Servicios de sesiones para los nodos finales clientes y las LU locales
- Servicios de direccionamiento intermedio de una red APPN

**nodo de red APPN.** Véase *nodo de red Advanced Peer-to-Peer Networking (APPN)*.

**nodo de red de entrada baja (LEN).** Nodo que proporciona un rango de servicios de usuario final, se conecta directamente con otros nodos utilizando protocolos de igual a igual y hace derivar servicios de red de un nodo de red APPN adyacente implícitamente, es decir, sin el uso directo de sesiones de CP-CP.

**nodo de red (NN).** Véase *nodo de red Advanced Peer-to-Peer Networking (APPN)*.

**nodo final Advanced Peer-to-Peer Networking (APPN).** Nodo que proporciona un amplio rango de servicios de usuario final y da soporte a las sesiones entre su punto de control (CP) local y el CP de un nodo de red adyacente. Utiliza estas sesiones con el fin de registrar dinámicamente sus recursos con el CP adyacente (su servidor de nodos de red) para enviar y recibir peticiones de búsqueda en directorios y obtener servicios de gestión. Un nodo final APPN también puede conectarse a una red de subárea como nodo periférico o a otros nodos finales.

**nodo final de red de entrada baja (LEN).** Nodo LEN que recibe servicios de red de un nodo de red APPN adyacente.

**nodo final (EN).** (1) Véase *nodo final Advanced Peer-to-Peer Networking (APPN)* y *nodo final de red de entrada baja (LEN)*. (2) En comunicaciones, nodo que se conecta frecuentemente a un solo enlace de datos y no puede realizar funciones de direccionamiento intermedio.

**nodo intermedio.** Nodo que está al final de más de una rama. (T)

**nodos adyacentes.** Dos nodos conectados conjuntamente por una vía de acceso, como mínimo, que no conecta ningún otro nodo. (T)

**nombre de comunidad.** En el protocolo Simple Network Management Protocol (SNMP), serie de octetos que identifica a una comunidad.

**nombre de dominio.** En el conjunto de protocolos de Internet, nombre de un sistema principal. Un nombre de dominio está compuesto por una secuencia de subnombres separados por un carácter delimitador. Por ejemplo, si el nombre de dominio calificado al completo (FQDN) de un sistema principal es `ra1vm7.vnet.ibm.com`, cada uno de los siguientes es un nombre de dominio:

- `ra1vm7.vnet.ibm.com`
- `vnet.ibm.com`
- `ibm.com`

#### **notación de sintaxis de abstracción 1 (ASN.1).**

Método de Interconexión de Sistemas Abiertos (OSI) para la sintaxis de abstracción que se especifica en las normas siguientes:

- ITU-T recomendación X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T recomendación X.680 (1994) | ISO/IEC 8824-1: 1994

Véase también *normas básicas de codificación (BER)*.

**número de LP.** Número de partición lógica. Permite que diversas particiones lógicas de sistema principal, LP, compartan una sola fibra de ESCON. Este valor está definido en el programa de configuración de la entrada/salida (IOCP) del sistema principal mediante la instrucción de macro RESOURCE. Si el sistema principal no utiliza EMIF, utilice el valor por omisión de 0 para el número de LP.

**número de puerto.** En comunicaciones de Internet, identificación de una entidad de aplicación para el servicio de transporte.

**número de secuencia.** En comunicaciones, número asignado a una trama o paquete en particular para controlar el flujo de la transmisión y la recepción de datos.

**número de sistema autónomo.** En TCP/IP, número asignado a un sistema autónomo por la misma autorización central que también asigna direcciones IP. El número de sistema autónomo hace posible que los algoritmos de direccionamiento automatizado distingan los sistemas autónomos.

**Nways Switch.** Sinónimo con IBM 2220 Nways BroadBand Switch.

## O

**objeto de la MIB.** Sinónimo de *variable de la MIB*.

**Open Shortest Path First (OSPF).** En el conjunto de protocolos de Internet, función que proporciona transferencia de información intradominio. Como alternativa al protocolo Routing Information Protocol (RIP), OSPF permite el direccionamiento de menor coste y lo maneja en grandes redes regionales o corporativas.

**Organización Internacional para la Normalización (ISO).** Organización de corporaciones nacionales de normas de varios países establecida para promocionar el desarrollo de normas con el fin de facilitar el intercambio internacional de artículos y servicios además de

desarrollar la cooperación en la actividad intelectual, científica, tecnológica y económica.

**origen.** Unidad lógica (LU) externa o programa de aplicación de donde parten un mensaje u otros datos. Véase también *destino*.

## P

**paquete.** En la comunicación de datos, secuencia de dígitos binarios, con inclusión de señales de control y datos, que se transmite y se conmuta como un todo compuesto. Los datos, las señales de control y, posiblemente, la información de control de errores se ordenan siguiendo un formato específico. (I)

**paquete de datos.** En comunicaciones de X.25, paquete utilizado para la transmisión de datos de usuario dentro de un circuito virtual en la interfaz DTE/DCE.

**paquete de petición de llamada.** (1) Paquete de supervisión de llamada que un equipo terminal de datos (DTE) transmite con el fin de solicitar que se establezca una conexión para una llamada en la red. (2) En comunicaciones de X.25, paquete de supervisión de llamada transmitido por un DTE para solicitar el establecimiento de una llamada en la red.

**paquete de petición de restablecimiento.** En comunicaciones X.25, paquete transmitido por el equipo terminal de datos (DTE) al equipo de terminación de circuito de datos (DCE) para solicitar que se restablezca una llamada virtual o un circuito virtual permanente. En el paquete también puede especificarse la razón de la petición.

**paquete de recepción no preparada (RNR).** Véase *paquete de RNR*.

**paquete de RNR.** Paquete utilizado por un equipo terminal de datos (DTE) o por un equipo de terminación de circuito de datos (DCE) con el fin de indicar una incapacidad temporal para aceptar paquetes adicionales de petición de llamada virtual o circuito virtual permanente.

**paquete explorador.** En las LAN, paquete que está generado por el sistema principal de origen y que atraviesa toda la parte de direccionamiento de origen de una LAN con el fin de recoger información sobre las posibles vías de acceso que se encuentran disponibles para el sistema principal.

**parámetro de configuración.** Variable de una definición de configuración cuyos valores pueden caracterizar la relación de un producto con otros productos de la misma red o pueden definir características del producto en sí.

**par de valores de atributo (AVP).** Método uniforme de codificación de tipos y cuerpos de mensajes. Este método maximiza la extensibilidad mientras permite la interoperatividad de L2TP.

**partición lógica.** Número asignado a una partición de un sistema principal que puede funcionar en modalidad lógicamente particionada (LPAR). En modalidad LPAR, el adaptador de ESCON puede compartir una conexión de fibra física con diversas particiones de sistema principal.

**pasarela.** (1) Unidad funcional que interconecta dos redes de sistema con arquitecturas de red diferentes. Una pasarela conecta redes o sistemas de arquitecturas diferentes. Un puente interconecta redes o sistemas con la misma arquitectura o con arquitecturas similares. (T) (2) En la Red en Anillo de IBM, dispositivo y software asociado que conectan una red de área local a otra red de área local o sistema principal que utiliza protocolos de enlace lógico diferentes. (3) En TCP/IP, sinónimo de *direccionador*.

**pasarela exterior.** En comunicaciones de Internet, pasarela de un sistema autónomo que comunica con otro sistema autónomo. Compárese con *pasarela interior*.

**pasarela interior.** En comunicaciones de Internet, pasarela que sólo comunica con su propio sistema autónomo. Compárese con *pasarela exterior*.

**período de duración (TTL).** Técnica utilizada por los protocolos de entrega de mayor eficacia para impedir que los paquetes se repitan en bucle de manera interminable. El paquete se elimina si el contador de TTL alcanza el valor de 0.

**petionario de LU dependientes (DLUR).** Nodo final APPN o nodo de red APPN que posee LU dependientes pero solicita que un servidor de LU dependientes proporcione los servicios del SSCP para estas LU dependientes.

**Point-to-Point Protocol (PPP).** Protocolo que proporciona un método para encapsular y transmitir paquetes sobre enlaces serie punto a punto.

**portadora.** Tren de pulsaciones u ondas eléctricas o electromagnéticas que puede variar según una señal con información a transmitir sobre un sistema de comunicaciones. (T)

**procesador de componente frontal.** Procesador, como, por ejemplo, el IBM 3745 ó el 3174, que releva a un sistema principal de las tareas de control de comunicaciones.

**proceso a tiempo real.** Manipulación de los datos que un proceso necesita o genera mientras el proceso está en funcionamiento. Normalmente, los resultados se

utilizan para influir en el proceso y quizá en procesos relacionados, mientras se está desarrollando.

**proporción de pérdida de un paquete.** Probabilidad que tiene un paquete de no alcanzar su destino o de no alcanzarlo dentro del período especificado.

**protocolo.** (1) Conjunto de normas semánticas y sintácticas que determinan el comportamiento de las unidades funcionales a la hora de conseguir la comunicación. (I) (2) En la arquitectura Interconexión de Sistemas Abiertos, conjunto de normas semánticas y sintácticas que determinan el comportamiento de las entidades de la misma capa a la hora de desempeñar funciones de comunicación. (T) (3) En SNA, significados y normas de puesta en secuencia de las peticiones y respuestas que se utilizan para gestionar la red, transferir datos y sincronizar los estados de los componentes de la red. Sinónimo con *disciplina de control de línea* y *disciplina de línea*. Véase *protocolo delimitador* y *protocolo de enlace*.

**protocolo de acceso de enlace equilibrado (LAPB).** Protocolo utilizado para acceder a una red X.25 en el nivel de enlace. LAPB es un protocolo simétrico, asíncrono y dúplex que se utiliza en la comunicación punto a punto.

**protocolo de control de enlace lógico (LLC).** En una red de área local, protocolo que dirige el intercambio de tramas de transmisión entre estaciones de datos independientemente de cómo está compartido el medio de transmisión. (T) El protocolo de LLC se desarrolló en la comisión de IEEE 802 y es común a todas las normas de LAN.

**protocolo de control del acceso al medio (MAC).** En una red de área local, protocolo que dirige el acceso al medio de transmisión, teniendo en cuenta los aspectos topológicos de la red, con el fin de permitir el intercambio de datos entre estaciones de datos. (T)

**protocolo de direccionamiento.** Técnica utilizada por un direccionador para encontrar otros direccionadores y mantener información actualizada sobre la mejor manera de acceder a las redes asequibles.

**protocolo de interfaz de gestión local (LMI).** En un NCP, conjunto de procedimientos y mensajes de gestión de red Frame-Relay utilizados por nodos Frame-Relay adyacentes para intercambiar información de estado de línea sobre el DLCI X'00'. Un NCP da soporte tanto a la versión del protocolo de LMI del American National Standards Institute (ANSI) como a la de la Comisión Consultiva de la Telefonía y Telegrafía Internacionales (ITU-T/CCITT). Estas normas se refieren al protocolo de LMI como *pruebas de verificación de integridad de enlace (LIVT)*.

**prueba de bucle de retorno.** Prueba donde las señales de un comprobador se repiten en bucle en un módem u otro elemento de red hacia el comprobador para tomar medidas que determinen o verifiquen la calidad de la vía de acceso de comunicaciones.

**puente.** Unidad funcional que interconecta diversas LAN (local o remotamente) que utilizan el mismo protocolo de control de enlace lógico pero que pueden utilizar diferentes protocolos de control del acceso al medio. Un puente reenvía una trama a otro puente basándose en la dirección del control del acceso al medio (MAC).

**puente de ruta.** Función de un programa de puente de IBM que permite que dos sistemas de puente utilicen un enlace de telecomunicaciones para conectar dos LAN. Cada sistema de puente se conecta directamente a una de las LAN y el enlace de telecomunicaciones conecta los dos sistemas de puente.

**puente raíz.** Puente que es la raíz de un árbol de expansión formado entre otros puentes activos de la red de funciones de puente. El puente raíz origina y transmite unidades de datos de protocolo de puente (BPDU) a otros puentes activos para mantener la topología de árbol de expansión. Es el puente con la prioridad superior de la red.

**puentes paralelo.** Par de puentes conectados al mismo segmento de LAN que crean vías de acceso redundantes para el segmento.

**puerto.** (1) Punto de acceso para la entrada o salida de datos. (2) Conector de un dispositivo al que se conectan cables para otros dispositivos, como, por ejemplo, estaciones de pantalla o impresoras. (3) Representación de una conexión física con el hardware de enlace. A veces, un puerto viene referido como adaptador; no obstante, en un adaptador puede haber más de un puerto. Un solo proceso de DLC puede controlar uno o más puertos. (4) En el conjunto de protocolos de Internet, número de 16 bits utilizado para la comunicación entre TCP o el protocolo User Datagram Protocol (UDP) y una aplicación o protocolo de nivel superior. Algunos protocolos, como, por ejemplo, File Transfer Protocol (FTP) y Simple Mail Transfer Protocol (SMTP), utilizan el mismo número de puerto conocido en todas las implementaciones de TCP/IP. (5) Abstracción utilizada por protocolos de transporte para establecer diferencias entre los diversos destinos en una máquina de sistema principal. (6) Sinónimo con *socket*.

**puerto de destino.** Adaptador asíncrono de 8 puertos que sirve de punto de conexión con un servicio serie.

**punto de acceso a servicios de destino (DSAP).** En SNA y TCP/IP, dirección lógica que permite que un sistema direcciona datos desde un dispositivo remoto al



soporte de comunicaciones correspondiente. Compárese con *punto de acceso a servicios de origen (SSAP)*.

**punto de acceso a servicios de origen (SSAP).** En SNA y TCP/IP, dirección lógica que permite que un sistema envíe datos a un dispositivo remoto desde el soporte de comunicaciones correspondiente. Compárese con *punto de acceso a servicios de destino (DSAP)*.

**punto de acceso a servicios (SAP).** (1) En la arquitectura Interconexión de Sistemas Abiertos (OSI), punto en el que una entidad de una capa proporciona los servicios de esta capa a una entidad de la capa superior más próxima. (T) (2) Punto lógico que queda disponible mediante un adaptador y donde puede recibirse y transmitirse información. Muchos enlaces pueden terminar en un solo punto de acceso a servicios.

**punto de control (CP).** (1) Componente de un nodo APPN o LEN que gestiona los recursos de dicho nodo. En un nodo APPN, el CP puede dedicarse a establecer sesiones de CP-CP con otros nodos APPN. En un nodo de red APPN, el CP también proporciona servicios a nodos finales adyacentes de la red APPN. (2) Componente de un nodo que gestiona los recursos de dicho nodo y, opcionalmente, proporciona servicios a otros nodos de la red. Pueden citarse como ejemplos el punto de control de servicios del sistema (SSCP) de un nodo de subárea de tipo 5, el punto de control de nodo de red (NNCP) de un nodo de red APPN y el punto de control de nodo final (ENCP) de un nodo final APPN o LEN. Un SSCP y un NNCP pueden proporcionar servicios a otros nodos.

**punto de control de servicios del sistema (SSCP).** Componente de una red de subárea destinado a gestionar la configuración, coordinar las peticiones del operador de red y las de determinación de problemas y proporcionar servicios de directorio además de otros servicios de sesiones para los usuarios de la red. Diversos SSCP, cooperando como iguales entre sí, pueden dividir la red en dominios de control y tener, cada uno de los SSCP, una relación de control jerárquica con las unidades físicas y las unidades lógicas de su propio dominio.

**punto de entrada (EP).** En SNA, nodo de tipo 2.0, tipo 2.1, tipo 4 ó tipo 5 que proporciona soporte de gestión de redes distribuidas. Envía datos de gestión de redes sobre sí mismo y los recursos que controla a un punto focal para el proceso centralizado, y recibe y ejecuta los mandatos iniciados por el punto focal para gestionar y controlar sus recursos.

## R

**rastreo.** (1) Registro de la ejecución de un programa de sistema. Muestra las secuencias en que se han ejecutado las instrucciones. (A) (2) Para los enlaces de datos, registro de las tramas y bytes transmitidos o recibidos.

**recepción no preparada (RNR).** En comunicaciones, mandato o respuesta de enlace de datos que indica una condición temporal de incapacidad para aceptar tramas de entrada.

**reconfiguración dinámica (DR).** Proceso consistente en cambiar la configuración de una red (las PU y LU periféricas) sin regenerar las tablas de configuración al completo ni desactivar el nodo principal afectado.

**recurso.** En Nways Switch, elemento de hardware o entidad lógica creados por Control Program. Por ejemplo, los adaptadores, LIC y líneas son recursos físicos. Los puntos de control y conexiones son recursos lógicos.

**red.** (1) Configuración de software y dispositivos de proceso de datos conectados para el intercambio de información. (2) Grupo de nodos y los enlaces que los interconectan.

**red Advanced Peer-to-Peer Networking (APPN).** Conjunto de nodos de red interconectados y sus nodos finales clientes.

**red APPN.** Véase *red Advanced Peer-to-Peer Networking (APPN)*.

**red de área amplia (WAN).** (1) Red que proporciona servicios de comunicación a un área geográfica mayor que la servida por una red de área local o una red de área metropolitana, y que puede utilizar o proporcionar recursos públicos de comunicación. (T) (2) Red de comunicación de datos diseñada para servir a un área de cientos o miles de kilómetros; por ejemplo, las redes públicas y privadas de conmutación de paquetes y las redes telefónicas nacionales. (3) Compárese con *red de área local (LAN)* y *red de área metropolitana (MAN)*.

**red de área local (LAN).** (1) Red de sistema ubicada en el lugar de un usuario dentro de un área geográfica limitada. La comunicación dentro de una red de área local no está sujeta a reglamentos externos; no obstante, la comunicación más allá de la frontera de una LAN puede estar sujeta a alguna forma de reglamento. (T) (2) Red en la que un conjunto de dispositivos están conectados entre sí para la comunicación y que puede conectarse a una red mayor. (3) Véase también *Ethernet* y *Red en Anillo*. (4) Compárese con *red de área metropolitana (MAN)* y *red de área amplia (WAN)*.

**red de área metropolitana (MAN).** Red formada por la interconexión de dos o más redes que puede funcionar a una velocidad mayor que éstas, puede atravesar fronteras administrativas y puede utilizar diversos métodos de acceso. (T) Compárese con *red de área local (LAN)* y *red de área amplia (WAN)*.

**red de clase A.** En comunicaciones de Internet, red en la que el bit situado más a la izquierda (más significativo) de la dirección IP está establecido en 0 y el identificador de sistema principal ocupa los tres octetos situados más a la derecha.

**red de clase B.** En comunicaciones de Internet, red en la que los dos bits situados más a la izquierda (más significativo y próximo al más significativo) de la dirección IP están establecidos en 1 y 0, respectivamente, y el identificador de sistema principal ocupa los dos octetos situados más a la derecha.

**red de entrada baja (LEN).** Posibilidad de los nodos de conectarse directamente entre sí utilizando protocolos básicos de igual a igual para dar soporte a sesiones múltiples y en paralelo entre unidades lógicas.

**red de tipo anillo.** (1) Red en la que cada nodo tiene exactamente dos ramas conectadas y en la que hay exactamente dos vías de acceso entre dos nodos cualesquiera. (T) (2) Configuración de red en la que los dispositivos están conectados mediante enlaces de transmisión unidireccional para formar una vía de acceso cerrada.

**red digital de servicios integrados (RDSI).** Red digital de telecomunicaciones de extremo a extremo que da soporte a diversos servicios, los cuales incluyen voz y datos pero no se limitan a ello.

**Nota:** Las RDSI se utilizan en arquitecturas de red públicas y privadas.

**Red en Anillo.** (1) Según la norma IEEE 802.5, tecnología de red que controla el acceso al medio pasando una señal (paquete o trama especial) entre las estaciones conectadas al medio. (2) Red FDDI o IEEE 802.5 con una topología de anillo que pasa señales de una estación de anillo de conexión (nodo) a otra. (3) Véase también *red de área local (LAN)*.

**red óptica síncrona (SONET).** Norma de los EE.UU. para la transmisión de información digital sobre interfaces ópticas. Está estrechamente relacionada con la recomendación sobre la jerarquía digital síncrona (SDH).

**red según Red en Anillo.** (1) Red de tipo anillo que permite la transmisión de datos unidireccional entre estaciones de datos, mediante un procedimiento consistente en pasar señales, de tal manera que los datos transmitidos vuelven a la estación transmisora. (T)

(2) Red que utiliza una topología de anillo, según la cual pasan señales en un circuito de nodo a nodo. Un nodo que está preparado para emitir puede capturar la señal e insertar datos para la transmisión.

**red troncal.** Red central a la que se conectan redes más pequeñas, casi siempre de menor velocidad. Normalmente, la red troncal tiene una capacidad muy superior a las redes a las que ayuda a interconectarse o es una red de área amplia (WAN), como, por ejemplo, una red pública de datagramas de paquetes conmutados.

**reensamblaje.** En comunicaciones, proceso consistente en volver a juntar paquetes segmentados después de haberlos recibido.

**Registro sin vuelta a cero y con cambios en los unos (NRZ-1).** Método de registro donde los unos están representados mediante un cambio en la condición de magnetización y los ceros están representados mediante la ausencia de cambio. Sólo se registran explícitamente las señales de los unos. (Denominado anteriormente registro *sin vuelta a cero invertido*, NRZI.)

**Remote Execution Protocol (REXEC).** Protocolo que permite la ejecución de un mandato o programa en cualquier sistema principal de la red. El sistema principal local recibe los resultados de la ejecución del mandato.

**remoto.** (1) Perteneciente a un sistema, programa o dispositivo al que se accede mediante una línea de telecomunicaciones. (2) Sinónimo de *conectado mediante enlace*. (3) Compárese con *local*.

**Request for Comments (RFC).** En comunicaciones de Internet, serie de documentos que describe una parte del conjunto de protocolos de Internet y experimentos relacionados. Todas las normas de Internet están documentadas como RFC.

**resolución de direcciones.** (1) Método para correlacionar direcciones de capa de red con direcciones específicas de los medios. (2) Véase también *Address Resolution Protocol (ARP)* y *AppleTalk Address Resolution Protocol (AARP)*.

**resolución de nombres.** En comunicaciones de Internet, proceso consistente en correlacionar un nombre de máquina con la dirección Internet Protocol (IP) correspondiente. Véase también *Sistema de nombres de dominio (DNS)*.

**respuesta a excepción (ER).** En SNA, protocolo solicitado en el campo de formato de respuesta solicitado de la cabecera de una petición que indica al receptor que devuelva una respuesta sólo si la petición no es aceptable tal como se recibe o si no puede procesarse;

es decir, puede devolverse una respuesta negativa, pero no una respuesta positiva. Compárese con *respuesta definida y sin respuesta*.

**restablecimiento.** En un circuito virtual, reinicialización del control del flujo de datos. En el restablecimiento, se eliminan todos los datos en tránsito.

**ritmo.** (1) Técnica mediante la cual un componente de recepción controla la velocidad de transmisión de un componente de emisión para evitar un desbordamiento o una congestión. (2) Véase también *control del flujo*, *ritmo de recepción*, *ritmo de emisión*, *ritmo de nivel de sesión* y *ritmo de ruta virtual (VR)*.

**rlogin (inicio de sesión remoto).** Servicio ofrecido por los sistemas de Berkeley basados en UNIX que permite que los usuarios autorizados de una máquina se conecten con otros sistemas UNIX en una internet e interactúen como si sus terminales estuvieran conectados directamente. El software rlogin pasa información sobre el entorno del usuario (por ejemplo, el tipo de terminal) a la máquina remota.

**Routing Information Protocol (RIP).** En el conjunto de protocolos de Internet, protocolo de pasarela interior utilizado para intercambiar información de direccionamiento intradominio y para determinar las rutas óptimas entre los sistemas principales de internet. RIP determina las rutas óptimas sobre la base de la métrica de ruta y no sobre la base de la velocidad de transmisión de un enlace.

**Routing Table Maintenance Protocol (RTMP).** En redes AppleTalk, protocolo que proporciona generación y mantenimiento de información de direccionamiento en la capa de transporte por medio de la tabla de direccionamiento AppleTalk. La tabla de direccionamiento AppleTalk dirige la transmisión de paquetes por la internet de socket de origen a socket de destino.

**RouTing update Protocol (RTP).** Protocolo de Virtual NETworking System (VINES) que mantiene la base de datos de direccionamiento y permite el intercambio de información de direccionamiento entre nodos VINES. Véase también *Internet Control Protocol (ICP)*.

**rsh.** Variante del mandato rlogin que invoca un interpretador de mandatos en una máquina remota UNIX y pasa los argumentos de línea de mandatos al interpretador de mandatos saltándose completamente el paso de inicio de sesión.

**ruta.** (1) Secuencia ordenada de nodos y grupos de transmisión (TG) que representan una vía de acceso de un nodo de origen a un nodo de destino por la que pasa el tráfico intercambiado entre éstos. (2) Vía de acceso que el tráfico de red utiliza para ir del origen al destino.

**ruta estática.** Ruta entre sistemas principales y/o redes que se entra manualmente en una tabla de direccionamiento.

**ruta explícita (ER).** En SNA, serie de uno o más grupos de transmisión que conectan dos nodos de subárea. Una ruta explícita se identifica mediante una dirección de subárea de origen, una dirección de subárea de destino, un número de ruta explícita y un número de ruta explícita inversa. Compárese con *ruta virtual (VR)*.

**ruta virtual (VR).** (1) En SNA, (a) conexión lógica entre dos nodos de subárea que se realiza físicamente como una ruta explícita en particular o (b) conexión lógica contenida en su totalidad dentro de un nodo de subárea para las sesiones intranodo. Una ruta virtual entre nodos de subárea distintos impone una prioridad de transmisión sobre la ruta explícita subyacente, proporciona control del flujo mediante el ritmo de ruta virtual y proporciona la integridad de los datos mediante la numeración en secuencia de las unidades de información de vía de acceso (PIU). (2) Compárese con *ruta explícita (ER)*. Véase también *vía de acceso y extensión de ruta (REX)*.

**rutina de carga.** (1) Secuencia de instrucciones cuya ejecución hace que se carguen y se ejecuten unas instrucciones adicionales hasta que se haya almacenado todo el programa de sistema. (T) (2) Técnica o dispositivo diseñado para que entre en un estado determinado por medio de su propia acción, por ejemplo, una rutina de máquina cuyas primeras instrucciones sean suficientes para que el resto de la misma entre en el sistema desde un dispositivo de entrada. (A)

## S

**salto.** (1) En APPN, parte de una ruta que no tiene nodos intermedios. Está compuesto por un solo grupo de transmisión que conecta nodos adyacentes. (2) Para la capa de direccionamiento, distancia lógica entre dos nodos en una red.

**SAP.** Véase punto de acceso a servicios.

**segmentación.** En OSI, función realizada por una capa para correlacionar una unidad de datos de protocolo (PDU) de la capa a la que da soporte con diversas PDU.

**segmento.** (1) Sección de cable entre componentes o dispositivos. Un segmento puede estar compuesto por un solo cable provisional, diversos cables provisionales conectados o una combinación de cables provisionales y de construcción conectados. (2) En comunicaciones de Internet, unidad de transferencia entre funciones de TCP en diferentes máquinas. Cada segmento contiene campos de control y de datos; la posición de corriente

de bytes actual y los bytes de datos reales se identifican conjuntamente con una suma de comprobación para validar los datos recibidos.

**segmento de anillo.** Parte de un anillo que puede aislarse (desenchufando conectores) del resto del anillo. Véase *segmento de LAN*.

**segmento de LAN.** (1) Cualquier parte de una LAN (por ejemplo, un bus o un anillo) que puede funcionar independientemente pero está conectada a otras partes de la red por medio de puentes. (2) Red de tipo bus o anillo sin puentes.

**señal.** (1) En una red de área local, símbolo de autorización pasado sucesivamente de una estación de datos a otra para indicar la estación que tiene temporalmente el control del medio de transmisión. Cada estación de datos tiene una oportunidad de obtener y utilizar la señal para controlar el medio. Una señal es un mensaje o patrón de bits determinado que significa el permiso para transmitir. (T) (2) En las LAN, secuencia de bits pasada de un dispositivo a otro por el medio de transmisión. Cuando la señal tiene datos añadidos, se convierte en una trama.

**Serial Line Internet Protocol (SLIP).** Protocolo utilizado sobre una conexión punto a punto entre dos sistemas principales de IP de una línea serie, como, por ejemplo, un cable serie o una conexión RS232 con un módem, de una línea telefónica.

**Service Advertising Protocol (SAP).** En Internetwork Packet Exchange (IPX), protocolo que proporciona lo siguiente:

- Un mecanismo que permite que los servidores IPX de una internet anuncien sus servicios por el nombre y el tipo. Los servidores que utilizan este protocolo tienen registrados su nombre, tipo de servicios y dirección en todos los servidores de archivos que ejecutan NetWare.
- Un mecanismo que permite que una estación de trabajo difunda una consulta para descubrir las identidades de todos los servidores de todos los tipos, todos los servidores de un tipo específico o el servidor más cercano de un tipo específico.
- Un mecanismo que permite que una estación de trabajo consulte cualquier servidor de archivos que ejecute NetWare para descubrir nombre y dirección de todos los servidores de un tipo específico.

**servicio de directorio (DS).** Elemento de servicio de aplicaciones que convierte los nombres simbólicos utilizados por procesos de aplicaciones en direcciones de red completas utilizadas en un entorno de OSI. (T)

**servicios de directorio (DS).** Componente del punto de control de un nodo APPN que mantiene la información sobre la ubicación de los recursos de red.

**servicios de gestión de punto de control (CPMS).** Componente de un punto de control que consta de conjuntos de funciones de servicios de gestión y proporciona recursos de ayuda para realizar la gestión de problemas, gestión del rendimiento y de la contabilidad, gestión de los cambios y gestión de la configuración. Las posibilidades proporcionadas por los CPMS incluyen el envío de peticiones a los servicios de gestión de unidad física (PUMS) para probar recursos del sistema, la reunión de información estadística (por ejemplo, datos de errores y del rendimiento) de los PUMS sobre los recursos del sistema y el análisis y presentación de los resultados de las pruebas y la información estadística reunida sobre los recursos del sistema. Las responsabilidades del análisis y de la presentación para la determinación de problemas y la supervisión del rendimiento pueden distribuirse entre los diversos CPMS.

**servicios de gestión de SNA (SNA/MS).** Servicios proporcionados como ayuda para la gestión de las redes SNA.

**servidor.** Unidad funcional que proporciona servicios compartidos a estaciones de trabajo sobre una red; por ejemplo, un servidor de archivos, un servidor de impresión, un servidor de correo. (T)

**servidor de acceso a red (NAS).** Dispositivo que proporciona a los usuarios acceso a red temporal a petición. Este acceso es punto a punto por medio de líneas PSTN o RDSI.

**servidor de configuración de emulación de LAN (LECS).** Componente de LAN Emulation Service que centraliza y difunde datos de configuración.

**servidor de emulación de LAN (LES).** Componente de LAN Emulation Service que resuelve destinos de LAN en direcciones ATM.

**servidor de informes de configuración (CRS).** En el programa Bridge para la Red en Anillo de IBM, servidor que acepta mandatos del LAN Network Manager (LNM) para obtener información de estaciones, establecer parámetros de estación y eliminar estaciones de su anillo. Este servidor también recoge y reenvía informes de configuración generados por estaciones de su anillo. Los informes de configuración incluyen los nuevos informes del supervisor activo y los informes de estación contigua activa de donde proceden los datos (NAUN).

**servidor de nombres.** En el conjunto de protocolos de Internet, sinónimo de *servidor de nombres de dominio*.

**servidor de nombres de dominio.** En el conjunto de protocolos de Internet, programa servidor que sumi-

nistra la conversión de nombres en direcciones correlacionando nombres de dominio con direcciones IP. Sinónimo con *servidor de nombres*.

**servidor de puentes de LAN (LBS).** En el programa Bridge para la Red en Anillo de IBM, servidor que mantiene información estadística sobre las tramas reenviadas entre dos o más anillos (mediante un puente). El LBS envía estas estadísticas a los gestores de LAN correspondientes mediante el mecanismo de información de LAN (LRM).

**servidor de red L2TP (LNS).** Un LNS funciona en cualquier plataforma capacitada que pueda ser una estación final de PPP. El LNS maneja la parte del servidor del protocolo L2TP. Puesto que L2TP sólo se apoya en el único medio por el que llegan los túneles de L2TP, el LNS sólo tiene una interfaz LAN o WAN, aunque puede terminar las llamadas que lleguen de cualquier interfaz del rango completo de interfaces PPP soportadas por un LAC. Entre éstas se incluyen la RDSI asíncrona, RDSI síncrona, V.120 y otros tipos de conexiones.

**sesión.** (1) En la arquitectura de red, con el fin de la comunicación de datos entre unidades funcionales, todas las actividades que tienen lugar durante el establecimiento, mantenimiento y liberación de la conexión. (T) (2) Conexión lógica entre dos unidades de red accesibles (NAU) que puede activarse, adaptarse, para proporcionar varios protocolos y desactivarse de la manera solicitada. Cada sesión está identificada de manera exclusiva en la cabecera de transmisión (TH) que acompaña a cualquier transmisión intercambiada durante la sesión. (3) En L2TP, L2TP crea una sesión cuando se intenta una conexión PPP de extremo a extremo entre un usuario de marcación y los LNS; sin tener en cuenta si el usuario inicia la sesión o si el LNS inicia una llamada hacia fuera. Los datagramas para la sesión se envían por el túnel entre el LAC y el LNS. Los LNS y LAC mantienen la información de estado para cada usuario conectado a un LAC.

**Simple Network Management Protocol (SNMP).** En el conjunto de protocolos de Internet, protocolo de gestión de red que se utiliza para supervisar direccionadores y redes conectadas. SNMP es un protocolo de capa de aplicación. La información sobre los dispositivos gestionados está definida y almacenada en la Base de la información de gestión (MIB) de la aplicación.

**simulación.** Para los enlaces de datos, técnica mediante la cual un protocolo iniciado en una estación final se reconoce con acuse de recibo y se procesa en un nodo intermedio en nombre del destino final. En la conmutación del enlace de datos del IBM 6611, por ejemplo, las tramas de SNA se encapsulan en paquetes de TCP/IP para el transporte a través de una

red de área amplia diferente de SNA, se desempaquetan en otro IBM 6611 y pasan al destino final. Una ventaja de la simulación es que se evitan tiempos de espera excedidos de sesión de final a final.

**síncrono.** (1) Perteneciente a dos o más procesos que dependen de la aparición de sucesos específicos, como, por ejemplo, señales comunes de temporización. (T) (2) Que se produce con una relación temporal regular o previsible.

**sintaxis de abstracción.** Especificación de datos que incluye todas las distinciones necesarias en las transmisiones de datos, pero que omite (excluye) otros detalles, como, por ejemplo, los que dependen de las arquitecturas específicas de los sistemas. Véase también *notación de sintaxis de abstracción 1 (ASN.1)* y *normas básicas de codificación (BER)*.

**sistema.** En el proceso de datos, conjunto de personas, máquinas y métodos organizados para llevar a cabo un conjunto de funciones específicas. (I) (A)

**sistema autónomo.** En TCP/IP, grupo de redes y direccionadores bajo una sola autorización administrativa. Estas redes y estos direccionadores cooperan estrechamente para propagar la información de asequibilidad (y direccionamiento) de la red entre ellos utilizando un protocolo de pasarela interior de su elección.

**sistema de juego reducido de instrucciones (RISC).** Sistema que utiliza un juego pequeño y simplificado de instrucciones de uso frecuente para la ejecución rápida.

**sistema de nombres de dominio (DNS).** En el conjunto de protocolos de Internet, sistema de bases de datos distribuidas utilizado para correlacionar nombres de dominio con direcciones IP.

**sistema principal.** En el conjunto de protocolos de Internet, sistema final. El sistema final puede ser cualquier estación de trabajo; no es necesario que sea un sistema principal.

**socket.** (1) Punto final para la comunicación entre procesos o programas de aplicación. (2) Abstracción proporcionada por la Distribución de software de Berkeley de la Universidad de California (software que suele recibir el nombre de UNIX de Berkeley o UNIX de BSD) que funciona como punto final para la comunicación entre procesos o aplicaciones.

**sonda de paquetes Internet (PING).** (1) En comunicaciones de Internet, programa utilizado en redes TCP/IP para probar la capacidad de alcanzar destinos enviando a los mismos una petición con eco de Internet Control Message Protocol (ICMP) y esperando una respuesta. (2) En comunicaciones, prueba de asequibilidad.

**sondeo.** (1) En una conexión multipunto o conexión punto a punto, proceso consistente en invitar a las estaciones de datos a transmitir, una por una. (I) (2) Interrogar a dispositivos con el fin de evitar contenciones, determinar el estado operativo o determinar la disposición para enviar o recibir datos. (A)

**soporte de diversos dominios (MDS).** Técnica para transportar datos de servicios de gestión entre conjuntos de funciones de servicios de gestión sobre sesiones de LU-LU y CP-CP. Véase también *unidad de mensajería de soporte de diversos dominios (MDS-MU)*.

**StreetTalk.** En Virtual NETworking System (VINES), sistema exclusivo de denominación y direccionamiento de red amplia que permite que los usuarios ubiquen cualquier recurso de la red y accedan al mismo sin conocer la topología de la red. Véase también *Internet Control Protocol (ICP)* y *RouTing update Protocol (RTP)*.

**subárea.** Parte de la red SNA compuesta por un nodo de subárea, nodos periféricos conectados y recursos asociados. En un nodo de subárea, todas las unidades de red accesibles (NAU), enlaces y estaciones de enlace adyacentes (de nodos de subárea o nodos periféricos conectados) que son dirigibles dentro de la subárea comparten una dirección de subárea común y tienen direcciones de elementos distintas.

**subcapa del control del acceso al medio (MAC).** En una red de área local, parte de la capa de enlace de datos que aplica un método de acceso al medio. La subcapa del MAC da soporte a funciones dependientes de la topología y utiliza los servicios de la capa física para proporcionar servicios a la subcapa de control de enlace lógico. (T)

**Subnetwork Access Protocol (SNAP).** En las LAN, protocolo encargado de establecer diferencias entre protocolos de 5 bytes que identifica la familia de protocolos estándares distintos de IEEE a la que pertenece un paquete. El valor de SNAP se utiliza para diferenciar los protocolos que utilizan \$AA como valor de punto de acceso a servicios (SAP).

**subred.** (1) En TCP/IP, parte de una red que se identifica mediante una parte de la dirección IP. (2) Sinónimo de *subred (grupo de nodos)*.

**subred (grupo de nodos).** (1) Cualquier grupo de nodos que tienen un conjunto de características comunes, como, por ejemplo, el mismo identificador de red. (2) Sinónimo con *subred*.

**subsistema.** Sistema secundario o subordinado que a menudo puede funcionar de manera independiente o asíncrona respecto a un sistema de control. (T)

**suma de comprobación.** (1) Suma de un grupo de datos que se asocia con el grupo y se utiliza con fines

de comprobación. (T) (2) En la detección de errores, función de todos los bits de un bloque. Si las sumas grabadas y las calculadas no coinciden, se indica que hay un error. (3) En un disquete, datos grabados en un sector con fines de detección de errores; una suma de comprobación calculada que no coincide con la suma de comprobación de los datos grabados en el sector indica que hay un sector anómalo. Los datos son numéricos u otras series de caracteres consideradas numéricas con el fin de calcular la suma de comprobación.

**supervisor.** (1) Dispositivo que observa y registra actividades seleccionadas en un sistema de proceso de datos para el análisis. Sus usos posibles son para indicar cualquier desviación significativa de la norma o para determinar los niveles de utilización de unidades funcionales en particular. (T) (2) Software o hardware que observa, supervisa, controla o verifica operaciones de un sistema. (A) (3) Función necesaria para iniciar la transmisión de una señal del anillo y para proporcionar recuperación de errores de software en el caso de que se pierdan señales, tramas en circulación u otras dificultades. La posibilidad está presente en todas las estaciones de anillo.

**supervisor activo.** En una Red en Anillo, función realizada en cualquier momento por una estación de anillo que inicia la transmisión de señales y proporciona recursos de recuperación de errores de señales. Cualquier adaptador activo del anillo tiene la posibilidad de proporcionar la función de supervisor activo si falla el supervisor activo actual.

**SYNTAX.** En el protocolo Simple Network Management Protocol (SNMP), cláusula del módulo de la MIB que define la estructura de datos abstracta correspondiente a un objeto gestionado.

**Systems Network Architecture (SNA).** Descripción de la estructura lógica, formatos, protocolos y secuencias operativas para la transmisión de unidades de información a través de las redes y para el control de la configuración y del funcionamiento de las mismas. La estructura de capas de SNA permite que los orígenes y destinos finales de la información, es decir, los usuarios, sean independientes de los servicios y recursos de red SNA específicos utilizados para el intercambio de información y que no se vean afectados por dichos servicios y recursos.

## T

**T1.** En los Estados Unidos, línea de acceso público de 1,544 Mbps. Está disponible en veinticuatro canales de 64 Kbps. La versión europea (E1) transmite a 2,048 Mbps.

**tabla de correlación de direcciones (AMT).** Tabla

mantenida en el direccionador AppleTalk que proporciona la correlación actual de las direcciones de nodo con las direcciones de hardware.

**tabla de direccionamiento.** Conjunto de rutas utilizadas para dirigir el reenvío de datagramas o para establecer una conexión. La información pasa entre direccionadores para identificar la topología de red y la factibilidad de los destinos.

**tabla de información de zonas (ZIT).** Listado de números de red y sus correlaciones con los nombres de zonas asociadas de internet. Cada direccionador de internet mantiene este listado en una internet AppleTalk.

**TCP/IP.** (1) Transmission Control Protocol/Internet Protocol. (2) Protocolo de interconexión de sistemas basado en Ethernet/de tipo UNIX que desarrolló originalmente el Departamento de Defensa de los EE.UU. TCP/IP facilitó ARPANET (Advanced Research Projects Agency Network), una red de paquetes conmutados para la investigación en que la capa 4 era TCP y la capa 3, IP.

**Telnet.** En el conjunto de protocolos de Internet, protocolo que proporciona un servicio de conexión de terminales remotos. Permite que los usuarios de un sistema principal se conecten con un sistema principal remoto e interactúen como usuarios de terminal conectado directamente de este sistema principal.

**terminal de datos preparado (DTR).** Señal para el módem que se utiliza con el protocolo EIA 232.

**tiempo de espera excedido.** (1) Suceso que se produce al final de un período predeterminado de tiempo que ha empezado al aparecer otro suceso especificado. (1) (2) Intervalo de tiempo asignado para que tengan lugar determinadas operaciones; por ejemplo, la respuesta a un sondeo o direccionamiento antes de que se interrumpa el funcionamiento del sistema y deba reiniciarse.

**topología.** En comunicaciones, ordenación física o lógica de los nodos de una red, especialmente las relaciones de un nodo con otro nodo y los enlaces entre los mismos.

**trama.** (1) En la arquitectura Interconexión de Sistemas Abiertos, estructura de datos perteneciente a un área particular de información y compuesta por ranuras que pueden aceptar los valores de atributos específicos y de las que pueden deducirse inferencias mediante conexiones apropiadas de procedimiento. (T) (2) Unidad de transmisión en algunas redes de área

local, incluida la Red en Anillo de IBM. Incluye delimitadores, caracteres de control, información y caracteres de comprobación. (3) En SDLC, vehículo para cada mandato, cada respuesta y toda información transmitida con procedimientos de SDLC.

**trama de información (I).** Trama de formato I que se utiliza para la transferencia de información numerada.

**trama exploradora.** Véase *paquete explorador*.

**trama I.** Trama de información.

**transceptor (transmisor-receptor).** En las LAN, dispositivo físico que conecta una interfaz de sistema principal a una red de área local, como, por ejemplo, Ethernet. Los transceptores de Ethernet contienen elementos electrónicos que aplican señales al cable y que detectan colisiones.

**Transmission Control Protocol/Internet Protocol (TCP/IP).** Conjunto de protocolos de comunicaciones que dan soporte a funciones de conectividad de igual a igual para redes de área local y amplia.

**Transmission Control Protocol (TCP).** Protocolo de comunicaciones utilizado en Internet y en cualquier red que siga las normas del Departamento de Defensa de los EE.UU. para el protocolo interredes. TCP proporciona un protocolo fiable de sistema principal a sistema principal entre sistemas principales en redes de comunicaciones de paquetes conmutados y en los sistemas interconectados de dichas redes. Utiliza Internet Protocol (IP) como protocolo subyacente.

**transporte de vector de gestión de red (NMVT).** Unidad de petición/respuesta (RU) de servicios de gestión que fluye sobre una sesión activa entre servicios de gestión de unidad física y servicios de gestión de punto de control (sesión de SSCP-PU).

**troncal.** (1) En una configuración de anillo de diversos puentes de una red de área local, enlace de gran velocidad al que se conectan los anillos por medio de puentes o direccionadores. Un troncal puede configurarse como bus o como anillo. (2) En una red de área amplia, enlace de gran velocidad al que se conectan nodos o intercambios de conmutaciones de datos (DSE).

**túnel.** Un túnel está definido mediante un par LNS-LAC. El túnel lleva datagramas de PPP entre el LAC y el LNS. Un solo túnel puede multiplexar muchas sesiones. Una conexión de control que funciona sobre el mismo túnel controla el establecimiento, liberación y mantenimiento de todas las sesiones y del túnel en sí.

## U

**umbral.** (1) En programas de puente de IBM, valor asignado al número máximo de tramas que no se reen-vían por un puente debido a errores antes de que se cuente una aparición de "umbral sobrepasado" y se indique en los programas de gestión de red. (2) Valor inicial a partir del cual un contador disminuye hasta 0 o valor hasta el que aumenta o disminuye un contador a partir de un valor inicial.

**unidad básica de transmisión (BTU).** En SNA, unidad de datos e información de control que pasa entre los componentes del control de la vía de acceso. Una BTU puede constar de una o más unidades de información de vía de acceso (PIU).

**unidad de datos de protocolo de control de enlace lógico (LLC).** Unidad de información intercambiada entre estaciones de enlace de diferentes nodos. La unidad de datos de protocolo de LLC contiene un punto de acceso a servicios de destino (DSAP), un punto de acceso a servicios de origen (SSAP), un campo de control y datos de usuario.

**unidad de datos de protocolo (PDU).** Unidad de datos especificada en un protocolo de una capa determinada y compuesta por información de control de protocolo de esta capa además de, posiblemente, datos de usuario de esta capa. (T)

**unidad de información de vía de acceso (PIU).** Unidad de mensaje compuesta por una sola cabecera de transmisión (TH) o por una TH seguida de una unidad básica de información (BIU) o un segmento de BIU.

**unidad de mensaje de soporte de diversos dominios (MDS-MU).** Unidad de mensaje utilizada en el soporte de diversos dominios que contiene datos de servicios de gestión y fluye entre conjuntos de funciones de servicios de gestión sobre las sesiones de LU-LU y CP-CP. Esta unidad de mensaje, así como los datos reales de servicios de gestión que contiene, tiene el formato de corriente de datos general (GDS). Véase también *unidad de servicios de gestión de punto de control (CP-MSU)*, *unidad de servicios de gestión (MSU)* y *transporte de vector de gestión de red (NMVT)*.

**unidad de red accesible (NAU).** Unidad lógica (LU), unidad física (PU), punto de control (CP) o punto de control de servicios del sistema (SSCP). Es el origen o el destino de la información transmitida por la red de control de la vía de acceso. Sinónimo con *unidad de red direccionable*.

**unidad de red direccionable (NAU).** Sinónimo de *unidad de red accesible*.

**unidad de servicio de canal (CSU).** Unidad que proporciona la interfaz a una red digital. La CSU proporciona funciones de acondicionamiento (o igualación) de línea, que mantienen la uniformidad del rendimiento de la señal a lo largo del ancho de banda de canal; remodelación de señal, que constituye la corriente de pulsaciones binarias; y prueba de bucle de retorno, que incluye la transmisión de señales de prueba entre la CSU y la unidad de canal de oficina de la portadora de red. Véase también *unidad de servicio de datos (DSU)*.

**unidad de servicio de datos (DSU).** Dispositivo que proporciona una interfaz de servicio de datos digital al equipo terminal de datos de manera directa. La DSU proporciona igualación de bucle y posibilidades de pruebas locales y remotas, así como una interfaz EIA/CCITT estándar.

**unidad de servicios de gestión de punto de control (CP-MSU).** Unidad de mensaje que contiene datos de servicios de gestión y fluye entre los conjuntos de funciones de servicios de gestión. Esta unidad de mensaje tiene el formato de corriente de datos general (GDS). Véase también *unidad de servicios de gestión (MSU)* y *transporte de vector de gestión de red (NMVT)*.

**unidad EIA.** Unidad de medida que ha establecido la Electronic Industries Association y es igual a 44,45 milímetros (1,75 pulgadas).

**unidad física (PU).** (1) Componente que gestiona y supervisa los recursos (como, por ejemplo, enlaces conectados y estaciones de enlace adyacentes) asociados con un nodo tal como lo solicita un SSCP mediante una sesión de SSCP-PU. Un SSCP activa una sesión con la unidad física con el fin de gestionar indirectamente, a través de la PU, recursos del nodo, como, por ejemplo, enlaces conectados. Este término sólo se aplica a los nodos de tipo 2.0, tipo 4 y tipo 5. (2) Véase también *PU periférica* y *PU de subárea*.

**unidad lógica (LU).** Tipo de unidad de red accesible que permite que los usuarios obtengan acceso a recursos de red y se comuniquen entre sí.

**unidad máxima de transmisión (MTU).** En las LAN, la mayor unidad de datos posible que puede enviarse por un medio físico determinado en una sola trama. Por ejemplo, la MTU para Ethernet tiene 1500 bytes.

**Unión de Telecomunicaciones Internacionales (ITU).** Agencia de telecomunicaciones especializada de las Naciones Unidas que se ha establecido con el fin de proporcionar procedimientos y prácticas para la normalización de las comunicaciones, lo cual incluye asignación de frecuencia y regulaciones de la radio universales.

**User Datagram Protocol (UDP).** En el conjunto de protocolos de Internet, protocolo que proporciona un



servicio no fiable de datagramas sin conexiones. Permite que un programa de aplicación de una máquina o proceso envíe un datagrama a un programa de aplicación de otra máquina o proceso. UDP utiliza Internet Protocol (IP) para entregar datagramas.

**V.25.** En la comunicación de datos, especificación de la CCITT que define el equipo de respuesta automática y el equipo de llamada automática paralelo de la red telefónica general conmutada, incluidos los procedimientos de inhabilitación de dispositivos controlados con eco para las llamadas establecidas de manera manual y automática.

**V.35.** En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito de datos (DCE) con varias velocidades de datos.

**V.34.** Recomendación del ITU-T para la comunicación por módem sobre canales estándares de transmisión de voz de 33,6 Kbps (y más lentos) disponibles comercialmente.

**V.36.** En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito de datos (DCE) con las velocidades de 48, 56, 64 ó 72 kilobits por segundo.

**V.24.** En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito de datos (DCE).

## V

**valor por omisión.** Perteneciente a un atributo, condición, valor u opción que se supone cuando no se especifica nada de forma explícita. (I)

**variable de corriente de datos general (GDS).** Tipo de subestructura de RU que va precedida de un identificador y un campo de longitud e incluye datos de aplicación, datos de control de usuario o datos de control definidos según SNA.

**variable de la MIB.** En el protocolo Simple Network Management Protocol (SNMP), instancia específica de datos definida en un módulo de la MIB. Sinónimo con *objeto de la MIB*.

**vector de control de selección de ruta (RSCV).** Vector de control que describe una ruta de una red

APPN. El RSCV consta de una secuencia ordenada de vectores de control que identifican los TG y nodos que componen la vía de acceso de un nodo de origen a un nodo de destino.

**velocidad de información comprometida.** Cantidad máxima de datos en bits que la red acepta entregar.

**velocidad de transferencia de datos.** Promedio de los bits, caracteres o bloques por unidad de tiempo que pasan entre los miembros del equipo correspondiente en un sistema de transmisión de datos. (I)

### Notas:

1. La velocidad se expresa en bits, caracteres o bloques por segundo, minuto u hora.
2. Debe indicarse el equipo correspondiente; por ejemplo, módems, equipo intermedio u origen y destino.

**versión.** Programa bajo licencia independiente que a menudo tiene un nuevo código o una nueva función significativos.

**vertimiento múltiple.** (1) Transmisión de los mismos datos a un grupo seleccionado de destinos. (T)  
(2) Forma especial de difusión en que se entregan copias de un paquete a un subconjunto de todos los destinos posibles solamente.

**vía de acceso.** (1) En una red, cualquier ruta entre dos nodos cualesquiera. Una vía de acceso puede incluir más de una rama. (T) (2) Serie de componentes de red de transporte (control de la vía de acceso y control de enlace de datos) por los que pasa la información intercambiada entre dos unidades de red accesibles. Véase también *ruta explícita (ER)*, *extensión de ruta* y *ruta virtual (VR)*.

**VINES.** Virtual NETworking System.

**Virtual Networking System (VINES).** Sistema operativo de red y software de red de Banyan Systems, Inc. En una red VINES, la función de enlace virtual permite que todos los dispositivos y servicios aparenten estar conectados directamente entre sí cuando en realidad pueden encontrarse a miles de kilómetros de distancia. Véase también *StreetTalk*.

**vista de la MIB.** En el protocolo Simple Network Management Protocol (SNMP), conjunto de objetos gestionados, conocidos por el agente, que es visible en una comunidad en particular.

**vuelco.** (1) Datos que se han volcado. (T)  
(2) Copiar el contenido de la totalidad o de parte del almacenamiento virtual con el fin de reunir información de errores.

## W

**X.25.** (1) Recomendación de la Comisión Consultiva de la Telefonía y Telegrafía Internacionales (CCITT) relativa a la interfaz entre un equipo terminal de datos y las redes de datos de paquetes conmutados.  
(2) Véase también *conmutación de paquetes*.

## X

**X.21.** Recomendación de la Comisión Consultiva de la Telefonía y Telegrafía Internacionales (CCITT) relativa a una interfaz de fines generales entre un equipo terminal de datos y un equipo de terminación de circuito de datos para las operaciones síncronas en una red pública de datos.

**Xerox Network Systems (XNS).** Conjunto de protocolos de internet desarrollados por Xerox Corporation. Aunque es similar a los protocolos TCP/IP, XNS utiliza unos formatos de paquete y una terminología diferentes. Véase también *Internetwork Packet Exchange (IPX)*.

## Z

**zona.** En redes AppleTalk, subconjunto de nodos dentro de una internet.

**Zone Information Protocol (ZIP).** En redes AppleTalk, protocolo que proporciona un servicio de gestión de zonas manteniendo una correlación de los nombres de zonas y los números de red de la internet en la capa de sesión.

# Índice

## A

- access-control
  - IPv6, mandato de supervisión 503
- activate
  - APPN, mandato de supervisión 237
- activate\_new\_config
  - APPN, mandato de configuración 219
- add
  - AppleTalk Phase 2, mandato de configuración 300
  - APPN, mandato de configuración 157
  - IPv6, mandato de configuración 482
  - IPv6, mandato de configuración de update packet filter 498
  - NDP, mandato de configuración 514
  - OSI, mandato de configuración 394
  - RIP6, mandato de configuración 548
  - VINES, mandato de configuración 323
- Address Resolution Protocol (ARP)
  - VINES 319
- addresses
  - OSI/DECnet V, mandato de supervisión 422
- antes de configurar 38
- aping
  - APPN, mandato de supervisión 237
- AppleTalk Control Protocol
  - para PPP 292
- AppleTalk Phase 2
  - básicos, procedimientos de la configuración 291, 294
  - configuración 291
  - direccionador, parámetros 291
  - red, parámetros 292, 295
  - supervisión 299
- AppleTalk Phase 2, mandatos de configuración
  - add 300
  - delete 301
  - disable 302
  - enable 304
  - list 305
  - set 307
- AppleTalk Phase 2, mandatos de supervisión
  - atecho 309
  - cache 310
  - clear counters 310
  - counters 311
  - dump 311
  - interface 312
- APPN 94
  - supervisión 232
- APPN (DLSw) 27
  - APPN, mandatos de configuración
    - activate\_new\_config 219
    - add 157
    - delete 219
    - enable/disable 121
    - list 219
    - set 121
    - TN3270 119
  - APPN, mandatos de supervisión
    - acceso 232
    - activate 237
    - aping 237
    - deactivate link 238
    - dump 238
    - list 238
    - log 265
    - memory 270
    - restart 275
    - resumen 232
    - rtp status 273
    - rtp switchpath 273
    - rtp test 274
    - stop 275
    - tn3270e 275, 276
    - transmit 276
  - APPN, reconfiguración dinámica 288
  - APPN, Red de conexiones BAN Frame Relay 47, 202, 203
  - atecho
    - AppleTalk Phase 2, mandato de supervisión 309
  - ATM
    - APPN, utilización 69
  - ATM, Emulación de LAN
    - configuración de DNA IV 335
  - ayuda
    - consola, mandato 300

## B

- BGP, mandatos de supervisión
  - destinos
    - recibidas 584
- BGP6, mandatos de configuración 562, 569, 571, 573, 574
  - add
    - aggregate 562
    - neighbor 563
    - no-receive 565
    - receive 566
    - send 568
  - change
    - change originate 570
    - change receive 570

BGP6, mandatos de configuración (*continuación*)  
 change (*continuación*)  
 change send 571  
 delete  
 aggregate 571  
 neighbor 571  
 no 572  
 originate 572  
 receive 572  
 send 572  
 disable  
 bgp sin clase 573  
 BGP6 speaker 573  
 neighbor 573  
 enable 573  
 BGP6 speaker 573  
 compare-med-from-diff-AS 574  
 neighbor 574  
 list  
 aggregate 574  
 all 574  
 BGP6 speaker 575  
 neighbor 575  
 no 575  
 originate 576  
 receive 576  
 send 576  
 move 576  
 policy-to-neighbor 570, 572, 576  
 set 577  
 update 577  
 BGP6, mandatos de supervisión  
 disable neighbor 580  
 dump routing tables 581  
 enable neighbor 581  
 list 581  
 neighbors 584  
 parameter 586  
 paths 586  
 ping6 587  
 policy-list 587  
 reset neighbor 588  
 sizes 588  
 traceroute6 589  
 BGP6, reconfiguración dinámica 589  
 Border Gateway Protocol para IPv6--véase BGP6 589  
 Border Node  
 COS, tabla de correlación 216  
 direccionamiento, lista 213  
 Branch Extender 16, 20, 31, 185, 186, 187, 212, 213

## C

cache  
 AppleTalk Phase 2, mandato de supervisión 310  
 IPv6, mandato de supervisión 504

clear 403  
 PIM, mandato de supervisión 534  
 clnp-Stats  
 OSI/DECnet V, mandato de supervisión 423  
 CLNP, protocolo 374  
 conexiones, redes 15  
 configurable, Cola de alertas retenidas 24, 38, 156  
 configuración, cambios, efecto en el direccionador 26  
 configuración, opciones 26  
 configuración, requisitos 26  
 configurar TN3270 bajo APPN 94  
 contabilidad y nodos, estadísticas 42  
 COS 38  
 CoS, tabla de correlación 36  
 counters  
 AppleTalk Phase 2, mandato de supervisión 311  
 IPv6, mandato de supervisión 504  
 VINES, mandato de supervisión 328

## CH

change  
 IPv6, mandato de configuración 489  
 IPv6, mandato de configuración de update packet  
 filter 500  
 NDP, mandato de configuración 516  
 RIP6, mandato de configuración 548  
 change metric  
 OSI/DECnet V, mandato de supervisión 423  
 change prefix-address 401

## D

DDDLU 99  
 Creación de LU en VTAM 99  
 ejemplo, definición de PU de VTAM 101  
 Supresión de LU de VTAM 100  
 utilización de Network Dispatcher con 100  
 deactivate link  
 APPN, mandato de supervisión 238  
 deactivate LU  
 TN3270E, mandato de supervisión 276  
 DECnet NCP  
 Véase NCP 333  
 delete  
 AppleTalk Phase 2, mandato de configuración 301  
 APPN, mandato de configuración 219  
 IPv6, mandato de configuración 489  
 IPv6, mandato de configuración de update packet  
 filter 501  
 NDP, mandato de configuración 518  
 OSI, mandato de configuración 404  
 PIM, mandato de configuración 527  
 RIP6, mandato de configuración 551  
 VINES, mandato de configuración 324

- destino, dispositivos 449
- dhcpv6-relay
  - NDP, mandato de supervisión 520
- Digital Network Architecture (DNA) phase IV 333
- dinámica, reconfiguración
  - APPN 288
  - BGP6 589
  - IPv6 510
  - MFC 543
  - MFC para IPv6 544
  - NDP6 521
  - NHRP, servidor 473
  - PIM 541
  - PIM para IPv6 542
  - RIP6 559
- direccionamiento, lista 35
- direccionamiento, tablas
  - BGP6, mandato dump 581
- disable
  - AppleTalk Phase 2, mandato de configuración 302
  - APPN, mandato de configuración 121
  - IPv6, mandato de configuración 489
  - NDP, mandato de configuración 518
  - OSI, mandato de configuración 406
  - PIM, mandato de configuración 527
  - RIP6, mandato de configuración 551
  - VINES, mandato de configuración 324
- DLUR 11, 38, 43
- DLUR, algoritmo de reintentos 43
- DNA IV
  - acceso, control
    - configuración 339
    - exclusivo 341
    - gestión del tráfico 338
    - inclusivo 340
  - áreas, direccionadores
    - descripción 336
    - nivel 1 336
    - nivel 2 336
  - áreas, filtros de direccionamiento 341
  - áreas, soporte de 333
  - combinación de dominios 344
  - configuración
    - para X.25 348
  - configuración sobre la Emulación de LAN de
    - ATM 335
  - designado para, direccionador 336
  - direccionamiento 335
  - direccionamiento, parámetros 337
  - direccionamiento, tablas 336
  - especiales, consideraciones y limitaciones 334
  - LAT, protocolo 333
  - MOP, soporte de 333
  - Network Control Program (NCP) 337
    - Véase NCP 333
  - sistema de dirección
    - 802.5, Red en Anillo 334
- DNA IV (*continuación*)
  - sistema de dirección (*continuación*)
    - descripción 334
    - Ethernet, enlace de datos 334
    - X.25, enlace de datos 335
    - terminología y conceptos 334
- DNA IV, mandatos de configuración
  - define
    - circuit 352
    - executor 356
    - module access 360
    - module routing 361
    - node 361
  - help 352
  - purge
    - module access 362
    - module routing 362
  - show
    - area 363
    - node 364
  - show/list
    - circuit 365
    - executor 368
    - module access 370
    - module routing 371
  - zero
    - circuit 371
    - executor 372
    - module access 371, 372
- DNA IV, mandatos de supervisión
  - define
    - circuit 352
    - executor 356
    - module access 360
    - module routing 361
    - node 361
  - help 352
  - purge
    - module access 362
    - module routing 362
  - show
    - area 363
    - node 364
  - show/list
    - circuit 365
    - executor 368
    - module access 370
    - routing 371
  - zero
    - circuit 371
    - executor 372
    - module access 372
    - module\_access 371
- DNA V
  - redes 346
  - X.25, configuración
    - Cuenta 2 348

## DNAV-info

OSI/DECnet V, mandato de supervisión 425  
DSPU de VTAM 12

## dump

AppleTalk Phase 2, mandato de supervisión 311  
APPN, mandato de supervisión 238  
IPv6, mandato de supervisión 504  
NDP, mandato de supervisión 521  
PIM, mandato de supervisión 533  
RIP6, mandato de supervisión 558  
VINES 329

## dump routing tables

BGP6, mandato de supervisión 581

## E

el direccionador como punto de entrada 22

## enable

AppleTalk Phase 2, mandato de configuración 304  
APPN, mandato de configuración 121  
IPv6, mandato de configuración 490  
NDP, mandato de configuración 519  
OSI, mandato de configuración 407  
PIM, mandato de configuración 527  
RIP6, mandato de configuración 553  
VINES, mandato de configuración 325

enlace, listas de parámetros de nivel 51

Enterprise Extender, soporte para el HPR sobre IP 24

## es-adjacencias

OSI/DECnet V, mandato de supervisión 426

## es-is-stats

OSI/DECnet V, mandato de supervisión 426

ES-IS, protocolo 374

descripción 387

hello, mensaje 388

esfera de control 22

establecimiento de características de grupo de transmisión 38

exclusión, listas 449

exit 300

consola, mandato 300

VINES, mandato de supervisión 331

Extended Border Node 17, 20

configuración 32

CoS, tabla de correlación 36

direccionamiento, lista 35

red, requisitos 20

## extensiones

IBM, extensiones privadas del proveedor 450

vía de acceso, extensiones de información 450

## F

focal, punto 22, 38

## funciones

IP versión 6 (IPv6) 475

## G

Germinación, direccionador

AppleTalk Phase 2 292, 295

gestión de nodos de red 21

gestión del nodo de red direccionador 21

## H

HIDLU 102

HPR 8, 37

## I

IBM, extensiones específicas

NHRP 450

implementación en el direccionador 4

implícito, punto focal 24, 210

Interconexión de Sistemas Abiertos (OSI)

autenticación, contraseñas 387

conectados, direccionadores IS de L2 383

designado, IS 381

dirección, codificación de prefijos 386, 387

direccionamiento, métrica 384

direccionamiento, tablas 383

dominio, parte específica (DSP) 375

enlaces, actualizaciones del estado 382

enlaces, bases de datos de estado 382

ES-IS, protocolo 387

externo, direccionamiento 385

final, mensajes hello de sistema 388

final, sistema (ES) 373

inicial, parte de dominio (IDP) 375

descripción 375

intermedio, sistema (IS) 373

interno, direccionamiento 385

IS a IS, mensajes hello (IIH) 380, 381

IS-IS, áreas 378

IS-IS, dominio 378

IS-IS, formato de sistema de dirección 375

AFI 386

área, dirección 375

dirección, formato 376

fija, IDI de longitud 386

no pseudonodo 382, 383

omisión, prefijos de dirección 387

pseudonodo 382, 383

punto a punto 381

selector 376

sistema, ID 375

variable, IDI de longitud 386

IS, mensajes hello 388

L1, actualizaciones del estado de los enlaces 382

L1, direccionamiento 383

L1, mensaje IIH 380

L2, actualizaciones del estado de los enlaces 383

L2, direccionamiento 384

- Interconexión de Sistemas Abiertos (OSI) (*continuación*)
    - L2, mensajes IIH 381
    - NSAP, sistema de dirección 374
    - protocolos en ejecución bajo 374
    - pseudonodo 381
    - red, direcciones 374
    - red, estructura de dirección 374
    - red, Título de entidad (NET) 375
    - red, unidades de datos de protocolo (NPDU) 373
    - sin conectar, direccionadores IS de L2 383
    - sinónimas, áreas 379
    - vertimiento múltiple, direcciones 376
  - interface
    - AppleTalk Phase 2, mandato de supervisión 312
    - IPv6, mandato de supervisión 505
    - PIM, mandato de supervisión 534
  - internal
    - IPv6, mandato de supervisión 505
  - IP
    - paquete, tamaño 592
  - IPv6
    - configuración 481
    - utilización 475
    - visión general 475
  - ipv6, mandato 481
  - IPv6, mandatos de configuración
    - add 482
    - change 489
    - delete 489
    - disable 489
    - enable 490
    - list 490
    - move 493
    - resumen 481
    - set 493
    - update 497
  - IPv6, mandatos de configuración de update packet filter
    - add 498
    - change 500
    - delete 501
    - list 502
    - move 501
  - IPv6, mandatos de supervisión
    - acceso 502
    - access-control 503
    - cache 504
    - counters 504
    - dump 504
    - interface 505
    - internal 505
    - mcast 505
    - mld 506
    - packet-filter 507
    - path-mtu 508
    - ping6 508
    - reset 506
  - IPv6, mandatos de supervisión (*continuación*)
    - resumen de 502
    - route 506
    - sizes 506
    - sniffer 507
    - static 507
    - traceroute6 509
    - tunnels 510
  - IPv6, reconfiguración dinámica 510
  - is-adjacencies
    - OSI/DECnet V, mandato de supervisión 429
  - is-is-stats
    - OSI/DECnet V, mandato de supervisión 429
  - IS-IS, mensajes
    - IS a IS, mensajes hello (IIH) 380
    - punto a punto 381
  - IS-IS, protocolo
    - descripción 377
    - IS a IS, mensajes hello (IIH)
      - L1 380
      - L2 381
    - IS-IS, áreas 378
    - IS-IS, dominio 378
    - visión general 374
- ## J
- join
    - PIM, mandato de supervisión 535
- ## L
- I1-routes
    - OSI/DECnet V, mandato de supervisión 431
  - I1-Summary
    - OSI/DECnet V, mandato de supervisión 432
  - I1-Update
    - OSI/DECnet V, mandato de supervisión 433
  - I2-Routes
    - OSI/DECnet V, mandato de supervisión 431
  - I2-Summary
    - OSI/DECnet V, mandato de supervisión 433
  - I2-Update
    - OSI/DECnet V, mandato de supervisión 434
  - LANE, interfaz de atajo (LSI)
    - NHRP 447
  - leave
    - PIM, mandato de supervisión 535
  - list
    - AppleTalk Phase 2, mandato de configuración 305
    - APPN, mandato de configuración 219
    - APPN, mandato de supervisión 238
    - IPv6, mandato de configuración 490
    - IPv6, mandato de configuración de update packet filter 502
    - NDP, mandato de configuración 519

list (*continuación*)

- NDP, mandato de supervisión 521
- OSI, mandato de configuración 407
- PIM, mandato de configuración 528
- RIP6, mandato de configuración 554
- RIP6, mandato de supervisión 558
- TN3270E, mandato de supervisión 277
- VINES, mandato de configuración 325
- Local Area Terminal (LAT), protocolo 333
- log
  - APPN, mandato de supervisión 265
- LSI 447
  - Véase también LANE, interfaz de atajo (LSI)
- LU, lista de parámetros 52

## M

- Marcación bajo pedido 55
  - APPN, utilización 55
- mcache
  - PIM, mandato de supervisión 535
- mcast
  - IPv6, mandato de supervisión 505
- memory
  - APPN, mandato de supervisión 270
- MFC para IPv6, reconfiguración dinámica 544
- MFC, reconfiguración dinámica 543
- mgroups
  - PIM, mandato de supervisión 536
- mld
  - IPv6, mandato de supervisión 506
- move
  - IPv6, mandato de configuración 493
  - IPv6, mandato de configuración de update packet filter 501
- mstats
  - PIM, mandato de supervisión 536
- Multicast Forwarding Cache- véase MFC 543

## N

- NCP
  - descripción de 337
- NCP, mandatos de configuración
  - purge 362
  - resumen de 351
  - set 362
  - show 363
  - show circuit 365
  - zero 371
- NCP, mandatos de supervisión
  - purge 362
  - resumen de 351
  - set 362
  - show 363
  - show circuit 365

NCP, mandatos de supervisión (*continuación*)  
zero 371

- NDP
  - configuración 513
- NDP, mandato 513
- NDP, mandatos de configuración
  - add 514
  - change 516
  - delete 518
  - disable 518
  - enable 519
  - list 519
  - resumen 513
  - set 519
- NDP, mandatos de supervisión
  - acceso 520
  - dhcpv6-relay 520
  - dump 521
  - list 521
  - ping6 521
  - resumen de 520
- NDP6, reconfiguración dinámica 521
- neighbor
  - PIM, mandato de supervisión 538
- Neighbor Discovery Protocol para IPv6--véase NDP6 521
- Next Hop Resolution Protocol
  - Véase también NHRP
  - visión general 439
- NHR, reconfiguración dinámica de servidor 473
- NHRP 439
  - destino, dispositivos 449
  - ejemplos
    - clásico, IP, entorno 442
    - clásico, IP, entorno con dispositivo sin NHRP 442
    - LAN, conmutadores 444
    - LAN, emulación 443
    - mixto, IP clásico y ELAN 445
    - salida, direccionador 446
  - exclusión, listas 449
  - implementación 446
    - anulados, atajos de direccionador a direccionador 451
    - IBM, extensiones específicas 450
  - LANE, atajos 447
  - limitaciones 441
  - siguiente salto, direccionadores 449
  - ventajas 440
  - virtual, interfaz de red (VNI) 446
- NHRP, interfaces
  - configuración 439
  - supervisión 455
- NHRP, mandatos de configuración 439
  - acceso 455
  - add 458



NHRP, mandatos de configuración (*continuación*)  
  advanced 456  
  change 460  
  delete 459  
  disable 456  
  enable 456  
  list 456, 461  
  resumen 455  
  set 462  
NHRP, mandatos de supervisión  
  acceso 466  
  lista de 466  
nodo, ajuste 41  
nodo, listas de parámetros de nivel 52  
nodos, tipos 1

## O

obtención de ayuda 300  
opcionales, funciones 7  
OSI  
  configuración 390  
  X.25 sobre OSI 396  
OSI, mandatos de configuración  
  add 394  
  clear 403  
  change prefix address 401  
  delete 404  
  disable 406  
  enable 407  
  list 407  
  resumen de 393  
  set 414  
OSI/DECnet V  
  supervisión 393  
OSI/DECnet V, mandatos de supervisión  
  addresses 422  
  clnp-stats 423  
  change metric 423  
  designated-router 425  
  DNAV-info 425  
  es-adjacencias 426  
  es-is-stats 426  
  is-adjacencias 429  
  is-is-stats 429  
  l1-routes 431  
  l1-summary 432  
  l1-update 433  
  l2-routes 431  
  l2-summary 433  
  l2-update 434  
  OSI/DECnet V, mandato de supervisión 425  
  ping-1139 435  
  resumen de 421  
  route 435  
  send (echo packet) 436

OSI/DECnet V, mandatos de supervisión (*continuación*)  
  subnets 436  
  toggle (alias/no alias) 437  
  traceroute 437

## P

packet-filter  
  IPv6, mandato de supervisión 507  
paquete, tamaño 591  
path-mtu  
  IPv6, mandato de supervisión 508  
PIM  
  configuración 525  
  PIM, mandato de supervisión 539  
PIM para IPv6, reconfiguración dinámica 542  
PIM, mandato 526  
PIM, mandatos de configuración  
  delete 527  
  disable 527  
  enable 527  
  list 528  
  resumen 527  
  set 529  
PIM, mandatos de supervisión  
  acceso 532  
  clear 534  
  dump 533  
  interface 534  
  join 535  
  leave 535  
  mcache 535  
  mgroups 536  
  mstats 536  
  neighbor 538  
  pim 539  
  ping 540  
  reset 540  
  resumen de 532  
  summary pim 539  
  traceroute 540  
  variables 540  
PIM, reconfiguración dinámica 541  
ping  
  PIM, mandato de supervisión 540  
ping-1139  
  OSI/DECnet V, mandato de supervisión 435  
ping6  
  BGP6, mandato de supervisión 587  
  IPv6, mandato de supervisión 508  
  NDP, mandato de supervisión 521  
  RIP6, mandato de supervisión 559  
Point-to-Point Protocol (PPP)  
  AppleTalk Control Protocol 292  
policy-list  
  BGP6, mandato de supervisión 587

protocolo de direccionamiento Protocol Independent  
Multicast--véase PIM 541  
protocolos  
  Digital Network Architecture (DNA) Phase IV 333  
protocolos Network Control Protocol (NCP)  
  para interfaces PPP  
    AppleTalk Control Protocol 292  
puerto, listas de parámetros de nivel 51  
puertos, tipos soportados 24

## R

rastreo 42  
rastreos 42  
RDSI, circuito permanente  
  APPN, utilización 52  
RDSI, conexión permanente 52  
Red en Anillo 4/16  
  paquete, tamaño 592  
reset  
  IPv6, mandato de supervisión 506  
  PIM, mandato de supervisión 540  
  RIP6, mandato de supervisión 559  
restart  
  APPN, mandato de supervisión 275  
restricciones 46  
resumen de  
  NCP, mandatos de configuración 351  
  NCP, mandatos de supervisión 351  
resumen de los mandatos  
  BGP 561, 579  
  DNA IV 351  
reunión de datos de sesión intermedia 42  
RIP6  
  configuración 547  
RIP6, mandato 547  
RIP6, mandatos de configuración  
  add 548  
  change 548  
  delete 551  
  disable 551  
  enable 553  
  list 554  
  resumen 547  
  set 554  
RIP6, mandatos de supervisión  
  acceso 557  
  dump 558  
  list 558  
  ping6 559  
  reset 559  
  resumen de 558  
  traceroute6 559  
RIP6, reconfiguración dinámica 559  
route  
  IPv6, mandato de supervisión 506

route (*continuación*)  
  OSI/DECnet V, mandato de supervisión 435  
Routing Information Protocol para IPv6--véase  
  RIP6 559  
rtp status  
  APPN, mandato de supervisión 273  
rtp switchpath  
  APPN, mandato de supervisión 273  
rtp test  
  APPN, mandato de supervisión 274  
RU, tamaño 41, 138

## S

SDLC 72  
  APPN, utilización 72  
send (Echo Packet)  
  OSI/DECnet V, mandato de supervisión 436  
set  
  AppleTalk Phase 2, mandato de configuración 307  
  APPN, mandato de configuración 121  
  IPv6, mandato de configuración 493  
  NDP, mandato de configuración 519  
  OSI, mandato de configuración 414  
  PIM, mandato de configuración 529  
  RIP6, mandato de configuración 554  
  VINES, mandato de configuración 326  
siguiente salto, direccionadores 449  
sizes  
  IPv6, mandato de supervisión 506  
sniffer  
  IPv6, mandato de supervisión 507  
SNMP, utilización del direccionador como nodo gestio-  
nado por 23  
soportadas, unidades de mensajes 23  
soportadas, unidades de mensajes, alertas relacionadas  
  con APPN 23  
static  
  IPv6, mandato de supervisión 507  
stop  
  APPN, mandato de supervisión 275  
subnets  
  OSI/DECnet V, mandato de supervisión 436  
summary pim  
  PIM, mandato de supervisión 539  
supervisión  
  APPN 232  
  IPv6, mandatos de supervisión 502  
  NDP, mandatos de supervisión 520  
  PIM, mandatos de supervisión 532  
  RIP6, mandatos de supervisión 558

## T

talk  
  OPCON, mandato 232, 481, 502, 513, 520, 526,  
  532, 547, 557

- TG, funciones 38
- TN3270 89
  - qué es 89
  - tn3270E, configuración del servidor 94
- tn3270e
  - APPN, mandato de supervisión 275, 276
- tn3270E, configuración del servidor 94
- TN3270E, mandatos de supervisión
  - deactivate LU 276
  - list 277
- TN3270E, Servidor 26, 90
  - carga, equilibrio entre diversas PU 109
  - cliente con LU, correlación 103
  - cliente, correlación de dirección IP con LU/agrupación 104
  - Configuración, con DLUR 110
  - Configuración, con identificador de nodo local 116
  - configuración, mandatos 220
  - Configuración, parámetros 220
  - ejemplo, configuraciones 109
  - puerto, dirección IP, correlación 108
  - servidor, correlación de puerto TCP con agrupación 107
  - supervisión, mandatos 276
- toggle (Alias/No Alias)
  - OSI/DECnet V, mandato de supervisión 437
- topología, Base de datos, Garbage Collection 23
- traceroute
  - OSI/DECnet V, mandato de supervisión 437
  - PIM, mandato de supervisión 540
- traceroute6
  - BGP6, mandato de supervisión 589
  - IPv6, mandato de supervisión 509
  - RIP6, mandato de supervisión 559
- transmit
  - APPN, mandato de supervisión 276
- transporte de datos 47
- tunnels
  - IPv6, mandato de supervisión 510

## U

- unidades de mensajes soportadas, alertas relacionadas con APPN 23
- update
  - IPv6, mandato de configuración 497
- utilización del direccionador como nodo gestionado por SNMP 23

## V

- V.25 bis 68
  - APPN, utilización 68
- variables
  - PIM, mandato de supervisión 540

- VINES 325
  - Address Resolution Protocol (ARP) 319
  - básicos, procedimientos de la configuración 321
  - clientes, nodos 313
  - configuración 313
  - contiguos, tablas 318
    - establecimiento del tamaño 327
  - direccionamiento, tablas 317
    - establecimiento del tamaño 327
    - vuelco 329
  - establecimiento del número de nodos clientes 326
  - habilitación de una interfaz 325
  - habilitación global 325
  - inhabilitación de una interfaz 324
  - inhabilitación global 324
  - neighbor tables
    - vuelco 329
  - red, protocolos de capa 314
    - Address Resolution Protocol (ARP) 319
    - Internet Control Protocol (ICP) 319
    - Routing Update Protocol (RTP) 316
    - VINES IP 314
  - RTP, implementación 319
  - servicio, nodos 313
  - supervisión 323
  - supervisión, mandatos 327
  - visión general 313
- VINES, mandatos de configuración 323
- VINES, mandatos de supervisión
  - counters 328
  - dump 329
  - exit 331
- virtual, interfaz de red (VNI)
  - NHRP 446
- VNI 446
  - Véase también* virtual, interfaz de red (VNI)

## W

- WAN, redireccionamiento 59
- WAN, restauración 66



---

# Hoja de Comentarios

**Nways Multiprotocol Access Services**  
**Consulta de configuración y supervisión**  
**de protocolos Volumen 2**  
**Versión 3.4**

**Número de Publicación SC10-3433-01**

**En general, ¿está Ud. satisfecho con la información de este libro?**

	Muy satisfecho	Satisfecho	Normal	Insatisfecho	Muy insatisfecho
Satisfacción general	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**¿Cómo valora los siguientes aspectos de este libro?**

	Muy bien	Bien	Acep- table	Insatisfecho	Muy insatisfecho
Organización	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Información completa y precisa	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Información fácil de encontrar	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Utilidad de las ilustraciones	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Claridad de la redacción	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Calidad de la edición	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Adaptación a los formatos, unidades, etc. del país	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Comentarios y sugerencias:**

Nombre

Dirección

Compañía u Organización

Teléfono



Dóblese por la línea de puntos

**Por favor no lo grape**

Dóblese por la línea de puntos

PONER  
EL  
SELLO  
AQUÍ

IBM, S.A.  
National Language Solutions Center  
Av. Diagonal, 571  
08029 Barcelona  
España

Dóblese por la línea de puntos

**Por favor no lo grape**

Dóblese por la línea de puntos





SC10-3433-01

