Nways Multiprotocol Routing Services

Manual de consulta de supervisión y configuración de protocolos Volumen 2 Versión 3.3

SC10-3428-00

Nways Multiprotocol Routing Services

Manual de consulta de supervisión y configuración de protocolos Volumen 2 Versión 3.3

SC10-3428-00

Nota

Antes de usar el presente documento, lea la información general que se encuentra bajo “Avisos” en la página xv.

Primera edición (junio de 1999)

Este manual es la traducción del original inglés *IBM Nways Multiprotocol Routing Services Protocol Configuration and Monitoring Reference Volume 2 Version 3.3 (SC30-3865-05).*

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

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

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

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

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

Contenido

Figuras

Tablas

Avisos

Las referencias hechas en esta publicación a productos, programas o servicios de IBM no implican que IBM tenga la intención de comercializarlos en todos los países en los que realiza operaciones. Cualquier referencia a un producto, programa o servicio de IBM no pretende afirmar ni implicar que sólo pueda utilizarse el mencionado producto, programa o servicio de IBM. En su lugar, puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no vulnere ninguno de los derechos de propiedad intelectual de IBM. La evaluación y verificación del funcionamiento junto con otros productos, excepto los expresamente indicados por IBM, son responsabilidad del usuario.

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

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

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

Aviso para los usuarios de versiones en línea de este manual

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

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

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

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

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

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

Marcas registradas

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

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

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

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

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

Prefacio

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

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

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

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

Acerca del software

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

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

  El código base viene instalado de fábrica en el 2210.
- El programa de configuración Configuration Program para IBM Nways Multiprotocol Routing Services (denominado así en este manual: *Configuration Program*) es una interfaz gráfica de usuario que permite configurar el dispositivo desde una estación de trabajo autónoma. El Configuration Program incluye la función de comprobación de errores e información de ayuda en línea.

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

También puede obtener el Configuration Program para IBM Nways Multiprotocol Routing 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 configuració de productos Nways Multiprotocol Access Services Products,* 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 encerradas entre corchetes y separadas por la palabra "o". Por ejemplo:

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

   Elija una de las palabras clave como valor del parámetro.

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

   ```
   time host ...
   ```

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

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

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

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

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

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

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

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

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

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

Publicaciones de IBM 2210 Nways Multiprotocol Router

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

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

Actualizaciones y correcciones de la información: Para mantenerse informado de los cambios técnicos, aclaraciones y arreglos implementados después de la impresión de los manuales, consulte las páginas de presentación del IBM 2210 en:

`http://www.networking.ibm.com/220/220prod.html`

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

Gestión de red y operaciones

SC10-3427 *Guía del usuario de software*

En este manual se explica cómo:

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

SC10-3329 *Utilización y configuración de las características*

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

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

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

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

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

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

Configuración

Ayuda en línea

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

GC10-3430 *Guía del usuario del programa de configuración de productos Nways Multiprotocol Access Services Products*

Este manual describe cómo utilizar el Configuration Program.

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

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

Seguridad

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

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

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

Planificación e instalación

GA27-4068 *IBM 2210 Introduction and Planning Guide*
GC30-3867 *IBM 2210 Nways Multiprotocol Router Installation and Initial Configuration Guide*

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

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

Diagnósticos y mantenimiento

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

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

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

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

- **Nuevas funciones:**
  - El Subsistema de codificación (ES)
  - Los servicios del protocolo Dynamic Host Configuration Protocol (DHCP)
  - La red privada virtual (VPN)

    - Los servicios de directorios: el soporte del protocolo Lightweight Directory Access Protocol (LDAP)
    - El soporte de ISAKMP/Oakley
    - Layer 2 Forwarding (L2F)
    - Point to Point Tunneling Protocol (PPTP)
    - Servicios diferenciados
  - El soporte de 6 Mbps de J2 como máximo para Bc, Be y CIR de Frame Relay
  - La fragmentación de paquetes de Frame Relay
  - El reenvío de paquetes de Voz sobre Frame Relay
- **Funciones mejoradas:**
  - Mejoras en IP
    - La política genérica de direccionamiento de IPv4
    - Los filtros de paquetes de IPv6, la reconfiguración dinámica y el soporte de los agentes de relay de DHCP
  - Mejoras en SDLC
    - El sondeo de grupos primarios
    - La comunicación simultánea en dos direcciones
  - Los parámetros de configuración de DLSw para permitir el control del número de mensajes sin sesión puestos en cola en el direccionador
  - Mejoras en TN3270
    - La definición de LU dinámica iniciada por sistema principal
    - Múltiples SA de PU sobre DLSw
  - La mejora en la función de puente
    - El soporte de SR-TB de IPX
  - El soporte de la reconfiguración dinámica de X.25
  - Mejoras en IPX
    - Los ciclos de RIP configurables
    - Los SVC IPXWAN sobre Frame Relay
  - La función de finalización de mandatos de la interfaz de línea de mandatos

Cómo obtener ayuda

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

Cómo salir de un entorno de nivel inferior

La naturaleza de múltiples niveles del software le coloca en entornos de nivel secundario, terciario e incluso inferiores al configurar el 2210 o al servirse del mismo. Para volver al nivel superior más próximo, entre el mandato **exit**. Para obtener el nivel secundario, continúe entrando **exit** hasta que reciba el indicador de nivel secundario (`Config>` o +).

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

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

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

Utilización de APPN

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

¿Qué es APPN?

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

Comunicaciones de igual a igual

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

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

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

Tipos de nodos APPN

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

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

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

Nodo de red APPN

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

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

Los nodos de red APPN también:

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

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

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

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

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

Nodos finales APPN

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

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

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

Nodos LEN

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

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

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

Nodos PU 2.0

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

¿Qué funciones de APPN se implementan en el direccionador?

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

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

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

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

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

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

Notas:

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

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

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

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

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

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

Funciones opcionales del nodo de red APPN

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

087 Mejoras de Garbage Collection

1002 Nombre de la estación de enlace adyacente

1007 TG paralelos

1012 Nombre LU = Nombre CP

1016 Extended Border Node

1061 Requisitos previos de las Extensiones SS para soporte NNS

1063 Soporte NNS de las extensiones SS

1067 Peticionario de LU dependientes

1071 Uso generalizado de ODAI

1101 Antememoria de directorios cargada previamente

1107 Registro central de recursos (de LU)

1116 Soporte del servidor de nodos de la red al registro de LU servido por el DLUS

1119 Informe de la topología de ramas a un gestor

1120 Branch Awareness

1121 Branch Extender

1200 Puesta en antememoria de árboles y de TG

1400 Direccionamiento de alto rendimiento (HPR)

1401 Rapid Transport Protocol (RTP)

1402 Flujos de control sobre RTP

1405 HPR Border Node

Ajuste del rendimiento del nodo

Rastreos de servicios del nodo

Captación de estadísticas de nodo y de contabilidad

Direccionamiento de alto rendimiento

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

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

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

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

Interoperabilidad

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

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

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

Tipos de tráfico

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

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

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

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

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

- Para los puertos de Frame Relay:

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

  – Formato de trama direccionado RFC 1490/2427

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

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

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

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

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

– Formato puenteado RFC 1490/2427

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

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

Consulte la Tabla 3 en la página 31 para obtener una lista de los DLC que dan soporte a HPR.

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

Peticionario de LU dependientes (DLUR)

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

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

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

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

Consulte la Tabla 3 en la página 31 para saber cuáles son los tipos de puertos que dan conexión a la PU de comunicación directa (DSPU) que tienen soporte.

Funciones con soporte

La opción APPN DLUR incluye las funciones siguientes:

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

Restricciones

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

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

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

Consideraciones de VTAM para DLUR

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

Debe consultar el manual *VTAM Resource Definition Reference* (Consulta de definiciones de recursos de VTAM) SC31-6427, para obtener información de las sentencias del parámetro DLC de las definiciones Switched Major Node.

```
DABDLURX VBUILD TYPE=SWNET,MAXGRP=400,MAXNO=400,MAXDLUR=20
*************************************************************************
*IN THE DLCADDR, THE 'SUBFIELD_ID' = CV SUBFIELD OF THE CV91           *
* MINUS 0X90.                                                          *
*FOR EXAMPLE, THE CV94 SUBFIELD IS CODED ON DLCADDR=(4,X,...           *
*************************************************************************
*************************************************************************
* Following are PU Statements for 2.0 and for 2.1
*************************************************************************
*************************************************************************
* 2.0 PU STATEMENT
*************************************************************************
*PU20RT   PU   ADDR=05,PUTYPE=2,MAXPATH=8,ANS=CONT,USSTAB=AUSSTAB,
*              ISTATUS=ACTIVE,MAXDATA=521,IRETRY=YES,MAXOUT=7,
*              PASSLIM=5,IDBLK=017,IDNUM=00035,MODETAB=AMODETAB
*              LOGAPPL=ECHO71,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=ECHO71,DLOGMOD=M23278I   1
*************************************************************************
*************************************************************************
*
* Following are examples of path statement coding for various
* DLC types.
*
 * There is no difference in the path statement definitions
* between a PU 2.0 and a PU 2.1
*
* Path statements are required if VTAM is initiating the connection
* to the DSPU.
*
*************************************************************************
*************************************************************************
* Below is SDLC
*************************************************************************
*A20RT   PATH  PID=1,
*              DLURNAME=GREEN,
*              DLCADDR=(1,C,SDLCNS),
*              DLCADDR=(2,X,5353),  2  **nombre puerto
*              DLCADDR=(3,X,C1)     3a **dirección estación
```

```
*************************************************************************
* Below is Frame Relay
*************************************************************************
*A20RT   PATH  PID=2,
*              DLURNAME=GREEN,
*              DLCADDR=(1,C,FRPVC),
*              DLCADDR=(2,X,4652303033),  2 **nombre puerto
*              DLCADDR=(3,X,04),      3 **dirección SAP
*              DLCADDR=(4,X,0024)     4 **DLCI
*************************************************************************
* Below is Frame Relay BAN
*************************************************************************
*A20RT   PATH  PID=3,
*              DLURNAME=GREEN,
*              DLCADDR=(1,C,FRPVC),
*              DLCADDR=(2,X,4652303033),         2 **nombre puerto
*              DLCADDR=(3,X,04),           3 **dirección SAP
*              DLCADDR=(4,X,0024),         4 **DLCI
*              DLCADDR=(6,X,400000000001)  5 **dirección MAC
*************************************************************************
* Below is DLSw
*************************************************************************
*A20RT   PATH  PID=3,
*              DLURNAME=GOLD,
*              DLCADDR=(1,C,TR), 7
*              DLCADDR=(2,X,444C53323534), 2 **nombre puerto
*              DLCADDR=(3,X,04),           3 **dirección SAP
*              DLCADDR=(4,X,400000000001)  6 **dirección MAC
*
*************************************************************************
** Below is Token Ring
*************************************************************************
*PATHT20  PATH  PID=1,
*               DLURNAME=RED,
*               DLCADDR=(1,C,TR),
*               DLCADDR=(2,X,5452303030),   2 **nombre puerto
*               DLCADDR=(3,X,04),           3 **dirección SAP
*               DLCADDR=(4,X,400000011088)  6 **dirección MAC
*************************************************************************
** Below is Ethernet
*************************************************************************
*PATHE20 PATH  PID=1,
*               DLURNAME=PURPLE,
*               DLCADDR=(1,C,ETHERNET),
*               DLCADDR=(2,X,454E303030),   2 **nombre puerto
*               DLCADDR=(3,X,20),           3 **dirección SAP
*               DLCADDR=(4,X,400000011063)  6 **dirección MAC

*************************************************************************
* Below is X25 SVC
*************************************************************************
*A20RT   PATH  PID=3,
*              DLURNAME=GREEN,
*              DLCADDR=(1,C,X25SVC),
*              DLCADDR=(2,X,583235303033),    2 **nombre puerto
*              DLCADDR=(4,X,C3),      8 **Identificador protocolo
*              DLCADDR=(21,X,000566666), 9 **dirección DTE destino
*************************************************************************
* Below is X25 PVC
*************************************************************************
*A20RT   PATH  PID=3,
*              DLURNAME=GREEN,
*              DLCADDR=(1,C,X25PVC),
*              DLCADDR=(2,X,583235303033),   2 **nombre puerto
*              DLCADDR=(3,X,0001)           10 **Número canal lógico
*************************************************************************
```

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

Notas:

1 La diferencia entre el codificado de sentencias PU es:
- Para las definiciones de 2.0, la sentencia PU tiene IDBLK=...,IDNUM=....
- Para las definiciones de 2.1, la sentencia PU tiene CPNAME=....

2 Nombre del puerto en ASCII definido en el direccionador y usado por la DSPU

3 SAP de la DSPU (no canónica, salvo para Ethernet)

3a Dirección de la estación para SDLC

4 DLCI debe tener 4 dígitos ya que es media palabra

5 Dirección del MAC de la DSPU (no canónica) para Frame Relay BAN

6 Dirección del MAC de la DSPU (no canónica, salvo para la dirección MAC de Ethernet, que es canónica)

7 DLSw aparece a VTAM como un DLC de red en anillo

8 Identificador de protocolo

9 Dirección del DTE de destino (000566666, donde:
00 es fijo
05 es la longitud de la dirección del DTE
66666 es la dirección del DTE)

10 Número de canal lógico. Debe tener 4 dígitos ya que es media palabra.

11 Codificado de la LU

Consulte “Servidor de TN3270E” en la página 24 para ver un ejemplo de una sentencia de vía de acceso de PU interna.

Red de conexiones APPN

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

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

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

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

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

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

Cuando se define una red de conexiones, se le da un nombre. Este nombre se convierte en el nombre del CP del VRN y debe cumplir todos los requisitos de cualquier nombre de CP. Consulte la Tabla 24 en la página 159 para obtener una lista de los mencionados requisitos.

Restricciones

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

Branch Extender

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

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

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

Una BrNN:

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

Las limitaciones de Branch Extender son:

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

Extended Border Nodes

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

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

lamiento topológico entre las dos subredes y, además, permite que las sesiones y los flujos de servicios de directorio atraviesen los límites de la subred.

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

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

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

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

Ejemplo de topología de red

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

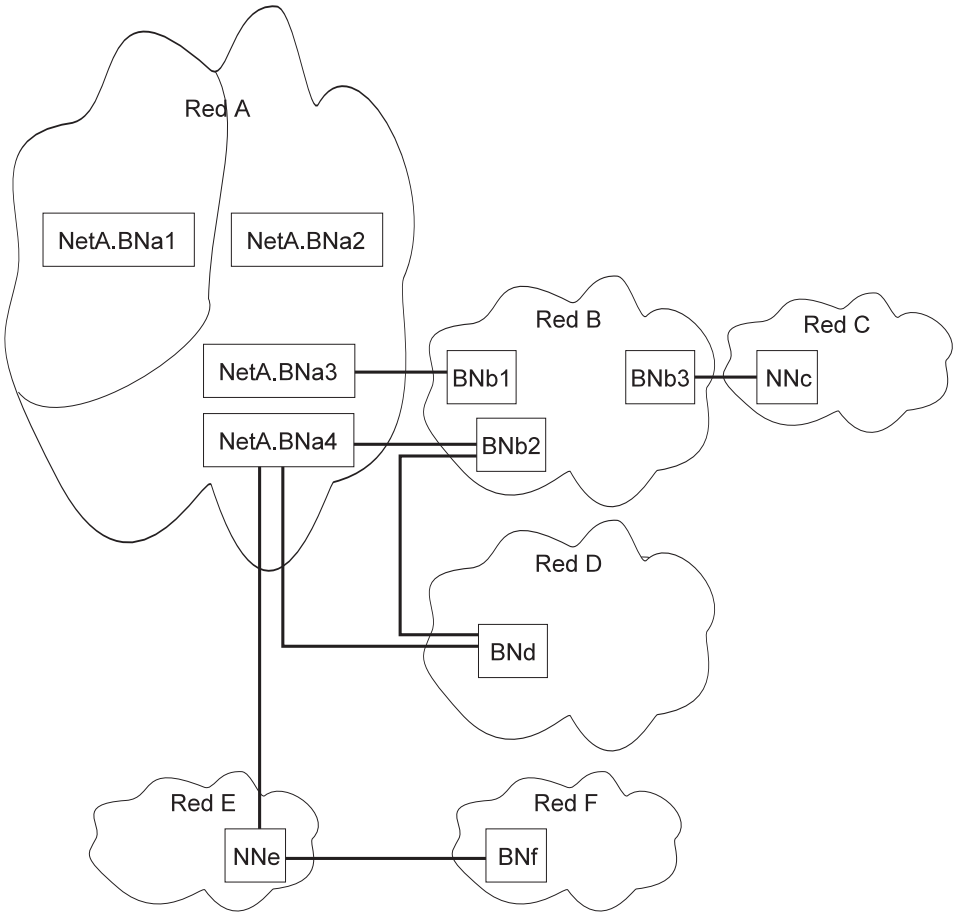


Figura 1. Conectividad de Extended Border Node

Nota: Las líneas en negrita representan los TG intersubred.

En esta figura:

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

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

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

Extensiones de servicios de sesión (SSE) para soporte NNS

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

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

Requisitos de red

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

- APPN Ver1 con el conjunto de opciones 1013, posibilidad de funcionar con extended border node (nodos de límite ampliado) periféricos
- APPN Ver2, donde el conjunto de opciones 1013 forma parte del software básico.

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

Comparación de Branch Extender con Extended Border Node

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

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

Ninguno de los dispositivos de comunicación directa de Branch Extender puede ser un nodo de red, un DLUR, VTAM o un nodo final de VTAM.

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

Extended Border Node es la opción adecuada cuando se desea unir varias redes o bien cuando se tiene una red grande que se desea subdividir, sin que haya restricción alguna sobre los tipos de nodos permitidos en las partes subdivididas. No existe el concepto de ascendente o de comunicación directa y se pueden tener extended border nodes, nodos de red, nodos finales, nodos de DLUR, VTAM o finales VTAM adicionales situados en cualquier lugar de la red. A diferencia de Branch Extender, un Extended Border Node no puede registrar recursos en otra red.

Gestión de un nodo de red

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

Puede usar SNMP para acceder a estos MIB estandarizados de IETF:

- APPC (RFC 2051)
- APPN (RFC 2155)
- HPR (RFC 2238)
- DLUR (RFC 2232)

También puede usar SNMP para acceder a estos MIB específicos de empresa:

- IBM APPN Memory
- IBM Accounting
- IBM HPR NCL
- IBM HPR Route Test
- IBM Branch Extender Node
- IBM Extended Border Node (EBN)

Posibilidades del punto de entrada para alertas relacionadas con APPN

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

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

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

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

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

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

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

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

Notas:

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

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

Los procesos de gestión del punto de control del direccionador están gestionados por el componente de los servicios de gestión del punto de control (CPMS). El componente CPMS del nodo de red del direccionador recoge datos de gestión de

problemas no solicitados en los recursos del dominio del direccionador y los reenvía al punto focal adecuado.

Unidades de mensaje con soporte

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

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

Posibilidades de SNMP para MIB de APPN

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

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

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

Cola de alertas retenidas configurable

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

Nota: Si configura un valor grande para **Held Alert Queue Size** (tamaño de la cola de alertas retenidas), deberá tener en cuenta la memoria adicional. Podrá hacerlo dejando que el algoritmo de ajuste calcule automáticamente el valor **Maximum Shared Memory** (memoria compartida máxima). Consulte “Ajuste del nodo APPN” en la página 47 para obtener información adicional acerca del algoritmo de ajuste de nodos.

Punto focal implícito

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

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

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

Definición dinámica de LU dependientes (DDDLU)

La definición dinámica de las LU dependientes (DDDLU) es un recurso de VTAM para conocer las unidades lógicas cuando se conectan con él, en vez de conocerlas durante la activación del nodo principal de la PU relacionada. Con este soporte, VTAM crea definiciones de LU a partir de definiciones de LU modelo reutilizables, en vez de usar LU definidas previamente. Las definiciones de LU se sustituyen o cambian cada vez que el dispositivo que las contiene se enciende (o notifica que está habilitado y puede iniciarse).

La posibilidad DDDLU requiere la aplicación de algunos cambios menores en VTAM y depende de que la activación de la unidad física (PU) se efectúe mediante una ACTPU de formato 1. Esta ACTPU puede transportar el vector de control de las posibilidades de la PU . Dicho vector indicará si el nodo de envío da soporte a NMVT (transporte de vectores de gestión de la red) no solicitados para Reply Product Set ID (ID del establecimiento del producto de respuesta - PSID). Si se da soporte a NMVT no solicitados para Reply PSID, se podrá conseguir la DDDLU.

El NMVT de Reply PSID contiene la dirección local de cada LU, un indicador de encendido y apagado, el tipo de máquina y el número de modelo del dispositivo y, opcionalmente, otra información que depende del dispositivo, necesaria para definir las unidades lógicas. VTAM usa esta información para elegir una sentencia de definición de LU modelo apropiada para crear una definición de LU.

Los vectores NMVT se muestran en la Tabla 2.

Tabla 2 (Página 1 de 2). Vectores NMVT de dispositivo

Dispositivo/modelo	Vector NMVT
Pantalla 3270 mod 2	3270002
Pantalla 3270 mod 3	3270003
Pantalla 3270 mod 4	3270004

Tabla 2 (Página 2 de 2). Vectores NMVT de dispositivo	
Dispositivo/modelo	**Vector NMVT**
Pantalla 3270 mod 5	3270005
Impresora 3270	3270P
Impresora SCS	SCSP

Definición dinámica de LU dependientes iniciada por el sistema principal

En la sección anterior se analiza la definición dinámica de LU dependientes cuando las inicia la PU mediante un NMVT. El sistema principal también puede definir dinámicamente LU dependientes. En dicho caso, no será necesario configurar ninguna LU dependiente. El único requisito necesario es que la estación de enlace o la PU local estén configuradas para permitir la definición de LU dinámicas. En el caso de la definición dinámica de LU iniciada por el sistema principal, las LU dependientes deben estar definidas en el archivo de nodo principal del sistema y debe especificarse INCLUD0E=YES (para las PU de subárea) en la sentencia PU. La palabra clave INCLUD0E tiene soporte de VTAM V4R4 con los APAR OW31805 y OW31436. Para las conexiones de subáreas remotas a través de NCP, se necesita V7R6 para el soporte de la palabra clave INCLUD0E.

A medida que se procesan las peticiones ACTLU, se crean las LU usando el nombre 0E del vector de control. Esto reduce en gran medida el tiempo de configuración de las LU dependientes. Si el sistema principal es un DLUS y la PU está recibiendo servicio de un DLUR en otro nodo, es posible que el CV0E de la petición ACTLU no se reenvíe a la PU desde el DLUR. En dicho caso, las LU no se crearán dinámicamente. Una vez creadas dinámicamente, las LU sólo se pueden eliminar suprimiéndolas manualmente mediante la configuración o volviendo a arrancar el sistema. Si se cambian los nombres de LU en el archivo de nodo principal del sistema principal después de crear dinámicamente las LU, los nombres locales no cambiarán.

Servidor de TN3270E

El servidor de TN3270E proporciona una función de pasarela de TN3270 para clientes de TN3270 de comunicación directa de un sistema principal SNA que ejecute una aplicación 3270. Los clientes se conectan con el servidor usando una conexión TCP. Esta conexión se correlaciona con una sesión de LU-LU dependiente de SNA que el servidor mantiene con el sistema principal SNA. El servidor de TN3270E maneja la conversión entre el flujo de datos de TN3270 y un flujo de datos de SNA 3270. La función Servidor de TN3270E cumple RFC 1646 y RFC 1647.

Las sesiones de TN3270 pueden atravesar las redes APPN así como las redes IP que usen HPR sobre IP.

El servidor de TN3270E puede usar una conexión de subárea o la función APPN DLUR para comunicarse con el sistema principal.

Consulte “Soporte para las conexiones SNA de subárea desde el servidor de TN3270E al sistema principal” en la página 29 para obtener más información y “Configuración de TN3270E usando DLUR” en la página 94 y “Configuración de

TN3270E usando una conexión de subárea” en la página 96 para ver ejemplos de configuraciones.

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

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

Nota:

1 077EEEE7 representa el bloque de ID/número de ID de la PU local

El dispositivo tiene dos servidores de telnet: la consola remota y el servidor de TN3270E. Se designará una dirección IP como dirección/puerto del servidor de TN3270E. Los telnets a esta dirección/puerto serán tn3270 y no llegarán a la consola remota. La configuración de TN3270E incluye el mandato `TN3270E config>` **set** para configurar la dirección/puerto IP del servidor de TN3270E.

Sólo puede especificarse una dirección para TN3270E.

- Uso de una dirección de interfaz

  Se puede asignar un número ilimitado de direcciones a una interfaz. Si el administrador del sistema no desea perder la capacidad de enviar telnet al direccionador usando una dirección de interfaz ya existente, puede añadirse una dirección adicional (con una máscara de subred que anunciarán RIP y OSPF) a una interfaz. Se recomienda designar una dirección de interfaz como dirección del servidor de TN3270E.

- Uso del id de dispositivo

  Para los fines de TN3270, esta dirección es como una dirección de interfaz.

- Uso de la dirección interna

  Esta dirección se anuncia en todos los protocolos de direccionamiento dinámicos. También se puede acceder a ella continuamente, mientras que, en el caso de las direcciones de interfaz, sólo se puede acceder a ellas cuando la

interfaz está activada. No se recomienda esta dirección como dirección del servidor de TN3270E, salvo en los casos en que se garantice la posibilidad de acceder a ella, independientemente del estado de la interfaz (activada o desactivada).

Agrupación de LU de TN3270E

La agrupación de LU representa una mejora de la función del servidor de TN3270E que facilita la configuración de algunas redes del servidor de TN3270E. Esta función permite que las LU de SNA se agrupen en "agrupaciones" con nombre. Así, los clientes de TN3270E pueden solicitar una conexión usando el nombre de la agrupación como nombre de LU. El servidor de TN3270E elegirá una LU de la agrupación especificada para servir a la solicitud del cliente.

Una agrupación es un grupo lógico de LU. Estas LU pueden ser de PU diferentes o de la misma PU, de sistemas principales diferentes o del mismo, etc. Cuando un cliente especifica un nombre de agrupación determinado, puede seleccionarse cualquier LU de la agrupación.

Como mínimo, siempre hay una agrupación de estaciones de trabajo implícita. Esta agrupación se denomina agrupación global por omisión. El nombre se define con el mandato `TN3270E config>` **set**. Las LU se añaden a esta agrupación mediante los mandatos `TN3270E config>` **add lu** o `TN3270E config>` **add implicit-pool**.

Diversos puertos de TN3270E

Esta mejora permite que los usuarios definan diversos puertos TCP para que el servidor de TN3270E "escuche". Este soporte permite que los clientes especifiquen el recurso de SNA que deseen usando un número de puerto.

Cuando se añaden los puertos, el usuario puede definir una agrupación de LU que se asociará con el número de puerto. A los clientes que se conecten con dicho puerto y no especifiquen ningún nombre de LU, se les asignará una LU de esta agrupación. Recuerde que el puerto siempre estará asociado a una agrupación de LU. Por omisión, se asociará a la agrupación global por omisión.

Una alternativa a la utilización de la asociación de agrupación de LU con puerto para elegir una LU es la utilización de la correlación de la dirección IP del cliente del servidor de TN3270E con el nombre de la LU, que se trata en “Correlación de la dirección IP del cliente del servidor de TN3270E con el nombre de LU” en la página 27. Si habilita esta correlación, se elegirá por omisión la LU usando las normas de correlación de nombres de LU en vez de usar la asociación de agrupación de LU con puerto. Por consiguiente, por omisión, cuando se habilita la correlación de nombres de LU, se aplica a todos los puertos. No obstante, incluso cuando se habilita esta opción, es posible configurar el puerto de tal manera que la función de correlación de nombres de LU se ignore y se use la agrupación de LU asociada con el puerto para elegir la LU.

También pueden definirse los puertos del servidor de TN3270E para un tipo determinado de soporte de servidor de TN3270 (básico o TN3270E). Dado que algunos clientes del TN3270 básico no negocian adecuadamente con los servidores de TN3270E, ahora puede definirse un puerto para que estos clientes se conecten con él.

Como mínimo, tiene que haber siempre un puerto definido para que lo use el servidor. Este puerto se especifica mediante el mandato `TN3270E Config>` **set**.

Cómo mínimo, siempre hay un puerto definido para que lo use el servidor. Este puerto se especifica mediante el mandato `TN3270E config>` **set**. La agrupación asociada al puerto es siempre la agrupación global por omisión.

Correlación de la dirección IP del cliente del servidor de TN3270E con el nombre de LU

La función de correlación de la dirección IP del cliente del servidor de TN3270E con el nombre de LU proporciona un mecanismo para que los administradores controlen el acceso de clientes a los recursos del servidor de TN3270E (por ejemplo, LU).

La correlación mejora la administración central permitiendo que el administrador configure con qué recursos de SNA (LU/agrupación) se correlacionarán las subredes/dirección de IP del cliente y qué recursos se utilizarán sin modificar las configuraciones del cliente.

La correlación elimina, en el lado del cliente, el pesado trabajo de tener que conectarse con un puerto específico o solicitar una LU/agrupación específica en la solicitud de conexión. Estas decisiones se mantienen en el servidor.

Cuando un cliente se conecta mientras está habilitada la correlación, el servidor empezará a ejecutar AND de la dirección IP del cliente con la máscara de subred de cada definición de correlación. La coincidencia más larga entre la dirección IP del cliente de entrada y la definición de correlación determinará qué definición de correlación se intentará primero. Si están utilizándose todos los recursos elegibles de la definición de correlación, se buscará de nuevo en las definiciones de correlaciones para encontrar la siguiente coincidencia más específica.

Si una definición de correlación contiene una máscara de subred completa (255.255.255.255) indicando que la entrada es para un cliente específico y el cliente no solicita una LU/agrupación específica, podrá intentarse 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 intentarán las entradas de la agrupación de la definición de correlación. Es necesario tener la correlación de subredes con una agrupación. En el caso de las LU individuales de estaciones de trabajo con impresoras asociadas, sólo es necesario que la LU de la estación de trabajo esté en la definición de correlación.

Puede añadirse una mezcla de tipos de LU y agrupaciones (estación de trabajo o impresora) a una correlación determinada. El recurso seleccionado se basará en el tipo de solicitud de conexión. El orden seguido en la definición de los recursos en la correlación será el orden en que se elija para una solicitud de conexión determinada.

Cómo se eligen las LU para las conexiones de clientes

Cuando se habilita la correlación de la dirección IP con el nombre de LU, por omisión se aplican las normas de correlaciones de dirección IP del cliente con nombre de LU a todos los puertos. La dirección IP del cliente se usa para determinar qué LU/agrupación se usará. No obstante, hay dos maneras de usar la asociación de agrupación de LU con puerto mientras se tiene también la función de correlación de nombres LU habilitada.

- Cuando defina el puerto, indique que no desea utilizar la función de correlación de nombres de LU para el puerto.
- Añada una correlación de dirección IP que especifique <*DEFLT*> como nombre de la agrupación.

En ambos casos, el número del puerto de destino se usará para determinar el recurso SNA a utilizar basándose en la tabla indicada a continuación. La tabla también se usará cuando esté activada la correlación pero no existan definiciones de correlaciones.

Si el cliente especifica un nombre de LU/agrupación en la petición de conexión, dicho nombre deberá coincidir con un recurso de una definición de correlación. Si el nombre especificado por el cliente es un nombre de LU contenido dentro de una agrupación, este nombre DEBERÁ estar en la definición de correlación para que la conexión sea aceptada. No basta con que un nombre de agrupación de LU aparezca en la definición de la correlación.

Cuando no se habilita la correlación de la dirección IP con el nombre de LU, la tabla siguiente describe cómo se asignan los recursos SNA.

Conexión de cliente	Definición de puerto	Resultado
Se especifica explícitamente una LU o un nombre de agrupación	Se define un nombre de agrupación	Se usa un nombre explícito siempre y cuando el nombre de entrada coincida con el nombre definido.
Se especifica explícitamente una LU o un nombre de agrupación	<DEFLT> definido como nombre de agrupación	Se usa un nombre explícito siempre y cuando el nombre de entrada se haya definido.
Se especifica explícitamente una LU o un nombre de agrupación	No se define nombre de agrupación en el puerto	Se usa un nombre explícito siempre y cuando el nombre de entrada se haya definido.
No se ha especificado ningún nombre de recurso	Se define un nombre de agrupación	Se usa el nombre definido en el puerto
No se ha especificado ningún nombre de recurso	<DEFLT> especificado como nombre de agrupación	Se usa la agrupación global por omisión

El servidor de TN3270E y DDDLU

Si así lo solicita VTAM, la función del servidor de TN3270E usará DDDLU para crear las LU locales en VTAM. En vez de enviar todos los PSID de respuesta al recibir la ACTPU, el servidor esperará hasta que sea realmente necesario definir la LU. La definición de la LU se producirá cuando un cliente de TN3270 se conecte y necesite una LU que no se haya definido en VTAM.

El servidor de TN3270E y la definición dinámica de LU iniciada por el sistema principal

Las LU dependientes creadas dinámicamente cuando se procesan peticiones ACTLU están disponibles para el servidor de TN3270E como LU de estación de trabajo. El tiempo de configuración del servidor de TN3270E se reduce en gran medida gracias a la función de definición dinámica de LU. No obstante, el cliente de la estación de trabajo TN3270 debe solicitar explícitamente el nombre de la LU; estas LU no pertenecen a una agrupación de LU y no están disponibles para los clientes de la impresora. Las LU dependientes dinámicas no están disponibles para la función de correlación de la dirección IP del cliente del servidor con el nombre de LU. Sólo pueden usarse con la función de correlación las LU que están configuradas.

Soporte para las conexiones SNA de subárea desde el servidor de TN3270E al sistema principal

La conexión con un sistema principal para establecer una sesión de LU-LU dependiente puede efectuarse mediante una conexión de subárea tradicional o una conexión APPN junto con la función APPN DLUS/DLUR. La solución APPN DLUS/DLUR permite que el nodo aparezca a VTAM como varios dispositivos PU que dan soporte, cada uno de ellos, hasta a 253 LU dependientes. También debe aparecer como varias PU de un sistema principal conectado, un nodo que ofrezca servicios del servidor de TN3270E en una conexión de subárea para más de 253 clientes a la vez.

Las conexiones de subárea tienen soporte sobre los tipos de DLC siguientes:

- Ethernet
- Red en anillo
- FDDI
- LSA
- Frame Relay
- Frame Relay BAN
- DLSw

Nota: El soporte para conexiones SNA de subárea para servicios del servidor de TN3270E elimina la necesidad de APPN en el sistema principal. No obstante, APPN debe seguir configurándose en el direccionador.

En la Figura 2 en la página 30 se muestra una configuración de nodo SNA conectado a subárea con un dispositivo que ejecuta la función de servidor de TN3270E y que aparece a VTAM como varias PU de comunicación directa.

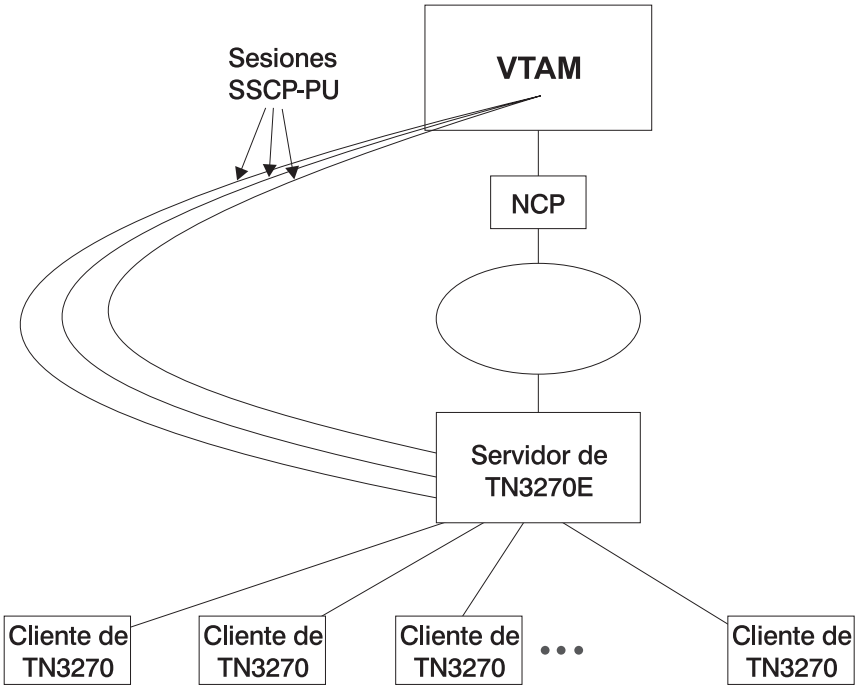


Figura 2. Diversas PU para nodos SNA conectados a una subárea

Consulte “Configuración de TN3270E usando una conexión de subárea” en la página 96 para obtener un ejemplo de configuración.

Soporte de Enterprise Extender para HPR sobre IP

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

DLC con soporte

La Tabla 3 en la página 31 muestra los puertos de DLC que tienen soporte del dispositivo sobre APPN:

Tabla 3. Tipos de puerto con soporte para direccionamiento de APPN

Tipo de puerto	Estándar	HPR	ISR	DLUR*
Ethernet	Versión 2	Sí	Sí	Sí
Ethernet	IEEE 802.3	Sí	Sí	Sí
TR	802.5	Sí	Sí	Sí
PPP en serie		Sí	Sí	No
FR en serie (puenteado y direccionado) **		Sí	Sí	Sí
Frame Relay BAN		Sí	Sí	Sí
Puenteo de LAN en serie		ND	ND	ND
SDLC		No	Sí	Sí
X.25	CCITT X.25	No	Sí	Sí
DLSw (sólo remoto) ***		No	Sí	Sí
APPN/PPP/RDSI		Sí	Sí	No
APPN/FR/RDSI		Sí	Sí	Sí
APPN/PPP/V.25bis		Sí	Sí	No
APPN/PPP/V.34		Sí	Sí	No
LANE	Se ajusta al Forum	Sí	Sí	Sí
ATM		Sí	No	Sí
HPR sobre IP		Sí	No	Sí
100Mbps Ethernet		Sí	Sí	Sí
100Mbps TR	802.5	Sí	Sí	Sí

Notas:

1. * Esta columna se refiere al puerto que proporciona la conexión con la PU de comunicación directa (DSPU).
2. ** Use formato puenteado cuando tenga dos dispositivos conectados por Frame Relay y uno de ellos no tenga APPN. De lo contrario, use formato direccionado debido a su mejor rendimiento.
3. *** Dado que APPN se ejecuta sobre DLSw y éste se ejecuta sobre X.25, puede direccionar tráfico de APPN ISR sobre X.25 ejecutando APPN sobre DLSw.

Proceso de configuración del direccionador

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

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

- ID de red del nodo de red
- Nombre del punto de control del nodo de red
- Número XID (de nodo de red) para la conexión de subárea
- Tipo de nodo adyacente (de estación de enlace)

- Cambio de la función de nodo (EBN, BN, NN)
- Cualquier parámetro que esté bajo las opciones siguientes:
  - Direccionamiento de alto rendimiento (HPR) en el nivel de nodo
  - Peticionario de LU dependientes (DLUR) en el nivel de nodo
  - Red de conexiones
  - Clase de servicio
  - Ajuste de nodo
  - Gestión de nodo
  - Puntos focales
  - Correlaciones de nombres de modalidades
  - Parámetros de supresión de TN3270E
  - Listas de direccionamientos
  - Tablas de correlaciones de COS

Requisitos de configuración de APPN

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

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

Configuración del direccionador como nodo de red de APPN

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

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

Configuración mínima

Este grupo de pasos de configuración de APPN:

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

Si elige la configuración mínima, los nodos adyacentes deberán definir conexiones con el nodo de red del direccionador para asegurar la conectividad. Dado que los nodos APPN pueden iniciar sesiones de CP-CP con el nodo de red del

direccionador, no es necesario definir estos nodos en la configuración del direccionador. Por lo general, cuando configure APPN en el direccionador, podrá simplificar en gran medida esta tarea si permite que el nodo de red del direccionador acepte solicitudes de conexión de cualquier nodo. Si configura el nodo de red de esta manera, no tendrá que definir información sobre los nodos adyacentes, salvo en los casos siguientes:

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

En dichos casos, debe especificar información sobre el nodo adyacente cuando habilite el direccionamiento de APPN en el puerto específico que está usando para conectarse con el mencionado nodo y debe seguir los pasos de configuración descritos en “Configuración de inicio de conexiones” en la página 34.

Siga el procedimiento siguiente para los pasos de configuración mínima:

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

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

Notas:

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

Configuración de inicio de conexiones

Este conjunto de pasos de configuración de APPN:

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

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

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

Si ninguno de estos casos se puede aplicar a la configuración, siga los pasos de configuración descritos en “Configuración mínima” en la página 32.

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

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

Nota: Dado que *Service Any* está habilitado por omisión, el nodo aceptará cualquier solicitud de conexión que reciba de otro nodo.

4. Defina las estaciones de enlace de APPN en los puertos de DLC seleccionados para los nodos adyacentes con los que este nodo de red puede iniciar conexión.

   Nota: No es necesario definir las estaciones de enlace en todos los puertos, únicamente en aquellos sobre los que desee iniciar conexiones con nodos adyacentes.

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

Configuración de control de las conexiones

Este grupo de pasos de configuración de APPN:

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

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

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

1. Seleccione los puertos sobre los que desee establecer conexiones con nodos adyacentes desde los tipos de puertos de DLC siguientes con soporte de APPN:
   - Puerto de LAN en anillo
   - Puerto de LAN Ethernet
   - Puerto serie Frame-relay
   - Puerto serie PPP

- X.25
- DLSw
- SDLC
- Puerto IP

2. Defina los puertos seleccionados como puertos APPN directos con los parámetros siguientes:
   - Habilite *APPN routing* (direccionamiento APPN) en este puerto
   - Inhabilite el parámetro *service any port* (servir cualquier puerto)
3. Si está configurando APPN usando un puerto DLSw:
   - Habilite el puenteo en el nodo
   - Habilite DLSw en el nodo.
   - Defina los puertos de DLSw con el parámetro siguiente:
     – Defina una dirección del MAC administrada localmente para DLSw
     – Inhabilite el parámetro de nodo *Service any* (servir cualquiera)
4. Habilite el direccionamiento de APPN en el puerto.
5. Defina las estaciones de enlace de APPN en los puertos de DLC seleccionados para los nodos adyacentes:
   - que pueden iniciar una conexión con este nodo de red.
   - con los que desea que este nodo de red de direccionador inicie una conexión.

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

Configuración de Branch Extender

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

1. Use el mandato **set node** para:
   a. Responder 1 para elegir Branch Extender cuando se le pregunte *Enable Branch Extender or Border Node* (Habilitar Branch Extender o Border Node). Si responde 0, no aparecerá ninguna de las preguntas de Branch Extender.
   b. Responder yes (sí) o no a la pregunta *Permit search for unregistered LUs* (Permitir búsqueda de LU no registradas) según si desea permitir o no búsquedas desde la red troncal de LU que no se registraron en el servidor de nodos de red.
   c. La respuesta que dé a la pregunta *Branch uplink* (enlace hacia arriba de la rama) determinará el valor por omisión de la pregunta análoga del nivel de enlace.
2. Use el mandato **add link** para:
   a. Responder sí a la pregunta *Branch uplink* si desea que el direccionador aparezca como nodo final en este enlace. Un nodo final es para enlaces con los nodos de red de la red troncal. Tenga en cuenta que esta pregunta no aparece y su valor será sí, si ha definido la estación de enlace adyacente para que sea un nodo de red en uno de los indicadores de configuración anteriores. Responda no si desea que el direccionador aparezca como nodo de red en este enlace. Un nodo de red es para enlaces con nodos finales.
   b. La pregunta *Is uplink to another Branch Extender node* (Es enlace hacia arriba con otro nodo de Branch Extender) sólo se pregunta si este enlace se ha definido como recurso limitado y también como enlace hacia arriba de Branch Extender. Responda sí si el nodo adyacente es otro Branch Extender.
   c. La pregunta *Preferred network node server* (servidor de nodos de red preferido) sólo se pregunta si el nodo adyacente es un nodo de red y las sesiones de CP-CP tienen soporte en este enlace. Dado que sólo puede tener un único servidor de nodos de red preferido, esta pregunta no volverá a aparecer una vez haya respondido sí en algún enlace.

Configuración de Extended Border Nodes

Para configurar extended border nodes (nodos de límite ampliado) deberá configurar uno o varios de los parámetros siguientes:

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

Set node

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

Subnetwork visit count (Recuento de visitas a la subred) es el primer indicador. Este parámetro define el número máximo de subredes topológicas que puede atravesar una sesión. El valor indicado se usará como valor por omisión para el nodo de límite ampliado. Puede especificar valores diferentes para *subnetwork visit count* cuando añada puertos, enlaces o listas de direccionamientos.

Cache search time (Tiempo de búsqueda en la antememoria) es el indicador de nivel de nodo siguiente. Este parámetro especifica el tiempo en minutos durante el cual el nodo de límite ampliado mantendrá información en las búsquedas efectuadas en varias subredes. El objetivo es que este parámetro sirva de mecanismo primario para limitar el tamaño de la antememoria.No obstante, el parámetro siguiente también se puede usar para controlar dicho tamaño.

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

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

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

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

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

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

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

Limited (Limitado) Este valor aumenta la lista de nombres de CP de salto siguiente obtenida a partir de la lista de direccionamientos configurada según mejor coincidencia, con nombres de CP obtenidos a partir de los conocimientos que tiene el nodo de límite ampliado de los recursos y la topología existentes. Estos nombres de CP adicionales se obtienen:

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

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

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

Si habilita *List optimization* (Optimización de lista), el reordenamiento descrito en la página 38 se repetirá otra vez y los nombres de CP obtenidos a partir de los datos configurados también podrán volver a ordenarse.

Add port

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

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

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

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

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

Non-native
(No nativo) El nodo adyacente no forma parte de la subred topológica del nodo de límite ampliado.

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

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

Add link

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

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

Add Routing List(s)

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

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

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

El número de nombres de LU y de CP usados en las listas de direccionamientos tiene un límite. Los límites pueden variar de acuerdo con el modelo de direccionador que tenga. Consulte la Tabla 38 en la página 191 para obtener infor-

mación detallada sobre el mandato. El límite se ha establecido para poder disfrutar de la mayor flexibilidad posible en los diversos entornos. La capacidad del direccionador para manejar la especificación de varias listas de direccionamientos, cada una de ellas con varios nombres de LU y de CP, está limitada por la disponibilidad de memoria no volátil de configuración, memoria del direccionador y memoria compartida de APPN. Consulte “Ajuste del nodo APPN” en la página 47 para obtener información sobre los parámetros de ajuste de APPN que controlan la cantidad de memoria compartida.

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

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

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

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

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

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

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

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

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

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

Add COS Mapping Table

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

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

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

El número de nombres de redes no nativas usado en las tablas de correlaciones de COS tiene un límite. Los límites pueden variar de acuerdo con el modelo de direccionador que tenga. Consulte la Tabla 39 en la página 194 para obtener información detallada sobre el mandato. El límite se ha establecido para poder disfrutar de la mayor flexibilidad posible en los diversos entornos. La capacidad del direccionador para manejar la especificación de varias tablas de correlaciones de COS, cada una de ellas con varios nombres de redes no nativas y pares de nombres de COS, está limitada por la disponibilidad de memoria no volátil de configuración, memoria del direccionador y memoria compartida de APPN. Consulte “Ajuste del nodo APPN” en la página 47 para obtener un análisis detallado de los parámetros de ajuste de APPN que controlan la cantidad de memoria compartida.

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

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

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

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

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

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

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

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

Direccionamiento de alto rendimiento

Consulte la Tabla 3 en la página 31 para obtener una lista de los puertos que dan soporte a HPR.

Consulte “Requisitos de configuración de APPN” en la página 32 para obtener información sobre cómo configurar los protocolos que dan soporte al direccionamiento APPN y HPR sobre los DLC directos en el direccionador. En el caso de los parámetros de HPR como el temporizador de conmutación de vías de acceso y el de reintento, la configuración se efectúa en el nivel de nodo y no se especifica en adaptadores individuales.

DLUR

Consulte la Tabla 3 en la página 31 para obtener una lista de los puertos que dan soporte al DLUR.

Configuración de los puntos focales

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

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

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

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

Configuración del tamaño de la cola de retención de alertas

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

A medida que aumente el tamaño de la cola de retención de alertas, necesitará memoria adicional. Si la establece en un valor elevado, es posible que desee ajustar el valor "Maximum Shared Memory" (Memoria compartida máxima). Consulte “Ajuste del nodo APPN” en la página 47 para obtener información adicional.

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

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

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

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

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

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

Calculo de rutas de APPN usando las características de los TG

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

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

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

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

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

Opciones de COS

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

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

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

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

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

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

- Usar tablas de COS estándar o las tablas de COS mejoradas (para ATM).
- Definir un nombre de modalidad nuevo y su correlación en un nombre de COS.
- Cambiar un nombre de modalidad en una correlación de 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 especificado previamente, con un nombre de COS diferente.

Consulte el análisis detallado de los servicios de direccionamiento y topología en *SNA APPN Architecture Reference*, SC30–3422, para obtener una descripción de las tablas ATM COS estándares.

Ajuste del nodo APPN

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

- Estableciendo manualmente los valores de los parámetros de ajuste *maximum shared memory* (memoria compartida máxima), *percent of APPN shared memory to be used for buffers* (porcentaje de memoria compartida APPN a usar para los almacenamientos intermedios) y *maximum cached directory entries* (número máximo de entradas de directorio en antememoria) usando la opción **talk 6** de la interfaz de la línea de mandatos.
- Seleccionando valores para los parámetros *maximum number of ISR sessions* (número máximo de sesiones de ISR), *maximum number of adjacent nodes* (número máximo de nodos adyacentes) y otros parámetros que aparecen en la Tabla 9 en la página 117 y haciendo que el algoritmo de ajuste calcule automáticamente los valores de los parámetros *maximum shared memory* y *maximum cached directory entries*.

  Use el Configuration Program para invocar el algoritmo de ajuste.

El parámetro *maximum shared memory* influye en la cantidad de almacenamiento disponible para el nodo de red APPN para efectuar operaciones de red. Por ejemplo, puede permitir que APPN tenga un tamaño de RU de 4K estableciendo *maximum shared memory* en un mínimo de 1 Megabyte y *percent of APPN shared memory used for buffers* en un valor lo suficientemente grande como para permitir que haya un mínimo de 1 Megabyte de memoria disponible para el gestor de almacenamientos intermedios.

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

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

Notas de ajuste

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

Servicio de nodo (Rastreos)

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

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

Los rastreos APPN se agrupan en las 5 categorías siguientes:

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

Mejoras en los rastreos de APPN

A continuación, presentamos las mejoras a los rastreos de APPN:

- Ahora puede habilitar/inhabilitar todos los distintivos de rastreo a través de `talk 6` usando la pregunta *Turn all trace flags off* (Desactivar todos los distintivos de rastreo) realizada con el mandato **set trace** o usando el Configuration Program. Consulte la página 120 para obtener más información.
- Ahora puede filtrar los datos de rastreo de transmisiones y recepciones de control de enlace de datos según el tipo de mensaje o especificando la longitud máxima de los datos por paquete a rastrear. Consulte la Tabla 15 en la página 134 para obtener más información.

Estadísticas de nodo y de contabilidad

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

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

Si habilita el parámetro *collect intermediate session information* (recoger información de sesión intermedia) instruirá al direccionador para que tome los nombres de sesión y lea los contadores de todas las sesiones intermedias activas. Si habilita el parámetro *save RSCV information for intermediate sessions* (guardar infor-

mación de RSCV para sesiones intermedias) instruirá al direccionador para que recoja datos de RSCV para sesiones intermedias activas. Esto datos son útiles para supervisar rutas de sesión. En ambos casos, puede recuperar los datos en sesiones activas emitiendo los mandatos de SNMP **get** y **get-next** para variables de la APPN Management Information Base (Base de información de gestión de APPN - MIB).

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

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

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

Notas:

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

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

   Para habilitar implícitamente la recogida, establezca *create intermediate session records* (crear registros de sesiones intermedias) en yes. Este valor alterará temporalmente el de *collect intermediate session information*.

2. Los cambios de configuración en los parámetros de contabilidad de APPN efectuados usando la interfaz **talk 6** no entrarán en vigor hasta que el direccionador o la función APPN del direccionador se reinicien. No obstante, puede realizar los cambios interactivamente, emitiendo los mandatos **set** de SNMP para modificar las variables APPN MIB asociadas a los parámetros de configuración. Consulte el manual *Software User's Guide* para obtener una lista de estas variables de MIB.

3. Los datos sobre RSCV de sesiones intermedias se obtienen examinando la petición BIND usada para activar una sesión entre dos LU. Los datos de RSCV no se recogen para sesiones que ya se hayan establecido ya que la información de BIND para dichas sesiones no está disponible.

4. Los datos de las sesiones intermedias no se recogen para sesiones de HPR ya que dichas sesiones no forman parte de HPR. Si el direccionador contiene un límite ISR/HPR, los datos de la sesión intermedia se recogerán cuando pasen por el mencionado límite.

Algoritmo de reintento del DLUR

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

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

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

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

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

Hay dos casos en los que se determina el algoritmo de reintento:

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

     Nota: Si *Perform long retries to restore disrupted pipe* es No, no se efectuará ningún reintento.

  6. Intenta acceder al DLUS de reserva.
  7. Si el intento no es satisfactorio, intenta acceder al DLUS de seguridad.

  Ejemplo:

  – Supongamos los valores de parámetro siguientes:

    - *Delay before initiating retries* = 120 sec
    - *Perform short retries to restore disrupted pipe* = yes
    - *Short retry timer* = 60 sec

- *Short retry count* = 2
- *Perform long retries to restore disrupted pipe* = yes
- *Long retry timer* = 300 sec

– Se produce un fallo en la activación del conducto.

– Espera 120 segundos (el valor de *Delay before initiating retries*).

– Vuelve a intentar el DLUS primario y, si falla, reintenta el DLUS de seguridad.

– Si el reintento falla, espera 300 segundos (el valor de *Long retry timer*), reintenta el DLUS primario y, si falla este reintento, vuelve a intentar el DLUS de seguridad.

– Si falla el reintento, sigue reintentando el DLUS primario y de seguridad, esperando 300 segundos entre las secuencias de reintento, mientras la DSPU solicita la ACTPU.

- En el resto de los casos de fallo de conducto, el DLUR reintentará el DLUS primario y el DLUS de seguridad inmediatamente después. Si falla, el DLUR:

  1. Esperará el tiempo especificado por el mínimo de los parámetros *short retry timer* y *Delay before initiating retries*.
  2. Intentará acceder al DLUS de reserva.
  3. Si el intento no es satisfactorio, intentará acceder al DLUS de seguridad.
  4. Si la activación del conducto sigue fallando, el DLUR hará tantos reintentos (el proceso de reintento se describe en los pasos 1 - 3), como se especifique en *short retry count*.

     Si *short retry count* se agota, el DLUR hará reintentos, tal como se define en los pasos 5 - 7, mientras la DSPU solicite la ACTPU.
  5. Espera la cantidad de tiempo especificada por *Long retry timer*

     Nota: Si *Perform long retries to restore disrupted pipe* es No, no se efectuará ningún reintento.

  6. Intenta acceder al DLUS primario.
  7. Si el intento no es satisfactorio, intenta acceder al DLUS de seguridad.

  Ejemplo:

  – Supongamos los valores de parámetro siguientes:

  - *Delay before initiating retries* = 120 sec
  - *Perform short retries to restore disrupted pipe* = yes
  - *Short retry timer* = 60 sec
  - *Short retry count* = 2
  - *Perform long retries to restore disrupted pipe* = yes
  - *Long retry timer* = 300 sec

  – Se produce un fallo en la activación del conducto.

  – Reintenta inmediatamente el DLUS primario y de seguridad.

  – Si este reintento falla, espera durante 60 segundos (el valor de *Short retry timer*).

  – Reintenta el DLUS primario. Si el reintento falla, reintenta el DLUS de seguridad. Se trata del intento núm. 1 de *Short retry count*.

– Si falla, espera durante 60 segundos (el valor de *Short retry timer*).
– Vuelve a intentar el DLUS primario y, a continuación, el DLUS de seguridad. Se trata del intento núm. 2 de *Short retry count*. Ahora, *Short retry count* estará agotado.
– Si el reintento sigue fallando, espera 300 segundos (el valor de *Long retry timer*). A continuación, vuelve a intentar el DLUS primario. Si el reintento falla, reintenta el DLUS primario.
– Mientras el reintento falla, sigue reintentando el DLUS primario y el de seguridad, esperando 300 segundos entre las secuencias de reintento, mientras la DSPU solicite la ACTPU.

Implementación de APPN en el direccionador usando DLSw

El direccionador también da soporte a APPN sobre DLSw en cuestiones de conectividad con nodos a través de un asociado DLSw remoto. En la Figura 3 podemos ver un ejemplo. Este soporte permite que los clientes que tengan configuraciones de DLSw, migren sus redes a 2210.

Nota: Se recomienda usar APPN sobre DLC directos cuando estén disponibles, en vez de APPN sobre DLSw.

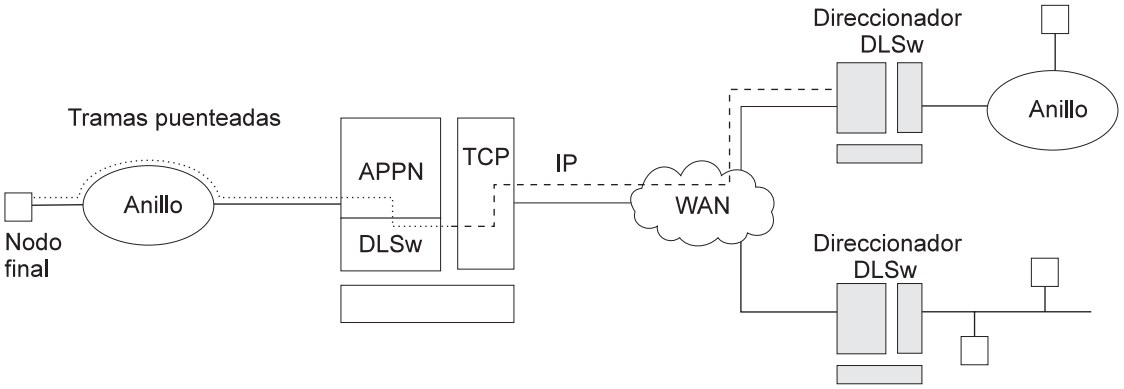


Figura 3. Flujo de datos en una configuración de APPN cuando se usa un puerto DLSw

Restricciones de la configuración de APPN cuando se usa DLSw:

- Conectividad únicamente a través de asociados de DLSw remotos.
- Sólo 1 puerto de DLSw por direccionador
- Uso de una dirección del MAC administrada localmente
- HPR no tiene soporte en los puertos de DLSw
- Los puertos de DLSw no pueden ser miembros de redes de conexiones
- Los TG paralelos no tienen soporte en los puertos de DLSw

Consulte “Configuración del direccionador como nodo de red de APPN” en la página 32 para obtener información sobre cómo configurar APPN usando DLSw.

Cómo usa APPN los puertos DLSw para transportar datos

Cuando configure APPN en el direccionador para que use un puerto de Data Link Switching (Conmutación de enlace de datos - DLSw), DLSw se usará para proporcionar una interfaz orientada a conexión (tipo 802.2 LLC) entre el componente APPN del direccionador y los nodos APPN y los nodos finales LEN conectados a un asociado de DLSw remoto.

Cuando configure un puerto DLSw para APPN en el direccionador, se asignará al nodo de red un par de direcciones MAC y SAP exclusivas que lo habilitarán para comunicarse con DLSw. La dirección del MAC para el nodo de red está administrada localmente y no debe corresponder a ninguna dirección del MAC física de la red DLSw.

Implementación de la red de conexiones APPN Frame Relay BAN

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

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

El SATF que aparece en la Figura 4 muestra que el APPN NN del direccionador debe definir una estación de enlace para cada nodo de la red en anillo para iniciar una conexión con cada nodo de ésta. El APPN NN debe saber la dirección DLCI para el enlace Frame Relay y la dirección del MAC de cada nodo de la red en anillo. Si los nodos de la red en anillo desean iniciar una conexión con el APPN NN, deberán definir una estación de enlace en el APPN NN del dispositivo y especificar:

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

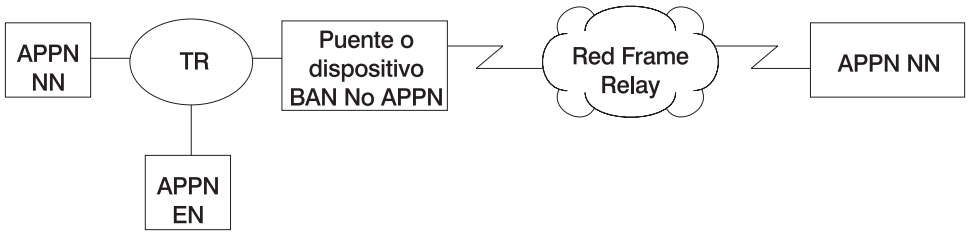


Figura 4. Vista lógica con soporte de red de conexiones BAN/Trama puenteada Frame Relay

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

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

La Figura 5 en la página 54 muestra todos los nodos como miembros de la misma red de conexiones. Los nodos usan la red de conexiones para establecer comunicación con el resto de los nodos, por lo que se elimina la necesidad de crear conexiones con el resto de los nodos en el SATF. Para convertirse en miembro de una red de conexiones, debe "conectarse" el puerto de un nodo APPN a dicha red definiendo una interfaz de red de conexiones. Cuando el puerto se activa, el componente APPN crea un TG de red de conexiones con un nodo de direccionamiento virtual (VRN). Este TG identifica la conexión directa desde el puerto con la red de conexiones. El nombre del CP del VRN es el de la red de conexiones.

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

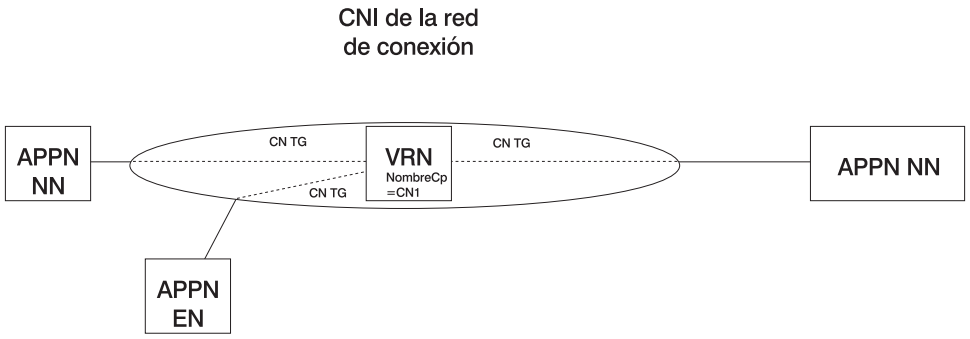


Figura 5. Trama puenteada de APPN Frame Relay con la red de conexiones BAN

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

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

Ejemplos de definiciones de red de conexiones APPN Frame Relay BAN

Ejemplo 1

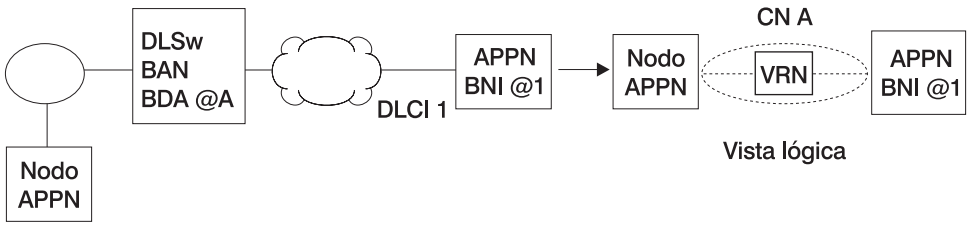


Figura 6. Red de conexiones única que usa BAN con 1 puerto de Frame Relay

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

Ejemplo 2

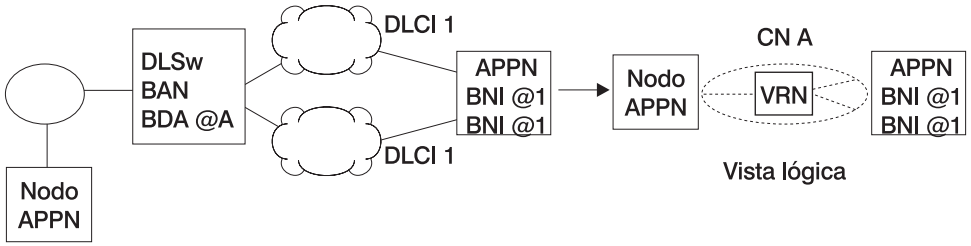


Figura 7. Red de conexiones única que usa BAN con varios puertos Frame Relay

Notas:

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

Ejemplo 3

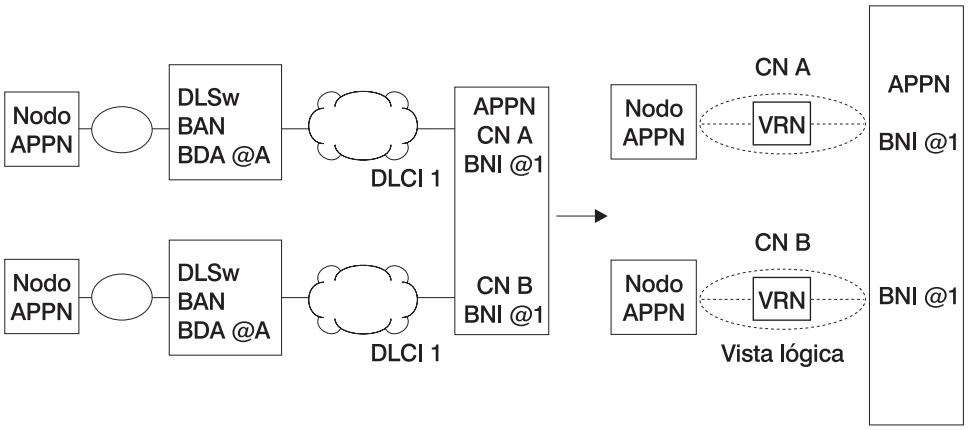


Figura 8. Diversas redes de conexiones que usan BAN

Notas:

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

Ejemplo 4

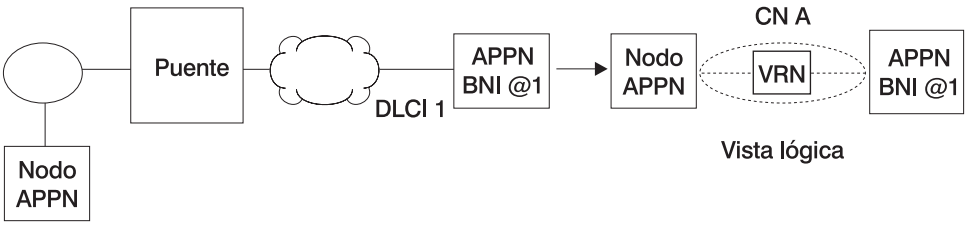


Figura 9. Red de conexiones única que usa el puenteo con 1 puerto de Frame Relay

Notas:

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

Ejemplo 5

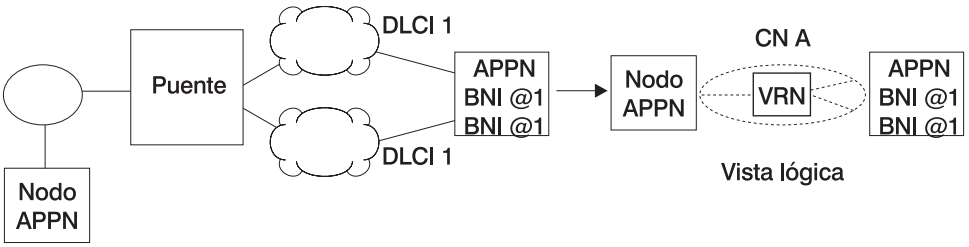


Figura 10. Red de conexiones única que usa el puenteo con diversos puertos Frame Relay

Notas:

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

Ejemplo 6

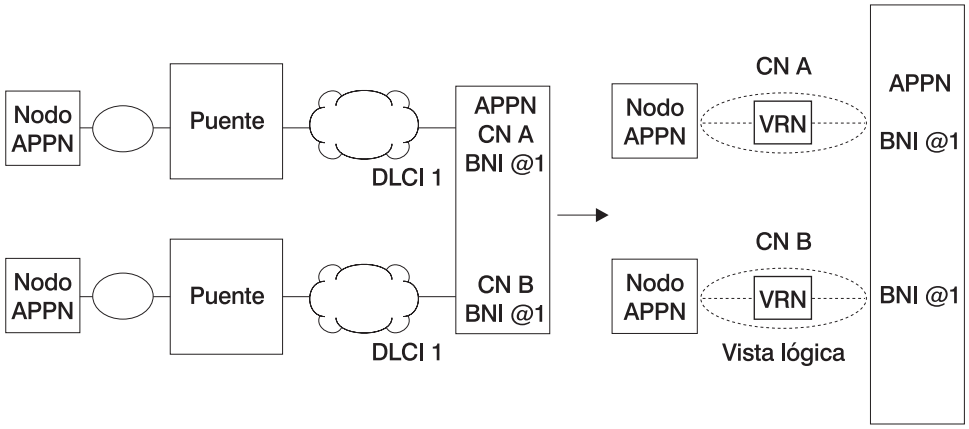


Figura 11. Diversas redes de conexiones que usan el puenteo

Notas:

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

Listas de parámetros del nivel de puerto

Use las tablas siguientes para configurar los puertos de APPN:

- Configuración del puerto en la página 139
- Definición de puertos en la página 146
- Características del TG por omisión del puerto en la página 150
- Características LLC por omisión del puerto en la página 155

Listas de parámetros del nivel de enlace

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

- Valores por omisión de HPR en la página 158
- Estaciones de enlace - Detalle en la página 159
- Modificación de las características de los TG en la página 171
- Modificación del servidor de LU dependientes en la página 174
- Modificación de las características del LLC en la página 175

- Modificación de los valores por omisión de HPR en la página 177

Lista de parámetros de LU

Use la tabla siguiente para configurar una LU:

- Nombre de la LU del nodo final LEN en la página 178

Listas de parámetros del nivel de nodo

Use las tablas siguientes para configurar un nodo APPN:

- Características básicas del nodo local en la página 105
- Direccionamiento de alto rendimiento (HRP) en la página 110
- Temporizador de HPR y opciones de reintento en la página 111
- Peticionario de LU dependientes en la página 113
- Red de conexiones - Detalle en la página 179
- Características de los TG (Red de conexiones en la página 184
- APPN COS - Puerto adicional a CN en la página 188
- Rastreos de nivel de nodo en la página 120
- Rastreos de señales entre procesos en la página 125
- Rastreos de la entrada y salida en módulos en la página 129
- Rastreos de nivel de componentes generales en la página 130
- Gestión de nodos APPN en la página 136
- “TN3270E” en la página 197
- Tabla 38 en la página 191
- Tabla 39 en la página 194

Notas sobre la configuración de APPN

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

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

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

Configuración de un circuito permanente usando RDSI

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

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

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

Config>n 6
Circuit configuration
FR Config>li all

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

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

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

FR Config>ex

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

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

  Maximum PVCs allowable =      64
  Total PVCs configured  =       1

            Circuit              Circuit   Circuit   CIR     Burst  Excess
             Name                Number     Type    in bps   Size   Burst
 ------------------------------- ------- ---------- ------- ------- -------
2210-21-i6          2             16     Permanent 64000    64000     0

  = circuit is required and belongs to a required PVC group
```

```
FR Config>ex
Config>p appn
APPN user configuration
APPN config>add p
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
 (S)DLC, (X)25,  (D)LSw, (A)TM, (IP) [  ] ? f
Interface number(Default 0): [0]?6
Port name (Max 8 characters) [FR006 ] ?
Enable APPN on this port (Y)es (N)o [Y ] ?
Port Definition
        Service any node: (Y)es (N)o[Y]?
        Limited resource: (Y)es (N)o[N]?
        High performance routing: (Y)es (N)o [Y]?
 Maximum BTU size (768-2044) [2044 ] ?
 Percent of link stations reserved for incoming calls (0-100) [0 ] ?
 Percent of link stations reserved for outcoming 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 all
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
         TONN1IS    FR006              16       YES     YES       0  4
LU NAME:
             LU NAME         STATION NAME           CP NAME
        ------------------------------------------------------------
APPN config>
```

Nota:

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

Configuración de APPN sobre circuitos de marcación bajo pedido

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

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

Consulte el manual *Software User's Guide* para obtener información adicional acerca de los circuitos de marcación bajo pedido.

Consideraciones sobre el nodo PU 2.1

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

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

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

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

Consideraciones sobre el nodo PU 2.0

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

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

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

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

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

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

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

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

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

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

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

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

********************************************************************************
Config>n 9
Circuit configuration
FR Config>li all

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

Inbound destination name        = 2210-15

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

FR Config>ex

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

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

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

*****************************************************************************
**** Configure the linkstation for the DOD link to NN15
*****************************************************************************
APPN config>add li
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 all
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
  TO15DOD   PPP009    000000000000       YES      NO       0   7
LU NAME:
             LU NAME         STATION NAME           CP NAME
 ------------------------------------------------------------
```

Nota:

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

Configuración del redireccionamiento de la WAN

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

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

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

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

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

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

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

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

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

Config>ex
*************************************************************************
*
**** Configure the Wan Reroute Primary and Alternate circuit
*
*************************************************************************
Config>fea wan  4
WAN Restoral user configuration
WRS Config>en wrs
WRS Config>add alt
Alternate interface number  [0 ] ? 4  2
Primary interface number  [0 ] ? 1  1
WRS Config>li all

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

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


*************************************************************************
*
**** Set Default and first stabilization times
*
*************************************************************************
*
WRS Config>set default firs 30
WRS Config>set def stab 10
WRS Config>li all
WAN Restoral is enabled.
Default Stabilization Time:       10 seconds
Default First Stabilization Time: 30 seconds
[No Primary-Secondary pairs defined ]
                      Alt.     1st  Subseq TOD Revert Back
Primary Interface  Alternate Interface     Enabled  Stab  Stab  Start    Stop
-----------------  ----------------------  -------  ----  ----  -------  -------
 1 - WAN Frame Re   4 - PPP Dial Circuit     No     dflt  dflt  Not Set  Not Set

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

```
*************************************************************************
*
*Configure APPN PORTS and LINKSTATIONS for the
*ALTERNATE and PRIMARY interfaces
*************************************************************************
Config>p appn
APPN user configuration
APPN config>add p  5
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
 (S)DLC, (X)25, (D)LSw, (A)TM, (IP) [  ] ? p
Interface number(Default 0): [0 ] ? 4
Port name (Max 8 characters) [PPP004 ] ?
Enable APPN on this port (Y)es (N)o [Y ] ?
Port Definition
        Service any node: (Y)es (N)o[Y]?
        Limited resource: (Y)es (N)o[N]?
        High performance routing: (Y)es (N)o [Y]?
 Maximum BTU size (768-2044) [2044 ] ?
        Local SAP address (04-EC) [4]?
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.
APPN config>add li  6
APPN Station
Port name for the link station [  ] ? ppp004
Station name (Max 8 characters) [  ] ? toNN6WRR
        Limited resource: (Y)es (N)o[N]?
        Activate link automatically (Y)es (N)o[Y]?
 Adjacent node type: 0 = APPN network node, 1 = APPN end node
2 = LEN end node [0]?
        High performance routing: (Y)es (N)o [Y]?
 Allow CP-CP sessions on this link (Y)es (N)o [Y ] ?
 CP-CP session level security (Y)es (N)o [N ] ?
 Configure CP name of adjacent node: (Y)es (N)o [N ] ?
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.
APPN config>add li   6
APPN Station
Port name for the link station [  ] ? fr001
Station name (Max 8 characters) [  ] ? tonn1pri
        Activate link automatically (Y)es (N)o[Y]?
 DLCI number for link (16-1007) [16 ] ? 121
 Adjacent node type: 0 = APPN network node, 1 = APPN end node
2 = LEN end node [0]?
        High performance routing: (Y)es (N)o [Y]?
 Allow CP-CP sessions on this link (Y)es (N)o [Y ] ?
 CP-CP session level security (Y)es (N)o [N ] ?
 Configure CP name of adjacent node: (Y)es (N)o [N ] ?
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.
```

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

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

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

Inbound destination name       = 2210-22

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

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

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

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

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

Nota:

1 La ruta primaria es la interfaz 1, Frame Relay

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

Configuración de la restauración de la WAN

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

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

Circuit configuration
FR Config>li al

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

Inbound destination name        = 2210-35

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

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

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

```
                                                    Secondary
   Primary Interface       Secondary Interface      Enabled
----------------------  ----------------------  --------
 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 al
NODE:
       NETWORK ID: STFNET
  CONTROL POINT NAME: NN6
       XID: 00000
       APPN ENABLED: YES
       MAX SHARED MEMORY: 4096
       MAX CACHED: 4000
DLUR:
  DLUR ENABLED: YES
  PRIMARY DLUS NAME: NETB.MVSC
 CONNECTION NETWORK:
             CN NAME       LINK TYPE  PORT INTERFACES
  ------------------------------------------------------------
COS:
       COS NAME
  --------
          BATCH
         BATCHSC
         CONNECT
           INTER
         INTERSC
         CPSVCMG
        SNASVCMG
 USRBAT
    USRNOT
 MODE:
   MODE NAME  COS NAME
  ---------------------
    USRBAT      USRBAT
    USRNOT      USRNOT
PORT:
         INTF     PORT      LINK      HPR    SERVICE   PORT
        NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
  ------------------------------------------------------------
      0      TR000   IBMTRNET    YES      YES      YES
**** < This is the port that will get backed up
      1     PPP001        PPP    YES      YES      YES   2
      2         SS       SDLC     NO      YES      YES
      3                  SDLC     NO      YES       NO
      4                   PPP    YES      YES       NO
      5      TR005   IBMTRNET    YES      YES      YES
    254                   DLS     NO      YES       NO
     17     PPP017        PPP    YES      YES      YES
      9     PPP009        PPP    YES      YES      YES

 STATION:
        STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
         NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
  ------------------------------------------------------------
     TONN1    TR000    0004AC4E7505       YES     YES       1
     TONN2    TR000    550020004020       YES     YES       1
     TONN9    TR000    0004AC4E951D       YES     YES       1
     TOPC4    TR000    0004AC9416B4       YES     YES       1
   TOVTAM1    TR000    400000003888       YES     YES       1
**** < this linkstation will get backed up
    TONN35   PPP001    000000000000       YES     YES       0  3
   TO15DOD   PPP009    000000000000       YES      NO       0
LU NAME:
             LU NAME         STATION NAME           CP NAME
  ------------------------------------------------------------
 APPN config>ex
Config>
*logout
Connection closed.
```

Nota:

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

Configuración de V.25bis

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

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



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



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

Address assigned name             Network Address
---------------------             ---------------

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

Base net                      = 0
Destination name              =
Circuit priority              = 8

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

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

```
Circuit config:   3>list all


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

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

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

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

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

Cable type                    = RS-232 DTE

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

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

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

Cable type                    = RS-232 DTE

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

Nota:

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

2 Un valor cero da como resultado un enlace alquilado

Configuración de V.34

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

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

Address assigned name             Network Address
---------------------             ---------------

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

Base net                       = 0
Destination name               =
Circuit priority               = 8

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

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

```
Circuit config:   3>list all


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

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

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

         V.34 System Net Configuration:

Local Network Address Name    = default_address
Local Network Address         = 9999999

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

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

Modem strings:
Initialization string         = at&f&s1l1&d2&c1x3
Speed (bps)                   = 115200

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

         V.34 System Net Configuration:

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

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

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

Modem strings:
Initialization string         = at&f&s1l1&d2&c1x3

Speed (bps)                   = 115200

V.34 System Net Config   2>
```

Notas:

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

2 Un valor cero da como resultado un enlace alquilado

Configuración de APPN sobre ATM

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

Notas:

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

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

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

```
nada205 APPN config>add li atm006 2
APPN Station
Station name (Max 8 characters) [ ]? tograya
WARNING!! You are changing an existing record.
        Limited resource: (Y)es (N)o[N]?
        Activate link automatically (Y)es (N)o[Y]?
        Virtual Channel Type (0 = PVC , 1 = SVC) [0]? 3
        Destination ATM Address  [39999999999999000099990101031689022594l1]?
        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  [39999999999999000099990101031689022594l1]?
        Broadband Bearer Class: 0 = CLASS_A, 1 = CLASS_C, 2 = CLASS_X [2]?
        Best Effort Indicator (Y)es (N)o [N]?
        Forward Traffic Peak Cell Rate (1-16777215) [30000]?
        Forward Traffic Sustained Cell Rate (1-16777215) [20000]?
        Forward Traffic Tagging (Y)es (N)o [Y]?
        Forward Traffic QOS Class: 0 = CLASS_0, 1 = CLASS_1, 2 = CLASS_2,
         3 = CLASS_3, 4 = CLASS_4 [0]?
        Backward Traffic Peak Cell Rate (1-16777215) [30000]?
        Backward Traffic Sustained Cell Rate (1-16777215) [20000]?
        Backward Traffic Tagging (Y)es (N)o [Y]?
        Backward Traffic QOS Class: 0 = CLASS_0, 1 = CLASS_1, 2 = CLASS_2,
         3 = CLASS_3, 4 = CLASS_4 [0]?
        Call out anonymously (Y)es (N)o [N]?
        ATM Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
        Shareable Connection Network Traffic (Y)es (N)o [N]?
        Shareable Other Protocol Traffic (Y)es (N)o [N]?
        Remote SAP(04-EC) [4]?
        Adjacent node type: 0 = APPN network node,
    1 = APPN end node or Unknown node type,
2 = LEN end node [0]?
        TG Number (0-20) [0]?
        Allow CP-CP sessions on this link (Y)es (N)o [Y]?
        CP-CP session level security (Y)es (N)o [N]?
        Configure CP name of adjacent node: (Y)es (N)o [N]?
        LDLC Retry Count(1-255) [3]?
        LDLC Timer Period(1-255 seconds) [1]?
Would you like TG characteristics updated to recommended
values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.


nada205 APPN config>
```

Notas:

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

Configuración de APPN usando SDLC

APPN da soporte a la estaciones de SDLC siguientes:

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

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

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

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

Consulte el manual Software User's Guide para obtener información adicional sobre la configuración de capas de la red SDLC.

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

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

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

Counters:  XID/TEST retry:  8
           SNRM retry:      6
           Poll retry:      10
SDLC 1 Config>ex
Config> CTRL p
* restart
Are you sure you want to restart the gateway? (Yes or [No]): yes

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

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

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

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

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

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

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

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

APPN config>list link tostnc1    **(will show link station definitions)
APPN config>add link sdlc001
APPN Station
Station name (Max 8 characters) [ ]? TOSTNC2
        Activate link automatically (Y)es (N)o[Y]?
 Station address(1-fe) [C2]?
      (Note: C2 must match to the remote secondary station)
 Adjacent node type: 0 = APPN network node, 1 = APPN end node
 2 = LEN end node, 3 = PU 2.0 node [0]?
Edit Dependent LU Server: (Y)es (N)o [N]?
 Allow CP-CP sessions on this link (Y)es (N)o [Y]?
 CP-CP session level security (Y)es (N)o [N]?
 Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>list link tostnc2
**(mostrará definiciones de estaciones de enlace)
APPN config>act
```

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

Nota:

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

Configuración de APPN sobre X.25

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

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

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

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

```
Boats APPN config>list port x25002
PORT:
       Interface number(DLSw = 254): 2
       PORT enable: YES
       Service any node: YES
       Link Type: X25
       MAX BTU size: 2048
       MAX number of Link Stations: 239
       Percent of link stations reserved for incoming calls: 0
       Percent of link stations reserved for outgoing calls: 0
       Cost per connect time: 0
       Cost per byte: 0
       Security:(0 = Nonsecure, 1 = Public Switched Network
          2 = Underground Cable, 3 = Secure Conduit,
          4 = Guarded Conduit, 5 = Encrypted, 6 = Guarded Radiation): 0
       Propagation delay:(0 = Minimum, 1 = Lan, 2 = Telephone,
          3 = Packet Switched Network, 4 = Satellite, 5 = Maximum): 3
       Effective capacity: 45
       First user-defined TG characteristic: 128
       Second user-defined TG characteristic: 128
       Third user-defined TG characteristic: 128
Boats APPN config>list link 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
       --------------------
```

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

X.25 PVC configuration

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

X.25 address translation configuration

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

Configuración de APPN sobre Frame Relay

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

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

Configuración de APPN sobre Frame Relay BAN

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

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

Configuración de TN3270E usando DLUR

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

```
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) [@01LU]?
     LU Type     ( 1 - 3270 mod 2 display
                   2 - 3270 mod 3 display
                   3 - 3270 mod 4 display
                   4 - 3270 mod 5 display) [1]?
     Specify LU Address Range(s) (y/n) [n]
     Number of Implicit LUs in Pool(1-253) [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 (2-254) [0] 2
     Station name (Max 8 characters) []? link1
         Class:
          1 = Explicit Workstation,
          2 = Implicit Workstation,
          3 = Explicit Printer,
          4 = Implicit Printer[3]?
     LU Type ( 5 - 3270 printer
               6 - SCS printer) [5]?
Write this record[Y]?
The record has been written.
TN3270E config>
TN3270E config>list all
TN3270E Server Definitions
TN3270E enabled: YES
TN3270E IP Address: 4.3.2.1
TN3270E Port Number: 23
Keepalive type: NOP          Frequency: 60
Automatic Logoff: N        Timeout: 30
        Enable IP Precedence: N
Link Station: link1
        Local Node ID: 11111
        Auto activate : YES
        Implicit Pool Informationø
                Number of LUs: 50
                LU Mask: @01LU
        LU Name   NAU addr     Class             Assoc LU Name   Assoc  NAU addr

        ---------------------------------------------------------------- --------
        printer1      2       Explicit Printer

TN3270E config>exit
APPN Config>exit
```

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

Routing

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

IP config>
*
```

Configuración de TN3270E usando una conexión de subárea

```
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.
```

```
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) [@01LU]?
     Specify LU Address Range(s) (y/n) [N]
     Number of Implicit LUs in Pool(1-253) [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 (2-254) [2]
     Station name (Max 8 characters) []? suba1
         Class:
          1 = Explicit Workstation,
          2 = Implicit Workstation,
          3 = Explicit Printer,
          4 = Implicit Printer[3]?
          LU Type ( 5 - 3270 printer
                    6 - SCS printer) [5]?
Write this record[Y]?
The record has been written.
TN3270E config>
TN3270E config>list all
TN3270E Server Definitions
TN3270E enabled: YES
TN3270E IP Address: 4.3.2.1
TN3270E Port Number: 23
Keepalive type: NOP          Frequency: 60
Automatic Logoff: N        Timeout: 30
        Enable IP Precedence: N
Link Station: suba1
        Local Node ID: 12345
        Auto activate : YES
        Implicit Pool Informationø
                Number of LUs: 50
                LU Mask: @01LU
        LU Name   NAU addr     Class             Assoc LU Name   Assoc  NAU addr

        ------------------------------------------------------------ --------
        printer1      2       Explicit Printer

TN3270E config>exit
APPN Config>exit


APPN config>act
```

Configuración del soporte de Enterprise Extender para HPR sobre IP

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

Configuración de redes de conexiones sobre HPR sobre IP

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

Configuración de un Extended Border Node

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

```
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.
```

Configuración y supervisión de APPN

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

- "Resumen de los mandatos de configuración de APPN"
- "Información detallada sobre los mandatos de configuración de APPN" en la página 105

Acceso al proceso de configuración de APPN

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

1. En el indicador *, entre **talk 6**. Se visualizará el indicador `Config>`.

   (Si no se visualiza, pulse de nuevo **Intro**).

2. Entre **protocol appn**. Aparecerá el indicador `APPN Config>`.
3. Entre un mandato de configuración de APPN.

Resumen de los mandatos de configuración de APPN

Tabla 4 (Página 1 de 2). Resumen de los mandatos de configuración de APPN

Mandato	Función	Consulte página:
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxv.	
Enable/Disable	Activa/desactiva:	105
	APPN	
	Dependent LU Requestor	
	Port *nombre del puerto*	
Set	Establece los elementos siguientes:	
	Node	105
	Traces	120
	HPR	110
	DLUR	113
	Management	136
	Tuning	117
Add	Añade o actualiza los elementos siguientes:	
	Port *nombre del puerto*	139
	Link-station *nombre de la estación de enlace*	159

Tabla 4 (Página 2 de 2). Resumen de los mandatos de configuración de APPN

Mandato	Función	Consulte página:
	LU-Name *Nombre LU*	178
	Connection-network *nombre de la red de conexiones*	179
	Additional-port-to-connection-network	188
	Mode	187
	Focal_point	189
	local-pu	189
	Routing_list	191
	COS_mapping_table	194
Delete	Suprime los elementos siguientes: • Port *nombre del puerto* • Link-station *nombre de la estación de enlace* • LU-Name *Nombre LU* • Connection-network *nombre de la red de conexiones* • Connection networks port interface (CN PORTIF) *nombre CN* • Mode *nombre modalidad* • Focal_point • local-pu • Routing_list • COS_mapping_table	196
List	Lista los elementos siguientes de la memoria de configuración: • All • Node • Traces • Management • HPR • DLUR • Port *nombre del puerto* • Link-station *nombre del enlace* • LU-Name *Nombre LU* • Mode *nombre modalidad* • Connection-network *nombre de la red de conexiones* • Focal_point • Routing_list • COS_mapping_table	196
Activate_new_config	Lee la configuración en memoria de configuración no volátil.	196
TN3270	Da acceso al indicador de mandatos `TN320E config>`	197
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxvi.	

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

Información detallada sobre los mandatos de configuración de APPN

Enable/Disable

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

Sintaxis:

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

Set

Use el mandato **set** para establecer:

Sintaxis:

set	node

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

Tabla 5 (Página 1 de 6). Lista de parámetros de configuración - Direccionamiento de APPN

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

Tabla 5 (Página 2 de 6). Lista de parámetros de configuración - Direccionamiento de APPN

Información de los parámetros
Parámetro Network ID (obligatorio) **Valores válidos** Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 **Nota:** Se sigue dando soporte a un identificador de una red existente, en la que el nodo de red del direccionador va a entrar como miembro, y que usa los caracteres especiales @, $ y # del juego de caracteres A; no obstante, dichos caracteres no deben usarse en los ID de red nuevos. **Valor por omisión** Ninguno **Descripción** Este parámetro especifica el nombre de la red APPN a la que pertenece este nodo de red. El ID de red debe ser el mismo para todos los nodos de la red APPN. Los nodos finales APPN y los nodos finales LEN conectados pueden tener ID de red diferentes.
Parámetro Control point name (obligatorio) **Valores válidos** Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 **Nota:** Sigue dándose soporte a nombres de CP ya existentes que adquiera este nodo y que en su nombre tengan los caracteres especiales @, $ y # del juego de caracteres A; no obstante, no deberán usarse estos caracteres en los nombres de CP nuevos. **Valor por omisión** Ninguno **Descripción** Este parámetro especifica el nombre del CP para este nodo de red APPN. El CP es responsable de la gestión del nodo de red APPN y de sus recursos. El nombre del CP es el nombre lógico del nodo de red APPN de la red. Este nombre debe ser único dentro de la red APPN y debe identificarse mediante el parámetro Network ID.
Parámetro Enable branch extender or border node **Valores válidos** 0 (no habilitar ninguno) 1 (habilitar branch extender) 2 (habilitar border node) **Valor por omisión** 0 **Descripción** Este parámetro especifica si la función de branch extender o la de border node o ninguna de las dos se habilitará en el nodo. Si habilita alguna de estas dos funciones, se harán las preguntas adicionales apropiadas.

Tabla 5 (Página 3 de 6). Lista de parámetros de configuración - Direccionamiento de APPN

Información de los parámetros
Parámetro Permit search for unregistered LUs **Valores válidos** Yes o No **Valor por omisión** No **Descripción** Este parámetro especifica si pueden efectuarse búsquedas de LU en este nodo (cuando actúa como nodo final) si las LU no se registraron en el servidor de nodos de red de Branch Extender. Si especificó *yes*, se pueden buscar LU en este nodo. **Nota:** Esta pregunta sólo se efectúa si el parámetro **Enable Branch Extender or Border Node** está en *branch extender*.
Parámetro Subnet visit count **Valores válidos** De 1 a 255 **Valor por omisión** 3 **Descripción** Especifica el valor por omisión del nivel de nodo para el número máximo de subredes que puede atravesar una sesión de varias subredes. El valor por omisión puede alterarse temporalmente como parte de la configuración de una lista de direccionamientos, enlaces o puertos. **Nota:** Esta es la primera de una serie de preguntas que se hacen sólo si se ha habilitado border node.
Parámetro Cache searches for (0-255) minutes **Valores válidos** De 0 a 255 **Valor por omisión** 8 **Descripción** Especifica cuántos minutos retiene el BN información en la antememoria de búsqueda de varias subredes una vez finalizada ésta.
Parámetro Maximum number of searches in cache **Valores válidos** De 0 a 32765 (0=ilimitado) **Valor por omisión** 0 **Descripción** Especifica el número máximo de entradas en la antememoria de búsqueda de varias redes. Una vez alcanzado el límite, se descartarán las entradas más antiguas. **Nota:** El mecanismo primario de supresión de estas entradas es el valor del tiempo de búsqueda en antememoria especificado en **cache searches for (0–255) minutes**.

Tabla 5 (Página 4 de 6). Lista de parámetros de configuración - Direccionamiento de APPN

Información de los parámetros
Parámetro Dynamic routing list updates **Valores válidos** 0 (ninguna) - No se añaden entradas dinámicas. 1 (completa) - Se añaden todos los nodos de límite nativos, todos los nodos de red y de límite no nativos adyacentes y los nodos que saben LU de destino con nombres similares. 2 (limitada) - Se añaden todos los nodos de límite nativos, todos los nodos de red y los de límite no nativos adyacentes ***con el mismo IDRED*** y los nodos que saben LU de destino con nombres similares. **Valor por omisión** 2 **Descripción** Indica el grado, si hay alguno, hasta el que un BN puede añadir a los datos de la lista de direccionamientos configurada, datos topológicos aprendidos por el código operativo. Estos datos adicionales no se guardan en SRAM.
Parámetro Enable routing list optimization **Valores válidos** Yes o No **Valor por omisión** Yes **Descripción** Indica si un BN puede volver a ordenar o no la copia temporal de una lista de direccionamientos de subred del código operativo, para que las entradas que tengan más posibilidades de éxito se encuentren primero. **Nota:** Esta es la última de una serie de preguntas que se hacen sólo si se ha activado border node.
Parámetro Route addition resistance **Valores válidos** De 0 a 255 **Valor por omisión** 128 **Descripción** Este parámetro indica el deseo de direccionar a través de este nodo. Se usa en el cálculo de la ruta basado en la clase de servicio. Los valores inferiores indican mayores niveles de deseabilidad.
Parámetro XID number for subarea connection (consulte las notas de la tabla) **Valores válidos** Una serie de 5 dígitos hexadecimales **Valor por omisión** X'00000' **Descripción** Este parámetro especifica un número de ID único (identificador) para el nodo de red. El número de XID se combina con un número de bloque de ID (que identifica un producto de IBM específico) para formar una identificación de nodo XID. Las identificaciones de nodo se intercambian entre nodos adyacentes cuando éstos están estableciendo una conexión. El nodo de red del direccionador añade automáticamente un número de bloque de ID a este parámetro durante el intercambio de XID para crear una identificación de nodo XID. El número de ID que asigne a este nodo debe ser único dentro del nodo APPN identificado por el parámetro Network ID. Póngase en contacto con el administrador de red para verificar que el número de ID sea único.

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

Información de los parámetros
Nota: Por lo general, las identificaciones de nodo se intercambian entre nodos T2.1 durante el establecimiento de la sesión de CP-CP. Si el nodo de red está comunicando con el producto IBM Virtual Telecommunications Access Method (VTAM) a través del nodo LEN T2.1 y éste tiene definido para él un nombre de CP, el parámetro de número XID no será necesario. Si el nodo LEN adyacente no es T2.1 o no tiene un nombre de CP definido explícitamente, el parámetro de número de XID deberá especificarse para establecer una conexión con el nodo LEN. Las versiones de VTAM anteriores a la versión 3 release 2 no permiten definir nombres de CP para los nodos LEN.
Parámetro Use enhanced BATCH COS **Valores válidos** Yes o No **Valor por omisión** Yes **Descripción** Este parámetro especifica si deben utilizarse tablas de COS mejoradas. Estas tablas asignan pesos razonables a TG de ATM basándose en el coste, velocidad y retardo. Para ATM, el orden de preferencia es: • Campus Best Effort (SVC o PVC)/Reserved PVC (WAN o Campus) • Campus Reserved SVC • WAN Best Effort (SVC o PVC) • WAN Reserved SVC
Parámetro Use enhanced BATCHSC COS **Valores válidos** Yes o No **Valor por omisión** Yes **Descripción** Este parámetro especifica si deben utilizarse tablas de COS mejoradas. Estas tablas asignan pesos razonables a TG de ATM basándose en el coste, velocidad y retardo. Para ATM, el orden de preferencia es: • Campus Best Effort (SVC o PVC)/Reserved PVC (WAN o Campus) • Campus Reserved SVC • WAN Best Effort (SVC o PVC) • WAN Reserved SVC
Parámetro Use enhanced INTER COS **Valores válidos** Yes o No **Valor por omisión** Yes **Descripción** Este parámetro especifica si deben utilizarse tablas de COS mejoradas. Estas tablas asignan pesos razonables a TG de ATM basándose en el coste, velocidad y retardo. Para ATM, el orden de preferencia es: • Campus Reserved (SVC o PVC) • Campus Best Effort (SVC o PVC)/WAN reserved PVC • WAN Reserved SVC • WAN Best Effort (SVC o PVC)

Tabla 5 (Página 6 de 6). Lista de parámetros de configuración - Direccionamiento de APPN
Información de los parámetros
Parámetro Use enhanced INTERSC COS **Valores válidos** Yes o No **Valor por omisión** Yes **Descripción** Este parámetro especifica si deben utilizarse tablas de COS mejoradas. Estas tablas asignan pesos razonables a TG de ATM basándose en el coste, velocidad y retardo. Para ATM, el orden de preferencia es: • Campus Reserved (SVC o PVC) • Campus Best Effort (SVC o PVC)/WAN reserved PVC • WAN Reserved SVC • WAN Best Effort (SVC o PVC)

Sintaxis:

set high-performance routing

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

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

Tabla 7 (Página 1 de 4). Lista de parámetros de configuración - Temporizador de HPR y opciones de reintento
Información de los parámetros
Tráfico con prioridad de transmisión baja

Tabla 7 (Página 2 de 4). Lista de parámetros de configuración - Temporizador de HPR y opciones de reintento

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

Tabla 7 (Página 3 de 4). Lista de parámetros de configuración - Temporizador de HPR y opciones de reintento

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

Tabla 7 (Página 4 de 4). Lista de parámetros de configuración - Temporizador de HPR y opciones de reintento	
Información de los parámetros	
Parámetro	Maximum RTP retries
Valores válidos	De 0 a 10
Valor por omisión	6
Descripción	Este parámetro especifica el número máximo de reintentos antes de que RTP inicie una conmutación de vías de acceso en una conexión HPR que tenga tráfico con prioridad de transmisión de red.
Parámetro	Path switch timer
Valores válidos	De 0 a 7200 segundos
Valor por omisión	180 segundos
Descripción	Este parámetro especifica el tiempo máximo que puede intentarse una conmutación de vías de acceso en una conexión HPR que tenga tráfico con prioridad de transmisión de red. Un valor de cero indica que la función de conmutación de vías de acceso está inhabilitada y que no se realizará la mencionada conmutación.

Sintaxis:

set dlur

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

Tabla 8 (Página 1 de 4). Lista de parámetros de configuración - Peticionario de LU dependientes	
Información de los parámetros	
Parámetro	Enable dependent LU requester (DLUR) on this network node
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro especifica si un peticionario de LU dependientes se habilitará funcionalmente en este nodo.

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

Información de los parámetros	
Parámetro	Default fully-qualified CP name of primary DLUS (obligatorio cuando el DLUR está habilitado)
Valores válidos	Una serie con un máximo de 17 caracteres presentados en forma de *IDred.nombreCP*, donde: • *IDred* es un ID de red de 1 a 8 caracteres • *nombreCP* es un nombre de CP que tiene entre 1 y 8 caracteres Cada nombre debe respetar las normas siguientes: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 **Nota:** Sigue dándose soporte a nombres de CP plenamente calificados que usan los caracteres especiales @, $ y # del juego de caracteres A; no obstante, estos caracteres no deben usarse en los nombres de CP nuevos.
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre del punto de control (CP) plenamente calificado del servidor de LU dependientes (DLUS) que se usa por omisión. El servidor primario por omisión puede alterarse temporalmente en estaciones de trabajo. Este servidor se usa para las solicitudes de entrada de las PU de comunicación de sentido directo cuando no se ha especificado un DLUS primario para la estación de enlace asociada.
Parámetro	Default fully-qualified CP name of backup dependent LU server (DLUS)
Valores válidos	Una serie con un máximo de 17 caracteres presentados en forma de *IDred.nombreCP*, donde: • *IDred* es un ID de red de 1 a 8 caracteres • *nombreCP* es un nombre de CP que tiene entre 1 y 8 caracteres Cada nombre debe respetar las normas siguientes: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 **Nota:** Sigue dándose soporte a nombres de CP plenamente calificados que usan los caracteres especiales @, $ y # del juego de caracteres A; no obstante, estos caracteres no deben usarse en los nombres de CP nuevos.
Valor por omisión	Nulo
Descripción	Este parámetro especifica el nombre del punto de control (CP) plenamente calificado del servidor de LU dependientes (DLUS) que se usa como elemento de seguridad por omisión. No se necesita un elemento de seguridad y el valor nulo (que representa la ausencia de entradas) indica la ausencia de un servidor de seguridad por omisión. El servidor de seguridad por omisión puede alterarse temporalmente en estaciones de trabajo.

Tabla 8 (Página 3 de 4). Lista de parámetros de configuración - Peticionario de LU dependientes

Información de los parámetros	
Parámetro	Perform retries to restore disrupted pipe
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro especifica si el DLUR intentará restablecer el conducto en un DLUS después de un fallo de éste. Si el DLUR recibe un UNBIND de no interrupción y este parámetro está en No, el DLUR esperará indefinidamente a que un DLUS restablezca el conducto roto. Si el conducto falla por cualquier otra razón y este parámetro está en No, el DLUR intentará alcanzar el DLUS primario una vez. Si no lo consigue, intentará alcanzar el DLUS de seguridad. Si este intento también falla, el DLUR esperará indefinidamente a que un DLUS restablezca el conducto. Consulte "Algoritmo de reintento del DLUR" en la página 50 para obtener una descripción del algoritmo de reintento.
Parámetro	Delay before initiating retries
Valores válidos	De 0 a 2 756 000 segundos
Valor por omisión	120 segundos
Descripción	Este parámetro especifica el tiempo necesario para dos casos diferentes en caso de que se rompa el conducto entre el DLUR y el DLUS. • En caso de recibir un UNBIND de no interrupción: Este parámetro especifica el tiempo que debe esperar el DLUR antes de intentar alcanzar el DLUS primario. Un valor de 0 indica que el DLUR efectúa un reintento inmediato. • En el resto de los casos de fallo del conducto: El DLUR intentará el DLUS primario e, inmediatamente después, el DLUS de seguridad. Si falla, el DLUR esperará el tiempo especificado por el mínimo de *short retry timer* y el presente parámetro antes de intentar alcanzar el DLUS primario. Consulte "Algoritmo de reintento del DLUR" en la página 50 para obtener una descripción completa del algoritmo de reintento.
Parámetro	Perform short retries to restore disrupted pipe
Valores válidos	Yes, No
Valor por omisión	Si *Perform retries to restore disrupted pipes* está en Yes, el valor por omisión será Yes. De lo contrario, dicho valor será No.
Descripción	Consulte "Algoritmo de reintento del DLUR" en la página 50 para obtener una descripción completa del algoritmo de reintento.

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

Información de los parámetros	
Parámetro	Short retry timer
Valores válidos	De 0 a 2 756 000 segundos
Valor por omisión	120 segundos
Descripción	En todos los casos de fallo del conducto que no sean un UNBIND de no interrupción, el tiempo mínimo de *Delay before initiating retries* y el presente parámetro especificarán el tiempo que esperará el DLUR antes de intentar alcanzar el DLUS primario después de que haya fallado un intento de establecer esta conexión. Consulte “Algoritmo de reintento del DLUR” en la página 50 para obtener una descripción completa del algoritmo de reintento.
Parámetro	Short retry count
Valores válidos	De 0 a 65535
Valor por omisión	5
Descripción	En todos los casos de fallo del conducto que no sean un UNBIND de no interrupción, este parámetro especifica cuantas veces el DLUR intentará realizar reintentos cortos para alcanzar el DLUS después de que haya fallado un intento de establecer esta conexión. Consulte “Algoritmo de reintento del DLUR” en la página 50 para obtener una descripción completa del algoritmo de reintento.
Parámetro	Perform long retries to restore disrupted pipe
Valores válidos	Yes, No
Valor por omisión	Si *Perform retries to restore disrupted pipes* está en Yes, el valor por omisión será Yes. De lo contrario, dicho valor será No.
Descripción	Consulte “Algoritmo de reintento del DLUR” en la página 50 para obtener una descripción completa del algoritmo de reintento.
Parámetro	Long retry timer
Valores válidos	De 0 a 2 756 000 segundos
Valor por omisión	300 segundos
Descripción	Este parámetro especifica el tiempo que esperará el DLUR cuando efectúe reintentos largos. Consulte “Algoritmo de reintento del DLUR” en la página 50 para obtener una descripción completa del algoritmo de reintento.

Sintaxis:

set tuning

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

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

Tabla 9 (Página 1 de 4). Lista de parámetros de configuración - Ajuste del nodo APPN

Información de los parámetros	
Parámetro	Maximum number of adjacent nodes
Valores válidos	De 1 a 2800
Valor por omisión	100
Descripción	Este parámetro es un cálculo del número máximo de nodos que espera que sean adyacentes de forma lógica a este nodo de red de direccionador en cualquier momento. El algoritmo de ajuste automático usa este parámetro junto con el parámetro *Maximum number of ISR sessions* (Número máximo de sesiones de ISR) para calcular los valores de los parámetros *Maximum shared memory* (Memoria compartida máxima) y *Maximum cached directory entries* (Número máximo de entradas en el directorio de antememoria). Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro	Maximum number of network nodes sharing the same APPN network id
Valores válidos	De 10 a 8000
Valor por omisión	50
Descripción	Este parámetro es un cálculo del número máximo de nodos que espera en la subred (es decir, en la topología conocida por este nodo). Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro	Maximum number of TGs connecting network nodes with the same APPN network id
Valores válidos	De 9 a 64000
Valor por omisión	El valor de *maximum number of network nodes in the subnetwork* (número máximo de nodos de red en la subred) multiplicado por 3.
Descripción	Este parámetro es un cálculo del número máximo de TG que conectan los nodos de red en la subred (es decir, en la topología conocida por este nodo). Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro	Maximum number of ISR sessions
Valores válidos	De 10 a 7500
Valor por omisión	200
Descripción	Este parámetro especifica un cálculo del número máximo de sesiones de direccionamiento de sesiones intermedias (ISR) al que se espera que dé soporte este nodo de red del direccionador en cualquier momento. El algoritmo de ajuste automático usa este parámetro junto con el del número máximo de nodos adyacentes para calcular los valores de los parámetros de ajuste del número máximo de entradas de directorio en antememoria y el máximo de memoria compartida. Este parámetro sólo se puede configurar con el Configuration Program.

Tabla 9 (Página 2 de 4). Lista de parámetros de configuración - Ajuste del nodo APPN

Información de los parámetros
Parámetro Percent of adjacent nodes with CP-CP sessions using HPR **Valores válidos** De 0 a 100% **Valor por omisión** 0 (ninguna) **Descripción** Este parámetro especifica un cálculo del número máximo de EN y NN adyacentes con sesiones de CP-CP que usan el conjunto de opciones 1402 (flujos de control sobre el conjunto de opciones RTP). Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro Maximum percent of ISR sessions using HPR data connections **Valores válidos** Del 0 al 100 por ciento **Valor por omisión** 0 por ciento **Descripción** Este parámetro especifica el porcentaje más elevado de sesiones de ISR que usan correlaciones de ISR a HPR. Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro Percent adjacent nodes that function as DLUR PU nodes **Valores válidos** Del 0 al 100 por ciento **Valor por omisión** 0 por ciento **Descripción** Este parámetro especifica el porcentaje más elevado de nodos adyacentes permitido para funcionar como nodos adyacentes DLUR PU. Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro Maximum percent ISR sessions used by DLUR LUs **Valores válidos** Del 0 al 100 por ciento **Valor por omisión** 0 por ciento **Descripción** Este parámetro especifica el porcentaje más elevado de sesiones de ISR que usan las DLUR LU. Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro Maximum number of ISR accounting memory buffers **Valores válidos** 0 ó 1 **Valor por omisión** 0 (el valor por omisión es 1 si se activa la contabilidad de sesión ISR) **Descripción** Este parámetro especifica el número máximo de almacenamientos intermedios que se reservarán para la contabilidad de sesiones de ISR. Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro Maximum memory records per ISR accounting buffer **Valores válidos** De 0 a 2000 **Valor por omisión** 100 **Descripción** Este parámetro especifica el número máximo de registros en memoria por almacenamiento intermedio de contabilidad de ISR. Este parámetro sólo se puede configurar con el Configuration Program.

Tabla 9 (Página 3 de 4). Lista de parámetros de configuración - Ajuste del nodo APPN

Información de los parámetros	
Parámetro	Override tuning algorithm
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Cuando se habilita, este parámetro altera temporalmente los cálculos de ajuste generados por la línea de mandatos y le habilita para especificar valores explícitos para el parámetro Maximum shared memory y el de Maximum cached directory entries. Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro	Number of local-pus for TN3270E support
Valores válidos	
Valor por omisión	
Descripción	Este parámetro especifica el número de PU locales disponibles para el soporte de TN3270. Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro	Total number of LUs for TN3270E
Valores válidos	
Valor por omisión	
Descripción	Este parámetro especifica el número total de LU disponible para el soporte de TN3270E. Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro	Maximum shared memory
Valores válidos	De 0 a 5108 KB
Valor por omisión	5108 KB
Descripción	Este parámetro especifica la cantidad de memoria compartida dentro del direccionador asignada al nodo de red APPN. APPN usa la asignación de memoria compartida para realizar operaciones de red y para mantener las tablas y directorios necesarios. Puede permitir que APPN tenga un tamaño RU de 4K estableciendo *percent of APPN shared memory used for buffers* en un valor lo suficientemente grande como para permitir, como mínimo, 1 megabyte de memoria disponible para el gestor del almacenamiento intermedio. Este parámetro sólo se puede configurar con el Configuration Program y desde **talk 6**

Tabla 9 (Página 4 de 4). Lista de parámetros de configuración - Ajuste del nodo APPN

Información de los parámetros	
Parámetro	Percent of APPN shared memory to be used for buffers
Valores válidos	De 10 a 50
Valor por omisión	10% o 512 Kilobytes, según cuál sea más grande.
Descripción	Este parámetro especifica la cantidad de memoria compartida que usará APPN para los almacenamientos intermedios. Puede permitir que APPN tenga un tamaño RU de 4K estableciendo *maximum shared memory* en un mínimo de 1 megabyte y *percent of APPN shared memory used for buffers* en un valor lo suficientemente grande como para permitir que haya un mínimo de 1 megabyte de memoria disponible para el gestor de almacenamientos intermedios. Este parámetro sólo se puede configurar con el Configuration Program y desde **talk 6**
Parámetro	Maximum cached directory entries
Valores válidos	De 0 a 65535
Valor por omisión	4000
Descripción	Este parámetro especifica el número de entradas de directorio que el nodo de red del direccionador almacenará o pondrá en antememoria. Si una entrada de directorio de un nodo se pone en antememoria, el direccionador no necesitará difundir una solicitud de búsqueda para localizarlo. Esto reduce el tiempo necesario para iniciar sesiones con el nodo. Este parámetro sólo se puede configurar con el Configuration Program y desde **talk 6**

Sintaxis:

set traces

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

Tabla 10 (Página 1 de 2). Lista de parámetros de configuración - Preguntas de configuración de los rastreos

Información de los parámetros	
Parámetro	Turn all trace flags off
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita los distintivos de rastreo.

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

Información de los parámetros	
Parámetro	Edit Node-Level Traces
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Consulte la Tabla 11 en la página 121 para saber cuáles serán las preguntas que se le harán si habilita esta opción.
Parámetro	Edit Interprocess Signals
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Consulte la Tabla 12 en la página 125 para saber cuáles serán las preguntas que se le harán si habilita esta opción.
Parámetro	Edit Module Entry and Exit
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Consulte la Tabla 13 en la página 129 para saber cuáles serán las preguntas que se le harán si habilita esta opción.
Parámetro	Edit General
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Consulte la Tabla 14 en la página 130 para saber cuáles serán las preguntas que se le harán si habilita esta opción.

Tabla 11 (Página 1 de 5). Lista de parámetros de configuración - Rastreos de nivel de nodo

Información de los parámetros	
Parámetro	Process management
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de los procesos de gestión dentro del nodo de red APPN, incluyendo la creación y terminación de procesos, los procesos que entran en un estado de espera y el envío de procesos.

Tabla 11 (Página 2 de 5). Lista de parámetros de configuración - Rastreos de nivel de nodo

Información de los parámetros	
Parámetro	Process to process communication
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de los mensajes intercambiados entre procesos dentro del nodo de red APPN, incluyendo la puesta en cola y recepción de dichos mensajes.
Parámetro	Locking
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de los bloqueos obtenidos y liberados en procesos del nodo de red APPN.
Parámetro	Miscellaneous tower activities
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de actividades varias dentro del nodo de red APPN.
Parámetro	I/O to and from the system
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca del flujo de mensajes que entra y sale del nodo de red APPN.
Parámetro	Storage management
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de la memoria compartida obtenida y liberada por el nodo de red APPN.

Tabla 11 (Página 3 de 5). Lista de parámetros de configuración - Rastreos de nivel de nodo

Información de los parámetros	
Parámetro	Queue data type management
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de todas las llamadas del nodo de red APPN que gestionan colas de objetivo general.
Parámetro	Table data type management
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de todas las llamadas del nodo de red APPN que gestionan tablas de objetivo general, incluyendo llamadas para añadir entradas de tabla y llamadas para consultar tablas para entradas específicas.
Parámetro	Buffer management
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de los almacenamientos intermedios del nodo de red APPN que se obtuvieron y liberaron.
Parámetro	Configuration control
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de las actividades del componente de control de la configuración del nodo de red APPN. Este componente gestiona información sobre los recursos de nodo.
Parámetro	Timer service
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de las solicitudes de servicio del temporizador desde el nodo de red APPN.

Tabla 11 (Página 4 de 5). Lista de parámetros de configuración - Rastreos de nivel de nodo

Información de los parámetros	
Parámetro	Service provider management
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de la definición y habilitación o inhabilitación de servicios dentro del nodo de red APPN.
Parámetro	Inter-process message segmenting
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de la transferencia y liberación de almacenamientos intermedios de mensajes en cadena dentro del nodo de red APPN.
Parámetro	Control of processes outside scope of this tower
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de la definición y activación de procesos externos al nodo de red APPN como cuando el recurso de operador del nodo (NOF) define el control de la configuración de procesos externos.
Parámetro	Monitoring existence of processes, services, towers
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de las solicitudes que inician o detienen la supervisión de procesos o servicios dentro del nodo de red APPN.
Parámetro	Distributed environment control
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de las solicitudes dentro del nodo de red APPN que definen subsistemas y crean entornos.

Tabla 11 (Página 5 de 5). Lista de parámetros de configuración - Rastreos de nivel de nodo

Información de los parámetros
Parámetro Process to service dialogs **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de todas las llamadas del nodo de red APPN que abren, cierran o envían datos en un diálogo.
Parámetro AVL Tree Support **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de todas las llamadas que gestionan árboles AVL.

Tabla 12 (Página 1 de 4). Lista de parámetros de configuración - Rastreos de señales entre procesos

Información de los parámetros
Parámetro Address space manager **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente del gestor de espacios de direcciones.
Parámetro Attach manager **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente del gestor de conexiones.
Parámetro Configuration services **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de servicios de configuración.

Tabla 12 (Página 2 de 4). Lista de parámetros de configuración - Rastreos de señales entre procesos

Información de los parámetros
Parámetro Dependent LU requester **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de peticionario de LU dependientes.
Parámetro Directory services **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de servicios de directorio.
Parámetro Half Session **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de semisesión.
Parámetro HPR Path Control **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de control de la vía de acceso HPR.
Parámetro LUA RUI **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente LUA RUI.

Tabla 12 (Página 3 de 4). Lista de parámetros de configuración - Rastreos de señales entre procesos

Información de los parámetros	
Parámetro	Management Services
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de servicios de gestión.
Parámetro	Node Operator Facility
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de recurso del operador de nodo.
Parámetro	Path Control
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de control de las vías de acceso.
Parámetro	Presentation Services
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de servicios de presentación.
Parámetro	Resource manager
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de gestor de recursos.

Tabla 12 (Página 4 de 4). Lista de parámetros de configuración - Rastreos de señales entre procesos

Información de los parámetros
Parámetro Session connector manager **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del gestor del conector de sesiones.
Parámetro Session connector **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del conector de sesiones.
Parámetro Session manager **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del gestor de sesiones.
Parámetro Session services **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente del gestor de servicios de sesión.
Parámetro Topology and routing services **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, de los servicios de topología y direccionamiento.

Tabla 13 (Página 1 de 2). Lista de parámetros de configuración - Rastreos de la entrada y salida en módulos

Información de los parámetros
Parámetro Attach manager **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de la entrada y salida en módulos del gestor de conexiones.
Parámetro Half session **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, el parámetro indica al recurso de rastreo que incluya datos de rastreo de la entrada y salida en módulos del componente de semisesión.
Parámetro LUA RUI **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de entrada y salida en módulos del componente LUA RUI.
Parámetro Node operator facility **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, el parámetro indica al recurso de rastreo que incluya datos de rastreo de entrada y salida en módulos del recurso del operador de nodos.
Parámetro Presentation services **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, el parámetro indica al recurso de rastreo que incluya datos de rastreo de la entrada y salida en módulos de los servicios de presentación.

Tabla 13 (Página 2 de 2). Lista de parámetros de configuración - Rastreos de la entrada y salida en módulos

Información de los parámetros
Parámetro Rapid transport protocol **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, el parámetro indica al recurso de rastreo que incluya datos de rastreo de la entrada y salida en módulos del componente de protocolo de transporte rápido.
Parámetro Resource manager **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de la entrada y salida en módulos del gestor de recursos.
Parámetro Session manager **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de la entrada y salida en módulos del gestor de sesiones.

Tabla 14 (Página 1 de 5). Lista de parámetros de configuración - Rastreos de nivel de componentes generales

Información de los parámetros
Parámetro Accounting services **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general de los servicios de contabilidad.
Parámetro Address space manager **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del gestor de espacios de direcciones.

Tabla 14 (Página 2 de 5). Lista de parámetros de configuración - Rastreos de nivel de componentes generales

Información de los parámetros
Parámetro Architected transaction programs **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del componente de los programas de transacciones arquitecturadas.
Parámetro Configuration services **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general de los servicios de configuración.
Parámetro Dependent LU requester **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del peticionario de LU dependientes.
Parámetro Directory services **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general de los servicios de directorio.
Parámetro HPR path control **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del control de vías de acceso HPR.

Tabla 14 (Página 3 de 5). Lista de parámetros de configuración - Rastreos de nivel de componentes generales

Información de los parámetros
Parámetro LUA RUI **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del componente LUA RUI.
Parámetro Management services **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general de los servicios de gestión.
Parámetro Node operator facility **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del recurso del operador de nodo.
Parámetro Path control **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del control de vías de acceso.
Parámetro Problem determination services **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del componente de determinación de problemas.

Tabla 14 (Página 4 de 5). Lista de parámetros de configuración - Rastreos de nivel de componentes generales

Información de los parámetros
Parámetro Rapid transport protocol **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del control del transporte rápido.
Parámetro Session connector manager **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del gestor del conector de sesiones.
Parámetro Session connector **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del conector de sesiones.
Parámetro Session services **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general de los servicios de sesión.
Parámetro SNMP subagent **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del subagente SNMP.

Tabla 14 (Página 5 de 5). Lista de parámetros de configuración - Rastreos de nivel de componentes generales

Información de los parámetros	
Parámetro	TN3270E Server
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del servidor de TN3270E.
Parámetro	Topology and routing services
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general de los servicios de topología y direccionamiento.

Tabla 15 (Página 1 de 2). Lista de parámetros de configuración - Rastreos varios

Información de los parámetros	
Parámetro	Data link control transmissions and receptions
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Si se habilita este parámetro, el recurso de rastreo de APPN rastreará todos los XID y PIU que el nodo APPN transmita y reciba.
Parámetro	Filter the Data
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Si se activa este parámetro, el recurso de rastreo de APPN filtrará los datos de rastreo según la forma en que responda a las preguntas siguientes.
Parámetro	Truncate the data
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Si se activa este parámetro, el recurso de rastreo de APPN truncará los datos de rastreo. Se le solicitará que especifique la *length to trace* (longitud a rastrear)
Parámetro	Length to trace
Valores válidos	De 1 a 3600
Valor por omisión	100
Descripción	Este parámetro especifica el número de bytes de datos de rastreo a acumular.

Tabla 15 (Página 2 de 2). Lista de parámetros de configuración - Rastreos varios

Información de los parámetros
Parámetro Trace Locates **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Si se activa este parámetro, el recurso de rastreo de APPN rastreará las localizaciones.
Parámetro Trace TDU **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Si se activa este parámetro, el recurso de rastreo de APPN rastreará las actualizaciones de datos topológicos.
Parámetro Trace route setups **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Si se activa este parámetro, el recurso de rastreo de APPN rastreará las configuraciones de ruta.
Parámetro Trace CP Capabilities **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Si se activa este parámetro, el recurso de rastreo de APPN rastreará las posibilidades de rastreo del CP.
Parámetro Trace Session Control **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Si se activa este parámetro, el recurso de rastreo de APPN rastreará el tráfico de control de sesiones.
Parámetro Trace XID **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Si se activa este parámetro, el recurso de rastreo de APPN rastreará los XID.

Sintaxis:

set management

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

Tabla 16 (Página 1 de 2). Lista de parámetros de configuración - Gestión de nodos APPN

Información de los parámetros	
Parámetro	Collect intermediate session information
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro especifica si el nodo APPN debe reunir datos sobre las sesiones intermedias que pasan por el nodo (contadores de sesión y características de sesión). Los datos se capturan en variables SNMP MIB para APPN.
Parámetro	Save RSCV information for intermediate sessions
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro especifica si el nodo APPN debe guardar el vector de control de selección de ruta (RSCV) para una sesión intermedia. Los datos se capturan en una variable asociada SNMP MIB para APPN. El RSCV de sesión se transporta en la solicitud BIND usada para activar una sesión entre dos LU. Describe la ruta óptima a través de una red APPN de una sesión LU-LU determinada. El RSCV de sesión contiene los nombres de CP y TG asociados con cada par de nodos adyacentes situados a lo largo de una ruta que va de un nodo de origen a uno de destino.
Parámetro	Create intermediate session records
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita la creación de registros de datos para sesiones intermedias que pasan a través de este nodo. Los registros contienen información sobre contadores de sesiones y características de las sesiones. También se incluye la información de RSCV en los registros de datos si está habilitado el parámetro Save RSCV information for intermediate sessions. Si este parámetro está en yes, el valor de *collect intermediate session information* se alterará temporalmente.
Parámetro	Record creation threshold
Valores válidos	De 0 a 4 294 967, en incrementos de 1 KB
Valor por omisión	0
Descripción	Este parámetro especifica un umbral de bytes para crear registros de sesión intermedios. Cuando los datos de sesión superan el valor de este contador de bytes en una cantidad par múltiplo, se crea un registro.

Tabla 16 (Página 2 de 2). Lista de parámetros de configuración - Gestión de nodos APPN

Información de los parámetros	
Parámetro	Held alert queue size
Valores válidos	De 0 a 255
Valor por omisión	10
Descripción	Este parámetro establece el tamaño de la cola de alertas retenidas configurable. Esta cola se usa para guardar las alertas de APPN antes de enviarlas a un punto focal. Si la cola se desborda, se descartarán las alertas más antiguas.

Tabla 17 (Página 1 de 2). Lista de parámetros de configuración - Soportes de registro de APPN ISR

Información de los parámetros	
Parámetros de memoria	
Parámetro	Memory (consulte las notas de tabla)
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita la captación de datos de sesiones intermedias en la memoria local del direccionador.
Parámetro	Maximum memory buffers
Valores válidos	Del 0 al 1
Valor por omisión	1
Descripción	Este parámetro especifica el número de almacenamientos intermedios que se asignarán en la memoria local del direccionador para almacenar registros de sesiones intermedias.
Parámetro	Maximum memory records per buffer
Valores válidos	De 0 a 2000
Valor por omisión	100
Descripción	Este parámetro especifica el número máximo de registros de sesiones intermedias que pueden almacenarse en el almacenamiento intermedio de memoria del direccionador.
Parámetro	Memory buffers full
Valores válidos	Stop recording (Dejar de registrar) (0), Wrap (Acomodar) (1)
Valor por omisión	Dejar de registrar (0)
Descripción	Este parámetro especifica la acción que debe seguirse cuando el almacenamiento intermedio de memoria asignado para almacenar registros de sesiones intermedias se llena. Seleccione **Stop recording** (Dejar de registrar) para indicar al direccionador que descarte cualquier registro de sesión intermedia nuevo. Seleccione **Wrap** (Acomodar) para permitir que los registros nuevos sobrescriban registros ya existentes en el almacenamiento intermedio. Primero se sobrescribirán los registros más antiguos del almacenamiento intermedio.

Tabla 17 (Página 2 de 2). Lista de parámetros de configuración - Soportes de registro de APPN ISR

Información de los parámetros
Parámetro Memory record format **Valores válidos** ASCII (0), Binary (Binario) (1) **Valor por omisión** ASCII (0) **Descripción** Este parámetro especifica el formato en que los registros de sesiones intermedias se almacenarán en la memoria local del direccionador.
Parámetro Time between database updates **Valores válidos** De 60 a 1440 minutos **Valor por omisión** 60 **Descripción** Este parámetro establece el tiempo, en minutos, entre actualizaciones de base de datos topológica.
Nota: • Cuando habilita la captación de registros de sesiones intermedias, los datos asociados a los registros también se captan, por omisión, en SNMP • Variables MIB para APPN. En dicho caso, las variables MIB se actualizarán, independientemente de que el parámetro de captación de información de sesiones intermedias (en la Tabla 16 en la página 136) se haya habilitado. • Los datos de sesiones intermedias pueden almacenarse en la memoria del direccionador.

Add

Use el mandato **add** para añadir o actualizar:

Sintaxis:

add port

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

Tabla 18 (Página 1 de 3). Lista de parámetros de configuración - Configuración de puertos

Información de los parámetros	
Parámetro	Link type
Valores válidos	Ethernet (E) Red en anillo (T) ATM (A) DLSw (D) PPP (P) Frame relay (F) SDLC (S) X.25 (X) IP
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el tipo de enlace asociado a este puerto.
Parámetro	Interface number
Valores válidos	De 0 a 65533
Valor por omisión	0
Descripción	Este parámetro define el número de interfaz física de la interfaz de hardware a la que está conectado este dispositivo.
Parámetro	Port name
Valores válidos	Serie que tiene entre 1 y 8 caracteres, donde el primer carácter es alfabético y del 2 al 8 los caracteres son alfanuméricos.
Valor por omisión	Un nombre único no calificado que se genera automáticamente. El nombre estará formado por: • TR (red en anillo) • EN (Ethernet) • DLS (DLSw) • IP255 • ATM • FR (Frame Relay) • X25 (X.25) • SDLC (SDLC) • PPP (punto a punto) • IP seguido del número de la interfaz.
Descripción	Puede cambiar el nombre de puerto por un nombre de su elección. Este parámetro especifica el nombre que representa este puerto.
Parámetro	Enable APPN routing on this port
Valores válidos	Yes, No
Valor por omisión	Yes
Descripción	Este parámetro especifica si el direccionamiento de APPN debe habilitarse en este puerto.

Tabla 18 (Página 2 de 3). Lista de parámetros de configuración - Configuración de puertos

Información de los parámetros
Parámetro Support multiple PU **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro especifica si el puerto dará soporte a varias subáreas.
Parámetro Service any node **Valores válidos** Yes, No **Valor por omisión** Yes **Descripción** Este parámetro especifica cómo responde el nodo de red del direccionador a una solicitud de otro nodo para establecer una conexión sobre este puerto. Cuando se habilita este parámetro, el nodo de red acepta cualquier solicitud que reciba de otro nodo para establecer conexión. Cuando se inhabilita este parámetro, el nodo de red acepta las solicitudes de conexión únicamente de los nodos que haya definido explícitamente (mediante definiciones de estaciones de enlace). Esta opción proporciona un nivel añadido de seguridad al nodo de red del direccionador. **Nota:** Cuando se inhabilita este parámetro, sólo se aceptan las solicitudes de conexión de un nodo adyacente si el parámetro del nombre del CP plenamente calificado del nodo se ha configurado para una estación de enlace definida en este puerto. Cuando este parámetro está habilitado (valor por omisión), puede que siga deseando que este nodo de red pueda iniciar conexiones con nodos específicos sobre este puerto.
Parámetro High-performance routing (HPR) supported **Valores válidos** Yes, No **Valor por omisión** Yes para puertos de red en anillo, Ethernet, Frame Relay y PPP. **Descripción** Este parámetro indica si las estaciones de enlace de este puerto darán soporte a HPR. El valor puede alterarse temporalmente en la definición de la estación de enlace.
Parámetro IPv4 Precedence **Valores válidos** Yes o No **Valor por omisión** No **Descripción** Este parámetro establece el valor de precedencia de IPv4, lo que permite el filtro de precedencia BRS de los paquetes encapsulados IPv4.
Parámetro Limited Resource (únicamente PPP y FR sobre circuitos de marcación) **Valores válidos** Yes, No **Valor por omisión** Si el circuito de marcación es *bajo pedido*, el valor por omisión será Yes. De lo contrario, dicho valor será No. **Descripción** Este parámetro especifica si las estaciones de enlace de este puerto son un recurso limitado. Este valor puede alterarse temporalmente en la definición de la estación de enlace.

Tabla 18 (Página 3 de 3). Lista de parámetros de configuración - Configuración de puertos

Información de los parámetros
Parámetro Support bridged formatted frames (sólo Frame relay) **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro especifica si el puerto de Frame Relay dará soporte a las tramas formateadas puenteadas. Si está configurando Frame Relay para que dé soporte al formato puenteado, también necesitará configurar un identificador de nodo límite.
Parámetro Boundary node identifier (sólo Frame Relay) **Valores válidos** De X'0000 0000 0001' a X'7FFF FFFF FFFF' **Valor por omisión** X'4FFF 0000 0000' **Descripción** Este parámetro especifica la dirección del MAC del identificador del nodo límite. El direccionador usa esta dirección del MAC para reconocer que la trama es una trama puenteada de Frame Relay destinada a APPN.
Parámetro Subnet visit count **Valores válidos** De 1 a 255 **Valor por omisión** El valor por omisión se toma del parámetro de nivel de nodo equivalente **Descripción** Este parámetro especifica el valor por omisión de este puerto para el número máximo de subredes que puede atravesar una sesión de varias subredes. **Nota:** Esta pregunta sólo se hace si la función de border node está habilitada en este nodo.
Parámetro Adjacent node subnet affiliation **Valores válidos** • 0 (nativa) • 1 (no nativa) • 2 (negociable) **Valor por omisión** 2 **Descripción** Este parámetro especifica el valor por omisión de todos los enlaces a través de este puerto así como si el nodo adyacente está en la subred APPN nativa de este nodo o en una subred APPN no nativa. Un valor de *2* instruye al nodo para que negocie en el momento de activación del enlace para determinar si la estación de enlace adyacente es nativa o no. **Nota:** Esta pregunta sólo se hace si la función de border node está habilitada en este nodo.

Tabla 19 (Página 1 de 4). Lista de parámetros de configuración - Configuración de puerto para ATM

Información de los parámetros
Parámetro Local ATM Address **Valores válidos** Cualquier serie de 14 caracteres hexadecimales **Valor por omisión** Ninguno **Descripción** Este parámetro especifica la serie de 7 bytes que incluye la parte del usuario de la dirección ATM local. La parte del usuario es el ESI de 6 bytes y el campo del selector de 1 byte. Esta parte del usuario debe ser única en relación con la parte de la red de la dirección ATM, que se recupera del adaptador de ATM. El selector debe ser único para cada tipo de protocolo.
Parámetro Enable incoming calls **Valores válidos** Yes o No **Valor por omisión** Yes **Descripción** Este parámetro determina si se rechazarán las llamadas en el nivel de ATM.
Parámetro ATM Network Type **Valores válidos** Campus o Widearea **Valor por omisión** Campus **Descripción** Este parámetro especifica el tipo de red usado para los valores por omisión para las redes de conexiones y otras estaciones de enlace definidas en este puerto.
Parámetro Shareable connection network traffic **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro especifica si el tráfico de red de conexión puede direccionarse en el ATM VC configurado para una estación de enlace de este puerto.
Parámetro Shareable other protocol traffic **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro especifica si otro tráfico de protocolo de mayor nivel puede direccionarse en el ATM VC configurado para una estación de enlace de este puerto.

Tabla 19 (Página 2 de 4). Lista de parámetros de configuración - Configuración de puerto para ATM

Información de los parámetros
Parámetro Broadband Bearer Class **Valores válidos** Clase_A, Clase_C, Clase_X **Valor por omisión** Clase_X **Descripción** Este parámetro especifica la clase de portador solicitada desde la red ATM. Las clases se definen: **Clase A** Velocidad de bit constante (CBR) con requisitos de tiempo de extremo a extremo **Clase C** Velocidad de bit variable (VBR) sin requisitos de tiempo de extremo a extremo **Clase X** Servicio que permite el tipo de tráfico definido por el usuario y requisitos de tiempo
Parámetro Best Effort Indicator **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro indica si se requiere una garantía completa en este SVC. Si el valor de este parámetro es *yes*, los VCC asociados a esta interfaz se asignarán basándose en la anchura de banda disponible.
Nota: Los parámetros siguientes son parámetros de tráfico de reenvío.
Parámetro Forward Traffic Peak Cell Rate **Valores válidos** Del 1 al 85% de velocidad de línea **Valor por omisión** Capacidad efectiva por omisión del puerto/48 **Descripción** Este parámetro indica un límite superior en la velocidad de transmisión de células.
Parámetro Forward Traffic Sustained Cell Rate **Valores válidos** Del 1 al 85% de velocidad de línea **Valor por omisión** Capacidad efectiva por omisión del puerto/48 **Descripción** Este parámetro indica un límite superior en la velocidad media de transmisión de células. No puede especificar este parámetro si está usando la conexión de Mejor esfuerzo.
Parámetro Forward Traffic Tagging **Valores válidos** Yes, No **Valor por omisión** Yes **Descripción** Este parámetro indica que las células que no cumplen la especificación de tráfico de prioridad 0 de pérdida de células, pero sí que cumplen la especificación de tráfico de prioridad 1 de dicha pérdida se marcan y pueden entrar en la red ATM. No puede especificar este parámetro si está usando la conexión de Mejor esfuerzo.

Tabla 19 (Página 3 de 4). Lista de parámetros de configuración - Configuración de puerto para ATM

Información de los parámetros
Parámetro Forward QoS **Valores válidos** CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, donde **CLASS_0** Clase sin especificar. La red no especifica ninguna QoS. **CLASS_1** El rendimiento es comparable al de la línea privada digital actual. **CLASS_2** Clase destinada al vídeo y audio en paquetes para las aplicaciones multimedia y de vídeoconferencia. **CLASS_3** Clase destinada al interfuncionamiento de protocolos orientados a la conexión como, por ejemplo, Frame Relay. **CLASS_4** Clase destinada al interfuncionamiento de protocolos sin conexión como, por ejemplo, IP. **Valor por omisión** CLASS_0 **Descripción** Este parámetro indica qué clase de servicio se proporciona a una conexión virtual ATM. Este parámetro siempre es CLASE_0 para una conexión de Mejor esfuerzo.
Nota: Los parámetros siguientes son parámetros de tráfico hacia atrás.
Parámetro Backward Traffic Peak Cell Rate **Valores válidos** Del 1 al 85% de velocidad de línea **Valor por omisión** Capacidad efectiva por omisión del puerto/48 **Descripción** Este parámetro indica un límite superior en la velocidad de transmisión de células.
Parámetro Backward Traffic Sustained Cell Rate **Valores válidos** Del 1 al 85% de velocidad de línea **Valor por omisión** Capacidad efectiva por omisión del puerto/48 **Descripción** Este parámetro indica un límite superior en la velocidad media de transmisión de células. No puede especificar este parámetro para una conexión de Mejor esfuerzo.
Parámetro Backward Traffic Tagging **Valores válidos** Yes, No **Valor por omisión** Yes, a menos que se tenga una conexión de Mejor esfuerzo **Descripción** Este parámetro indica que las células que no cumplen la especificación de tráfico de prioridad 0 de pérdida de células, pero sí que cumplen la especificación de tráfico de prioridad 1 de dicha pérdida se marcan y pueden entrar en la red ATM. No puede especificar este parámetro para una conexión de Mejor esfuerzo.

Tabla 19 (Página 4 de 4). Lista de parámetros de configuración - Configuración de puerto para ATM

Información de los parámetros
Parámetro Backward QoS **Valores válidos** CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, donde **CLASS_0** Clase sin especificar. La red no especifica ninguna QoS. **CLASS_1** El rendimiento es comparable al de la línea privada digital actual. **CLASS_2** Clase destinada al vídeo y audio en paquetes para las aplicaciones multimedia y de vídeoconferencia. **CLASS_3** Clase destinada al interfuncionamiento de protocolos orientados a la conexión como, por ejemplo, Frame Relay. **CLASS_4** Clase destinada al interfuncionamiento de protocolos sin conexión como, por ejemplo, IP. **Valor por omisión** CLASS_0 **Descripción** Este parámetro indica qué clase de servicio se proporciona a una conexión virtual ATM. No puede especificar este parámetro para una conexión de Mejor esfuerzo.
Parámetro Callout Anonymously **Valores válidos** Yes, No **Valor por omisión** no **Descripción** Este parámetro indica si APPN pasará la dirección de origen cuando llame.
Parámetro LDLC retry count **Valores válidos** De 1 a 255 **Valor por omisión** 3 **Descripción** Este parámetro se usa junto con el período del temporizador LDLC para proporcionar una entrega fiable de XID. La cuenta de reintentos se inicializa cuando un mandato o solicitud se transmite por primera vez sobre un enlace. Si el período del temporizador LDLC expira antes de recibir una respuesta, se volverá a transmitir el mandato o solicitud, la cuenta de reintentos disminuirá y el período del temporizador LDLC se reiniciará. Si el temporizador expira con la cuenta de reintentos en 0, se presupondrá que el enlace no es operativo.
Parámetro LDLC Timer Period **Valores válidos** De 1 a 255 segundos **Valor por omisión** Para ATM: 1 segundo Para IP: 15 segundos **Descripción** Este parámetro especifica el período de tiempo usado con **LDLC retry count**.

Tabla 20 (Página 1 de 4). Lista de parámetros de configuración - Definición de puertos

Información de los parámetros	
Parámetro	Maximum BTU size
Valores válidos	De 768 a 1496 bytes para Ethernet De 768 a 17745 bytes para la red en anillo 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 2048 bytes para todos los demás puertos
Valor por omisión	1289 bytes para Ethernet 2048 bytes para red en anillo 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
Descripción	Este parámetro especifica el número de bytes de la unidad de transmisión básica (BTU) más grande que puede procesar (transmitida o recibida) una estación de enlace definida en este puerto. **Nota:** Si se recibe un BIND negociable con un tamaño de RU superior a 2048, normalmente el dispositivo elegirá un tamaño de RU máximo de 2048. Si se recibe un BIND no negociable con un tamaño de RU superior a 2048, el dispositivo dará soporte al tamaño de RU más grande, hasta un tamaño máximo de 4096.
Parámetro	Maximum number of link stations
Valores válidos	De 1 a 127 para puertos SDLC De 1 a 239 para puertos X.25
Valor por omisión	Si SDLC está configurado como multipunto y primario, este parámetro tendrá un valor por omisión de 127. De lo contrario, se establecerá en 1 y no será configurable. 239 para puertos X.25
Descripción	Este parámetro especifica el número máximo de estaciones de enlace que podrán usar este puerto. Este parámetro permite que los recursos del nodo APPN y este puerto se restrinjan.

Tabla 20 (Página 2 de 4). Lista de parámetros de configuración - Definición de puertos

Información de los parámetros	
Parámetro	Percent of link stations reserved for incoming calls (únicamente Ethernet, red en anillo, FR, X.25)
Valores válidos	De 0 a 100 La suma del porcentaje de las estaciones de enlace reservadas para las llamadas de entrada y el porcentaje de estaciones de enlace reservadas para las llamadas de salida no puede superar el 100%.
Valor por omisión	0
Descripción	Este parámetro especifica el porcentaje del número máximo de estaciones de enlace que se reservará para las llamadas de entrada. Las estaciones de enlace que no se reserven para llamadas de entrada o de salida estarán disponibles para ambos objetivos según la demanda.
Parámetro	Percent of link stations reserved for outgoing calls
Valores válidos	De 0 a 100 La suma del porcentaje de las estaciones de enlace reservadas para las llamadas de entrada y el porcentaje de estaciones de enlace reservadas para las llamadas de salida no puede superar el 100%. Si SDLC es primario y multipunto, el valor válido será 100.
Valor por omisión	0 Si SDLC es primario y multipunto, el valor por omisión será 100.
Descripción	Este parámetro especifica el porcentaje del número máximo de estaciones de enlace que se reservará para las llamadas de salida. Las fracciones resultado del cálculo se truncarán. Las estaciones de enlace que no se reserven para llamadas de entrada o de salida estarán disponibles para ambos objetivos según la demanda.
Parámetro	UDP port number for XID exchange
Valores válidos	De 1024 a 65535
Valor por omisión	11000
Descripción	Este parámetro especifica el número de puerto UDP que se usará para el intercambio de XID y que se usa durante la definición de puerto IP. Este número de puerto debe ser el mismo que el definido en otros dispositivos de la red.
Parámetro	UDP port number for network priority traffic
Valores válidos	De 1024 a 65535
Valor por omisión	11001
Descripción	Este parámetro especifica el número de puerto UDP que se usará para el tráfico de prioridad de red.
Parámetro	UDP port number for high priority traffic
Valores válidos	De 1024 a 65535
Valor por omisión	11002
Descripción	Este parámetro especifica el número de puerto UDP que se usará para tráfico de alta prioridad.

Tabla 20 (Página 3 de 4). Lista de parámetros de configuración - Definición de puertos

Información de los parámetros
Parámetro UDP port number for medium priority traffic **Valores válidos** De 1024 a 65535 **Valor por omisión** 11003 **Descripción** Este parámetro especifica el número de puerto UDP que se usará para tráfico de prioridad media.
Parámetro UDP port number for low priority traffic **Valores válidos** De 1024 a 65535 **Valor por omisión** 11004 **Descripción** Este parámetro especifica el número de puerto UDP que se usará para el tráfico de baja prioridad.
Parámetro IP network type **Valores válidos** Campus o Widearea **Valor por omisión** Widearea **Descripción** Este parámetro especifica el tipo de red IP.
Parámetro Local APPN SAP address **Valores válidos** Múltiplos de cuatro en el rango hexadecimal incluido entre X'04' y X'EC' **Valor por omisión** X'04' **Descripción** Este parámetro especifica la dirección de SAP local que se usará para las comunicaciones con las estaciones de enlace de APPN definidas en este puerto.
Parámetro Local HPR SAP address (sólo para Ethernet y redes en anillo) **Valores válidos** Múltiplos de cuatro en el rango hexadecimal incluido entre X'04' y X'EC' **Valor por omisión** X'C8' **Descripción** Este parámetro indica el punto de acceso de servicio local que se usará para las comunicaciones con las estaciones de enlace HPR definidas en este puerto.

Tabla 20 (Página 4 de 4). Lista de parámetros de configuración - Definición de puertos

Información de los parámetros	
Parámetro	Branch uplink
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro indica si el valor por omisión de las estaciones de enlace que usan este puerto será hacia arriba o hacia abajo. Si se especifica *yes*, las estaciones de enlace que usen este puerto darán como valor por omisión para **Branch uplink** *yes*. **Notas:** 1. Esta pregunta sólo se hace si el parámetro de nivel de nodo **Enabled Branch Extender** está en *yes*. 2. Si **Branch uplink** está en yes, Branch Extender presentará su apariencia de nodo final a esta estación de enlace. De lo contrario, Branch Extender presentará su apariencia de nodo de red. 3. Por lo general, **Branch uplink** se establece en yes para nodos de red conectados a una WAN y no para nodos de red conectados a una LAN.

Tabla 21 (Página 1 de 6). Lista de parámetros de configuración - Características del TG por omisión del puerto

Información de los parámetros	
Parámetro	Cost per connect time
Valores válidos	De 0 a 255
Valor por omisión	Para SVC ATM: **Campus ATM best effort (Mejor esfuerzo de campus ATM)** 0 **Campus ATM reserved (Reservado a campus ATM)** 64 **WAN ATM best effort (Mejor esfuerzo de WAN ATM)** 0 **WAN ATM reserved (Reservado a WAN ATM)** 128 Para PVC ATM: **Campus ATM best effort (Mejor esfuerzo de campus ATM)** 0 **Campus ATM reserved (Reservado a campus ATM)** 0 **WAN ATM best effort (Mejor esfuerzo de WAN ATM)** 0 **WAN ATM reserved (Reservado a WAN ATM)** 0 Para IP: 0 para Campus y WAN Para el resto: 0
Descripción	Este parámetro especifica el coste por característica de TG del tiempo de conexión para todas las estaciones de enlace de este puerto. El coste por característica de TG dle tiempo de conexión expresa el coste relativo de mantener una conexión sobre el TG asociado. Las unidades están definidas por el usuario y normalmente se basan en las tarifas aplicables del recurso de transmisión que se está usando. Los valores asignados deben reflejar el gasto real del mantenimiento de una conexión sobre el TG en relación con el resto de los TG de la red. Un valor de cero significa que las conexiones sobre el TG pueden establecerse sin ningún costo adicional (como en el caso de varios de los recursos no conmutados). Los valores más altos representan costes más altos.

Tabla 21 (Página 2 de 6). Lista de parámetros de configuración - Características del TG por omisión del puerto

Información de los parámetros	
Parámetro	Cost per byte
Valores válidos	De 0 a 255
Valor por omisión	Para SVC ATM y PVC ATM: **Campus ATM best effort (Mejor esfuerzo de campus ATM)** 0 **Campus ATM reserved (Reservado a campus ATM)** 0 **WAN ATM best effort (Mejor esfuerzo de WAN ATM)** 128 **WAN ATM reserved (Reservado a WAN ATM)** 0 Para IP: 0 para Campus y WAN Para el resto: 0
Descripción	Este parámetro especifica la característica de TG de coste por byte de todas las estaciones de enlace definidas en este puerto. La característica de TG de coste por byte expresa el coste relativo de transmitir un byte sobre un TG asociado. Las unidades están definidas por el usuario y el valor asignado debe reflejar los gastos reales de transmisión sobre el TG en relación con el resto de TG de la red. Un valor de cero significa que los bytes pueden transmitirse sobre el TG sin pagar ningún coste adicional. Los valores más altos representan costes más altos.

Tabla 21 (Página 3 de 6). Lista de parámetros de configuración - Características del TG por omisión del puerto

Información de los parámetros	
Parámetro	Security
Valores válidos	**Nonsecure (no fiable)** el resto (por ejemplo, conectado por satélite o localizado en un país no fiable). **Public switched network (Red conmutada pública)** fiable en el sentido de que la ruta no se determina previamente **Underground cable (Cable subterráneo)** situado en un país fiable (determinado por el administrador de red) **Secure conduit (Conducto fiable)** Sin guardar, (por ejemplo, conducto presurizado) **Guarded conduit (Conducto guardado)** protegido contra las intervenciones físicas **Encrypted (Cifrado)** se proporciona un cifrado de nivel de enlace **Guarded radiation (Radiación vigilada)** conducto vigilado que contiene el medio de transmisión; protegido contra la intervención de radiación y la intervención física
Valor por omisión	Para SVC ATM y PVC ATM: **Campus ATM best effort (Mejor esfuerzo de campus ATM)** Nonsecure (no fiable) **Campus ATM reserved (Reservado a campus ATM)** Nonsecure (no fiable) **WAN ATM best effort (Mejor esfuerzo de WAN ATM)** Public switched network (Red conmutada pública) **WAN ATM reserved (Reservado a WAN ATM)** Public switched network (Red conmutada pública) Para IP: **Campus** Nonsecure (no fiable) **WAN** Public switched network (Red conmutada pública) Para el resto: Nonsecure (No fiable)
Descripción	Este parámetro especifica la característica de TG de seguridad de todas las estaciones de enlace definidas en este puerto. Esta característica indica el nivel de protección de seguridad asociada al TG. Si se necesitan atributos de seguridad que no sean los definidos arquitecturalmente, puede usarse una de las características de TG definidas por el usuario para especificar valores adicionales.

Tabla 21 (Página 4 de 6). Lista de parámetros de configuración - Características del TG por omisión del puerto

Información de los parámetros	
Parámetro	Propagation delay
Valores válidos	**Minimum LAN (LAN mínima)** menos de 480 microsegundos **Telephone (Teléfono)** entre 0,48 y 49,152 milisegundos **Packet switched (Paquete conmutado)** entre 49,152 y 245,76 milisegundos **Satellite (Satélite)** superior al máximo de 245,76 milisegundos
Valor por omisión	Para SVC ATM y PVC ATM: **Campus ATM best effort (Mejor esfuerzo de campus ATM)** Telephone **Campus ATM reserved (Reservado a campus ATM)** Minimum LAN **WAN ATM best effort (Mejor esfuerzo de WAN ATM)** Packet switched **WAN ATM reserved (Reservado a WAN ATM)** Telephone Para IP: **Campus** Telephone **WAN** Packet switched
Descripción	Este parámetro especifica la característica del TG del retardo de propagación de todas las estaciones de enlace definidas en este puerto. Esta característica especifica el rango aproximado de tiempo que tarda una señal en propagarse de un extremo del TG al otro.

Tabla 21 (Página 5 de 6). Lista de parámetros de configuración - Características del TG por omisión del puerto

Información de los parámetros	
Parámetro	Effective capacity
Valores válidos	2 dígitos hexadecimales incluidos en el rango que va de X'00' a X'FF'
Valor por omisión	FR: X'45' (64 Kbps) PPP: X'45' (64 Kbps) DLSw: X'75' (4 Mbps) SDLC: X'45' (64 Kbps) X.25: X'45' (64 Kbps) TR: X'85' (16 Mbps) TR: X'75' (4 Mbps) ENET: X'80' (10 Mbps) Para SVC ATM (25 Mbps) y PVC ATM (25Mbps): Campus ATM best effort: X'8A' Campus ATM reserved: X'8A' WAN ATM best effort: X'8A' WAN ATM reserved: X'8A' Para IP: Campus: X'75' WAN: X'43'
Descripción	Este parámetro especifica la característica de TG de capacidad efectiva para todas las conexiones asociadas (TG) de este puerto. Este parámetro especifica la velocidad de transmisión de bits máxima para los enlaces físicos y los lógicos. Observe que la capacidad efectiva de un enlace lógico puede ser inferior a la velocidad de enlace física. La velocidad está representada en los archivos COS como un número de coma flotante codificado en un único byte con unidades de 300 bps. La capacidad efectiva está codificada como una representación de un único byte. Los valores X'00' y X'FF' son casos especiales usados para denotar las capacidades mínima y máxima. El rango de codificación es muy amplio; no obstante, sólo se pueden especificar 256 valores del rango. Este parámetro proporciona el valor por omisión del parámetro de capacidad efectiva en la opción Modify TG Characteristics Command Line (Línea de mandatos de modificación de las características de TG). Esta opción le permite alterar temporalmente los valores por omisión .* asignados a características de TG en las estaciones de enlace individuales que defina.

Tabla 21 (Página 6 de 6). Lista de parámetros de configuración - Características del TG por omisión del puerto

Información de los parámetros
Parámetro First user-defined TG characteristic **Valores válidos** De 0 a 255 **Valor por omisión** 128 **Descripción** Este parámetro especifica la primera característica de TG definida por el usuario para todas las estaciones de enlace definidas en este puerto. Esta primera característica especifica la primera de tres características adicionales que pueden definir los usuarios para describir los TG de una red. El valor por omisión de 128 permite definir un subconjunto de TG como más o menos deseable que el resto sin tener que definir valores para todos los TG.
Parámetro Second user-defined TG characteristic **Valores válidos** De 0 a 255 **Valor por omisión** 128 **Descripción** Este parámetro especifica la segunda característica de TG definida por el usuario para todas las estaciones de enlace definidas en este puerto. Esta segunda característica especifica la segunda de tres características adicionales que pueden definir los usuarios para describir los TG de una red.
Parámetro Third user-defined TG characteristic **Valores válidos** De 0 a 255 **Valor por omisión** 128 **Descripción** Este parámetro especifica la tercera característica de TG definida por el usuario para todas las estaciones de enlace definidas en este puerto. Esta tercera característica especifica la tercera de tres características adicionales que pueden definir los usuarios para describir los TG de una red.

Tabla 22 (Página 1 de 4). Lista de parámetros de configuración - Características LLC por omisión del puerto

Información de los parámetros
Parámetro Remote APPN SAP **Valores válidos** Múltiplos de cuatro en el rango hexadecimal incluido entre X'04' y X'EC' **Valor por omisión** X'04' **Descripción** Este parámetro especifica el SAP asociado a la estación de enlace de APPN del nodo adyacente.

Tabla 22 (Página 2 de 4). Lista de parámetros de configuración - Características LLC por omisión del puerto

Información de los parámetros	
Parámetro	Maximum number of outstanding I-format LPDUs (TW)
Valores válidos	De 1 a 127
Valor por omisión	26
Descripción	Este parámetro especifica el número máximo de LLC de LPDU (TW) de formato I pendientes para todas las estaciones de enlace de este puerto. El número máximo de LPDU de formato I pendientes define la opción de transmisión de la línea de mandatos (TW) que es el número máximo de LPDU de formato I numeradas secuencialmente que la estación de enlace puede tener pendientes de acuse de recibo.
Parámetro	Receive window size
Valores válidos	De 1 a 127
Valor por omisión	26
Descripción	Este parámetro especifica el tamaño de la opción LLC receive Command Line (RW) de todas las estaciones de enlace de este puerto. El parámetro RW especifica el número máximo de LPDU de formato I numeradas secuencialmente y sin acuse de recibo que puede recibir la estación de enlace de la estación de enlace remota. RW se notifica en tramas SNA XID y tramas IEEE 802.2 XID. El receptor XID debe establecer el TW efectivo en un valor inferior o igual al del RW recibido a fin de evitar desbordamientos.
Parámetro	Inactivity timer (Ti)
Valores válidos	De 1 a 254 segundos
Valor por omisión	30 segundos
Descripción	Este parámetro especifica el temporizador de inactividad (Ti) de LLC de todas las estaciones de enlace de este puerto. Una estación de enlace LLC usa Ti para detectar una condición no operativa en la estación de enlace remota o en el soporte de transmisión. Si no se recibe una LPDU en el intervalo de tiempo especificado por el Ti, se transmitirá una LPDU de mandato de formato S con bit de sondeo para solicitar el estado de la estación de enlace remota. La recuperación se basará en el temporizador de respuesta (T1).

Tabla 22 (Página 3 de 4). Lista de parámetros de configuración - Características LLC por omisión del puerto

Información de los parámetros
Parámetro Reply timer (T1) **Valores válidos** De 1 a 254 semisegundos **Valor por omisión** 2 semisegundos **Descripción** Este parámetro especifica el temporizador de respuesta LLC (T1) de todas las estaciones de enlace de este puerto. Una estación de enlace LLC usa T1 para detectar un fallo en la recepción de un acuse de recibo necesario o una respuesta de la estación remota de enlace. Cuando T1 expira, la estación de enlace envía una unidad de datos de protocolo de la capa de enlace (LPDU) de mandato de formato S con el bit de sondeo establecido, para solicitar el estado de la estación de enlace remota o cualquier LPDU de mandato de formato U que no haya recibido respuesta. La duración de T1 debe tener en cuenta cualquier retardo introducido en las capas inferiores.
Parámetro Maximum number of retransmissions (N2) **Valores válidos** De 1 a 254 **Valor por omisión** 8 **Descripción** Este parámetro especifica el número máximo de retransmisiones (N2) de todas las estaciones de enlace de este puerto. El parámetro N2 especifica el número máximo de veces que se retransmitirá una LPDU después de la expiración del temporizador de respuesta (T1).
Parámetro Receive acknowledgment timer (T2) **Valores válidos** De 1 a 254 semisegundos **Valor por omisión** 1 semisegundo **Descripción** Este parámetro especifica el temporizador de acuse de recibo de LLC (T2) de todas las estaciones de enlace de este puerto. Puede usarse el parámetro T2 con el contador N3 para reducir el tráfico de acuse de recibo. Una estación de enlace usa T2 para retrasar el envío de un acuse de recibo de una LPDU de formato I recibida. T2 se inicia cuando se recibe una LPDU de formato I y se restablece cuando se envía un acuse de recibo en una LPDU de formato I o formato S. Si T2 expira, la estación de enlace deberá enviar un acuse de recibo tan pronto como sea posible. El valor de T2 debe ser inferior al de T1, para asegurarse de que la estación de enlace remota reciba el acuse de recibo retrasado antes de que expire su T1.

Tabla 22 (Página 4 de 4). Lista de parámetros de configuración - Características LLC por omisión del puerto

Información de los parámetros	
Parámetro	Acknowledgments needed to increment working window
Valores válidos	De 0 a 127
Valor por omisión	1
Descripción	Cuando la ventana de trabajo (Ww) no es igual al tamaño máximo de la ventana de transmisión (Maximum Transmit Window Size - Tw), este parámetro será la cantidad de LPDU de formato I transmitidas cuyo acuse de recibo debe efectuarse antes de poder incrementar la ventana de trabajo (en 1). Cuando se detecta una congestión, por la pérdida de LPDU de formato I, Ww se establece en 1.

Tabla 23. Lista de parámetros de configuración - Valores por omisión de la alteración temporal de HPR

Información de los parámetros	
Parámetro	Inactivity timer override for HPR
Valores válidos	De 1 a 254 segundos
Valor por omisión	2 segundos
Descripción	Este parámetro especifica el temporizador de inactividad de LLC (HPR Ti) que se usará para todas las estaciones de enlace de este puerto que den soporte a HPR cuando el parámetro de soporte de HPR esté habilitado en dicho puerto. Este valor por omisión alterará temporalmente el valor del parámetro del temporizador de inactividad (Ti) del LLC especificado en el parámetro de las características del LLC por omisión.
Parámetro	Reply timer override for HPR (HPR T1)
Valores válidos	De 1 a 254 semisegundos
Valor por omisión	2 semisegundos
Descripción	Este parámetro especifica el temporizador de respuesta del LLC (HPR T1) que se usará en todas las estaciones de enlace de este puerto que den soporte a HPR, cuando el parámetro de HPR con soporte esté habilitado en él. Este valor por omisión altera temporalmente el valor del parámetro del temporizador de respuesta del LLC (T1) especificado en el parámetro de las características del LLC por omisión.
Parámetro	Maximum number of retransmissions for HPR (HPR N2)
Valores válidos	De 1 a 254
Valor por omisión	3
Descripción	Este parámetro especifica el número máximo de retransmisiones (HPR N2) de LLC que se va a usar para todas las estaciones de enlace de este puerto que den soporte a HPR, cuando el parámetro de HPR con soporte esté habilitado en este puerto. Este valor por omisión altera temporalmente el valor por omisión del parámetro del número máximo de LLC de retransmisiones (N2) por omisión especificado en el parámetro de las características del LLC por omisión.

Sintaxis:

add link-station

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

Tabla 24 (Página 1 de 9). Lista de parámetros de configuración - Estaciones de enlace - Detalle

Información de los parámetros	
Parámetro	Does link support APPN function
Valores válidos	Yes o No
Valor por omisión	Yes
Descripción	Este parámetro especifica si esta estación de enlace dará soporte a la función de APPN. Si la respuesta es *no*, no se harán preguntas sobre sesiones de CP-CP, seguridad, codificación, nombre de CP, tipo de nodo adyacente, branch extender y extended border node y todas estas funciones se inhabilitarán. Además, se inhabilitará HPR y no se hará ninguna pregunta de HPR.
Parámetro	Link station name (obligatorio)
Valores válidos	Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de una estación de enlace que representa el TG (enlace) entre el nodo de red del direccionador y el nodo adyacente. El nombre de la estación de enlace debe ser único en este nodo de red.
Parámetro	Port name
Valores válidos	Un nombre único no calificado que se genera automáticamente. El nombre estará formado por: • TR (red en anillo) • EN (Ethernet) • DLS (DLSw) • FR (Frame Relay) • X25 (X.25) • SDLC (SDLC) • PPP (punto a punto) • IP seguido del número de la interfaz.
Valor por omisión	El nombre del puerto en el que está definida esta estación de enlace.
Descripción	Este parámetro especifica el nombre que representa al puerto en el que está definida esta estación de enlace. El puerto debe estar ya configurado para APPN.

Tabla 24 (Página 2 de 9). Lista de parámetros de configuración - Estaciones de enlace - Detalle

Información de los parámetros	
Parámetro	Tipo de enlace (únicamente X.25 y ATM) Si *limited resource* = yes está configurado para esta estación de enlace, entonces el parámetro del tipo de enlace tendrá como valor por omisión un valor de 1 (SVC) y no se podrá configurar.
Valores válidos	Si es PVC, especifique un número de canal lógico dentro del rango incluido entre 1 y 4095 Si es SVC, especifique una dirección del DTE cuya longitud variable puede alcanzar los 15 dígitos
Valor por omisión	0, a menos que sea un recurso limitado.
Descripción	Este parámetro especifica si el enlace X.25 es un PVC o SVC.
Parámetro	MAC address of adjacent node (obligatorio) (únicamente formato puenteado Ethernet, de red en anillo, DLSw y FR)
Valores válidos	Puertos de red en anillo y DLSw: • 12 dígitos hexadecimales dentro del rango incluido entre X'000000000001' y X'7FFFFFFFFFFF' Puertos de Ethernet/802.3: • 12 dígitos hexadecimales con formato *X' xyxxxxxxxxxx'* donde: *x* es cualquier dígito hexadecimal *y* es un dígito hexadecimal del juego {0, 2, 4, 6, 8, A, C, E}
Valor por omisión	Ninguno
Descripción	Este parámetro especifica la dirección de la capa de control de acceso al soporte (MAC) del nodo adyacente. Se usan formatos diferentes para red en anillo y Ethernet/802.3. Puertos de red en anillo y DLSw: La dirección del MAC se especifica en formato no canónico. En el formato de dirección no canónico, el bit de cada octeto que se transmitirá en primer lugar se representa como el bit más significativo. Puertos de Ethernet/802.3: La dirección del MAC se especifica en formato canónico. En el formato de dirección canónico, el bit de cada octeto que se transmitirá en primer lugar se representa como el bit menos significativo.
Parámetro	IP address of adjacent node
Valores válidos	Cualquier dirección IP válida
Valor por omisión	ninguno
Descripción	Cada enlace del puerto HPR/IP debe tener una dirección de IP de destino única.

Tabla 24 (Página 3 de 9). Lista de parámetros de configuración - Estaciones de enlace - Detalle

Información de los parámetros	
Parámetro	Adjacent node type
Valores válidos	APPN network node (nodo de red APPN), APPN end node (nodo final APPN) y LEN end node (nodo final LEN)
Valor por omisión	Nodo de red APPN
Descripción	Este parámetro identifica si el nodo adyacente es un nodo APPN, un nodo final (LEN) de red de entrada baja. Cuando se selecciona *APPN end node* y *Limited resource* está en No, APPN cambia el tipo de nodo adyacente internamente para *aprender* y trabaja con cualquier tipo de nodo. Si selecciona *APPN end node* y *Limited resource* está en Yes, el tipo de nodo adyacente permanecerá igual. Cuando seleccione *LEN end node*, el parámetro del nombre del punto de control plenamente calificado es obligatorio. Si este nodo de red está comunicando con el producto IBM Virtual Telecommunications Access Method (VTAM) a través del nodo LEN y éste no es un nodo T2.1 o no tiene un nombre de punto de control (CP) definido explícitamente, el número de XID del nodo de red del direccionador para el parámetro de conexión de subárea también debe especificarse para establecer una conexión. **Nota:** *LEN end node* (Nodo final de red) no es un tipo de nodo válido para la interfaz HPR/IP.

Tabla 24 (Página 4 de 9). Lista de parámetros de configuración - Estaciones de enlace - Detalle

Información de los parámetros	
Parámetro	fully-qualified CP name of adjacent node
Valores válidos	Una serie con un máximo de 17 caracteres presentados en forma de *IDred.nombreCP*, donde: • *IDred* es un ID de red de 1 a 8 caracteres • *nombreCP* es un nombre de punto de control que tiene entre 1 y 8 caracteres Cada nombre debe respetar las normas siguientes: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 **Nota:** Sigue dándose soporte a nombres de CP plenamente calificados que usan los caracteres especiales @, $ del juego de caracteres A; no obstante, estos caracteres no deben usarse en los nombres de CP nuevos.
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre del CP plenamente calificado del nodo adyacente. Para los casos en que este parámetro no sea obligatorio, el nombre del CP del nodo adyacente puede saberse dinámicamente durante el intercambio de XID; no obstante, si se especifica un nombre de CP, éste debe coincidir con la definición del nodo adyacente para que el enlace se active satisfactoriamente. **Nota:** Este parámetro es obligatorio cuando se produce una de las situaciones siguientes: • El parámetro *Service any node* está en Disable (inhabilitar). • El parámetro *Adjacent node type* está en LEN end node. • El parámetro *CP-CP session level security* está en Enable (Habilitar). • El enlace es un recurso limitado.
Parámetro	Activate link automatically Si es un recurso limitado, este parámetro se establece en No y no se podrá configurar.
Valores válidos	Yes, No
Valor por omisión	Yes
Descripción	Cuando se activa este parámetro, el nodo de red del direccionador activa automáticamente el enlace con el nodo adyacente e inicia una conexión.

Tabla 24 (Página 5 de 9). Lista de parámetros de configuración - Estaciones de enlace - Detalle

Información de los parámetros
Parámetro Allow CP-CP sessions on this link **Valores válidos** Yes, No **Valor por omisión** Yes, si el tipo de nodo adyacente es un nodo de red APPN o un nodo final APPN. No para el resto de tipos de nodo adyacente **Descripción** Este parámetro especifica si las sesiones entre puntos de control se activarán sobre esta estación de enlace. Este parámetro permite controlar el establecimiento de sesiones de CP-CP entre nodos de red adyacentes para que la carga asociada con las actualizaciones de base de datos de topología (TDU) se restrinja. **Nota:** Cada nodo de red APPN debe tener, como mínimo, una sesión de CP-CP establecida en otro nodo de red APPN a fin de mantener la conectividad mínima necesaria para actualizar la base de datos topológica. Además, es posible que se necesite más que la conectividad mínima para eliminar puntos aislados de fallo y para mejorar la dinámica de la red.
Parámetro CP-CP session level security **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro especifica si la seguridad de nivel de sesión se aplica a sesiones de CP-CP establecidas sobre esta estación de enlace. Cuando se habilita la seguridad de nivel de sesión, se intercambian datos cifrados y se comparan durante los flujos BIND (lo que incluye el BIND, la respuesta al BIND y una RU de seguridad FMH-12). Para establecer satisfactoriamente una sesión de CP-CP con la seguridad de nivel de sesión habilitada, los dos asociados deben estar configurados con la misma clave de cifrado. Actualmente, el soporte de la seguridad de nivel de sesión se limita al protocolo de verificación de LU-LU básico.
Parámetro Encryption key **Valores válidos** Hasta 16 dígitos hexadecimales. Si se especifican menos de 16 dígitos, se rellena el espacio de la derecha del valor con ceros. **Valor por omisión** Ninguno **Descripción** Este parámetro se usa para codificar los datos intercambiados durante los flujos BIND. Para establecer una sesión de CP-CP, los dos asociados deben estar configurados con la misma clave.
Parámetro Use enhanced session security (Si está habilitada la seguridad) **Valores válidos** Yes, No **Valor por omisión** No

Tabla 24 (Página 6 de 9). Lista de parámetros de configuración - Estaciones de enlace - Detalle

Información de los parámetros	
Parámetro	High-performance routing (HPR) supported
Valores válidos	Yes, No
Valor por omisión	APPN network node (nodo de red APPN), APPN end node (nodo final APPN) o LEN end node (nodo final LEN): el valor especificado en el parámetro de HPR con soporte por omisión para este puerto. El resto de tipos de nodo adyacentes: No
Descripción	Este parámetro indica si esta estación de enlace da soporte a HPR. El usuario deberá inhabilitar el soporte a HPR si el enlace subyacente no es fiable. No se establecerá una conexión HPR a menos que ambas estaciones de enlace anuncien su soporte a HPR durante el intercambio de XID.
Parámetro	DLCI number for link (únicamente Frame Relay)
Valores válidos	De 16 a 1007
Valor por omisión	16
Descripción	El parámetro DLCI identifica la conexión de enlace de datos lógicos de frame-relay con el nodo adyacente.
Parámetro	Station address of adjacent node (únicamente SDLC)
Valores válidos	Una dirección que esté incluida dentro del rango (1 - FE)
Valor por omisión	C1
Descripción	Este parámetro especifica la dirección del nodo adyacente.
Parámetro	Limited Resource (PPP, X.25 FR sobre circuitos de marcación, ATM)
Valores válidos	Yes o No
Valor por omisión	No Si el *link type* (tipo de enlace) es PPP o FR, el valor por omisión se tomará del parámetro *limited resource* para el puerto asociado.
Descripción	Este parámetro especifica si el TG para esta estación de enlace es un recurso limitado. Si responde *yes*, el **Virtual Channel Type** (Tipo de canal virtual) será *SVC*.
Parámetro	Branch uplink
Valores válidos	Yes o No
Valor por omisión	El valor especificado para **Branch Uplink** en el puerto.
Descripción	Este parámetro indica si este enlace será un enlace hacia la rama de arriba (a WAN) o hacia abajo (a LAN). Esta pregunta sólo se hace si se ha establecido **Enabled Branch Extender** en *yes* y si esta estación de enlace no es un nodo de red. Si **Enabled Branch Extender** está en *yes* y esta estación de enlace es un nodo de red, **Branch Uplink** tendrá como valor por omisión *yes.*

Tabla 24 (Página 7 de 9). Lista de parámetros de configuración - Estaciones de enlace - Detalle

Información de los parámetros
Parámetro Is uplink to another Branch Extender node **Valores válidos** Yes o No **Valor por omisión** No **Descripción** Este parámetro indica si el nodo adyacente tiene la función de Branch Extender habilitada. Esta pregunta sólo se hace si **Branch Extender** está habilitado en este nodo, se trata de un enlace hacia arriba y dicho enlace es un recurso limitado.
Parámetro Preferred Network Node Server **Valores válidos** Yes o No **Valor por omisión** No **Descripción** Este parámetro indica si este enlace hacia arriba es un servidor de nodos de red que debe utilizarse como servidor de nodos de red del nodo que da soporte a la función Branch Extender y actúa como nodo final. Si se especifica *yes*, este enlace hacia arriba se usará como servidor de nodos de red de este nodo. Esta pregunta sólo se hará si: • **Enabled Branch Extender** está en *yes,* • Esta estación es un nodo de red. • **Branch Uplink** está en *yes* y • las sesiones de CP-CP tienen soporte en este enlace.
Parámetro TG Number **Valores válidos** Si *limited resource* está en Yes, los valores válidos estarán incluidos entre 1 y 20. Si *limited resource* está en No y *link type* (tipo de enlace) es X.25 SVC, los valores válidos estarán incluidos entre 0 y 20. De lo contrario, estarán incluidos entre 0 y 20. **Valor por omisión** Si *limited resource* está en Yes, el valor por omisión será 1. Si *limited resource* está en NO, el valor por omisión será 0. De lo contrario, el valor por omisión es 0. **Descripción** Este parámetro identifica de forma única un TG entre nodos adyacentes.
Parámetro Solicit SSCP session **Valores válidos** Yes o No **Valor por omisión** No Si el parámetro **link station name** (nombre de la estación de enlace) es el mismo que **CP name** (nombre del CP), el valor por omisión será *yes*. **Descripción** Este parámetro indica si este enlace va a solicitar sesiones de SSCP.

Tabla 24 (Página 8 de 9). Lista de parámetros de configuración - Estaciones de enlace - Detalle

Información de los parámetros
Parámetro Enable Host Initiated Dynamic LU Definition **Valores válidos** Yes o No **Valor por omisión** No **Descripción** Este parámetro indica si las LU dependientes se crearán dinámicamente (en oposición a tener que configurarlas). Si se especifica *yes*, las LU se definirán para esta PU a medida que se reciban solicitudes ACTLU (con CV0E). Con esta función, no es necesario configurar las LU para el servidor TN3270E. **Nota:** Esta pregunta sólo se hace si **solicit sscp session** está en *yes*.
Parámetro Local Node ID **Valores válidos** 5 dígitos hexadecimales **Valor por omisión** X'00000' **Descripción** Este parámetro especifica el identificador del nodo local. Esta pregunta sólo se hace si **solicit sscp session** está en *yes*. El id del nodo local debe ser único.
Parámetro Local SAP address **Valores válidos** Cualquier dirección de SAP válida entre X'04' y X'EC'. **Valor por omisión** Valor tomado del puerto **Descripción** Este parámetro especifica la dirección de SAP local. **Notas:** 1. Esta pregunta sólo se visualiza si hay varias PU definidas en el puerto. 2. Si la dirección de SAP local no es la dirección de SAP local principal del puerto, el nombre del puerto y el nombre del SAP se visualizarán al supervisar y en la salida de la visualización de SNMP.
Parámetro Subnet visit count **Valores válidos** De 1 a 255 **Valor por omisión** El valor por omisión se toma del parámetro de nivel de puerto equivalente **Descripción** Este parámetro especifica el valor por omisión del número máximo de subredes que puede atravesar una sesión de varias subredes. **Nota:** Esta pregunta sólo se hace si la función de nodo límite está habilitada en este nodo.

Tabla 24 (Página 9 de 9). Lista de parámetros de configuración - Estaciones de enlace - Detalle

Información de los parámetros
Parámetro Adjacent node subnet affiliation **Valores válidos** 0 (nativa) 1 (no nativa) 2 (negociable) **Valor por omisión** El valor por omisión se toma del parámetro de nivel de puerto equivalente **Descripción** Este parámetro especifica si el nodo adyacente está en la subred APPN nativa del nodo o en una subred APPN no nativa. Un valor de *2* instruye al nodo para que negocie en el momento de activación del enlace para determinar si la estación de enlace adyacente es nativa o no. **Nota:** Esta pregunta sólo se hace si la función de border node está habilitada en este nodo.
Parámetro TG Number **Valores válidos** De 0 a 20 **Valor por omisión** 0 **Descripción** Este parámetro especifica el número de TG para el ATM VC.

Tabla 25 (Página 1 de 5). Lista de parámetros de configuración - Configuración de estación para ATM

Información de los parámetros
Parámetro Virtual Channel Type **Valores válidos** SVC, PVC **Valor por omisión** SVC **Descripción** Este parámetro identifica el tipo de canal ATM como un circuito virtual conmutado (SVC) o un circuito virtual permanente (PVC).
Nota: Los parámetros siguientes son comunes para los SVC y los PVC.
Parámetro Destination ATM Address **Valores válidos** Una serie de 40 caracteres hexadecimales **Valor por omisión** Ninguno **Descripción** Este parámetro especifica la serie de caracteres de 20 bytes que forma la dirección ATM de destino completa.
Parámetro ATM network type **Valores válidos** Campus, Widearea **Valor por omisión** Campus **Descripción** Este parámetro especifica el tipo de red ATM.

Tabla 25 (Página 2 de 5). Lista de parámetros de configuración - Configuración de estación para ATM

Información de los parámetros
Parámetro Shareable connection network traffic **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro especifica si el tráfico de la red de conexiones puede direccionarse en el ATM VC establecido para este TG.
Parámetro Shareable other protocol traffic **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro especifica si puede direccionarse otro tráfico de protocolo de nivel superior en el ATM VC establecido para este TG.
Parámetro LDLC retry count **Valores válidos** De 1 a 255 **Valor por omisión** 3 **Descripción** Este parámetro se usa junto con el período del temporizador LDLC para proporcionar una entrega fiable de XID. La cuenta de reintentos se inicializa cuando un mandato o petición se transmite por primera vez sobre un enlace. Si el período del temporizador LDLC se agota antes de recibir una respuesta, se volverá a transmitir el mandato o solicitud, la cuenta de reintentos disminuirá y el período del temporizador LDLC se reiniciará. Si el temporizador agota el tiempo con la cuenta de reintentos en 0, se presupondrá que el enlace no es operativo.
Parámetro LDLC Timer Period **Valores válidos** De 1 a 255 segundos **Valor por omisión** Para ATM: 1 segundo Para IP: 15 segundos **Descripción** Este parámetro especifica el período de tiempo usado con **LDLC retry count**.
Parámetro VPI **Valores válidos** De 0 a 255 **Valor por omisión** 0 **Descripción** Este parámetro identifica el VPI del PVC de la interfaz.
Parámetro VCI **Valores válidos** De 0 a 65535 **Valor por omisión** 0 **Descripción** Este parámetro identifica el VCI del PVC de la interfaz.

Tabla 25 (Página 3 de 5). Lista de parámetros de configuración - Configuración de estación para ATM

Información de los parámetros
Parámetro Broadband Bearer Class **Valores válidos** Class_A, Class_C, Class_X **Valor por omisión** Class_X **Descripción** Este parámetro especifica la clase de portadora solicitada desde la red ATM. Las clases se definen: **Class A** Velocidad de bit constante (CBR) con requisitos de tiempo de extremo a extremo **Class C** Velocidad de bit variable (VBR) sin requisitos de tiempo de extremo a extremo **Class X** Servicio que permite el tipo de tráfico definido por el usuario y requisitos de tiempo
Parámetro Best Effort Indicator **Valores válidos** Yes, No **Valor por omisión** No **Descripción** Este parámetro indica si se requiere una garantía completa en este SVC. Si el valor de este parámetro es *yes*, los VCC asociados a esta interfaz se asignarán basándose en la anchura de banda disponible.
Nota: Los parámetros siguientes son parámetros de tráfico de reenvío.
Parámetro Forward Peak Cell Rate **Valores válidos** 85% de la velocidad de línea **Valor por omisión** Capacidad efectiva por omisión del puerto/48 **Descripción** Este parámetro indica un límite superior en la velocidad de transmisión de células.
Parámetro Forward Sustained Cell Rate **Valores válidos** Del 1 al 85% de velocidad de línea **Valor por omisión** Capacidad efectiva por omisión del puerto/48 **Descripción** Este parámetro indica un límite superior en la velocidad media de transmisión de células. No puede especificar este parámetro para conexiones de Mejor esfuerzo.
Parámetro Forward Tagging **Valores válidos** Yes, No **Valor por omisión** Yes **Descripción** Este parámetro indica que las células que no cumplen la especificación de tráfico de prioridad 0 de pérdida de células, pero sí que cumplen la especificación de tráfico de prioridad 1 de dicha pérdida se marcan y pueden entrar en la red ATM. No puede especificar este parámetro para conexiones de Mejor esfuerzo.

Tabla 25 (Página 4 de 5). Lista de parámetros de configuración - Configuración de estación para ATM

Información de los parámetros
Parámetro QoS **Valores válidos** CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, donde **CLASS_0** Clase sin especificar. La red no especifica ninguna QoS. **CLASS_1** El rendimiento es comparable al de la línea privada digital actual. **CLASS_2** Clase destinada al vídeo y audio en paquetes para las aplicaciones multimedia y de vídeoconferencia. **CLASS_3** Clase destinada al interfuncionamiento de protocolos orientados a la conexión como, por ejemplo, Frame Relay. **CLASS_4** Clase destinada al interfuncionamiento de protocolos sin conexión como, por ejemplo, IP. **Valor por omisión** CLASS_0 **Descripción** Este parámetro indica qué clase de servicio se proporciona a una conexión virtual ATM. No puede especificar este parámetro para conexiones de Mejor esfuerzo.
Nota: Los parámetros siguientes son parámetros de tráfico hacia atrás.
Parámetro Backward Peak Cell Rate **Valores válidos** Del 1 al 85% de velocidad de línea **Valor por omisión** Tomado de la definición del puerto **Descripción** Este parámetro indica un límite superior en la velocidad de transmisión de células.
Parámetro Backward Sustained Cell Rate **Valores válidos** Del 1 al 85% de velocidad de línea **Valor por omisión** Tomado de la definición del puerto **Descripción** Este parámetro indica un límite superior en la velocidad media de transmisión de células. No puede especificar este parámetro para conexiones de Mejor esfuerzo.
Parámetro Backward Tagging **Valores válidos** Yes, No **Valor por omisión** Yes **Descripción** Este parámetro indica que las células que no cumplen la especificación de tráfico de prioridad 0 de pérdida de células, pero sí que cumplen la especificación de tráfico de prioridad 1 de dicha pérdida se marcan y pueden entrar en la red ATM. No puede especificar este parámetro para conexiones de Mejor esfuerzo.

Tabla 25 (Página 5 de 5). Lista de parámetros de configuración - Configuración de estación para ATM

Información de los parámetros	
Parámetro	QoS
Valores válidos	CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, donde **CLASS_0** Clase sin especificar. La red no especifica ninguna QoS. **CLASS_1** El rendimiento es comparable al de la línea privada digital actual. **CLASS_2** Clase destinada al vídeo y audio en paquetes para las aplicaciones multimedia y de vídeoconferencia. **CLASS_3** Clase destinada al interfuncionamiento de protocolos orientados a la conexión como, por ejemplo, Frame Relay. **CLASS_4** Clase destinada al interfuncionamiento de protocolos sin conexión como, por ejemplo, IP.
Valor por omisión	CLASS_0
Descripción	Este parámetro indica qué clase de servicio se proporciona a una conexión virtual ATM. No puede especificar este parámetro para conexiones de Mejor esfuerzo.
Parámetro	Callout Anonymously
Valores válidos	Yes, No
Valor por omisión	no
Descripción	Este parámetro indica si APPN pasará la dirección de origen cuando llame.

Tabla 26 (Página 1 de 3). Lista de parámetros de configuración - Modificación de las características de los TG

Información de los parámetros	
Parámetro	Cost per connect time
Valores válidos	De 0 a 255
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro expresa el coste relativo de mantener una conexión sobre un TG asociado. Las unidades están definidas por el usuario y normalmente se basan en las tarifas aplicables del recurso de transmisión que se está usando. Los valores asignados deben reflejar el gasto real del mantenimiento de una conexión sobre el TG en relación con el resto de los TG de la red. Un valor de cero significa que las conexiones sobre el TG pueden establecerse sin ningún coste adicional (como en el caso de varios de los recursos no conmutados). Los valores más altos representan costes más altos.

Tabla 26 (Página 2 de 3). Lista de parámetros de configuración - Modificación de las características de los TG

Información de los parámetros
Parámetro Cost per byte **Valores válidos** De 0 a 255 **Valor por omisión** El valor por omisión se toma del parámetro del puerto asociado. **Descripción** Este parámetro expresa el coste relativo de transmitir un byte sobre el TG asociado. Las unidades están definidas por el usuario y el valor asignado debe reflejar los gastos reales de transmisión sobre el TG en relación con el resto de TG de la red. Un valor de cero significa que los bytes pueden transmitirse sobre el TG sin costes adicionales. Los valores más altos representan costos más altos.
Parámetro Security **Valores válidos** • Nonsecure (no fiable) - el resto (por ejemplo, conectado por satélite o situado en un país no fiable). • Public switched network (red conmutada pública) - fiable en el sentido de que la ruta no se determina previamente. • Underground cable (cable subterráneo) - situado en un país fiable (determinado por el administrador de red). • Secure conduit (Conducto fiable) - sin guardar, (por ejemplo, conducto presurizado). • Guarded conduit (Conducto vigilado) - protegido contra las intervenciones físicas. • Encrypted (Cifrado) - se proporciona un cifrado de nivel de enlace. • Guarded radiation (Radiación vigilada) - conducto vigilado que contiene el medio de transmisión; protegido contra la intervención de radiación y la intervención física. **Valor por omisión** El valor por omisión se toma del parámetro del puerto asociado. **Descripción** Este parámetro indica el nivel de seguridad asociado al TG. Si se necesitan atributos de seguridad que no sean los definidos arquitecturalmente, puede usarse una de las características de TG definidas por el usuario para especificar valores adicionales.
Parámetro Propagation delay **Valores válidos** Minimum LAN (LAN mínima) – menos de 480 microsegundos Telephone (Teléfono) – entre 0,48 y 49,152 milisegundos Packet switched (Paquete conmutado) - entre 49,152 y 245,76 milisegundos Satellite (Satélite) - superior a 245,76 milisegundos Máximo **Valor por omisión** El valor por omisión se toma del parámetro del puerto asociado. **Descripción** Este parámetro especifica el rango aproximado del período de tiempo que tarda en propagarse una señal desde un extremo del TG hasta el otro.

Tabla 26 (Página 3 de 3). Lista de parámetros de configuración - Modificación de las características de los TG

Información de los parámetros	
Parámetro	Effective capacity
Valores válidos	2 dígitos hexadecimales del rango incluido entre X'00' y X'FF'
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro especifica la velocidad de transmisión de bits máxima para los enlaces físicos y los lógicos. Observe que la capacidad efectiva de un enlace lógico puede ser inferior a la velocidad de enlace físico. La capacidad efectiva está codificada en una representación de un único byte. Los valores X'00' y X'FF' son casos especiales usados para denotar las capacidades mínima y máxima. El rango de codificación es muy amplio; no obstante, sólo se pueden especificar 256 valores del rango.
Parámetro	First user-defined TG characteristic
Valores válidos	De 0 a 255
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro especifica la primera de tres características adicionales que los usuarios pueden definir para describir los TG de una red.
Parámetro	Second user-defined TG characteristic
Valores válidos	De 0 a 255
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro especifica la segunda de tres características adicionales que los usuarios pueden definir para describir los TG de una red.
Parámetro	Third user-defined TG characteristic
Valores válidos	De 0 a 255
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro especifica la tercera de tres características adicionales que los usuarios pueden definir para describir los TG de una red.

Tabla 27. Lista de parámetros de configuración - Modificación del servidor de LU dependientes

Información de los parámetros	
Parámetro	fully-qualified CP name of primary DLUS
Valores válidos	Una serie con un máximo de 17 caracteres presentados en forma de *IDred.nombreCP*, donde: • *IDred* es un ID de red de 1 a 8 caracteres • *nombreCP* es un nombre de punto de control que tiene entre 1 y 8 caracteres Cada nombre debe respetar las normas siguientes: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 **Nota:** Sigue dándose soporte a nombres de CP plenamente calificados que usan los caracteres especiales @, $ y # del juego de caracteres A; no obstante, estos caracteres no deben usarse en los nombres de CP nuevos.
Valor por omisión	El valor por omisión especificado en el parámetro del nombre del CP plenamente calificado del servidor de LU dependientes primario.
Descripción	Este parámetro especifica el nombre del CP plenamente calificado del servidor de LU dependientes (DLUS) que se va a usar para las solicitudes de entrada de la PU de comunicación de sentido directo asociada a esta estación de enlace.
Parámetro	fully-qualified CP name for backup DLUS
Valores válidos	Una serie con un máximo de 17 caracteres presentados en forma de *IDred.nombreCP*, donde: • *IDred* es un ID de red de 1 a 8 caracteres • *nombreCP* es un nombre de punto de control que tiene entre 1 y 8 caracteres Cada nombre debe respetar las normas siguientes: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 **Nota:** Sigue dándose soporte a nombres de CP plenamente calificados que usan los caracteres especiales @, $ y # del juego de caracteres A; no obstante, estos caracteres no deben usarse en los nombres de CP nuevos.
Valor por omisión	El valor especificado en el parámetro del nombre del CP plenamente calificado por omisión del servidor de LU dependientes.
Descripción	Este parámetro especifica el nombre del CP plenamente calificado del servidor de LU dependientes (DLUS) que se va a usar como elemento de seguridad para la PU de comunicación de sentido directo asociada a esta estación de enlace. Este parámetro permite alterar temporalmente el servidor de seguridad por omisión. No se necesita un elemento de seguridad y el valor NULL indica la ausencia de un servidor de seguridad. Tenga en cuenta que puede especificarse NULL, incluso cuando se ha definido un servidor de seguridad por omisión (borrando el valor por omisión que aparece para este parámetro).

Tabla 28 (Página 1 de 2). Lista de parámetros de configuración - Modificación de las características del LLC

Información de los parámetros
Parámetro Remote APPN SAP **Valores válidos** Múltiplos de cuatro del rango hexadecimal incluido entre X'04' y X'EC'. **Valor por omisión** El valor por omisión se toma del parámetro del puerto asociado. **Descripción** Este parámetro especifica la dirección de SAP de destino (DSAP) del nodo de destino al que se enviarán los datos. El valor de la dirección DSAP aparecerá en la trama LLC para identificar la dirección del punto de acceso de los servicios (SAP) asociada a la estación de enlace de APPN del nodo adyacente.
Parámetro Maximum number of outstanding I-format LPDUs (TW) **Valores válidos** De 1 a 127 **Valor por omisión** El valor por omisión se toma del parámetro del puerto asociado. **Descripción** Este parámetro especifica la opción de transmisión de la línea de mandatos que es la cantidad máxima de LPDU de formato I numeradas secuencialmente cuyo recibo puede haber dejado sin acusar, en algún momento, la estación de enlace.
Parámetro Receive window size **Valores válidos** De 1 a 127 **Valor por omisión** El valor por omisión se toma del parámetro del puerto asociado. **Descripción** Este parámetro especifica la cantidad máxima de LPDU de formato I numeradas secuencialmente y sin acuse de recibo que puede recibir la estación de enlace de LLC de la estación de enlace remota. RW se notifica en tramas SNA XID y tramas IEEE 802.2 XID. El receptor XID debe establecer el TW efectivo en un valor inferior o igual al del RW recibido a fin de evitar alteraciones temporales.
Parámetro Inactivity timer (Ti) **Valores válidos** De 1 a 254 segundos **Valor por omisión** El valor por omisión se toma del parámetro del puerto asociado. **Descripción** Una estación de enlace usa Ti para detectar una condición no operativa en la estación de enlace remota o en el soporte de transmisión. Si no se recibe una LPDU en el intervalo de tiempo especificado por Ti, se transmitirá una LPDU de mandato de formato S con bit de sondeo para solicitar el estado de la estación de enlace remota. La recuperación se basará en el temporizador de respuesta (T1).

Tabla 28 (Página 2 de 2). Lista de parámetros de configuración - Modificación de las características del LLC

Información de los parámetros
Parámetro Reply timer (T1) **Valores válidos** De 1 a 254 semisegundos **Valor por omisión** El valor por omisión se toma del parámetro del puerto asociado. **Descripción** Una estación de enlace usa T1 para detectar un fallo en la recepción de un acuse de recibo necesario o una respuesta de la estación remota de enlace. Cuando T1 expira, la estación de enlace envía una unidad de datos de protocolo de la capa de enlace (LPDU) de mandato de formato S con el bit de sondeo establecido para solicitar el estado de la estación de enlace remota o cualquier LPDU de mandato de formato U que no haya recibido respuesta. La duración de T1 debe tener en cuenta cualquier retardo introducido en las capas inferiores.
Parámetro Maximum number of retransmissions (N2) **Valores válidos** De 1 a 254 **Valor por omisión** El valor por omisión se toma del parámetro del puerto asociado. **Descripción** Este parámetro especifica el número máximo de veces que una LPDU se volverá a transmitir después de la expiración del temporizador de respuesta (T1).
Parámetro Receive acknowledgment timer (T2) **Valores válidos** De 1 a 254 semisegundos **Valor por omisión** El valor por omisión se toma del parámetro del puerto asociado. **Descripción** Este parámetro puede usarse junto con el contador N3 para reducir el tráfico de acuses de recibo. Una estación de enlace usa T2 para retrasar el envío de un acuse de recibo de una LPDU de formato I recibida. T2 se inicia cuando se recibe una LPDU de formato I y se restablece cuando se envía un acuse de recibo en una LPDU de formato I o formato S. Si T2 expira, la estación de enlace deberá enviar un acuse de recibo tan pronto como sea posible. El valor de T2 debe ser inferior al de T1, para asegurarse de que la estación de enlace remota reciba el acuse de recibo retrasado antes de que expire su T1.
Parámetro Acknowledgment needed to increment working window **Valores válidos** De 0 a 127 acuses de recibo **Valor por omisión** El valor por omisión se toma del parámetro del puerto asociado. **Descripción** Cuando la ventana de trabajo (Ww) no es igual al tamaño máximo de la ventana de transmisión (Maximum Transmit Window Size - Tw), este parámetro será la cantidad de LPDU de formato I transmitidas cuyo acuse de recibo debe efectuarse antes de poder incrementar la ventana de trabajo (en 1). Cuando se detecta una congestión, por la pérdida de LPDU de formato I, Ww se establece en 1.

Tabla 29. Lista de parámetros de configuración - Modificación de los valores por omisión de HPR

Información de los parámetros	
Parámetro	Inactivity timer override for HPR (HPR Ti)
Valores válidos	De 1 a 254 segundos
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro especifica el temporizador de inactividad de LLC de alteración temporal de HPR (HPR Ti) que se usará cuando HPR tenga soporte de esta estación de enlace. Este parámetro altera temporalmente el valor que se toma del valor por omisión de alteración temporal del temporizador de inactividad para el parámetro HPR. Este parámetro se impone sobre el valor asignado al parámetro del temporizador de inactividad (Ti) de LLC especificado en el parámetro de modificación de las características del control de enlace lógico (LLC) cuando se da soporte a HPR.
Parámetro	Reply timer override for HPR (HPR T1)
Valores válidos	De 1 a 254 semisegundos
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro especifica el temporizador de respuesta de LLC de alteración temporal de HPR (HPR T1) que se usará cuando HPR tenga soporte de esta estación de enlace. Este parámetro altera temporalmente el valor por omisión tomado del parámetro de alteración temporal del temporizador de respuesta para HPR especificado en los valores por omisión de HPR. Este parámetro se impone sobre el valor asignado al parámetro del temporizador de respuesta (T1) de LLC especificado en el parámetro de modificación de las características del control de enlace lógico (LLC) cuando se da soporte a HPR.
Parámetro	Maximum number retransmission (HPR N2)
Valores válidos	De 1 a 2160000
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro especifica el número máximo de LLC de alteración temporal de HPR de retransmisiones (HPR N2) que se usará cuando HPR tenga el soporte de esta estación de enlace. Este parámetro altera temporalmente el valor por omisión tomado del parámetro del número máximo de retransmisiones para HPR especificado en los valores por omisión de alteración del HPR LLC. Este parámetro se impone sobre el valor asignado al parámetro del número máximo de LLC de retransmisiones (N2) especificado en el parámetro de modificación de las características del control de enlace lógico (LLC) cuando HPR tiene soporte.
Parámetro	Limited Resource Timer
Valores válidos	De 1 a 216000 segundos
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro especifica el valor del temporizador asociado al recurso limitado.

Sintaxis:

add lu-name

Se le solicitará que entre un nombre de estación para asociarlo con esta LU.

También se le solicitará que entre un valor para el parámetro siguiente. El rango del parámetro se mostrará entre paréntesis ( ). El valor por omisión del parámetro se mostrará entre corchetes [ ].

Tabla 30. Lista de parámetros de configuración - Nombre de la LU del nodo final LEN

Información de los parámetros	
Parámetro	fully-qualified LU name
Valores válidos	Nombre de LU plenamente calificado (explícito); nombre de LU genérico (parcialmente explícito; entrada comodín Una serie con un máximo de 17 caracteres presentados en forma de *IDred.nombreLU*, donde: • *IDred* es un ID de red de 1 a 8 caracteres • *nombreLU* es un nombre de punto de control que tiene entre 1 y 8 caracteres Cada nombre debe respetar las normas siguientes: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 **Nota:** Sigue dándose soporte a nombres de LU plenamente calificados que usan los caracteres especiales @, $ y # del juego de caracteres A; no obstante, estos caracteres no deben usarse para nombres de LU nuevos. Para reducir el número de nombres de LU plenamente calificados que debe especificar, puede definir un nombre de LU genérico usando el carácter comodín (*) para representar una parte del nombre de LU (*nombreLU*). También puede definir una entrada comodín usando el carácter comodín como nombre de LU completo.
Valor por omisión	Ninguno
Descripción	Este parámetro especifica los nombres plenamente calificados de las LU asociadas a un nodo final LEN. Los nombres de LU que se especifiquen se registrarán en la base de datos de servicios del directorio del nodo de red. Si no se registra un nombre, el nodo de red no podrá localizar la LU (a menos que dicho nombre sea el mismo que el nombre del CP del nodo final LEN). Debe especificarse un nombre de LU plenamente calificado, formado por un ID de red y el nombre de la LU. El ID de red es el nombre de la red que contiene el nodo final LEN adyacente. El nombre de la LU es el nombre de una unidad lógica a la que se puede acceder a través del nodo final LEN adyacente.

Sintaxis:

add connection-network

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

Tabla 31 (Página 1 de 3). Lista de parámetros de configuración - Red de conexiones - Detalle

Información de los parámetros	
Parámetro	Fully-qualified Connection network name (obligatorio para todas las redes de conexiones definidas)
Valores válidos	Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 **Nota:** Sigue dándose soporte a una red de conexiones existente a la que este nodo desea pertenecer y cuyo nombre tiene los caracteres especiales @, $ y # del juego de caracteres A; no obstante, estos caracteres no deben usarse para nombres de red de conexiones nuevos.
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre plenamente calificado de la red de conexiones que se está definiendo en este nodo de red del direccionador. Dado que este nombre se convierte en el nombre del CP del nodo de direccionamiento virtual (VRN), deberá ser único entre todos los nombres de CP y de LU de la red APPN (igual que en el nombre del punto de control local). Todos los nodos que sean miembros de una red de conexiones determinada deben usar el mismo nombre de VRN. El nombre de VRN plenamente calificado (nombre del CP del VRN) tiene el formato: *IDRed.NombreRedConexión* donde *IDRed* es el identificador de red de este nodo de red del direccionador.
Parámetro	Port type (obligatorio)
Valores válidos	Token-ring (red en anillo), Ethernet, Frame Relay BAN, IP, ATM **Nota:** Si el **port type** es IP, no se especificará ningún **port name** ya que sólo habrá un puerto IP.
Valor por omisión	Ninguno
Descripción	Este parámetro especifica los tipos de puertos que dan conectividad al SATF para la red de conexiones que se está definiendo. Una red de conexiones determinada sólo dará soporte a un tipo de puerto con un conjunto de características.

Tabla 31 (Página 2 de 3). Lista de parámetros de configuración - Red de conexiones - Detalle

Información de los parámetros
Parámetro Port name (obligatorio) **Valores válidos** Nombre del puerto en el que se ha habilitado el direccionamiento de APPN. **Nota:** Si el **port type** es IP, no se especificará ningún **port name** ya que sólo habrá un puerto IP. **Valor por omisión** Ninguno **Descripción** Este parámetro especifica el nombre de un puerto que da conectividad con el recurso de transporte de acceso compartido (SATF) a la red de conexiones que se está definiendo. Todos los puertos definidos para una red de conexiones determinada deben ser del mismo tipo y tener las mismas características. **Nota:** Para un **tipo de puerto** de IP, los puertos adicionales añadidos a una red de conexiones IP pueden ser cualquiera cuyo uso se haya definido para IP. Debe añadirse como mínimo un puerto adicional al puerto IP para la red de conexiones que vaya a usarse. Dado que el puerto IP es un pseudo puerto que siempre se activa cuando el nodo se inicializa, deben añadirse al CN puertos reales sobre los que IP esté definido (TR, ATM, FR, ...). Cuando como mínimo uno de estos puertos reales esté activo, se presupondrá que el enlace de red de conexiones está activo. Cuando todos estos puertos reales estén inactivos, se presupondrá que el enlace de red de conexiones está inactivo.
Parámetro Limited Resource Timer **Valores válidos** De 1 a 216000 segundos **Valor por omisión** 180 **Descripción** Este parámetro especifica el valor del temporizador asociado a un recurso limitado.
Parámetro DLCI number **Valores válidos** De 16 a 1007 **Valor por omisión** Ninguno **Descripción** Este parámetro especifica el número de DLCI usado por el direccionador para conectarse con la red Frame Relay. Cuando el direccionador inicie una conexión con una estación de enlace de la LAN a través de la red de conexiones, usará este número de DLCI para conectarse con la red Frame Relay.

Tabla 31 (Página 3 de 3). Lista de parámetros de configuración - Red de conexiones - Detalle

Información de los parámetros	
Parámetro	BAN destination address (BDA)
Valores válidos	De X'0000 0000 0000' a X'7FFF FFFF FFFF'
Valor por omisión	X'0000 0000 0000'
Descripción	Este parámetro especifica la dirección de destino de la BAN configurada en el nodo que está ejecutando la función BAN. Si está usando el puenteo para conectar la red LAN con la red Frame Relay, especifique X'0000 0000 0000' como valor de este parámetro. En dicho caso, la dirección del MAC indicada a la topología APPN para el TG de la red de conexiones será la dirección BNI MAC codificada en el puerto APPN asociado a esta definición de red de conexiones.

Tabla 32 (Página 1 de 4). Lista de parámetros de configuración - Configuración de la red de conexiones para ATM

Información de los parámetros	
Parámetro	Port name (obligatorio)
Valores válidos	Nombre del puerto en el que se ha habilitado el direccionamiento de APPN.
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de un puerto que da conectividad con el recurso de transporte de acceso compartido (SATF) a la red de conexiones que se está definiendo. Todos los puertos definidos para una red de conexiones determinada deben ser del mismo tipo y tener las mismas características.
Parámetro	fully-qualified connection network name
Valores válidos	Una serie de 3 a 17 caracteres con la forma *IDred.nombreCN*, donde: • *IDred* es un ID de red de 1 a 8 caracteres • *nombreCN* es el nombre de una red de conexiones de 1 a 8 caracteres Cada nombre debe respetar las normas siguientes: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de CN plenamente calificado en el que este TG está definido.
Parámetro	Connection network TG number
Valores válidos	De 1 a 239
Valor por omisión	Ninguno
Descripción	Este parámetro especifica de forma única el número de TG identificando esta conexión del puerto local a la CN. El par compuesto por el nombre de CN y el número de TG debe ser único.

Tabla 32 (Página 2 de 4). Lista de parámetros de configuración - Configuración de la red de conexiones para ATM

Información de los parámetros	
Parámetro	Limited Resource
Valores válidos	Yes o No
Valor por omisión	Yes
Descripción	Este parámetro indica si hay que desactivar este TG cuando no se usa en el tráfico de sesión.
Parámetro	Limited Resource Timer
Valores válidos	De 1 a 2160000 segundos
Valor por omisión	180 segundos
Descripción	Este parámetro indica el límite de tiempo tras el cual debe desactivarse este CN TG cuando no lo usa una sesión de tráfico.
Parámetro	LDLC retry count
Valores válidos	De 1 a 255
Valor por omisión	3
Descripción	Este parámetro se usa junto con el período del temporizador LDLC para proporcionar una entrega fiable de los XID. La cuenta de reintentos se inicializa cuando un mandato o petición se transmite por primera vez sobre un enlace. Si el período del temporizador LDLC se agota antes de recibir una respuesta, se volverá a transmitir el mandato o solicitud, la cuenta de reintentos disminuirá y el período del temporizador LDLC se reiniciará. Si el temporizador agota el tiempo con la cuenta de reintentos en 0, se presupondrá que el enlace no es operativo.
Parámetro	LDLC Timer Period
Valores válidos	De 1 a 255 segundos
Valor por omisión	Para ATM: 1 segundo Para IP: 15 segundos
Descripción	Este parámetro especifica el período de tiempo usado con **LDLC retry count**.

Tabla 32 (Página 3 de 4). Lista de parámetros de configuración - Configuración de la red de conexiones para ATM

Información de los parámetros
Parámetro Broadband Bearer Class **Valores válidos** Class_A, Class_C, o Class_X **Valor por omisión** Class_X **Descripción** Este parámetro especifica la clase de portadora solicitada desde la red ATM. Las clases se definen: **Class A** Velocidad de bit constante (CBR) con requisitos de tiempo de extremo a extremo **Class C** Velocidad de bit variable (VBR) sin requisitos de tiempo de extremo a extremo **Class X** Servicio que permite el tipo de tráfico definido por el usuario y requisitos de tiempo
Parámetro Shareable Regular Network traffic **Valores válidos** Yes o No **Valor por omisión** Yes, si se trata de un CN de mejor esfuerzo. De lo contrario, no. **Descripción** Este parámetro especifica si el tráfico de este TG de la red de conexiones puede direccionarse en un ATM VC establecido para un TG regular u otro CN TG.
Parámetro Shareable other protocol traffic **Valores válidos** Yes o No **Valor por omisión** No **Descripción** Este parámetro especifica si el ATM VC establecido para este CN TG puede compartirse con otros protocolos de nivel superior del direccionador.
Nota: Los parámetros siguientes son parámetros de tráfico de reenvío.
Parámetro Forward Peak Cell Rate **Valores válidos** Del 1 al 85% de velocidad de línea **Valor por omisión** Tomado de la definición del puerto **Descripción** Este parámetro indica un límite superior en la velocidad de transmisión de células.
Parámetro Forward Sustained Cell Rate **Valores válidos** Del 1 al 85% de velocidad de línea **Valor por omisión** Tomado de la definición del puerto **Descripción** Este parámetro indica un límite superior en la velocidad media de transmisión de células.

Tabla 32 (Página 4 de 4). Lista de parámetros de configuración - Configuración de la red de conexiones para ATM

Información de los parámetros	
Parámetro	Forward Tagging
Valores válidos	Yes o No
Valor por omisión	Yes
Descripción	Este parámetro indica que las células que no cumplen la especificación de tráfico de prioridad 0 de pérdida de células, pero sí que cumplen la especificación de tráfico de prioridad 1 de dicha pérdida se marcan y pueden entrar en la red ATM.
Parámetro	QoS
Valores válidos	CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, donde **CLASS_0** Clase sin especificar. La red no especifica ninguna QoS. **CLASS_1** El rendimiento es comparable al de la línea privada digital actual. **CLASS_2** Clase destinada al vídeo y audio en paquetes para las aplicaciones multimedia y de vídeoconferencia. **CLASS_3** Clase destinada al interfuncionamiento de protocolos orientados a la conexión como, por ejemplo, Frame Relay. **CLASS_4** Clase destinada al interfuncionamiento de protocolos sin conexión como, por ejemplo, IP.
Valor por omisión	CLASS_3
Descripción	Este parámetro indica qué clase de servicio se proporciona a una conexión virtual ATM.

Tabla 33 (Página 1 de 3). Lista de parámetros de configuración - Características de los TG (red de conexiones)

Información de los parámetros	
Parámetro	Cost per connect time
Valores válidos	De 0 a 255
Valor por omisión	0
Descripción	Este parámetro expresa el coste relativo de mantener una conexión sobre un TG asociado. Las unidades están definidas por el usuario y normalmente se basan en las tarifas aplicables del recurso de transmisión que se está usando. Los valores asignados deben reflejar el gasto real del mantenimiento de una conexión sobre el TG en relación con el resto de los TG de la red. Un valor de cero significa que las conexiones sobre el TG pueden establecerse sin ningún coste adicional (como en el caso de varios de los recursos no conmutados). Los valores más altos representan costes más altos.

Tabla 33 (Página 2 de 3). Lista de parámetros de configuración - Características de los TG (red de conexiones)

Información de los parámetros
Parámetro Cost per byte **Valores válidos** De 0 a 255 **Valor por omisión** 0 **Descripción** Este parámetro expresa el coste relativo de transmitir un byte sobre el TG asociado. Las unidades están definidas por el usuario y el valor asignado debe reflejar los gastos reales de transmisión sobre el TG en relación con el resto de TG de la red. Un valor de cero significa que los bytes pueden transmitirse sobre el TG sin pagar ningún costo adicional. Los valores más altos representan costes más altos.
Parámetro Security **Valores válidos** Nonsecure (no fiable) - el resto (por ejemplo, conectado por satélite o situado en un país no fiable). Public switched network (red conmutada pública) - fiable en el sentido de que la ruta no se determina previamente. Underground cable (cable subterráneo) - situado en un país fiable (determinado por el administrador de red). Secure conduit (Conducto fiable) - sin guardar, (por ejemplo, conducto presurizado). Guarded conduit (Conducto vigilado) - protegido contra las intervenciones físicas. Encrypted (Cifrado) - se proporciona un cifrado de nivel de enlace. Guarded radiation (Radiación vigilada) - conducto vigilado que contiene el medio de transmisión; protegido contra la intervención de radiación y la intervención física. **Valor por omisión** Nonsecure (no fiable) **Descripción** Este parámetro indica el nivel de seguridad asociado al TG. Si se necesitan atributos de seguridad que no sean los definidos arquitecturalmente, puede usarse una de las características de TG definidas por el usuario para especificar valores adicionales.
Parámetro Propagation delay **Valores válidos** • Minimum LAN (LAN mínima) – menos de 480 microsegundos • Telephone (Teléfono) – entre 0,48 y 49,152 milisegundos • Packet switched (Paquete conmutado) – entre 49,152 y 245,76 milisegundos • Satellite (Satélite) – superior a 245,76 milisegundos Máximo **Valor por omisión** LAN **Descripción** Este parámetro especifica el rango aproximado del período de tiempo que tarda en propagarse una señal desde un extremo del TG hasta el otro.

Tabla 33 (Página 3 de 3). Lista de parámetros de configuración - Características de los TG (red de conexiones)

Información de los parámetros	
Parámetro	Effective capacity
Valores válidos	2 dígitos hexadecimales del rango incluido entre X'00' y X'FF'
Valor por omisión	X'75'
Descripción	Este parámetro especifica la velocidad de transmisión de bits máxima efectiva para este TG de red de conexiones. La capacidad efectiva especifica la velocidad efectiva máxima para los enlaces físicos y los lógicos. La capacidad efectiva está codificada como una representación de un único byte. Los valores X'00' y X'FF' son casos especiales usados para denotar las capacidades mínima y máxima. El rango de codificación es muy amplio; no obstante, sólo se pueden especificar 256 valores del rango.
Parámetro	First user-defined characteristic
Valores válidos	De 0 a 255
Valor por omisión	128
Descripción	Este parámetro especifica la primera de tres características adicionales que los usuarios pueden definir para describir los TG de la red. El valor por omisión de 128 permite definir un subconjunto de TG como más o menos deseable que el resto sin tener que definir valores para todos los TG.
Parámetro	Second user-defined characteristic
Valores válidos	De 0 a 255
Valor por omisión	128
Descripción	Este parámetro especifica la segunda de tres características adicionales que los usuarios pueden definir para describir los TG de la red. El valor por omisión de 128 permite definir un subconjunto de TG como más o menos deseable que el resto sin tener que definir valores para todos los TG.
Parámetro	Third user-defined characteristic
Valores válidos	De 0 a 255
Valor por omisión	128
Descripción	Este parámetro especifica la tercera de tres características adicionales que los usuarios pueden definir para describir los TG de la red. El valor por omisión de 128 permite definir un subconjunto de TG como más o menos deseable que el resto sin tener que definir valores para todos los TG.

Sintaxis:

add mode

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

Tabla 34. Lista de parámetros de configuración - APPN COS - Correlación del nombre de modalidad con el nombre de COS - Detalle

Información de los parámetros
Parámetro Mode name (obligatorio) **Valores válidos** Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 **Nota:** Se sigue dando soporte a un nombre de modalidad existente para una red existente a la cual este nodo de red del direccionador va a pertenecer y que usa los caracteres especiales @, $ y # del juego de caracteres A; no obstante, estos caracteres no deben usarse en los nombres de modalidad nuevos. **Valor por omisión** Ninguno **Descripción** Este parámetro especifica el nombre de modalidad para la correlación de nombre de modalidad con nombre de COS que se está definiendo. Consulte “Opciones de COS” en la página 46 para obtener información adicional sobre la correlación de nombre de modalidad con COS.
Parámetro COS name (obligatorio) **Valores válidos** El nombre de una definición de COS establecida previamente, seleccionado en la lista de nombres de COS definida para este nodo de red del direccionador. **Valor por omisión** Ninguno **Descripción** Este parámetro especifica el nombre de COS que se asociará al nombre de modalidad que se está definiendo para esta correlación de nombre de modalidad con nombre de COS.
Parámetro Session-level pacing Command Line option size **Valores válidos** De 1 a 63 **Valor por omisión** 7 **Descripción** Este parámetro especifica el tamaño de la opción de la línea de mandatos del ritmo del nivel de sesión. Este parámetro tendrá definiciones diferentes según el tipo de ritmo usado: • Para el ritmo de nivel de sesión fijo: – El parámetro del tamaño de la opción de la línea de mandatos del ritmo del nivel de sesión especificará la opción de la línea de mandatos del ritmo de recepción de este nodo. – El valor de este parámetro es la opción sugerida por la línea de mandatos de recepción para el nodo adyacente. • Para el ritmo de nivel de sesión adaptable: – El parámetro del tamaño de la opción de la línea de mandatos del ritmo del nivel de sesión especificará un parámetro de ajuste que se usará como tamaño mínimo para los mensajes de ritmo aislados enviados por los nodos adyacentes.

Sintaxis:

add additional-port-to-connection-network

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

Nota: Puede tener un máximo de 5 puertos por definición de red de conexiones.

Tabla 35. Lista de parámetros de configuración - Puerto adicional APPN a red de conexiones

Información de los parámetros	
Parámetro	Connection network name (fully-qualified) (obligatorio para todas las redes de conexiones definidas)
Valores válidos	Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 **Nota:** Sigue dándose soporte a una red de conexiones existente a la que este nodo desea pertenecer y cuyo nombre tiene los caracteres especiales @, $ y # del juego de caracteres A; no obstante, estos caracteres no deben usarse para nombres de red de conexiones nuevos.
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de la red de conexiones que se está definiendo en este nodo de red del direccionador. Dado que este nombre se convierte en el nombre del CP del nodo de direccionamiento virtual (VRN), deberá ser único entre todos los nombres de CP y de LU de la red APPN (igual que en el nombre del punto de control local). Todos los nodos que sean miembros de una red de conexiones determinada deben usar el mismo nombre de VRN. El nombre de VRN plenamente calificado (nombre del CP del VRN) tiene el formato: *IDRed.NombreRedConexión* donde *IDRed* es el identificador de red de este nodo de red del direccionador.
Parámetro	Port name
Valores válidos	Un nombre único no calificado que genera automáticamente la línea de mandatos. El nombre estará formado por: • TR (red en anillo) • EN (Ethernet)
Valor por omisión	Nombre no calificado generado por la línea de mandatos.
Descripción	Este parámetro especifica el nombre que representa este puerto. Cuando la red de conexiones a la que se está añadiendo el puerto es IP, sólo se podrán añadir al IP CN los puertos para los que se ha definido que IP tenga una interfaz. Debe añadirse al IP CN, como mínimo, un puerto real que tenga definido IP para que pueda activarse y usarse el CN.

Sintaxis:

add focal_point

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

Tabla 36. Lista de parámetros de configuración - Punto focal implícito de APPN

Información de los parámetros	
Parámetro	focal point
Valores válidos	Un nombre de CP plenamente calificado
Valor por omisión	Espacios en blanco
Descripción	Este parámetro especifica el nombre de CP plenamente cualificado que representa este punto focal. El primer punto focal que se añade es el punto focal implícito primario. Pueden añadirse hasta 8 puntos focales implícitos de seguridad adicionales invocando varias veces **Add punto_focal**. Si se saca el punto focal implícito primario de la lista de puntos focales con **Delete focal_point**, el primer punto focal implícito de seguridad, si existe, se convertirá en el punto focal implícito primario.

Sintaxis:

add local-pu

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

Tabla 37 (Página 1 de 2). Lista de parámetros de configuración - PU local de APPN

Información de los parámetros	
Parámetro	Station name
Valores válidos	Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre que representa el enlace entre el DLUR y la PU.
Parámetro	Primary DLUS name
Valores válidos	Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre que se usará para alterar temporalmente el DLUS primario configurado para este nodo.

Tabla 37 (Página 2 de 2). Lista de parámetros de configuración - PU local de APPN

Información de los parámetros
Parámetro Secondary DLUS name **Valores válidos** Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 **Valor por omisión** Ninguno **Descripción** Este parámetro especifica el nombre que se usará para alterar temporalmente el DLUS secundario configurado para este nodo.
Parámetro Autoactivate **Valores válidos** Yes o No **Valor por omisión** Yes **Descripción** Este parámetro especifica si se activa este enlace al arrancar. **Nota:** Si se va a usar el enlace local para una DDDLU PU, deberá especificar *yes* a esta pregunta. Si el enlace local no se establece en activación automática, el primer intento de usar la pu local (es decir, el primer intento de establecer una sesión TN3270) fallará ya que el enlace todavía no estará activado. Aunque este intento falle, hará que el enlace se active y dicho enlace estará disponible en el intento siguiente. Dado que el enlace se activa cuando se establece la sesión de SSCP-PU y esto es cuando el enlace se identifica como enlace DDDLU. No puede establecerse ninguna sesión DDDLU hasta identificar el enlace como enlace DDDLU.
Parámetro Enable Host Initiated Dynamic LU Definition **Valores válidos** Yes o No **Valor por omisión** No **Descripción** Este parámetro indica si las LU dependientes se crearán dinámicamente (en oposición a tener que configurarlas). Si se especifica *yes*, las LU se definirán para esta PU a medida que se reciban solicitudes ACTLU (con CV0E). No es necesario configurar las LU para el servidor TN3270E. **Nota:** Esta pregunta sólo se hace si **solicit sscp session** está en *yes*.

Sintaxis:

add routing_list

Nota: Estas preguntas sólo se hacen si ha configurado el nodo como border node.

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

Existe un cierto número de teclas de método abreviado de edición disponibles para acelerar la modificación de datos existentes en una lista de direccionamientos configurada previamente. Estas teclas pueden usarse cuando le pidan las **Destination LUs** (LU de destino) y los **Routing CPs** (CP de direccionamiento).

- **Intro** solo mantendrá el nombre visualizado actualmente.
- **Barra espaciadora** seguido de **Intro** suprimirá el nombre visualizado actualmente.
- Los datos de caracteres seguidos de **Intro** sustituirán el nombre visualizado actualmente por los datos de caracteres nuevos.
- **9** seguido de **Intro** saltará al final de la lista donde podrá añadir nombres nuevos.
- Al final de la lista, **Intro** solo completará la lista.

Tabla 38 (Página 1 de 3). Lista de parámetros de configuración - Configuración de la lista de direccionamientos

Información de los parámetros	
Parámetro	Routing list name
Valores válidos	Serie de caracteres que puede tener un máximo de 20 caracteres sin espacios en blanco intercalados. La mezcla de mayúsculas y minúsculas y de caracteres especiales está permitida.
Valor por omisión	Espacio en blanco
Descripción	Este parámetro identifica una lista de direccionamientos para que el código de configuración la modifique, liste o suprima. El código operativo no la usa. Puede configurarse un máximo de 255 listas de direccionamientos según la disponibilidad de la memoria de configuración. Se respetan las mayúsculas y minúsculas.
Parámetro	Subnet visit count
Valores válidos	De 1 a 255
Valor por omisión	El valor por omisión se toma del parámetro de nivel de nodo correspondiente
Descripción	Este parámetro especifica cuántas redes debe atravesar un procedimiento de búsqueda de localización.
Parámetro	Dynamic routing list updates
Valores válidos	0 (ninguna) 1 (completa) 2 (limitada)
Valor por omisión	El valor por omisión se toma del parámetro de nivel de nodo correspondiente
Descripción	Este parámetro controla si puede añadirse automáticamente entradas a la lista de direccionamientos de la subred temporal del nodo. Puede establecerse en los mismos valores que el parámetro de nivel de nodo análogo. Si se habilita esta función las entradas añadidas automáticamente sólo se añadirán a la copia temporal de la lista de direccionamientos.

Tabla 38 (Página 2 de 3). Lista de parámetros de configuración - Configuración de la lista de direccionamientos

Información de los parámetros	
Parámetro	Enable routing list optimization
Valores válidos	Yes o No
Valor por omisión	Yes
Descripción	Indica si el nodo tiene permiso para reordenar la lista de direccionamientos de la subred para que las entradas que tengan más posibilidades de tener éxito aparezcan en primer lugar. Este reordenamiento se produce en la copia temporal interna de la lista de direccionamientos.
Parámetro	Destination LU found via this list
Valores válidos	Nombre de LU plenamente calificado con caracteres comodín finales opcionales. Los caracteres legales para un nombre de LU son: A-Z, @, $, #, 0-9. El primer carácter de la parte NETID y de la parte del nombre de LU debe ser no numérico. Cualquiera de los nombres de FQ LU puede terminar con un carácter comodín "*" para designar el rango de LU. Por ejemplo, • * • NETI* • NETI.LUA*
Valor por omisión	Espacio en blanco
Descripción	Este parámetro especifica una lista de LU de destino que pueden encontrarse a través de esta lista de direccionamientos. Esta pregunta se repetirá hasta que termine con una entrada nula. **Notas:** 1. Sólo una única entrada de todas las listas de direccionamientos puede tener un "*" autónomo. Este coincidirá con todas las LU y la lista de direccionamientos que lo contenga será la lista de direccionamientos por omisión. 2. Todos los métodos abreviados de edición descritos al principio de esta tabla están disponibles para acelerar la modificación de una lista de uno o varios CP de direccionamiento configurada anteriormente. 3. No debe duplicarse ningún nombre de LU determinado en otra lista de direccionamientos. 4. El número máximo de nombres de LU que puede especificarse: • 2210 12x - sin soporte • 2210 14x o 24x - 98

Tabla 38 (Página 3 de 3). Lista de parámetros de configuración - Configuración de la lista de direccionamientos

Información de los parámetros	
Parámetro	Routing CP and optional subnet visit count
Valores válidos	Un nombre de CP plenamente calificado formado por un rango incluido entre 1 y 17 caracteres seguido de una cuenta numérica de las visitas a la subred opcional. Los caracteres legales para el nombre de CP son: A-Z, @, $, #, 0-9 El primer carácter de la parte NETID y de la parte del nombre del CP debe ser no numérico. El rango de la cuenta de visitas a la subred opcional está entre 1 y 255 y debe separarse del nombre de CP plenamente calificado por uno o varios espacios.
Valor por omisión	En blanco para un nombre de CP plenamente calificado y establecimiento del nivel de nodo para la cuenta de visitas a la subred.
Descripción	Este parámetro especifica una lista de uno o varios nombres de CP plenamente calificados que pueden saber cómo llegar a una o varias LU de destino configuradas previamente. En cualquier lista de direccionamientos pueden usarse una vez cada una de las palabras clave especiales siguientes: • "*" - equivale a especificar todos los BN nativos, todos los BN no nativos adyacentes y todos los NN no nativos adyacentes. • "*SELF" - equivale a especificar el nombre de CP plenamente calificado del nodo local • "*EBNS" - equivale a especificar todos los BN nativos Esta pregunta se repetirá hasta que termine con una entrada nula. **Notas:** 1. Todos los métodos abreviados descritos al principio de esta tabla están disponibles para acelerar la modificación de una lista de CP de direccionamientos configurada previamente. 2. Si configura "*SELF" como nombre de CP, no podrá configurar el nombre de CP del nodo local. 3. Cualquier lista de direccionamientos determinada puede tener el número máximo de nombres de CP y palabras clave siguiente: • 2210 12x - sin soporte • 2210 14x o 24x - 96 4. En todas las listas de direccionamientos no puede exceder el número de nombres de CP y palabras clave diferentes siguiente: • 2210 12x - sin soporte • 2210 14x o 24x - 96 5. Cualquier nombre de CP o palabra clave determinado no puede aparecer en más de 255 listas de direccionamientos.

Sintaxis:

add cos_mapping_table

Nota: Estas preguntas sólo se hacen si ha configurado el nodo como nodo límite.

Las tablas de correlaciones de COS no tienen soporte en los modelos 2210 12x.

Las teclas de método abreviado de edición especificadas al principio de la tabla de listas de direccionamiento también son válidas en este caso. Úselas para acelerar la modificación de los nombres de CP no nativos y los pares de nombres COS.

Tabla 39 (Página 1 de 2). Lista de parámetros de configuración - Configuración de la tabla de correlaciones de COS

Información de los parámetros
Parámetro COS mapping table name **Valores válidos** Serie de caracteres que puede tener un máximo de 20 caracteres sin espacios en blanco intercalados. La mezcla de mayúsculas y minúsculas y de caracteres especiales está permitida. **Valor por omisión** Espacio en blanco **Descripción** Este parámetro identifica una tabla de correlaciones de COS. Le permite identificar la tabla para que el software de configuración la modifique, liste o suprima. El software operativo no la usa. Puede configurarse un máximo de 255 tablas de correlaciones COS según la disponibilidad de la memoria de configuración. Se respetan las mayúsculas y minúsculas.
Parámetro Non-native NETID or CP name **Valores válidos** Un nombre de CP plenamente calificado con caracteres comodín finales opcionales. Los caracteres legales para el nombre de CP son: A-Z, @, $, #, 0-9 El primer carácter de la parte NETID y de la parte del nombre del CP debe ser no numérico. Cualquiera de los nombres de CP plenamente calificados puede terminar con un carácter comodín "*" para designar el rango de CP. Por ejemplo: • * • NET1* • NET1.LUA* **Valor por omisión** Espacio en blanco **Descripción** Este parámetro especifica una lista de una o varias redes no nativas en las que se aplica esta tabla de correlaciones. Esta pregunta se repetirá hasta que termine con una entrada nula. **Notas:** 1. Sólo una única entrada de todas las listas de direccionamientos puede tener un "*" autónomo. Este coincidirá con todas las redes no nativas y será conocido como la lista de direccionamientos por omisión. 2. No debe duplicarse ningún nombre de CP determinado en otra tabla de correlaciones de COS. 3. El número máximo de CP que puede especificarse: • 2210 12x - sin soporte • 2210 14x o 24x - 98

Tabla 39 (Página 2 de 2). Lista de parámetros de configuración - Configuración de la tabla de correlaciones de COS

Información de los parámetros	
Parámetro	Native and non-native COS-name pair
Valores válidos	Un par de nombres de COS separados por un espacio en blanco. Los caracteres legales son: A-Z, @, $, #, 0-9 El primer carácter de cada nombre debe ser no numérico.
Valor por omisión	Espacio en blanco
Descripción	Este parámetro identifica un par de nombres de COS. Un nombre de COS nativo va seguido del nombre de COS no nativo correspondiente. En cualquier tabla de correlaciones de COS, uno de los pares de nombres de COS puede especificar el nombre del COS no nativo como "*". Esto sirve para designar la entrada por omisión que se usará para todos los nombres de COS no nativos que no coincidan explícitamente con otra entrada de la tabla. Un par de nombres de COS no puede coincidir exactamente con otro par de nombres de COS en una tabla determinada. No obstante, puede usarse un nombre de COS nativo determinado en varias entradas y también es adecuado que un nombre de COS no nativo determinado se use en varias entradas. El software operativo usará la primera entrada que encuentre. Esta pregunta se repetirá hasta que termine con una entrada nula. **Notas:** 1. Los nombres nativo y no nativo no pueden ser idénticos. Sólo deben especificarse los nombres de COS que deban cambiarse. 2. Un nombre de COS nativo o no nativo determinado puede aparecer en varias entradas, pero no puede haber dos pares de nombres de COS idénticos. 3. Cuando haya varios nombres de COS nativos que se correlacionen con el mismo nombre de COS no nativo, el nodo de límite usará la primera de estas correlaciones cuando necesite efectuar una correlación de no nativo a nativo. Asimismo, cuando haya varios nombres de COS no nativos que se correlacionen con un nombre de COS nativo común, el nodo de límite usará la primera de estas correlaciones cuando necesite efectuar una correlación de nativo a no nativo. 4. Cualquier tabla de correlaciones de COS determinada puede tener el número máximo de pares de nombres de COS siguiente: • 2210 12x - sin soporte • 2210 14x o 24x - 46 5. En todas las tablas de correlaciones de COS, no puede usar más del número de nombres de COS nativos siguiente: • 2210 12x - sin soporte • 2210 14x o 24x - 96 Los nombres de COS no nativos no tienen un límite análogo. 6. Ningún nombre de COS nativo puede aparecer más de 255 veces en todas las listas de direccionamientos en general.

Delete

Use el mandato **delete** para suprimir:

Sintaxis:

delete
- port *nombre-puerto*
- link *nombre_estación_enlace*
- lu-name *nombre_lu*
- connection-network *nombre-red-conexión*
- additional-port-to-connection-network *nombre-puerto-cn*
- mode *nombre*
- focal_point *nombre-punto-focal*
- local-pu
- routing_list *nombre lista direccionamientos*
- cos_mapping_table *nombre tabla correlación*

List

Use el mandato **list** para hacer una lista de:

Sintaxis:

list
- all
- node
- traces
- management
- hpr
- dlur
- port *nombre del puerto*
- link station *nombre estación enlace*
- lu name *nombre lu*
- mode name *nombre modalidad*
- connection network *nombre red conexión*
- focal_point
- routing_list *nombre lista direccionamientos*
- cos_mapping_table *nombre tabla correlación*

Activate_new_config

Use el mandato **activate_new_config** para leer la configuración en la memoria no volátil.

Sintaxis:

ac**tivate_new_config**

TN3270E

Tabla 40. Resumen de los mandatos de configuración de TN3270E

Mandato	Función	Consulte página:
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxv.	
Set	tn3270e	197
Add	Añade o actualiza los elementos siguientes:	
	implicit-pool	200
	lu	202
	mapping	203
	port	205
Delete	Suprime los elementos siguientes: • implicit-pool • lu • mapping • port	206
List all	Lista la memoria de configuración	208
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxvi.	

Sintaxis:
set

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

Tabla 41 (Página 1 de 3). Lista de parámetros de configuración - Establecimiento de TN3270E

Información de los parámetros	
Parámetro	Enable TN3270E Server
Valores válidos	Yes o No
Valor por omisión	Yes
Descripción	Este parámetro especifica si se habilitará el soporte al servidor TN3270E.

Tabla 41 (Página 2 de 3). Lista de parámetros de configuración - Establecimiento de TN3270E

Información de los parámetros
Parámetro TN3270E Server IP Address **Valores válidos** Cualquier dirección IP **Valor por omisión** Ninguno **Descripción** Este parámetro es la dirección IP asociada al servidor TN3270E.
Parámetro Port number **Valores válidos** De 1 a 65535 **Valor por omisión** 23 **Descripción** Este parámetro especifica el número de puerto asociado al servidor de TN3270E.
Parámetro Enable Client IP address to LU name mapping? **Valores válidos** Yes o No **Valor por omisión** No **Descripción** Este parámetro especifica si se produce la correlación de dirección IP de cliente con nombre de LU.
Parámetro Default pool name **Valores válidos** Cualquier serie alfanumérica de 1 a 8 caracteres **Valor por omisión** PUBLIC **Descripción** Este parámetro especifica el nombre de la agrupación por omisión. Esta agrupación se usa cuando los clientes de TN3270 se conectan y no especifican un nombre de agrupación/LU.
Parámetro NetDisp Advisor Port Number **Valores válidos** De 1 a 65535 **Valor por omisión** 10008 **Descripción** Este parámetro establece el número de puerto de Network Dispatcher Advisor.
Parámetro Keepalive type **Valores válidos** **0** Ninguno **1** Timing mark (Marca de temporización) **2** NOP **Valor por omisión** 0 **Descripción** Este parámetro especifica el tipo de Keepalive. El tipo de Keepalive que corresponde a *Timing mark* requiere respuestas del cliente dentro del plazo de tiempo especificado con el parámetro **Timer** (Temporizador). El tipo de Keepalive *NOP* especifica que el cliente no devolverá una respuesta al mensaje Keepalive. La notificación de que el cliente ya no está allí proviene de TCP.

Tabla 41 (Página 3 de 3). Lista de parámetros de configuración - Establecimiento de TN3270E	
Información de los parámetros	
Parámetro	Frequency
Valores válidos	De 1 a 65535 segundos
Valor por omisión	60
Descripción	Este parámetro especifica la frecuencia con que se envía un mensaje Keepalive al cliente.
Parámetro	Timer
Valores válidos	De 1 a 65536 segundos
Valor por omisión	10
Descripción	Este parámetro establece el valor del temporizador que se usará con la función Keepalive.
Parámetro	Automatic logoff
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro especifica si se habilitará la desconexión automática.
Parámetro	Time
Valores válidos	De 1 a 65535 minutos
Valor por omisión	30
Descripción	Este parámetro establece el tiempo en que puede estar desocupado el enlace TN3270E antes de que se desconecte automáticamente.
Parámetro	IPv4 Precedence
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro establece el valor de precedencia de IPv4, lo que permite la puesta en cola prioritaria de paquetes encapsulados IPv4.

Sintaxis:

add implicit-pool

Este mandato define una agrupación de LU en oposición al mandato **add lu** que añade una LU única. Se le solicitará que entre los valores 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 2). Lista de parámetros de configuración - Añadir TN3270E implícito

Información de los parámetros	
Parámetro	Pool name
Valores válidos	Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	PUBLIC
Descripción	Este parámetro especifica el nombre de la agrupación de LU que se usará cuando los clientes de TN3270 se conecten.
Parámetro	Pool class
Valores válidos	1 ó 2, donde: 1. Estación de trabajo implícita 2. Impresora implícita
Valor por omisión	1
Descripción	Este parámetro especifica el tipo de agrupación de LU.
Parámetro	Station name
Valores válidos	Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre que representa el enlace entre el DLUR y la PU o el enlace de subárea sobre el que fluirán los datos de SNA.
Parámetro	LU Name Mask
Valores válidos	Una serie de 1 a 5 caracteres: • Primer carácter: De la A a la Z, @, $ y # • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	@01LU
Descripción	Este parámetro especifica la máscara que se usará para asegurarse de que los nombres de LU no dupliquen otros nombres de la red. Los nombres de LU se generan añadiendo la dirección NAU al final de la máscara de nombre de la LU. Cuando no se especifica un rango de dirección, se comprobarán las direcciones de NAU de 2 a 253 para ver si la dirección está sin usar. Si la dirección está disponible, se usará. De lo contrario, se intentará la siguiente dirección NAU. Por ejemplo, si la máscara de LU es FRED, los nombres de LU posible son [FRED2, FRED3, ..., FRED253].

Tabla 42 (Página 2 de 2). Lista de parámetros de configuración - Añadir TN3270E implícito

Información de los parámetros
Parámetro LU type **Valores válidos** • 1 - Pantalla 3270 mod 2 • 2 - Pantalla 3270 mod 3 • 3 - Pantalla 3270 mod 4 • 4 - Pantalla 3270 mod 5 • 5 - Impresora 3270 • 6 - Impresora SCS **Valor por omisión** 1 **Descripción** Este parámetro especifica el tipo de LU dependiente para la LU que se está añadiendo.
Parámetro Specify LU address range? **Valores válidos** Yes o No **Valor por omisión** No **Descripción** Este parámetro especifica si desea definir un rango de dirección de LU.

Parámetro LU address range
Valores válidos
Cualquier rango de valores comprendidos entre 2 y 253
Valor por omisión
ninguno
Descripción Este parámetro especifica el rango de dirección de LU.
La dirección de LU puede especificarse usando el formato siguiente:
`límite_dirección_inferior-límite_dirección_superior`
Si no hay ningún guión después del primer valor, se supone que el valor es una dirección de LU única. Pueden entrarse varios rango separados por comas. Por ejemplo, la serie siguiente especifica 2 rangos de direcciones y 2 direcciones de LU específicas:
`2-40,56,58,100-250`

Parámetro Number of implicit workstation definitions **Valores válidos** De 1 a 253 **Valor por omisión** 1 **Descripción** Este parámetro especifica el número de LU dependientes que se añadirán a la agrupación implícita.

add lu

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

Tabla 43 (Página 1 de 2). Lista de parámetros de configuración - Añadir LU TN3270E

Información de los parámetros
Parámetro LU name **Valores válidos** Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z, @, $ y # • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 **Valor por omisión** Ninguno **Descripción** Este parámetro especifica el nombre de LU de la LU dependiente que se está definiendo.
Parámetro NAU address **Valores válidos** De 2 a 254 **Valor por omisión** Ninguno **Descripción** Este parámetro especifica la dirección NAU de la LU que se está definiendo.
Parámetro Station name **Valores válidos** Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 **Valor por omisión** Ninguno **Descripción** Este parámetro especifica el nombre que representa el enlace entre el DLUR y la PU definido usando el mandato **add local-pu** o el enlace de subárea sobre el que fluirán los datos de SNA.
Parámetro Class **Valores válidos** **1** Estación de trabajo explícita **2** Estación de trabajo implícita **3** Impresora explícita **4** Impresora implícita **Valor por omisión** 1 **Descripción** Este parámetro especifica la clase de LU.
Parámetro LU type **Valores válidos** • 1 — Pantalla 3270 mod 2 • 2— Pantalla 3270 mod 3 • 3 — Pantalla 3270 mod 4 • 4 — Pantalla 3270 mod 5 • 5 — Impresora 3270 • 6 — Impresora SCS **Valor por omisión** 1 **Descripción** Este parámetro especifica el tipo de LU dependiente para la LU que se está añadiendo.

Tabla 43 (Página 2 de 2). Lista de parámetros de configuración - Añadir LU TN3270E	
Información de los parámetros	
Parámetro	Implicit pool name
Valores válidos	Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z, < • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	<DEFLT>
Descripción	Este parámetro especifica el nombre de la agrupación implícita que se usará en la definición de la LU. Sólo se hace esta pregunta si *class* es una estación de trabajo o una impresora implícita.
Parámetro	Define an associated printer
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro especifica si desea definir una impresora asociada.
Parámetro	Associated printer name
Valores válidos	Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z, @, $ y # • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de la impresora asociada.
Parámetro	Associated printer NAU address
Valores válidos	De 2 a 254
Valor por omisión	Ninguno
Descripción	Este parámetro especifica la dirección NAU para la definición de LU de la impresora asociada.

Sintaxis:

add map

Este mandato añade una correlación de dirección IP de cliente con nombre de LU. Se le solicitará que entre los valores para los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis ( ). El valor por omisión del parámetro se mostrará entre corchetes [ ].

Se aplican las normas de correlación siguientes:

- Si una definición de correlación contiene una máscara de subred completa (255.255.255.255) que indica que la entrada es para un cliente específico y el cliente no solicita una LU/agrupación específica, podrá intentarse 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 intentarán las entradas de la agrupación de la definición de correlación. No puede crear una definición que corre-

lacione una subred con una LU específica. Debe correlacionar la subred con una agrupación.

- En el caso de las LU individuales de estaciones de trabajo con impresoras asociadas, sólo es necesario que esté en la definición de correlación la LU de la estación de trabajo.
- Si se recibe una solicitud de conexión de un cliente y no hay entradas de correlación que coincidan, se rechazará la solicitud.
- Puede añadirse una mezcla de tipos de LU y agrupaciones a una correlación determinada. El recurso seleccionado se basará en el tipo de solicitud de conexión. El orden seguido en la definición de los recursos en la correlación será el seguido para elegir el recurso para una solicitud de conexión determinada.
- El nombre de LU no puede correlacionarse con la correlación de dirección IP de red.

Nota: Cuando un cliente se conecta mientras está habilitada la correlación, el servidor empezará a ejecutar AND de la dirección IP del cliente con la máscara de subred de cada correlación secuencial. La coincidencia más larga entre la dirección IP del cliente de entrada y la definición de correlación determinará qué definición de correlación se intentará primero. Si están utilizándose todos los recursos elegibles de la definición de correlación, se buscará de nuevo en las definiciones de correlaciones para encontrar la siguiente coincidencia más específica.

Tabla 44 (Página 1 de 2). Lista de parámetros de configuración - Añadir correlación de TN3270E

Información de los parámetros	
Parámetro	Client IP address or Network address
Valores válidos	Cualquier dirección IP válida
Valor por omisión	0.0.0.0
Descripción	Este parámetro especifica la definición de dirección IP del cliente o de correlación de red que debe añadirse.
Parámetro	Client IP address or Network address Mask
Valores válidos	Cualquier máscara de dirección IP válida
Valor por omisión	0.0.0.0
Descripción	Este parámetro especifica la definición de la máscara de dirección IP del cliente o la correlación de red que debe añadirse.

Tabla 44 (Página 2 de 2). Lista de parámetros de configuración - Añadir correlación de TN3270E

Información de los parámetros	
Parámetro	Pool name/LU name
Valores válidos	Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica un nombre de LU o un nombre de agrupación que se correlacionará con la dirección IP. El nombre de LU sólo puede correlacionarse con una dirección de sistema principal. Si la máscara es una máscara de red, el nombre especificado deberá ser un nombre de agrupación.

Sintaxis:

add port

Este mandato especifica el puerto adicional que el servidor de TN3270E escuchará. Se le solicitará que entre los valores para los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis ( ). El valor por omisión del parámetro se mostrará entre corchetes [ ].

Tabla 45 (Página 1 de 2). Lista de parámetros de configuración - Añadir puerto de TN3270E

Información de los parámetros	
Parámetro	Port number
Valores válidos	De 1 a 65536
Valor por omisión	ninguno
Descripción	Este parámetro especifica el número de puerto que debe añadirse.
Parámetro	Support TN3270E?
Valores válidos	Yes o No
Valor por omisión	Yes
Descripción	Este parámetro especifica si el puerto añadido negociará para ser un servidor de TN3270E. Si no es un servidor de “E”, no dará soporte a las solicitudes de impresión o del sistema.
Parámetro	Pool name
Valores válidos	Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de la agrupación asociada a este puerto. A los clientes que se conecten con este puerto y no especifiquen ningún nombre de LU o de agrupación, se les asignará una LU de esta agrupación.

Tabla 45 (Página 2 de 2). Lista de parámetros de configuración - Añadir puerto de TN3270E

Información de los parámetros	
Parámetro	Disable Client Filtering for this port?
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro especifica si las conexiones de entrada de este puerto deben usar la función de correlación de la dirección IP del cliente de caja con el nombre de la LU, si está habilitada.

Sintaxis:

delete lu

Este mandato elimina LU TN3270E. Se le solicitará que entre los valores 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 - Suprimir LU de TN3270E

Información de los parámetros	
Parámetro	LU name
Valores válidos	Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z, @, $ y # • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de LU de la LU dependiente que se va a eliminar.

Sintaxis:

delete implicit-pool

Este mandato elimina una agrupación implícita de TN3270E. Se le solicitará que entre los valores para los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis ( ). El valor por omisión del parámetro se mostrará entre corchetes [ ].

Tabla 47 (Página 1 de 2). Lista de parámetros de configuración - Supresión de TN3270E implícita

Información de los parámetros	
Parámetro	Pool name
Valores válidos	Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de la agrupación de LU que se va a suprimir.

Tabla 47 (Página 2 de 2). Lista de parámetros de configuración - Supresión de TN3270E implícita

Información de los parámetros	
Parámetro	Delete entire pool
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro especifica si se va a suprimir toda la agrupación o una entrada específica.
Parámetro	Station name
Valores válidos	Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de la estación que se va a suprimir.

Sintaxis:

delete map

Este mandato elimina una correlación de dirección IP de cliente con nombre de LU. Se le solicitará que entre los valores para los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis ( ). El valor por omisión del parámetro se mostrará entre corchetes [ ].

Tabla 48 (Página 1 de 2). Lista de parámetros de configuración - Suprimir correlación de TN3270E

Información de los parámetros	
Parámetro	Client IP address or Network address
Valores válidos	Cualquier dirección IP válida
Valor por omisión	0.0.0.0
Descripción	Este parámetro especifica la definición de dirección IP del cliente o de correlación de red que debe suprimirse.
Parámetro	Client IP address or Network address Mask
Valores válidos	Cualquier máscara de dirección IP válida
Valor por omisión	0.0.0.0
Descripción	Este parámetro especifica la definición de máscara de dirección IP del cliente o de correlación de red que debe suprimirse.
Parámetro	Delete all entries for this client?
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro especifica si se va a suprimir toda la agrupación o un nombre específico.

Tabla 48 (Página 2 de 2). Lista de parámetros de configuración - Suprimir correlación de TN3270E	
Información de los parámetros	
Parámetro	Pool name
Valores válidos	Una serie de 1 a 8 caracteres: • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de LU o el nombre de agrupación que se va a eliminar.

Sintaxis:

delete port

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

Tabla 49. Lista de parámetros de configuración - Suprimir puerto de TN3270E	
Información de los parámetros	
Parámetro	Port number
Valores válidos	De 1 a 65.536
Valor por omisión	ninguno
Descripción	Este parámetro especifica el número de puerto que debe añadirse.

Sintaxis:

list all

Este mandato lista una configuración de TN3270E.

Supervisión de APPN

Esta sección describe cómo supervisar APPN. Está formada por las secciones siguientes:

- "Acceso a los mandatos de supervisión de APPN"
- "Mandatos de supervisión de APPN" en la página 209

Acceso a los mandatos de supervisión de APPN

Siga el procedimiento siguiente para acceder a los mandatos de supervisión de APPN. Este proceso le dará acceso a un proceso de *supervisión* de APPN.

En el indicador OPCON, entre **talk 5**.

Después de entrar el mandato **talk 5**, el indicador de GWCON (+) aparecerá en el terminal. Si el indicador no aparece cuando entre por primera vez la configuración, pulse de nuevo **Retorno**.

Entre **protocolo APPN**. Por ejemplo:

```
* talk 5
+
+ protocol APPN
```

Mandatos de supervisión de APPN

Esta sección describe los mandatos de supervisión de APPN para supervisar las interfaces de APPN. Entre los mandatos en el indicador de APPN>.

Tabla 50 (Página 1 de 2). Resumen de los mandatos de supervisión de APPN

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 xxv.
Activate	Activa un enlace configurado
Aping	Ejecuta un ping en una dirección
Deactivate	Desactiva un enlace dinámico o configurado
List	Lista: • CP-CP_sessions (sesiones_CP-CP) - muestra información sobre sesiones de CP-CP. • ISR_sessions (sesiones_ISR) - muestra información sobre grupos de transmisión ISR activos. • Session_information (información_sesión) - Si *Save RSCV information for intermediate nodes* está en Yes, muestra el nombre de CP de origen, el nombre de la LU primaria y el nombre de la LU secundaria. • RTP_connections (conexiones_RTP) - muestra información sobre conexiones RTP. • Port_information (información_puerto) - muestra información sobre todos los puertos a menos que se solicite una interfaz determinada. • Link_information (información_enlace) - muestra información sobre todos los enlaces a menos que se solicite una interfaz determinada. • Focal_point (punto_focal) - muestra el punto focal activo actualmente. • Appc - muestra información sobre sesiones de APPC. • Local-link (enlace-local) • Log (anotación cronológica) • Incomplete_locates (localizaciones_incompletas) • DLUR information (información de DLUR) - muestra el estado del DLUR de las comunicaciones en sentido inverso y en sentido directo • Directory Services status (estado de los servicios de directorio) - muestra información estadística resumida sobre los servicios de directorio • Directory Services resources (recursos de los servicios de directorio) - muestra todos los recursos que los servicios de directorio del nodo conocen • Topology (topología) - muestra la lista de TG activos
Memory	Obtiene y muestra información del uso de la memoria de APPN.

Tabla 50 (Página 2 de 2). Resumen de los mandatos de supervisión de APPN

Mandato	Función
Restart	Reinicia APPN
Stop	Detiene APPN
Test	Realiza una prueba de direccionamiento HPR y muestra los resultados
TN3270	Accede al indicador de mandatos TN3270 + desde el que puede verse información sobre la configuración de TN3270. Consulte la Tabla 51 en la página 214.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxvi.

Activate

Use el mandato **activate link** para activar un enlace configurado. Use el mandato **list link** para ver el estado del enlace.

Sintaxis:

ac**tivate link** *nombre_enlace*

Aping

Use el mandato **aping** para enviar un mensaje a otra dirección y esperar una respuesta.

Nota: Cuando APING responda en menos de 1 milisegundo, la velocidad de los datos mostrada aparecerá como "-----".

Sintaxis:

ap**ing** *distintivos nombre_lu*

donde,

distintivos

Especifica las opciones del APING.

-m Nombre de modalidad

Valor por omisión: #INTER

-t Nombre TP

Valor por omisión: APING

-i Cuenta de los envíos y recepciones a emitir

Valor por omisión: 1

-x Cuenta de las conversaciones a ejecutar

Valor por omisión: 1

-y Cuenta de los TP a ejecutar

Valor por omisión: 1

-s Tamaño del paquete

Valor por omisión: 100

-q Lacónico

-b La visualización de fondo va a `talk 2`

nombre_lu

Especifica el nombre de LU plenamente calificado del destino del APING.

Valores válidos: Cualquier nombre de LU plenamente calificado válido

Valor por omisión: Ninguno

Deactivate

Use el mandato **deactivate link** para desactivar un enlace configurado. Use el mandato **list link** para ver el estado del enlace. Los enlaces configurados deben estar inactivos y los enlaces dinámicos deben desaparecer.

Sintaxis:

de**activate link** *nombre_enlace*

Dump

Use el mandato **Dump** para crear un vuelco APPN. Puede usar **Boot config**> en **talk 6** para determinar dónde se guardará el vuelco. El nombre del vuelco será el mismo que el vuelco del direccionador completo con _A.1' concatenado al final. Puede iniciar varios vuelcos. La concatenación se incrementará por cada vuelco. Cuando el nombre del vuelco haya llegado a '_A.5', se restablecerá en '_A.1'.

Sintaxis:

du**mp**

Puede comprobar el tamaño del servidor de vuelcos para saber cuándo acaba el vuelco.

El direccionador sigue ejecutándose mientras se produce el vuelco.

List

Use el mandato **List** para visualizar información sobre la configuración de APPN. El mandato lista:

Sintaxis:

list *nombre*

Mandato	Función
List cp	Muestra una tabla de todas las sesiones de cp.
List isr	Muestra una tabla de todos los grupos de transmisión ISR activos definidos.
List session_info	Muestra el nombre del CP de origen, el nombre de la LU primaria y el de la LU secundaria si *Save RSCV information for intermediate sessions* está en Yes.
List rtp	Muestra una tabla de todas las conexiones RTP.
List port	Muestra una tabla de resumen de todos los puertos.
List port *nombre puerto*	Muestra información detallada sobre el puerto solicitado.
List link	Muestra una tabla de resumen de todos los enlaces.

List link *nombre estación*
Muestra información detallada sobre la estación de enlace requerida.

List focal Muestra el punto focal activo actualmente, si hay uno.

List appc Muestra información sobre sesiones de APPC.

List local_link_information
Muestra información sobre los enlaces locales.

List routing_list Muestra información sobre todas las listas de direccionamientos configuradas.

list log Muestra las últimas 20 entradas del registro de anotaciones cronológicas.

list incomplete_locates
Muestra información sobre las localizaciones a la espera de respuesta.

list dlurinfo Muestra el estado del DLUR de las comunicaciones en sentido inverso y en sentido directo por cada PU dependiente interna y externa.

list dsresource Muestra todos los recursos que los servicios de directorio del nodo conocen.

list ds_status Muestra información estadística resumida sobre los servicios de directorio.

list topology Muestra la lista de TG activos.

Memory

Use el mandato **Memory** para visualizar información sobre el uso de la memoria de APPN.

Sintaxis:

m**emory**

Restart

Use el mandato **Restart** para reiniciar APPN después de que se haya detenido.

Sintaxis:

restart

Stop

Use el mandato **Stop** para que APPN se detenga.

Sintaxis:

s**top**

Test

Use el mandato **test rtp** para realizar una prueba de ruta HPR y mostrar los resultados. Use primero el mandato **list rtp** para determinar el tcid de la conexión RTP que desee probar.

Sintaxis:

te**st rtp** *tcid*

TN3270E

Use el mandato **tn3270e** para acceder al indicador de mandatos `TN3270E>` desde el que podrá visualizar información sobre la configuración de TN3270E. Consulte la Tabla 51.

Sintaxis:

tn**3270e**

Tabla 51. Resumen de los 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 xxv.
List	Lista los elementos siguientes de la memoria de configuración: • Pools • Pools *nombre agrupación* • Status • Connections • Connections *nombre LU* • Connections *dirección IP* • Maps • Ports
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxvi.

Mandato	Función
List pools	Muestra una tabla de agrupaciones en estado activo.
List pools *nombreagrupación*	Muestra detalles del nombre de agrupación específico.
List status	Muestra el estado del servidor de TN3270E.
List connections	Muestra todas las conexiones activas actualmente.
List connections *dirección ip*	Muestra todas las conexiones activas actualmente que se originan en la dirección IP especificada.
List connections *nombre lu/agrupación*	Muestra todas las conexiones que están activas actualmente y asociadas al nombre de LU o de agrupación especificado.
List maps	Muestra la correlación de nombre de LU con la dirección IP del cliente activa en el dispositivo.
List ports	Muestra todos los puertos activos que está escuchando el servidor TN3270E.

Uso de AppleTalk Phase 2

Este capítulo describe los mandatos de configuración de AppleTalk Phase 2 (AP2) e incluye las secciones siguientes:

Procedimientos de configuración básicos

Esta sección indica los pasos iniciales necesarios para activar el protocolo AppleTalk Phase 2 y ejecutarlo. La información sobre cómo efectuar más cambios de configuración se cubre en las secciones de mandatos del presente capítulo. Para que los cambios de configuración nuevos entren en vigor, deberá reiniciarse el direccionador.

Habilitación de parámetros del direccionador

Cuando configure un direccionador para que reenvíe paquetes de AppleTalk Phase 2, deberá habilitar algunos parámetros sin tener en cuenta el número o tipo de interfaces del direccionador. Si varios direccionadores transfieren paquetes de AppleTalk Phase 2, especifique estos parámetros para cada direccionador.

- Habilitación global de AppleTalk Phase 2 - Para empezar, deberá habilitar globalmente el software de AppleTalk Phase 2 usando el mandato de configuración **enable ap2** de éste. Si el direccionador muestra un error en este paso, significa que en la carga no hay software de AppleTalk Phase 2. En dicho caso, póngase en contacto con el representante del servicio al cliente.
- Habilitación de interfaces específicas - A continuación, deberá habilitar interfaces específicas sobre las que AppleTalk Phase 2 enviará paquetes. Use el mandato **enable interface** *interface number* para ello.

  Nota: Cuando habilite AppleTalk sobre ATM, deberá habilitar también las interfaces de LAN emulada específicas sobre las que AppleTalk enviará paquetes. No debe habilitar AppleTalk sobre la interfaz ATM física. El uso de la palabra “interfaz” en el resto del capítulo se refiere a la interfaz de LAN emulada y no a la interfaz física de ATM.
- Habilitación de la suma de comprobación - A continuación, podrá determinar si el direccionador calculará las sumas de comprobación DDP de los paquetes que origine. El software de suma de comprobación no funciona correctamente en algunas implementaciones de AppleTalk Phase 2, por lo que es posible que no desee originar paquetes con sumas de comprobación por cuestiones de compatibilidad con dichas implementaciones. No obstante, por lo general, deseará habilitar la generación de sumas de comprobación. Se comprobará la suma de comprobación de cualquier paquete reenviado con una.

Establecimiento de los parámetros de red

También debe especificar algunos parámetros por cada red e interfaz que envíe y reciba paquetes de AppleTalk Phase 2. Después de especificar los parámetros, use el mandato de listado de la configuración de AppleTalk Phase 2 para ver los resultados de ésta.

- Establezca el rango de red para los direccionadores de germinación - La coordinación de los rangos de red y las listas de zonas para todos los direccionadores de una red se simplifica designando direccionadores específicos como direccionadores de germinación. Los direccionadores de germinación se configuran con el rango de red y la lista de zonas, mientras que a los otros direccionadores se les dan valores nulos. Los valores nulos indican que el direccionador debe solicitar a la red valores de los direccionadores de germinación. Por cada red (segmento) de cada red de AppleTalk interconectada, debe configurarse, como mínimo, una interfaz de direccionador como direccionador de germinación para la red. Por lo general, en una red hay varios direccionadores de germinación por si falla uno de ellos. Además, un direccionador puede ser direccionador de germinación de algunas o todas las interfaces de red. Use el mandato **set net-range** para asignar el rango de red en los direccionadores de germinación.
- Establezca el número del nodo de inicio - Use el mandato **set node** para asignar el número de nodo de inicio para el direccionador. El direccionador hará AARP para este nodo, pero si ya se está usando, se elegirá un nodo nuevo.
- Añada un nombre de zona - Puede añadir uno o varios nombres de zona por cada red del conjunto de redes. Se puede añadir un nombre de zona para una red determinada en cualquier direccionador conectado a dicha red; no obstante, sólo el direccionador de germinación debe contener la información de nombre de zona para una red conectada. Los direccionadores conectados adquieren dinámicamente el nombre de zona de los direccionadores adyacentes usando el protocolo ZIP. Apple recomienda que, para una red determinada, elija el mismo direccionador de germinación para el número de red y el nombre de zona. El nombre de zona no puede configurarse para una red a menos que el número de red también esté configurado. Para añadir un nombre de zona por cada número de red, use el mandato de configuración **add zone** *nombre* de AppleTalk Phase 2.

AppleTalk sobre PPP

AppleTalk sobre PPP tiene dos modalidades, de direccionador completo y de semidireccionador. En la primera modalidad, otros direccionadores AppleTalk pueden ver la red punto a punto. En la modalidad de semidireccionador, otros direccionadores no pueden ver la red punto a punto, pero ésta sigue transmitiendo información de direccionamiento de AppleTalk y paquetes de datos.

Para establecer la red en la modalidad de direccionador completo, dé a cada direccionador del enlace PPP un número de red común, un nombre de zona común y un número de nodo único. Si configura un extremo del enlace PPP con un número de red que no sea cero, también deberá configurar dicho extremo para que tenga un número de nodo que no sea cero y para que tenga un nombre de zona. En dicho caso, el otro extremo del enlace debe tener:

- El mismo número de red y nombre de zona y un número de nodo diferente.

- Los números de nodo y red establecidos en cero. El direccionador se informará de dichos números en el direccionador configurado.

Para establecer la red en la modalidad de semidireccionador, configure los dos direccionadores del enlace PPP para que los números de red y de nodo se establezcan en cero y no se use ningún nombre de zona.

Filtros de zona de AppleTalk 2

El filtro de nombres de zona, aunque no sea obligatorio para AppleTalk, es una función muy útil para la seguridad y administración de grandes conjuntos de redes de AppleTalk. Existen también condiciones para restringir el acceso a redes por números de red.

Información general

AppleTalk está estructurado para que todas las redes se puedan identificar de dos maneras. La primera es un número de red o rango de números de red consecutivos que debe ser único en todo el conjunto de redes. El número de red combinado con el número de nodo identifica, de forma única, cualquier estación final del conjunto de redes.

El segundo identificador de la red es uno o varios ZoneNames (NombreZona). Estas series de ZoneName no son únicas en el conjunto de redes. La estación final se identifica de forma única mediante una serie combinada de **objeto:tipo:serie-ZoneName**.

Un direccionador tiene su primer conocimiento de una red cuando el rango de la red nueva aparece en la actualización de direccionamiento RTMP de un direccionador vecino. A continuación, el direccionador solicita al vecino los ZoneNames de dicha red. Tenga en cuenta que el rango de la red se repite en todas las actualizaciones de RTMP nuevas pero que los ZoneNames sólo se solicitan una vez.

Las estaciones finales obtienen los números de red de los paquetes RTMP de difusión (información de direccionamiento) y, a continuación, eligen un número de nodo. El par de red/nodo somete a AARP (investigación AARP) para ver si otra estación final ya ha reclamado su uso. Si responde otra estación, la estación final elegirá otro par de red/nodo y el proceso se repetirá hasta que no se reciba ninguna respuesta.

¿Por qué filtros de ZoneName?

Cuando la estación final típica de AppleTalk desea usar un servicio (impresora, servidor de archivos) en Apple Internet, primero busca todas las Zones (zonas) disponibles y selecciona una. A continuación, elige un tipo de servicio y solicita una lista de todos los nombres que notifican el tipo en la zona elegida. Este mecanismo hace que surjan varios problemas.

- Un conjunto de redes grandes puede tener varias zonas. Puede presentarse al usuario una larga lista para que elija a ciegas las que necesita (y, por lo tanto, inhibiendo la usabilidad de la lista).
- Es posible que el servidor no quiera estar disponible en toda la red (por razones de seguridad). Si el cliente no puede ver la zona en la que está el servicio, aumentará la seguridad.

- Restringir las zonas visibles de un departamento en relación con el resto de las redes permitirá al administrador dejar que el departamento controle (o no) su propio dominio además de no aumentar la sobrecarga en el resto de las redes (reducción de la administración).

El filtro de los números de red aumenta la seguridad y mejora la administración del conjunto de redes. El filtro de zonas sólo controla el acceso a la red de forma indirecta. Un departamento sin regular puede añadir redes con los mismos nombres de zona pero con números de red nuevos que entren en conflicto con otros departamentos. El filtro de números de red puede usarse para evitar que estas adiciones aleatorias de nombres de zona y de números de red tengan un impacto sobre el resto de la red.

¿Cómo añade filtros?

El direccionador se configura con una lista de zonas excluyente (que bloquea las zonas especificadas) o incluyente (permite únicamente las zonas especificadas) por cada dirección de cada interfaz. La interfaz especificada no volverá a anunciar la información de zonas filtrada en la dirección definida. Si se filtran todas las zonas de una lista de zonas de la red, la información de la red también se filtrará a través de la interfaz.

- Use los mandatos de configuración **add** y **delete** para crear la lista de filtros para una interfaz.
- Use los mandatos de configuración **enable** y **disable** para especificar cómo se aplica la lista de filtros.

  Use mandatos similares para crear filtros de números de red.

Otros mandatos:

Puede usar el mandato `AP2 CONFIG>` **list** para visualizar toda la información de filtro de las interfaces. Además, el mandato **list** acepta un *núm.interfaz* como argumento para que pueda listar información de una única interfaz.

Ejemplos de procedimientos de configuración

Esta sección trata los pasos necesarios para activar AP2 y ejecutarlo. Para obtener información sobre cómo efectuar más cambios de configuración, consulte “Mandatos de configuración de AppleTalk Phase 2” en la página 225. Para que los cambios de configuración entren en vigor, debe reiniciar el direccionador.

Para acceder al entorno de configuración de AP2, entre **protocol ap2** en el indicador `Config>`.

Habilitación de AP2

Cuando configure un direccionador para que reenvíe paquetes de AP2, deberá habilitar algunos parámetros. Si varios direccionadores transfieren paquetes de AP2, especifique estos parámetros por cada direccionador. Para habilitar AP2:

1. Use el mandato **enable ap2** para habilitar globalmente AP2 en el direccionador. Por ejemplo:

   ```
   AP2 config>enable ap2
   ```

2. Habilite las interfaces específicas sobre las que AP2 enviará paquetes. Por ejemplo:

   ```
   AP2 config>enable interface 1
   ```

Configuración de los parámetros de red

Para establecer el direccionador como direccionador de germinación, debe establecer el rango de red, un número de inicio de nodo y, como mínimo, un nombre de zona. Puede configurar algunas interfaces de un direccionador como direccionadores de germinación y dejar otras como direccionadores sin germinación. Debe tener, como mínimo, un direccionador de germinación por cada red AppleTalk y debe configurar varios direccionadores de germinación en la red por si falla uno de ellos.

Nota: No establezca un rango de red o un número de nodo para semidireccionadores.

1. Use el mandato **set net-range** para establecer el rango de red. Por ejemplo:

```
AP2 config>set net-range
          Interface # [0]? 1
First Network range number (1-65279, or 0 to delete) []? 1
Last Network range number (1-165279) []? 5
```

   Entre los mismos valores inicial y final para una red con un único número.

2. Use el mandato **set node-number** para establecer el Starting Node Number (número de nodo de inicio) para la interfaz. El direccionador hará AARP para este nodo. Si ya se está usando el número, el direccionador elegirá un número nuevo. Por ejemplo:

```
  AP2 config>set node-number
  Interface #  [0]? 1
  Node number (1-253, or 0 to delete) []?
1
```

3. Use el mandato **add zone** para añadir uno o varios nombres de zona a la red conectada a la interfaz. Si define un rango de red para una interfaz, también deberá definir los nombres de zonas para la interfaz. Si no ha definido un número de red, no defina nombres de zonas. Por ejemplo:

```
AP2 config>add zone
Interface # [0]? 1
Zone name []? Finance
```

Después de especificar los parámetros, puede usar el mandato **list** en el indicador `AP2 config>` para ver la configuración.

Configuración de filtros de zonas

El filtro de zonas le permite filtrar zonas en las dos direcciones de cada interfaz. Para filtrar los paquetes de entrada, establezca un filtro de entrada. Para filtrar los paquetes de salida, establezca un filtro de salida. La interfaz no volverá a anunciar la información de la zona filtrada en la dirección que defina. Siga los pasos siguientes para establecer un filtro de zona:

1. Añadir filtros de zona a una interfaz. Use el mandato **add zfilter in** para añadir un filtro de zona de entrada a una interfaz. Use el mandato **add zfilter out** para añadir un filtro de zona de salida a una interfaz. Por ejemplo:

```
AP2 config>add zfilter in
          Interface # [0]? 1
Zone name []? Admin
```

2. Habilite los filtros de zona que ha añadido. Esto activará el filtro y los controles, ya sea el filtro incluyente o excluyente. Los filtros incluyentes sólo reenvían la información de zona en dicho filtro. Los filtros excluyentes sólo bloquean la información de zona de dicho filtro. Por ejemplo:

```
AP2 config>enable zfilter in exc
          Interface # [0]? 1
```

A continuación, se muestran algunos ejemplos que explican cómo establecer filtros de zonas en el conjunto de redes que aparece en la Figura 12 en la página 222.

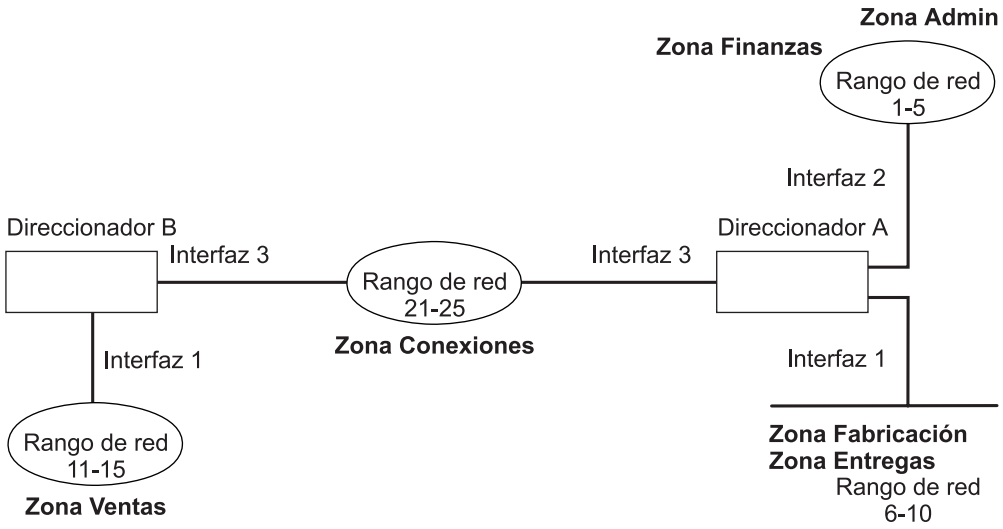


Figura 12. Ejemplo de filtro de zonas

Ejemplo 1

A continuación, se muestra un ejemplo de cómo filtrar la zona de Fabricación en relación con el resto de las redes. Para ello, deberá establecer un filtro de entrada en la interfaz 1 del direccionador A para excluir la zona de fabricación.

1. En el direccionador A, añada un filtro de zonas de entrada para la interfaz 1.

```
AP2 config> add zfilter in
            Interface # [0]? 1
  Zone name []? Manufacturing
```

2. Habilite el filtro de zonas de entrada y conviértalo en excluyente.

```
AP2 config>enable zfilter in exc
            Interface # [0]? 1
```

   Esto hará que la zona de fabricación no entre en el direccionador A, por lo que filtrará la zona en relación al resto del conjunto de redes.

Ejemplo 2

El ejemplo siguiente muestra cómo filtrar la zona de fabricación en la red 11-15, pero permitiendo que esta zona se pueda ver en la red 1-5. Para ello, deberá establecer un filtro de salida en la interfaz 3 del direccionador A para evitar que la información de la zona de fabricación se reenvíe fuera de la interfaz 3. La interfaz seguirá anunciando información de la zona de fabricación en las interfaces 1 y 2 del direccionador A, lo que la hará visible en la red 1-5.

1. Añada un filtro de zona de salida a la interfaz 3.

```
AP2 config>add zfilter out
Interface # [0]? 3
Zone name []? Fabricación
```

2. Habilite el filtro de las zonas de salida y conviértalo en excluyente.

```
AP2 config>enable zfilter out exc
Interface # [0]? 3
```

   Este filtro excluirá la información de la zona de fabricación de la salida de la interfaz 3.

Ejemplo 3

El ejemplo siguiente muestra cómo establecer un filtro para que la zona de administración sea visible en todas las redes y la zona de finanzas no sea visible en el resto del conjunto de redes.

1. Añada un filtro de zonas de entrada a la interfaz 2 del direccionador A.

```
AP2 config>add zfilter in
Interface # [0]? 2
Zone name []? Admin
```

2. Habilite el filtro de zonas de entrada y conviértalo en incluyente.

```
AP2 config>enable zfilter in inc
Interface # [0]? 2
```

   Estableciendo este filtro de entrada como incluyente, sólo se reenviará información de la zona de administración a través de la interfaz 2 al resto del conjunto de redes.

Establecimiento de filtros de red

Los filtros de red son similares a los filtros de zonas, salvo que permiten filtrar toda una red. Para establecer un filtro de red:

1. Añada un filtro de red. Use el mandato **add nfilter in** para añadir un filtro de red de entrada a una interfaz. Use el mandato **add nfilter out** para añadir un filtro de red de salida a una interfaz. Por ejemplo:

```
  AP2 config>add nfilter out
  Interface # [0]? 2
            First Network range number
(decimal) [0]?  11
  Last Network range number (decimal) [0]? 15
```

   El rango de red que entre aquí deberá coincidir con el rango que haya asignado a la red.

2. Habilite el filtro de red que ha añadido y conviértalo en incluyente o excluyente. Los filtros incluyentes sólo reenviarán información de red en dicho filtro. Los filtros excluyentes sólo bloquearán información de red en un filtro y permitirán reenviar el resto de la información de red.

```
AP2 config>enable nfilter in exc
Interface # [0]? 2
```

A continuación, mostramos algunos ejemplos de cómo establecer filtros en el conjunto de redes, tal como se muestra en la Figura 13 en la página 224.

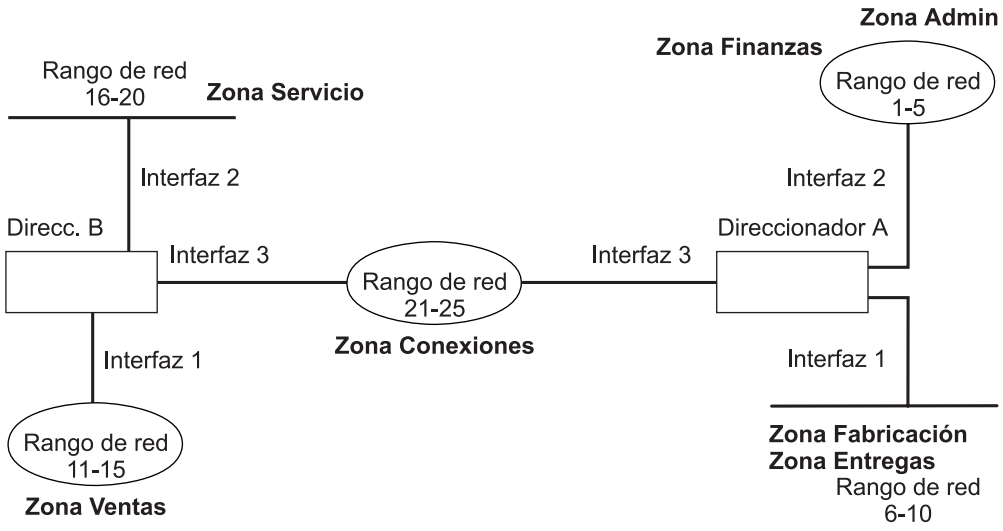


Figura 13. Ejemplo de filtro de red.

Los pasos siguientes muestran cómo filtrar la red 6-10 para que no sea visible a la red 16-20, tal como se muestra en la Figura 13.

1. Añada un filtro de red de salida para la red 6-10 en la interfaz 2 del direccionador B.

```
  AP2 config>add nfilter
out
  Interface # [0]? 2
  First Network range number (decimal) [0]? 6
            Last Network range number
(decimal) [0]?  10
```

2. Habilite el filtro de red de salida como excluyente.

```
  AP2 config>enable nfilter out exc
  Interface # [0]? 2
```

   Este filtro evitará que toda la información de la red 6-10 se reenvía a través de la interfaz 2 a la red 16-20.

Configuración y supervisión de AppleTalk Phase 2

Este capítulo describe los mandatos de configuración y supervisión de AppleTalk Phase 2 (AP2). Está formado por las secciones siguientes:

- "Acceso al entorno de configuración de AppleTalk Phase 2"
- "Mandatos de configuración de AppleTalk Phase 2"
- "Acceso al entorno de supervisión de AppleTalk Phase 2" en la página 234
- "Mandatos de supervisión de AppleTalk Phase 2" en la página 234

Acceso al entorno de configuración de AppleTalk Phase 2

Para acceder al entorno de configuración de AppleTalk Phase 2, entre el mandato siguiente en el indicador `Config>`:

```
Config> ap2
   AP2 Protocol user configuration
   AP2 Config>
```

Mandatos de configuración de AppleTalk Phase 2

Esta sección describe los mandatos de configuración de AppleTalk Phase 2.

Los mandatos de configuración de AppleTalk Phase 2 le permiten especificar parámetros de red para interfaces del direccionador que transmiten paquetes de AppleTalk Phase 2. La información que especifique con dichos mandatos se activará cuando reinicie el direccionador.

Entre los mandatos de configuración de AppleTalk Phase 2 en el indicador `AP2 config>`. La Tabla 52 en la página 226 muestra los mandatos.

Tabla 52. Resumen de mandatos de configuración de AppleTalk Phase 2

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxv.
Add	Añade nombres de zona, filtros de red y filtros de zona a una interfaz.
Delete	Suprime los nombres de zona, interfaces, filtros de red y filtros de zona.
Disable	Inhabilita interfaces, sumas de comprobación, direccionamientos de horizonte dividido, filtros de red o filtros de zona o bien inhabilita globalmente AppleTalk Phase 2.
Enable	Habilita interfaces, sumas de comprobación, direccionamientos de horizonte dividido, filtros de red o filtros de zona o bien habilita globalmente AppleTalk Phase 2.
List	Muestra la configuración actual de AppleTalk Phase 2.
Set	Establece el tamaño de la antememoria, el rango de red y el número de nodo.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxvi.

Add

Use el mandato **add** para añadir el nombre de zona a la lista de zonas de interfaces o bien para añadirlo a la mencionada lista como valor por omisión para la interfaz o para añadir filtros de red o de zona.

Sintaxis:

add zone . . .
defaultzone . . .
nfilter in . . .
nfilter out . . .
zfilter in . . .
zfilter out . . .

zone *núm.interfaz nombrezona*

Añade el nombre de zona a la lista de zonas de interfaces. Si define un número de red para una interfaz, también debe definir los nombres de zonas para la interfaz. Si no ha definido un número de red, no defina nombres de zonas.

Ejemplo:

```
ap2config>add zone
Interface # [0]? 0
Zone name []? Finance
```

defaultzone *núm.interfaz nombrezona*

Añade un nombre de zona por omisión para la interfaz. Si un nodo de la red solicita un nombre de zona que no es válido, el direccionador asignará el nombre de zona por omisión al nodo hasta que se elija otro

nombre de zona. Si añade más de un valor por omisión a una interfaz, el último que añada alterará temporalmente el valor por omisión anterior. Si no añade un valor por omisión, el valor por omisión será el primer nombre de zona añadido usando el mandato **zone**.

Ejemplo:

```
ap2config>add defaultzone
Interface # [0]? 0
Zone name []? Headquarters
```

nfilter in *núm.interfaz núm.primera red núm.última red*

Añade un filtro de red a la entrada en interfaz. El rango de red que entre debe coincidir con el rango de red que establezca para la interfaz. No puede filtrar únicamente una parte de un rango de red. Por ejemplo, si establece un rango de red de 1–10 y configura un filtro para 5–8, el direccionador filtrará el rango completo de red de 1–10.

Ejemplo:

```
ap2config>add nfilter in
           Interface # [0]? 0
           First Network range number (decimal) [0]? 1
           Last Network range number (decimal) [0]? 10
```

nfilter out *núm.interfaz núm.primera red núm.última red*

Añade un filtro de red a la salida de la interfaz. El rango de red que entre debe coincidir con el rango de red que establezca para la interfaz. No puede filtrar únicamente una parte de un rango de red. Por ejemplo, si establece un rango de red de 1–0 y configura un filtro para 5–8, el direccionador filtrará el rango completo de red de 1–10.

Ejemplo:

```
ap2config>add nfilter out
           Interface # [0]? 0
           First Network range number (decimal) [0]? 11
           Last Network range number (decimal) [0]? 20
```

zfilter in *núm.interfaz nombre zona*

Añade un filtro de nombre de zona a la entrada o salida de la interfaz.

Ejemplo:

```
ap2config>add zfilter in
Interface # [0]? 1
Zone name []? Marketing
```

zfilter out *núm.interfaz nombre zona*

Añade un filtro de nombre de zona a la salida de la interfaz.

Ejemplo:

```
ap2config>add zfilter out
Interface # [0]? 0
Zone name []? Corporate
```

Delete

Use el mandato **delete** para suprimir un nombre de zona de la lista de zonas de interfaces, suprimir filtros de red o de nombre de zona o toda la información de AppleTalk Phase 2 de una interfaz.

Sintaxis:

delete zone . . .
nfilter in . . .
nfilter out . . .
zfilter in . . .

zfilter out . . .
interface

zone *núm.interfaz nombrezona*
Suprime un nombre de zona de la lista de zonas de interfaces.

Ejemplo:

```
ap2config>delete zone 2 newyork
```

nfilter in *núm.interfaz núm.primera red núm.última red*
Suprime un filtro de red de la entrada en interfaz. Debe entrar los mismos números de rango de red que ha establecido usando el mandato **add nfilter in**.

Ejemplo:

```
ap2config>delete nfilter in
Interface núm. [0]? 0
First Network range number (decimal) [0]? 1
Last Network range number (decimal) [0]? 12
```

nfilter out *núm.interfaz*
Suprime un filtro de red de la salida de la interfaz. Debe entrar los mismos números de rango de red que ha establecido usando el mandato **add nfilter out**.

Ejemplo:

```
ap2config>delete nfilter out
Interface # [0]? 0
First Network range number (decimal) [0]? 11
Last Network range number (decimal) [0]? 20
```

zfilter in *núm.interfaz nombre zona*
Suprime un filtro de nombre de zona de la entrada en interfaz.

Ejemplo:

```
ap2config>delete nfilter in
Interface # [0]? 1
Zone name []? Marketing
```

zfilter out *núm.interfaz nombre zona*
Suprime un filtro de nombre de zona de la salida de la interfaz.

Ejemplo:

```
delete zfilter out

Interface # [0]? 1
Zone name []? Marketing
```

interface Use este mandato para suprimir una interfaz. Es la única manera de suprimir nombres de zonas que tienen caracteres que no se imprimen.

Ejemplo:

```
ap2config>delete interface 1
```

Disable

Use el mandato **disable** para inhabilitar AP2 en todas las interfaces o en una interfaz especificada, la suma de comprobación, filtros, la conversión APL/AP2 o el direccionamiento de horizonte dividido.

Sintaxis:

disable ap2
checksum
interface . . .

nfilter in . . .
nfilter out . . .
zfilter in . . .
zfilter out . . .
split-horizon-routing . . .

ap2 Inhabilita el reenviador de paquetes de AppleTalk Phase 2 para todas las interfaces.

Ejemplo:

```
ap2config>disable ap2
```

checksum

Especifica que el direccionador no calculará la suma de comprobación en los paquetes que genere. Por lo general, el direccionador efectúa la suma de comprobación de todos los paquetes que reenvía. Este es el valor por omisión.

Ejemplo:

```
ap2config>disable checksum
```

interface *núm.interfaz*

Inhabilita todas las funciones de AP2 en la interfaz de red especificada. La red sigue estando disponible para el resto de los protocolos.

Ejemplo:

```
ap2config>disable interface 2
```

nfilter in *núm.interfaz*

Inhabilita, pero no suprime, los filtros de red de entrada de esta interfaz.

Ejemplo:

```
ap2config>disable nfilter in
Interface # [0]? 2
```

nfilter out *núm.interfaz*

Inhabilita, pero no suprime, los filtros de red de salida de esta interfaz.

Ejemplo:

```
ap2config>disable nfilter out
Interface # [0]? 2
```

zfilter in *núm.interfaz*

Inhabilita, pero no suprime, los filtros de la zona de entrada de esta interfaz.

Ejemplo:

```
ap2config>disable zfilter in
Interface # [0]? 1
```

zfilter out *núm.interfaz*

Inhabilita, pero no suprime, los filtros de la zona de salida de esta interfaz.

Ejemplo:

```
ap2config>disable zfilter out 0
Interface # [0]? 1
```

split-horizon-routing *núm.interfaz*

Inhabilita el direccionamiento de horizonte dividido de esta interfaz. Sólo debe inhabilitarse el direccionamiento de horizonte dividido en las interfaces de Frame Relay que estén en un eje de una red Frame Relay parcialmente dividida. La inhabilitación del direccionamiento de hori-

zonte dividido hace que todas las tablas de direccionamientos se propaguen en esta interfaz.

Ejemplo:

```
ap2config>disable split-horizon-routing 0
```

Enable

Use el mandato **enable** para habilitar la función de suma de comprobación, habilitar una interfaz especificada, habilitar la función de pasarela de AppleTalk 2 o habilitar globalmente el protocolo AppleTalk Phase 2.

Sintaxis:

enable
ap2
checksum
interface . . .
nfilter in . . .
nfilter out . . .
split-horizon-routing . . .
zfilter . . .

ap2 Habilita el reenviador de paquetes de AppleTalk Phase 2 para todas las interfaces.

Ejemplo:

```
ap2config>enable ap2
```

checksum
Especifica que el direccionador calculará la suma de comprobación en los paquetes que genere. El direccionador calcula la suma de comprobación de todos los paquetes de AP2 que reenvía.

Ejemplo:

```
ap2config>enable checksum
```

interface *núm.interfaz*
Habilita el direccionador para que envíe paquetes de AppleTalk Phase 2 sobre interfaces específicas.

Ejemplo:

```
ap2config>enable interface 3
```

nfilter in *exclusive* **o** *exclusive núm.interfaz*
Habilita los filtros de entrada de la red y controla cómo se aplica el filtro a la interfaz. Inclusive (incluyente) reenvía las coincidencias. Exclusive (excluyente) elimina las coincidencias.

Ejemplo:

```
ap2config>enable filter in inc
Interface # [0]? 1
```

nfilter out *exclusive* **o** *exclusive núm.interfaz*
Habilita los filtros de salida de la red y controla cómo se aplica el filtro a la interfaz. Inclusive (incluyente) reenvía las coincidencias. Exclusive (excluyente) elimina las coincidencias.

Ejemplo:

```
ap2config>enable filter out exec
Interface # [0]? 1
```

split-horizon-routing *núm. interfaz*

Habilita el direccionamiento de horizonte dividido en la interfaz. El valor por omisión es *enabled*.

Ejemplo:

```
ap2config>enable split-horizon-routing 1
```

zfilter Habilita los filtros de zona asignados a una interfaz. Debe especificar si el filtro está “in” o “out” y si incluye o excluye. Si incluye, sólo los paquetes que coincidan con el filtro se direccionarán. Si excluye, todos los paquetes que coincidan con el filtro se descartarán.

Ejemplo:

```
ap2config>enable zfilter in inc
Interface # [0]?
```

Ejemplo:

```
ap2config>enable zfilter out exec
Interface # [0]? 0
```

List

Use el mandato **list** para visualizar la configuración actual de AP2. En el ejemplo, el direccionador es un direccionador de germinación en las interfaces 0 y 1

Nota: El mandato **list** acepta un *núm.interfaz* como argumento.

Sintaxis:

list

Ejemplo:

```
ap2config>list
APL2 globally  enabled
Checksumming  disabled
Cache size 500

List of configured interfaces:

 Interface       netrange         /  node        Zone
0               1000-1000         /  1       "SerialLine"(Def)
 Input ZFilters disabled
 Input NFilters (inclusive)
 Output ZFilters disabled
 Output NFilters disabled
 Split-horizon-routing enabled
1               10-19             /  52  "EtherTalk", "Sales"(Def)
 Input ZFilters disabled
 Input NFilters (inclusive)
 Output ZFilters disabled
 Output NFilters disabled
 Split-horizon-routing enabled
2               unseeded net      /  0
 Input ZFilters disabled
 Input NFilters (inclusive)
 Output ZFilters disabled
 Output NFilters disabled
 Split-horizon-routing disabled
```

APL2 globally

Indica si AppleTalk Phase 2 se habilita o inhabilita globalmente.

Checksumming

Indica si se habilita o inhabilita la suma de comprobación.

Cache size
(Tamaño de la antememoria) Número de entradas de antememoria de vía de acceso rápido.

List of configured interfaces
(Lista de interfaces configuradas) Lista cada número de interfaz y su rango de red, número de nodo y nombre o nombres de zona, así como la zona por omisión.

Por cada interfaz también lista si los filtros de zona de entrada y salida y los filtros de red están habilitados o inhabilitados. Si están habilitados, indica si son incluyentes o excluyentes.

Input/output Zfilters
Indica los filtros de zona asignados a una interfaz. Si incluye, sólo los paquetes que coincidan con el filtro se direccionarán. Si excluye, todos los paquetes que coincidan con el filtro se descartarán. Se visualizará el nombre de la zona filtrada. Input (entrada) significa que el filtro se aplica al tráfico que entra en la interfaz. Output (salida) significa que el filtro se aplica al tráfico que sale de la interfaz.

Input/output Nfilters
Indica los filtros de red asignados a una interfaz. Si incluye, sólo los paquetes que coincidan con el filtro se direccionarán. Si excluye, todos los paquetes que coincidan con el filtro se descartarán. Se visualizará el rango de redes filtradas. Input (entrada) significa que el filtro se aplica al tráfico que entra en la interfaz. Output (salida) significa que el filtro se aplica al tráfico que sale de la interfaz.

Split-horizon-routing
Muestra si el direccionamiento de horizonte dividido está habilitado o inhabilitado en cada interfaz.

Set

Use el mandato **set** para definir el tamaño de la antememoria de la vía de acceso rápida o parámetros específicos de AppleTalk Phase 2, incluyendo el rango de red en direccionadores de germinación y el número de nodo.

Sintaxis:

set cache-size . . .
net-range . . .
node . . .

cache-size *valor*
tamaño antememoria corresponde al número total de redes y nodos de AppleTalk que pueden comunicarse simultáneamente a través de este direccionador usando la función de vía de acceso rápida. (Fastpath (vía de acceso rápida) es un método de cálculo previo de cabeceras MAC que sirve para reenviar paquetes con mayor rapidez). El valor por omisión es 500, lo que permite a un máximo de 500 redes y nodos comunicarse simultáneamente a través del direccionador y seguir usando la vía de acceso rápida. Si el número de redes y nodos supera el tamaño de la antememoria, el direccionador seguirá reenviando los paquetes, pero no usará la vía rápida. Los valores válidos del tamaño de la antememoria son: 0 (inhabilitar) de 100 a 10000. Aunque no se recomienda, el establecimiento del tamaño de la antememoria en cero

inhabilita la función de vía de acceso rápida y no se usa memoria para la antememoria. Sólo debe cambiar este valor por omisión en el caso de las redes muy grandes. Cada entrada de tamaño de la antememoria usa 36 bytes de memoria.

Ejemplo:

```
ap2config>set cache-size 700
```

net-range *núm.interfaz primernúm. últimonúm.*

Asigna el rango de red de los direccionadores de germinación usando:

- núm.interfaz - Designa la interfaz del direccionador sobre la que trabajar.
- primernúm. - Asigna el número más bajo del rango de red. Los valores legales están incluidos entre 1 y 65279 (hexadecimal 10xFEFF).
- últimonúm. - Establece el número más alto del rango de red. Los valores legales están incluidos entre el *primernúm.* y 65279.

Una red con un único número tiene el primer valor y el último valor iguales. Si el primer valor es cero, se suprimirá el rango de red para la interface y convertirá la interfaz con “germinación” en una interfaz “sin germinación”. núm.primero y núm.último están incluidos en el rango de red.

Si establece el primer valor en cero en una interfaz Point-to-Point (PPP) permitirá a dicha interfaz funcionar en la modalidad "half-router" (semidireccionador). En dicha modalidad, ninguno de los dos extremos de la red PPP está configurado con un rango de red o una lista de zonas, lo que reduce la cantidad de configuración necesaria. Los dos direccionadores de una red PPP deben funcionar según la misma modalidad.

Nota: Cuando conecte un 2210 a un IBM 6611 usando una interfaz PPP, establezca el 2210 en la modalidad “semidireccionador”, la cual es la *única* modalidad de funcionamiento con soporte de IBM 6611 para comunicaciones AppleTalk sobre una interfaz PPP.

Ejemplo:

```
ap2config>set Net-Range 2 43 45
```

node *núm.interfaz núm.nodo*

Asigna el número de nodo de inicio para el direccionador. El direccionador hará AARP para este nodo, pero si ya se está usando, se elegirá un nodo nuevo. A continuación, explicamos cada uno de los argumentos que se entran después del mandato:

- núm.interfaz - Designa la interfaz del direccionador sobre la que trabajar.
- núm.nodo - Designa el primer número de nodo intentado. Los valores legales están incluidos entre 1 y 253. Un cero como valor núm.nodo suprime el número de nodo de la interfaz y obliga al direccionador a elegir uno de forma aleatoria.

Ejemplo:

```
ap2config>set node 2 2
```

Acceso al entorno de supervisión de AppleTalk Phase 2

Para acceder al entorno de supervisión de AppleTalk Phase 2, entre el mandato siguiente en el indicador + (GWCON):

```
+ protocol ap2
AP2>
```

Mandatos de supervisión de AppleTalk Phase 2

Esta sección describe los mandatos de supervisión de AppleTalk Phase 2 que le permiten ver los parámetros y estadísticas de las interfaces y redes que transmiten paquetes de AppleTalk Phase 2. Los mandatos de supervisión muestran los valores de configuración de los niveles de paquete, trama y físico. También puede visualizar los valores de los tres niveles de protocolo a la vez.

Entre los mandatos de supervisión de AppleTalk Phase 2 en el indicador AP2>. La Tabla 53 muestra los mandatos.

Tabla 53. 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 xxv.
Atecho	Envía solicitudes de eco y espera las respuestas.
Cache	Muestra las entradas de la tabla de antememorias.
Clear Counters	Borra todos los contadores de uso de la antememoria y los de desbordamiento de paquetes.
Counters	Muestra la cuenta de desbordamiento de paquetes AP2 por cada interfaz.
Dump	Muestra el estado actual de la tabla de direccionamientos de todas las redes en internet y sus nombres de zonas asociados.
Interface	Muestra las direcciones actuales de las interfaces.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxvi.

Atecho

El mandato **atecho** envía AppleTalk Echo Requests (solicitudes de eco) a un destino especificado y espera la respuesta. Este mandato puede usarse para verificar la conectividad básica de AppleTalk y aislar los problemas de la red AppleTalk.

Sintaxis:

a**techo** *red_dest nodo_dest*

dest_net Especifica el número de red AppleTalk de destino en decimales. Se trata de un parámetro obligatorio.

dest_node
Especifica el número de nodo AppleTalk de destino en decimales. Se trata de un parámetro obligatorio.

Nota: Para la mayoría de los nodos de AppleTalk, la dirección de red (número de red y número de nodo) se asigna dinámicamente y puede que no esté disponible al instante. No obstante, sigue habiendo varias formas de usar el mandato **atecho** con eficacia:

1. En la mayoría de los casos la dirección de AppleTalk para los nodos del direccionador se configura estáticamente. La conectividad entre los nodos del direccionador es crítica para la conectividad general de la red.
2. Si establece el número de nodo de destino de atecho en 255, puede solicitar todos los nodos del número de red especificado en una red AppleTalk conectada directamente. Las respuestas recibidas indicarán los números de nodo de los nodos. A continuación, podrá usar estos números para ejecutar echo en ellos desde direccionadores distantes a fin de verificar la conectividad.

src_net Número de red AppleTalk de origen. Se trata de un parámetro opcional. Si no se especifica, el direccionador usará su número de red de la interfaz en la interfaz de salida que lleva a la red de destino. Si la interfaz de salida es una interfaz PPP de semidireccionador no numerado, el direccionador usará cualquiera de sus nodos de red de interfaz con la LAN.

src_node Número de nodo AppleTalk de origen. Se trata de un parámetro opcional. Si no se especifica, el direccionador usará su número de nodo de interfaz en la interfaz de salida que lleva a la red de destino.Si la interfaz de salida es una interfaz PPP de semidireccionador no numerado, el direccionador usará cualquiera de sus nodos de red de interfaz con la LAN.

size Número de bytes que deben usarse en las solicitudes de eco de AppleTalk. Se trata de un parámetro opcional. El valor por omisión es 56 bytes.

rate Velocidad de envío de solicitudes de eco de AppleTalk. Se trata de un parámetro opcional. El valor por omisión es un segundo.

Nota: Si entra **atecho** sin parámetros, se le solicitarán el resto de los parámetros. Entre valores para los parámetros obligatorios y entre también valores para los parámetros opcionales o bien acepte los valores por omisión.

Cache

El mandato **cache** muestra información sobre las entradas de tamaño de la antememoria.

Sintaxis:

ca**che**

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
(Destino) Dirección del nodo de AppleTalk (número de nodo/número de red).

Net (Red) Número de la interfaz usada para reenviar al nodo de destino.

Usage (Uso) Número de veces que esta entrada de la antememoria se ha usado en este período de fijación, que es de cinco segundos. Una entrada no usada se suprimirá después de 10 segundos.

Next Hop (Salto siguiente) La dirección de AppleTalk del direccionador del salto siguiente usado para reenviar un paquete al nodo de destino, o Direct (directo) si el nodo de destino está conectado directamente a la interfaz.

Clear Counters

El mandato clear-counters borra todos los contadores de uso de la antememoria y los contadores de desbordamiento de paquetes.

Sintaxis:

clear-counters

Counters

Use el mandato **counters** para visualizar el número de desbordamientos de paquetes en cada red que envía y recibe paquetes de AppleTalk Phase 2. Este mandato muestra el número de veces que la cola de entrada del reenviador de AppleTalk Phase 2 estuvo llena cuando se recibieron paquetes de la red especificada.

Sintaxis:

c**ounters**

Ejemplo: `counters`

```
AP2 Input Packet Overflows

Net            Count
FR/0             0
Eth/0            4
PPP/0           22
```

Dump

Use el mandato **dump** para obtener información de la tabla de direccionamientos sobre las interfaces del direccionador que reenvía paquetes de AppleTalk Phase 2.

Nota: `dump` *núm.interfaz* muestra la parte de la red general e información de zona que es visible en la interfaz mencionada.

Sintaxis:

d**ump**

Ejemplo: `dump`

```
Dest Net    Cost     State   Next hop        Zone
  10-19       0       Dir    0/0       "Ethertalk", "Sales"
  40-49       1      Good    10/13     "Marketing", "CustomerSer",
                                       "TokenTalk"
  20-29       2      Sspct   10/13     "Fuchsia", "Backbone",
                                       "Engineering", "MKTING"

3 entries
```

También puede usar el mandato **dump** con una interfaz específica para mostrar las ruta visibles en dicha interfaz. Puede usar esta función para asegurarse de que los filtros estén configurados correctamente ya que muestra si las redes o zonas filtradas están visibles en una interfaz.

Ejemplo: `dump 0`

```
View for interface 0

Dest net   Cost  State   Next hop   Zone
 214-214   1     Good     152/152   "eth-214"
 153-153   0      Dir               "eth153"
 152-152   0      Dir               "ser152"

3 entries
```

Dest Net Especifica el número de red de destino en decimales.

Cost Especifica el número de saltos del direccionador a esta red de destino.

State Especifica el estado de la entrada de la tabla de direccionamientos. Incluye lo siguiente:

Next hop Especifica el salto siguiente de los paquetes que van a redes que no están directamente conectadas. Para las redes conectadas directamente, se trata del número de nodo 0.

Zone(s) Especifica el nombre comprensible para los humanos de la red. El nombre o nombres de zona se pone entre comillas en caso de que contenga espacios incorporados o caracteres que no se imprimen. Si el nombre de zona contiene caracteres del juego superior al juego de caracteres ASCII de 7 bits (caracteres de 8 bits), el nombre de zona que aparece dependerá de las características del terminal de supervisión.

Interface

Use el mandato **interface** para visualizar las direcciones en todas las interfaces del direccionador en las que esté habilitado AppleTalk Phase 2. Si la interfaz está presente en el direccionador pero está inhabilitada, este mandato mostrará el estado.

Nota: `interface` *núm.interfaz* muestra el filtro activo de la interfaz. Muestra la red, el nodo, la zona por omisión y los filtros activos de una interfaz.

Sintaxis:

interface

Ejemplo: `interface`

```
Interface     Addresses
  PPP/0       0/1 on net 1000-1000  default zone "SerialL ine"
  Eth/0       10/52 on net 10-19    default zone  "Sales"
  PPP/1       0/0 in startup range
  TKR/0       0/0 on net 20-29 default zone "Backbone"
```

También puede entrar el mandato interface seguido de un número de interfaz específico para ver la configuración de AP2 en dicha interfaz.

Ejemplo: **`interface 1`**

```
Eth/0   1/30 on net 1-5   default zone "marketing"

Input Net filters inclusive   1-5
Output Zone filters inclusive "finance"
Output Net filters exclusive  1-5
```

Uso de VINES

Este capítulo describe los mandatos que sirven para configurar el protocolo Banyan VINES e incluye las secciones siguientes:

Nota: Si necesita información más detallada sobre los protocolos de VINES, consulte la publicación de Banyan: *VINES Protocol Definition,* (Definición de protocolos VINES), número de pedido: 003673

Visión general de VINES

VINES sobre protocolos e interfaces de direccionador

El protocolo VINES direcciona paquetes VINES sobre las interfaces y protocolos siguientes:

- PPP Banyan Vines Control Protocol (PPP BVCP)
- Frame Relay
- Ethernet/802.3
- 802.5 Token Ring
- X.25
- Ethernet ATM LAN Emulation Client
- Token-Ring ATM LAN Emulation Client

También da soporte a paquetes en 802.5 Source Routing Bridge (SRB).

El protocolo VINES se implementa en la capa de red (capa 3) del modelo OSI. VINES direcciona paquetes desde la capa de transporte de un nodo a la de transporte de otro nodo. Como VINES direcciona los paquetes a los nodos de destino de estos, los paquetes pasan a través de las capas de red de los nodos intermedios donde se comprueba si tienen errores de bit. Un paquete VINES IP puede contener un máximo de 1500 bytes, incluyendo la cabecera de la capa de red y todos los datos y cabeceras de los protocolos de las capas superiores.

Nodos cliente y de servicio

La red VINES está formada por nodos de servicio y nodos cliente. Un nodo de servicio proporciona servicios de direccionamiento y de resolución de direcciones a los nodos cliente. Un nodo cliente es un vecino físico de la red VINES. Todos los direccionadores son nodos de servicio. Un nodo Banyan puede ser de servicio o cliente.

Cada nodo de servicio tiene una dirección de red de 32 bits y una de subred de 16 bits. IBM 2210 tiene una dirección de red configurable. Esta dirección identifica al direccionador como nodo de red de servicio para Vines. Banyan ha asignado el rango incluido entre 30800000 y 309FFFFF para que IBM lo use en sus

direccionadores. Este direccionador usa el rango incluido entre 30900000 y 3097FFFF.

Nota: Es muy importante que no se asigne la misma dirección de red a dos direccionadores. La dirección de red de un nodo de servicio de Banyan es el número de serie hexadecimal de 32 bits del nodo de servicio. La dirección de subred de todos los nodos de servicio es 1.

Por lo general, la dirección de red de cada nodo cliente es la dirección de red del nodo de servicio de la misma red. No obstante, si un nodo cliente se encuentra en una LAN que tiene más de un nodo de servicio, se le asignará la dirección de red del nodo de servicio que responda primero a la solicitud de asignación de dirección del nodo cliente. La dirección de subred de cada nodo cliente es un valor hexadecimal incluido entre 8000 y FFFE.

Protocolos de capa de red de VINES

Esta implementación de VINES está formada por los cuatro protocolos de capa de red siguientes. Las secciones siguientes describen estos protocolos y sus implementaciones.

- "VINES Internet Protocol (VINES IP)". Direcciona paquetes a través de la red.
- "Routing Update Protocol (RTP)" en la página 242. Distribuye información de topología para dar soporte a los servicios de direccionamiento proporcionados por VINES IP.
- "Internet Control Protocol (ICP)" en la página 245. Proporciona funciones de soporte y diagnóstico a algunas entidades de protocolo de la capa de transporte como, por ejemplo, notificar algunos errores de red y condiciones topológicas.
- "VINES Address Resolution Protocol (VINES ARP)" en la página 246. Asigna direcciones de internet de VINES a nodos cliente que todavía no tengan direcciones.

VINES Internet Protocol (VINES IP)

El protocolo VINES IP direcciona paquetes por la red usando el número de red de destino de la cabecera de VINES IP. VINES IP está formado por una cabecera de red de 18 bytes que sirve de prefijo a cada paquete. La Tabla 54 en la página 241 resume los campos contenidos en la cabecera.

Implementación de VINES IP

Cuando VINES IP recibe un paquete, comprueba que no tenga errores de excepción y tamaño. Un error de tamaño es un paquete con menos de 18 bytes o más de 1500 bytes. Si tiene un error de tamaño, VINES IP descartará el paquete. Un error de excepción es, por ejemplo, una suma de comprobación errónea o una cuenta de saltos que haya expirado.

Si el paquete no tiene errores de excepción o de tamaño, VINES IP comprobará la dirección de destino y reenviará el paquete como sigue:

- Si la dirección de destino es la misma que la dirección de VINES IP local y la suma de comprobación es válida, el nodo local aceptará el paquete.
- Si la dirección de destino es la misma que la dirección de reenvío y la suma de comprobación es válida, VINES IP aceptará el paquete, lo procesará

localmente y comprobará el campo de la cuenta de saltos de la cabecera IP. Si la cuenta de saltos es superior a 0, VINES IP la disminuirá en uno y volverá a reenviar el paquete a todos los soportes locales salvo al que recibió el paquete.

- Si la dirección de destino no es la misma que la dirección de VINES IP local o la dirección de difusión, VINES IP consultará las tablas de direccionamientos para saber cuál es el salto siguiente. Si la cuenta de saltos está en 0, VINES IP descartará el paquete. De lo contrario, disminuirá dicha cuenta en uno y reenviará el paquete al salto siguiente.

  Si la dirección de VINES IP de destino no está en la tabla de direccionamientos y se ha establecido el bit de error en el campo de control del transporte, VINES IP eliminará el paquete y enviará al origen, un mensaje indicando que es imposible llegar al destino. Si el bit de error del campo de control del transporte no está establecido, VINES IP descartará el paquete y no enviará ningún mensaje al origen.

Tabla 54 (Página 1 de 2). Resumen de los campos de la cabecera de Vines IP

Campo de la cabecera de VINES IP	**núm. de bytes**	**Descripción**
Checksum (suma comprob.)	2	Detecta una corrupción de error de bits en el paquete.
Packet Lenght (long. paq.)	2	Indica el número de bytes del paquete, incluyendo los datos y la cabecera de VINES IP.

Tabla 54 (Página 2 de 2). Resumen de los campos de la cabecera de Vines IP

Campo de la cabecera de VINES IP	núm. de bytes	Descripción
Transport Control (contr. trans.)	1	Está formado por los cinco subcampos siguientes: **Class** (Clase) Determina el tipo de nodos a los que se envían los paquetes de difusión de VINES. **Error** Si el bit de error está establecido, cuando no se puede direccionar un paquete a un nodo cliente o un nodo de servicio, se envía un paquete de notificación de excepción a la entidad de protocolo de la capa de transporte. **Metric** (Métrica) Solicita que el nodo de servicio del nodo cliente de destino indique al origen un coste de direccionamiento desde el nodo de servicio al nodo cliente de destino. **Redirect** (Redireccionar) Indica si el paquete contiene un mensaje RTP que especifica una ruta mejor. **Hop Count** (Cuenta de saltos) Especifica el rango por el que puede viajar un paquete. El rango de la cuenta de saltos puede estar incluido entre 0x0 y 0xf.
Protocol Type (Tipo prot.)	1	Especifica el protocolo de la capa de red VINES del paquete como VINES IP, RTP, ICP o VINES ARP.
Destination Network Number (Núm. red dest.)	4	Número de red de 4 bytes de la dirección VINES IP del destino.
Destination Subnetwork Number (Núm. subred dest.)	2	Número de subred de 2 bytes de la dirección VINES IP del destino.
Source Network Number (Núm. red origen)	4	Número de red de 4 bytes de la dirección VINES IP de origen.
Source Subnetwork Number (Núm. subred origen)	2	Número de subred de 2 bytes de la dirección VINES IP de origen.

Routing Update Protocol (RTP)

RTP reúne y distribuye información de direccionamiento que VINES IP usa para calcular rutas en toda la red. RTP habilita a cada direccionador para que difunda periódicamente tablas de direccionamientos a todos los vecinos. A continuación, el direccionador determina el vecino de destino que usará para direccionar el paquete.

Los nodos de servicio mantienen dos tablas: una tabla de direccionamientos y otra de vecinos. Ambas tablas tienen temporizadores que dan una antigüedad a su contenido para poder eliminar las entradas que hayan quedado anticuadas. Las actualizaciones de direccionamientos para las interfaces X.25 se efectúan cuando se produce un cambio en la base de datos de direccionamientos, por ejemplo, cuando un nodo se activa o desactiva o cuando se producen cambios métricos.

Tabla de direccionamientos

La tabla de direccionamientos contiene información sobre los nodos de servicio. La Figura 14 muestra una tabla de direccionamientos de ejemplo. Después de la figura, se describen los campos contenidos en la tabla.

```
Net Address  Next Hop Nbr Addr Nbr Intf   Metric   Age (secs)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

  S  30622222       30622222:0001    Eth/0       20       30

  H  0027AA21       0027AA21:0001    Eth/1       2        120

  P  0034CC11       0034CC11:0001    X.25/0      45       0

  3 Total Routes


S ⇒ Entry is suspended,  H ⇒ Entry is in Hold-down,
P ⇒ Entry is permanent
```

Figura 14. Tabla de direccionamientos de ejemplo

Descripción de campos de la tabla de direccionamientos

Net Address
(Dirección de la red) La dirección de la red es un número de 32 bits único. Si delante del campo de dirección de la red se encuentra una S, una H o una P, los significados serán los siguientes:

S Indica que el nodo de servicio está suspendido y se anuncia durante 90 segundos que está desactivado. Después de este tiempo, el direccionador elimina la entrada correspondiente a este nodo de la tabla de direccionamientos.

H Indica que el nodo de servicio está retenido y se anuncia durante 2 minutos que está desactivado. Después de este tiempo, el direccionador anunciará que el nodo de servicio está operativo. Si un nodo de servicio está suspendido y recibe un paquete RTP, el nodo de servicio entrará en estado de retención.

P Indica que la interfaz X.25 entra en estado permanente durante 4-1/2 minutos después de la inicialización. Después de este tiempo, el vecino entrará en dicho estado y su edad permanecerá en 0 mientras se encuentre así. Si la interfaz X.25 se desactiva, se eliminará la entrada de la tabla de direccionamientos.

Next Hop Nbr Addr
(Dir. vecino salto siguiente) Dirección del nodo de servicio vecino que es el salto siguiente de la vía de acceso de menos costo a la red.

Nbr Intf
(Núm. intf.) El soporte al que el nodo de servicio vecino del salto siguiente está conectado.

Metric
(Métrica) Costo estimado, en incrementos de 200 milisegundos, de direccionar el paquete VINES al nodo de servicio de destino.

Age (secs)
(Edad - segs) Edad actual, en segundos, de la entrada. Si un direccionador no recibe una actualización de un nodo de servicio que está en la tabla de direccionamientos en un período, como mínimo, de 360 segundos (6 minutos), el direccionador eliminará la entrada correspondiente al nodo de servicio de la tabla de direccionamientos.

Tablas de vecinos

La tabla de vecinos contiene información sobre los nodos de servicio vecinos y los nodos clientes conectados al direccionador. La Figura 15 muestra una tabla de vecinos de ejemplo y, después de la figura, se describen los campos contenidos en la tabla.

```
Nbr Address    Intf     Metric  Age(secs)   H/W Addr    RIF
- - - - - - - - - - - - - - - - - - - - - - - - - - - - -

30633333:0001  TKR/0     4        30     0000C0095012

0035CC10:8000  Eth/1     2        120    0000C0078221

2 Total Neighbors
```

Figura 15. Tabla de vecinos de ejemplo

Descripción de campos de la tabla de vecinos

Nbr Address
(Dirección vcn) La dirección del nodo vecino. En la Figura 15, la dirección 30633333:0001 es un nodo de servicio y la dirección 0035CC10:8000 es un nodo cliente.

Intf
(Intf.) El soporte al que está conectado el nodo vecino.

Metric
(Métrica) Costo estimado, en incrementos de 200 milisegundos, de direccionar el paquete VINES al nodo vecino.

Age (secs)
(Edad - segs) Edad actual, en segundos, de la entrada. Si un direccionador no recibe una actualización de direccionamiento de un vecino en un período, como mínimo, de 360 segundos (6 minutos), el direccionador eliminará la entrada correspondiente al vecino de la tabla de vecinos y, si el vecino es un nodo de servicio, de la tabla de direccionamientos.

H/W Addr
(Dir H/S) La dirección de LAN del nodo si el vecino está conectado a una LAN. Si se está ejecutando el protocolo Frame Relay, la H/W Addr será el identificador de conexión de enlace de datos (DLCI). Para las interfaces X.25, la H/W Addr es la dirección X.25 del vecino.

RIF

Campo de información del direccionamiento. Secuencia de números de puente y segmento, en hexadecimal, que indica una vía de acceso en la red entre dos estaciones. RIF es necesario para el direccionamiento de origen.

Implementación de RTP

Las entidades RTP emiten los paquetes siguientes:

- *Paquetes de solicitud RTP.* Solicitudes efectuadas a los nodos de servicio para obtener la topología de red actual. Durante la inicialización, una interfaz X.25 genera paquetes de solicitud de direccionamiento cada 90 segundos a cada destino X.25 de la interfaz X.25. Cuando la interfaz X.25 recibe un paquete de respuesta de direccionamiento, se envían tres actualizaciones completas de la base de datos de direccionamientos, separadas en períodos de 90 segundos, a los nodos de servicio que enviaron los paquetes de respuesta de direccionamiento. Cuando la interfaz X.25 haya recibido paquetes de respuesta de direccionamiento de todos los nodos de destino X.25, las solicitudes de direccionamiento ya no se enviarán a estas direcciones X.25.
- *Paquetes de actualización RTP.* Paquetes enviados por nodos cliente a los nodos de servicio para notificar a estos su existencia. Los nodos de servicio también envían estos paquetes para notificar su existencia a otros nodos y anunciar sus bases de datos de direccionamientos.
- *Paquetes de respuesta RTP.* Paquetes que envían los nodos de servicio como respuesta a los paquetes de solicitud RTP.
- *Paquetes de redireccionamiento RTP.* Informan a los nodos cuáles son las mejores vías de acceso existentes entre ellos para direccionar paquetes.

A menos que esté conectado mediante un circuito permanente, cada nodo cliente y de servicio difunde una actualización RTP cada 90 segundos. Esta actualización notifica a los vecinos la existencia del nodo, cuál es su tipo (nodo cliente o de servicio) y, en el caso de los nodos de servicio, anuncia sus bases de datos de direccionamientos. Cuando un direccionador recibe un paquete de actualización de un nodo de servicio, RTP extrae la dirección VINES IP y busca en la tabla de direccionamientos una entrada existente en dicho nodo de servicio. Si existe, RTP actualizará la entrada y restablecerá el temporizador de ésta. Si no existe una entrada, RTP creará una e inicializará el temporizador de ésta.

Internet Control Protocol (ICP)

ICP genera mensajes de información de la red sobre dos tipos de paquetes destinados al direccionador local:

- *Destination unreachable packet (Paquete cuyo destino no se puede alcanzar).* Indica que un paquete no ha podido llegar a su destino y que se ha devuelto a su origen. El direccionador emite entonces un mensaje ELS y desecha el paquete.
- *Delay metric packet. (Paquete de métrica retrasada).* Paquete de solicitud de un nodo de destino para saber la métrica de direccionamiento desde el nodo de servicio de destino hasta el nodo cliente de destino.

VINES Address Resolution Protocol (VINES ARP)

El protocolo VINES ARP asigna direcciones VINES IP únicas a los nodos cliente. VINES ARP incluye los tipos de paquete siguientes:

- *Paquete de solicitud de consulta.* Paquetes que los nodos cliente difunden al inicializar.
- *Paquete de respuesta de consulta.* Respuesta del nodo de servicios a un paquete de solicitud de consulta.
- *Paquete de solicitud de asignación.* Respuesta del nodo cliente a un paquete de respuesta de consulta.
- *Paquete de respuesta de asignación.* Incluye las direcciones de red y de subred que el nodo de servicio asignó al nodo cliente.

Para asignar una dirección VINES IP a un nodo cliente, VINES ARP implementa el algoritmo siguiente:

1. El nodo cliente difunde un paquete de solicitud de consulta.
2. Los nodos de servicio responden con un paquete de respuesta de consulta que contiene la dirección del MAC de destino del nodo cliente y una dirección VINES IP de difusión.
3. El nodo cliente emite un paquete de solicitud de asignación a un nodo de servicio que respondió con un paquete de respuesta de consulta.
4. El nodo de servicio responde con un paquete de respuesta de asignación que contiene las direcciones de subred y de red VINES.

Cada nodo cliente mantiene un temporizador que tiene una configuración por omisión de dos segundos. El temporizador se inicia cuando un nodo cliente transmite un paquete de solicitud de asignación o de solicitud de consulta. El nodo cliente detiene y restablece el temporizador cuando recibe un paquete de respuesta de consulta. Cuando un período de tiempo de espera supera los dos segundos, el nodo cliente se inicializa, difunde un paquete de solicitud de consulta y restablece el temporizador. La Tabla 55 resume los estados en los que entran los nodos de servicio y cliente durante la implementación de VINES ARP.

Tabla 55 (Página 1 de 2). Estados VINES ARP de los nodos de servicio y cliente

Estados de los nodos cliente	
Inicialización	El nodo cliente se está inicializando.
Consulta	El nodo cliente está transmitiendo un paquete de solicitud de consulta.
Solicitud	El nodo cliente recibió un paquete de respuesta de consulta de un nodo de servicio y ahora está transmitiendo un paquete de solicitud de asignación al nodo de servicio que escuchó.
Asignado	El nodo cliente ha recibido un paquete de respuesta de asignación que contiene las direcciones de subred y de red VINES.
Estados del nodo de servicio	
Inicialización	El protocolo VINES ARP se está inicializando.
Escucha	El nodo de servicio está esperando paquetes de solicitud de consulta de los nodos cliente.

Tabla 55 (Página 2 de 2). Estados VINES ARP de los nodos de servicio y cliente	
Servicio	El nodo de servicio ha recibido un paquete de solicitud de consulta y ha enviado un paquete de respuesta de consulta.
Asignación	El nodo de servicio emite un paquete de respuesta de asignación que contiene las direcciones de subred y red VINES.

Procedimientos de configuración básicos

Los pasos para configurar inicialmente cada direccionador que envía y recibe paquetes VINES son los siguientes:

1. Asigne una dirección hexadecimal única de 32 bits a cada direccionador de la red VINES. Con el mandato **set network-address** *núm. hex*, entre una dirección de red que esté dentro del rango incluido entre 30900000 y 3097FFFF. La dirección de red de los servidores Banyan es el número de serie hexadecimal de 32 bits del nodo de servicio. Este número se lee automáticamente en la clave del servidor de nodos.
2. Habilite globalmente el protocolo VINES con el mandato **enable VINES**.
3. Habilite las tarjetas de interfaz que deban transmitir y recibir los paquetes de VINES con el mandato **enable interface** *núm.interfaz*.

Para que los cambios de configuración entren en vigor, debe reiniciar el direccionador. Entre **restart** después del indicador OPCON (*) y responda **yes** a la solicitud siguiente:

```
Are you sure you want to restart the router? (Yes or No): yes
```

Para ver la configuración, entre el mandato **list** después del indicador `VINES config>`.

Ejecución de Banyan VINES en el direccionador de puenteo

Los servidores de Banyan VINES deben tener esta opción de Banyan para comunicarse con otros servidores o direccionadores:

Server-to-server LAN (LAN de servidor a servidor).

Para comunicarse por WAN X.25, los servidores VINES conectados directamente a la WAN necesitan las dos opciones siguientes:

Server-to-server WAN (WAN de servidor a servidor)
Soporte de X.25 en el servidor (hardware y software).

Ejecución de Banyan VINES sobre enlaces de WAN

Cuando establezca un enlace PPP, Frame Relay o X.25 para usarlo con VINES, debe establecer la velocidad HDLC del enlace, incluso si establece el reloj en external (externo).

Si establece la velocidad de HDLC en cero, VINES presupondrá que la velocidad es de 56 Kbps. No establezca la velocidad en un valor más rápido que la línea.

Configuración y supervisión de VINES

Este capítulo describe los mandatos de supervisión y configuración de VINES e incluye las secciones siguientes:

Acceso al entorno de configuración de VINES

Para acceder al entorno de configuración de VINES, entre el mandato siguiente en el indicador `Config>`:

```
Config> protocol vin
VINES Protocol user configuration
VINES Config>
```

Mandatos de configuración de VINES

Esta sección resume y después explica los mandatos de configuración de VINES. Entre estos mandatos en el indicador `VINES config>`.

Tabla 56. 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 xxv.
Add	Añade una conversión de dirección X.25.
Delete	Suprime una conversión de dirección X.25.
Disable	Inhabilita el protocolo VINES en todas las interfaces o en una única interfaz e inhabilita la suma de comprobación.
Enable	Habilita el protocolo VINES en todas las interfaces o en una única interfaz y habilita la suma de comprobación.
List	Muestra la configuración actual de VINES.
Set	Asigna las direcciones de red a direccionadores de la red VINES y establece el número máximo de nodos de servicio y de clientes vecinos físicos.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxvi.

Add

Añade una conversión de dirección X.25.

Sintaxis:

a**dd** interface ...

Especifica el número de interfaz.

remote-X.25-addr
Puede incluir un máximo de 15 dígitos. Si ha configurado la conexión del circuito virtual como PVC, la *remote-X.25-addr* de VINES deberá coincidir con la dirección PVC configurada en el indicador de X.25. Si las direcciones no coinciden, el sistema pasará por omisión a un circuito virtual conmutado (SVC).

handle Nombre que puede configurar el usuario y que identifica de forma única a cada servidor remoto.

Ejemplo: `add interface 0 4508907898 test`

Delete

Suprime una conversión de dirección X.25.

Sintaxis:

delete interface ...

\# Especifica el número de interfaz.

remote-X.25-addr
Puede incluir un máximo de 15 dígitos. Si la interfaz especificada no se ha configurado con el mandato **add interface** de VINES, el terminal mostrará el mensaje `That X.25 address has not been configured.` (No se ha configurado esta dirección X.25).

Ejemplo: `delete interface 1 4799999999 compress`

Disable

Use el mandato **disable** para inhabilitar el protocolo VINES en todas las interfaces o en una única interfaz o para inhabilitar la suma de comprobación.

Sintaxis:

disable checksumming ...
interface ...
vines

checksumming *núm.interfaz*
Inhabilita la suma de comprobación en los paquetes que genera la interfaz especifica, salvo los paquetes de difusión. En todas las interfaces, el valor por omisión es la inhabilitación de la suma de comprobación.

Ejemplo: `disable checksumming 0`

interface *núm.interfaz*
Inhabilita el protocolo VINES en la interfaz especificada.

Ejemplo: `disable interface 1`

vines Inhabilita el protocolo VINES en todas las interfaces.

Ejemplo: `disable vines`

Enable

Use el mandato **enable** para habilitar el protocolo VINES en todas las interfaces o en una única interfaz o para habilitar la suma de comprobación.

Sintaxis:

enable checksumming ...
interface ...
vines

checksumming *núm.interfaz*
Habilita la suma de comprobación en los paquetes que genera la interfaz especificada.

Ejemplo: `enable checksumming 0`

interface *núm.interfaz*
Habilita el protocolo VINES en la interfaz especificada.

Ejemplo: `enable interface 1`

vines Habilita globalmente el protocolo VINES. Si recibe un mensaje de error después de entrar este mandato, póngase en contacto con el representante del servicio al cliente. Es posible que no tenga el software de VINES en la carga de software.

Ejemplo: `enable vines`

List

Use el mandato **list** para visualizar la configuración de VINES.

Sintaxis:

list

Ejemplo `list`

```
VINES:  enabled/disabled
VINES network number (hex):
Maximum Number of Routing Table Entries:
Maximum Number of Neighbor Service Nodes:
Maximum Number of Neighbor Client Nodes:

List of interfaces configured for VINES:

intf 0        (checksumming enabled/disabled)
intf 1        (checksumming enabled/disabled)
intf 2        (checksumming enabled/disabled)

VINES X.25 Configuration

Interface     Remote X.25 Address        Remote Handle
    0            4508907898              test

VINES config>
```

VINES Indica si VINES está globalmente habilitado o inhabilitado.

VINES network number (hex)
Dirección hexadecimal de 32 bits configurable para direccionadores de la red VINES.

Maximum Number of Routing Table entries
Valor configurado que especifica el número máximo de entradas permitidas en la tabla de direccionamientos de VINES.

Maximum Number of Neighbor Service Nodes
Valor configurado que especifica el número máximo de nodos de servicio vecinos conectados al direccionador.

Maximum Number of Neighbor Client Nodes
Valor configurado que especifica el número máximo de nodos cliente conectados al direccionador.

List of interfaces configured for VINES
Muestra las interfaces que tienen VINES habilitado y si la suma de comprobación está habilitada o no.

VINES X.25 Configuration
Esta información representa los elementos siguientes:

Interface La interfaz configurada para X.25.

Remote X.25 Address
La dirección DTE del servidor remoto.

Remote Handle
Nombre que puede configurar el usuario y que identifica de forma única al servidor remoto.

Set

Use el mandato **set** para asignar direcciones de red a direccionadores de la red VINES y especificar el número máximo de nodos de servicio y cliente.

Sintaxis:

set client-node-neighbors ...
network-address ...
routing-table-size ...
service-node-neighbors ...

client-node-neighbors #
Especifica el número máximo de nodos cliente de la red. **Client-node-neighbors** incluye todos los nodos de cada red que estén conectados directamente a través del direccionador. El rango está comprendido entre 1 y 65535 y el valor por omisión es 25.

Nota: Se recomienda que establezca este número en un valor que sea bastante más alto que el número de nodos de la red. Esto permitirá que la red siga funcionando sin tener que volver a configurar y reiniciar los direccionadores cuando se añaden nodos adicionales. El aumento de este número dependerá del tamaño de la red y del volumen de crecimiento anticipado. Por norma general, establezca **client-node-neighbors** en un valor que sea un 25 % superior al número real de estaciones cliente en las LAN que sean locales para el direccionador.

Ejemplo: `set client-node-neighbors 20`

network-address *#hex*

Asigna una dirección de red a cada direccionador de la red VINES. *#hex* es un valor hexadecimal de 32 bits incluido entre 30900000 y 3097FFFF.

Ejemplo: `set network-address 30922222`

routing-table-size *#*

Especifica el número máximo de direccionadores y nodos de servicio en la red VINES. El rango está comprendido entre 1 y 65535 y el valor por omisión es 300.

Nota: Asegúrese de que el número que especifique sea lo suficientemente grande como para acomodar servidores VINES y 2210 adicionales a medida que crece la red.

Ejemplo: `set routing-table-size 250`

service-node-neighbors *#*

Especifica el número máximo de nodos de servicio vecinos físicos. El número incluye los servidores VINES y 2210 que son el primer punto de contacto después de atravesar una WAN. El rango está comprendido entre 1 y 65535 y el valor por omisión es 50.

Ejemplo: `set service-node-neighbors 100`

Acceso al entorno de supervisión de VINES

Para acceder al entorno de supervisión de VINES,

```
* t 5
```

A continuación, entre el mandato siguiente en el indicador **+**:

```
+ protocol vin
VINES>
```

Mandatos de supervisión de VINES

Esta sección describe los mandatos de supervisión de VINES. Entre estos mandatos en el indicador `VINES>`.

Tabla 57 (Página 1 de 2). Resumen de los mandatos de supervisión de VINES

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxv.
Counters	Muestra los errores de direccionamiento y el número de veces que la cola de entrada de VINES estaba llena cuando se recibieron paquetes de la interfaz especificada.
Dump	Muestra el contenido actual de las tablas vecinas y de direccionamientos de VINES.
Route	Muestra una entrada de la tabla de direccionamientos de VINES.

Tabla 57 (Página 2 de 2). Resumen de los mandatos de supervisión de VINES	
Mandato	Función
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxvi.

Counters

Use el mandato **counters** para visualizar los errores de direccionamiento y el número de veces que la cola de entrada de VINES estaba llena cuando se recibieron paquetes de la interfaz especificada.

Sintaxis:

counters

Ejemplo: `counters`

```
  Routing Errors
Count           Type
-----           ----
  2          Net Unreachable
  3          Hop Count Expired
  3          Routing Update from Orphan Client
  0          Routing Redirect Received
  0          Routing Response Received

  VINES Input Packet Overflows
   Net      Count
   ---      -----
  Eth/0      5
  Eth/1      1
```

Net Unreachable
(Imposible llegar a la red) Número de veces que el direccionador recibió un paquete destinado a un nodo que no estaba en la tabla de direccionamientos.

Hop Count Expired
(Cuenta de saltos agotada) Número de veces que el direccionador descartó un paquete porque la cuenta de saltos se había agotado.

Routing Update from Orphan Client
(Actualización de direccionamiento de un cliente huérfano) Número de veces que el direccionador recibió un paquete de actualización de un nodo cliente cuyo nodo de servicio no existía. Puede producirse una actualización de direccionamiento de un cliente huérfano cuando el direccionador arranca y oye primero al nodo cliente en vez de oír al nodo de servicio o bien, cuando un nodo de servicio del cliente está desactivado y se ha eliminado una entrada de la base de datos de direccionamientos.

Routing Redirect Received
(Redireccionamiento de ruta recibido) Número de veces que el direccionador recibió paquetes redireccionados de nodos de servicio.

Routing Response Received
(Respuesta de direccionamiento recibida) Número de veces que se generaron paquetes de respuesta como consecuencia de paquetes de solicitud iniciados por el direccionador.

VINES input packet overflows

(Desbordamiento de paquetes de entrada VINES) Número de veces que la cola de entrada del reenviador de VINES estaba llena cuando se recibieron paquetes de la interfaz especificada. Los paquetes se descartaron después.

Dump

Use el mandato **dump** para mostrar el contenido de las tablas vecinas y de direccionamientos de VINES.

Sintaxis:

dump neighbor-tables
routing-tables

neighbor-tables

Muestra información sobre cada nodo cliente y de servicio de vecinos conectados al direccionador.

Ejemplo: `dump neighbor-tables`

```
   Nbr Address    Intf     Metric  Age(secs)   H/W Addr    RIF
  ------------------------------------------------------------
   30622222:0001  TKR/0     4           30     0000C00     95012
   0035CC10:8000  Eth/0     2          120     0000C00     78221

2 Total Neighbors
```

Nbr Address

(Dirección vcn) La dirección del nodo vecino. En el ejemplo anterior, la dirección 30622222:0001 es un nodo de servicio y la dirección 0035CC10:8000 es un nodo cliente.

Intf (Intf.) El soporte al que está conectado el nodo vecino.

Metric (Métrica) Costo estimado, en 200 milisegundos, de direccionar el paquete VINES al nodo vecino.

Age (secs)

(Edad - segs) Edad actual, en segundos, de la entrada. Si un direccionador no recibe una actualización de direccionamiento de un vecino en un período, como mínimo, de 360 segundos (6 minutos), el direccionador eliminará la entrada correspondiente al vecino de la tabla de vecinos y, si el vecino es un nodo de servicio, de la tabla de direccionamientos.

H/W Addr

(Dir H/S) La dirección de LAN del nodo si el vecino está conectado a una LAN. Si se está ejecutando el protocolo Frame Relay, la H/W Addr será el identificador de conexión de enlace de datos (DLCI). Para las interfaces X.25, la H/W Addr es la dirección X.25 del vecino.

RIF Campo de información del direccionamiento. Secuencia de números de puente y segmento, en hexadecimales, que indica una vía de acceso en la red entre dos estaciones. RIF es necesario para el direccionamiento de origen.

routing-tables

Muestra información sobre cada nodo de servicio que conoce el direccionador.

Ejemplo: `dump routing-table`

```
Net Address  Next Hop Nbr Addr   Nbr Intf  Metric   Age (secs)
-----------  -----------------   --------  ------   ----------
S  30622222   30622222:0001      Eth/0        20         30
H  0027AA21   0027AA21:0001      Eth/1        2          120
P  0034CC11   0034CC11:0001      X.25/0       45         0

3 Total Routes

S ==> Entry is suspended, H ==> Entry is Holdown, P ==> Entry
is permanent
```

Net Address

(Dirección de la red) La dirección de la red es un número exclusivo hexadecimal de 32 bits, que se puede configurar con un valor del rango incluido entre 30900000 y 3097FFFF. Banyan ha asignado este rango de números a IBM. Es muy importante que no se asigne la misma dirección de red a dos direccionadores de una misma red. La dirección de red de un nodo de servicio Banyan es un número de serie hexadecimal de 32 bits del nodo de servicio. Si delante del campo de dirección de la red se encuentra una S, una H o una P, los significados serán los siguientes:

S: El nodo de servicio está suspendido y se anuncia durante 90 segundos que está desactivado. Después de este tiempo, el direccionador elimina la entrada correspondiente a este nodo de la tabla de direccionamientos.

H: El nodo de servicio está retenido y se anuncia durante 2 minutos que está desactivado. Después de este tiempo, el direccionador anunciará que el nodo de servicio está operativo. Si un nodo de servicio está suspendido y recibe un paquete RTP, el nodo de servicio entrará en estado de retención.

P: Después de la inicialización, la interfaz X.25 entra en estado permanente durante 4-1/2 minutos. Después de este tiempo, el vecino entrará en dicho estado y su edad permanecerá en 0 mientras se encuentre así. Si la interfaz X.25 se desactiva, se eliminará la entrada de la tabla de direccionamientos.

Next Hop Nbr Addr

(Dir. vecino salto siguiente) Dirección del nodo de servicio vecino que es el salto siguiente de la vía de acceso de menos costo a la red.

Nbr Intf (Intf. vecino) El soporte al que el nodo de servicio vecino del salto siguiente está conectado.

Metric (Métrica) Costo estimado, en 200 milisegundos, de direccionar el paquete VINES al nodo de servicio de destino.

Age (secs)
(Edad - segs) Edad actual, en segundos, de la entrada. Si un direccionador no recibe una actualización de direccionamiento de un nodo de servicio que está en la tabla de direccionamientos cada 360 segundos (6 minutos), como mínimo, el direccionador eliminará la entrada correspondiente al nodo de servicio de la tabla de direccionamientos.

Route

Use el mandato **route** para ver una entrada de la tabla de direccionamientos.

Sintaxis:

r**oute** given address

given address
La dirección de red del nodo de servicio.

Ejemplo: `route 30622222`

```
Net Address  Next Hop Nbr Addr   Nbr Intf  Metric   Age (secs)
-----------  -----------------   --------  ------   ----------
30622222      30622222:0001       Eth/0       2       30
```

Uso de DNA IV

Este capítulo describe la implementación de Digital Network Architecture Phase IV (DNA IV) que efectúa IBM e incluye las secciones siguientes:

Visión general de DNA IV

DNA IV es un conjunto de componentes de software que transfieren información entre redes conectadas mediante un soporte físico. Al transferir información, el software DNA IV facilita la comunicación entre los dispositivos de red como, por ejemplo, sistemas personales, servidores de archivos e impresoras.

El protocolo DNA IV es el protocolo subyacente de los productos de software DECnet de Digital Equipment Corporation así como de los productos compatibles con DNA. Este protocolo incluye:

- Software de direccionamiento para redes de protocolo DNA IV.
- NCP, una implementación de DNA IV Network Control Program (programa de control de red DNA IV). Para obtener más información, consulte la documentación de DECnet-VAX adecuada, publicada por Digital Equipment Corporation.
- Soporte del Maintenance Operations Protocol (MOP) de DNA IV.

DNA IV lleva a cabo dos funciones principales:

- Mantiene una base de datos completa de direccionamientos en todos los nodos de su área. (Si el direccionador funciona como direccionador de nivel 2, mantiene también la base de datos para todas las áreas).
- Direcciona paquetes de datos DECnet de entrada a los destinos adecuados basándose en su propia base de datos de direccionamientos. No tiene en cuenta los paquetes destinados al direccionador que no sean paquetes hello o de direccionamiento.

DNA IV da soporte a:

- Varias áreas en una red Ethernet o red en anillo .
- Operaciones de MOP básicas. DNA IV responde a un mensaje de ID de solicitud de MOP con un mensaje de ID de sistema de MOP. DNA IV también envía un mensaje de ID de sistema de MOP cuando se activa un circuito. Puede supervisar mensajes de MOP usando el módulo de configuración Ethernet bajo DECnet-VAX NCP. El NCP del direccionador no incluye un módulo de configuración de Ethernet.
- Protocolo LAT. El protocolo LAT no forma parte de la familia de protocolos DNA IV. Se trata de un protocolo destinado únicamente a Ethernet que sólo se ocupa de comunicaciones de corta distancia (tiempo de ida y vuelta limitado). (El protocolo CTERM proporciona soporte de terminales de área amplia usando protocolos DNA IV en los direccionadores). El mandato **set host** en DECnet-VAX proporciona el protocolo CTERM).

Debe prestarse una atención especial a las restricciones siguientes de DNA IV:

- DNA IV no da soporte a los protocolos NSP, Session o NICE.
- DNA IV no da soporte al protocolo de línea DDCMP en las líneas síncronas directamente conectadas.
- DNA IV no proporciona ninguna función de compatibilidad de Phase III ya que no da soporte a los protocolos de enlace de datos DDDCMP usados por todos los nodos Phase III.
- NCP (la implementación efectuada por el direccionador del DECnet Network Control Program) implementa un subconjunto de funciones y mandatos de NCP originales.

Terminología y conceptos de DNA IV

Esta sección contiene una breve descripción de la terminología DNA IV.

Direccionamiento

Cada nodo tiene una dirección de nodo de 16 bits, la cual es la misma para todas las interfaces de dicho nodo. Una dirección está formada por 2 campos: 6 bits de número de área y 10 bits de número de nodo. Las direcciones se imprimen en números decimales con un punto que separa el área; por ejemplo, 1.7 es el nodo 7 del área 1. Si no se indica ningun área se presupone el área 1. Cualquier dirección que esté en el rango incluido entre 1.1 y 63.1023 es legal. Ambos nodos y áreas deben empezar a numerarse a partir del 1 con poca holgura, si la hay. Esto se produce porque el número de nodo máximo y los números de área máximos son opciones de configuración y controlan el tamaño de varias estructuras de datos de direccionamiento.

No hay correlación directa entre las direcciones y el cableado físico. Las rutas se calculan en los nodos y no en los cables.

Direccionamiento de enlaces de datos Ethernet

Cada interfaz de Ethernet se establece en la misma dirección física de 48 bits, la cual es la concatenación de un prefijo de 32 bits (AA-00-04-00) y la dirección de nodo DNA IV de 16 bits. La dirección de nodo se conmuta por bytes (para convertir de PDP11 al orden de bytes de Ethernet). Por consiguiente, el nodo de DNA IV 1.1 tiene la dirección de Ethernet AA-00-04-00-01-04.

La difusión múltiple (no la difusión general) también se usa en el direccionamiento. Las tres direcciones de difusión múltiple usadas por DNA IV son AB-00-00-02-00-00, AB-00-00-03-00-00 y AB-00-00-04-00-00.

Direccionamiento de enlace de datos de red en anillo 802.5

La implementación de DNA sobre IEEE 802.5 Token Ring respeta la *DECnet Digital Networking Architecture (Phase IV) Token-Ring Data Link and Node Product Functional Specification*, Versión 1.0.0, que incluye soporte para direcciones de MAC arbitrarias (AMA).

Existen dos tipos de direccionamiento MAC, el direccionamiento DNA IV convencional, que es la concatenación de un prefijo de 32 bits (AA-00-04-00) y la dirección de nodo/área de DNA IV de 16 bits o AMA que permite al protocolo DNA ejecutarse en nodos IEEE 802.5 sin que este protocolo tenga que cambiar las direcciones de MAC. Esto es necesario si sigue algunas convenciones de protocolo

IBM. Puede seleccionar el tipo de direccionamiento que está usando a través del proceso de configuración de DNA (NCP>).

Otro tipo de representación del direccionamiento es el orden de bits nativo. Cuando se envía en la capa física, este tipo de dirección está agrupada por bytes. Por ejemplo, el prefijo de 32 bits canónico que se muestra arriba (utilizando guiones) se expresa como 55:00:20:00 en orden de bits nativos con el signo de dos puntos separando cada byte.

Nota: Cuando se configura DNA IV para ejecutarse sobre ATM LAN Emulation, debe usarse el AMA.

Direccionamiento de enlace de datos X.25

El direccionador da soporte a DECnet Phase IV sobre X.25 y puede funcionar con direccionadores que ejecuten la implementación de Digital de DECnet Phase IV sobre X.25.

La dirección DTE remota y local se establece con el mandato **set/define circuit** cuando establece un circuito DECnet. En el parámetro *call-userdata* se especifica la dirección DTE local en octetos hexadecimales (caracteres). En el parámetro *DTE-address*, se especifica la dirección remota en octetos hexadecimales. Tanto la dirección DTE remota como local pueden tener un máximo de 14 octetos hexadecimales de longitud con dos caracteres ASCII que representen un octeto hexadecimal.

Direccionamiento

DNA IV maneja tanto el reenvío de paquetes de datos DNA IV como el direccionamiento automático con otros nodos DNA IV. El direccionador ejecuta las funciones de DNA IV siguientes:

- Anuncia su presencia enviando mensajes hello a todas las redes que tienen habilitado DNA IV.
- Mantiene una lista de nodos DNA IV adyacentes a partir de los paquetes hello que recibe de otros nodos DNA IV.
- Intercambia información de direccionamiento con otros direccionadores.
- Reenvía paquetes entre nodos.

Todos los nodos de direccionamiento y finales difunden periódicamente mensajes hello a la dirección de difusión múltiple de todos los direccionadores. Esto permite que cada direccionador localice otros nodos de su área.

En cada red de difusión (por ejemplo, Ethernet, red en anillo), un direccionador se declara a sí mismo como direccionador designado para ese cable. Dicho direccionador difunde su presencia para que los nodos finales sepan cómo utilizarlo como pasarela por omisión. Cualquier nodo final que envíe un paquete a un nodo que no esté en ese cable lo enviará automáticamente al direccionador designado para que lo reenvíe.

En una DNA multiárea, asigne prioridades a direccionadores de tal manera que el direccionador designado sea un direccionador de nivel 2 o bien que probablemente sea el salto siguiente con más posibilidades para los destinos usados con más frecuencia. Esto reduce la posibilidad de que el tráfico de los nodos finales tenga que añadir un salto adicional.

Las decisiones de direccionamiento se basan en un algoritmo de menos costo. Cada enlace (por ejemplo, de punto a punto, red de difusión, salto) tiene un costo. Cada direccionador difunde (únicamente a otros direccionadores) su costo y el número de saltos para llegar a cada nodo de su área. Así, cada direccionador busca la vía de acceso más barata, en relación a una cuenta de saltos máxima.

Tablas de direccionamientos

Un direccionador reenvía al nodo adecuado, basándose en su tabla de direccionamientos, el paquete de datos DNA IV que recibe. A fin de mantener dicha tabla, un direccionador escucha las actualizaciones de nivel 1 y las envía a cada nodo de su área. Si el tipo del direccionador se establece en AREA, también intercambia actualizaciones de direccionamiento de nivel 2.

Cada direccionador mantiene una tabla de direccionamientos con una entrada por cada nodo (hasta la dirección máxima) y cada salto siguiente posible (todos los circuitos y hasta el máximo de direccionadores de difusión). Cada entrada de esta tabla contiene el costo y el salto para alcanzar un nodo a través de un circuito o el nodo del salto siguiente. Cada segundo la tabla de direccionamientos envía un temporizador de direccionamientos de difusión.

Direccionadores de áreas

Si se configura el direccionador como direccionador de áreas, éste mantendrá una base de datos similar para todas las áreas hasta el área máxima y podrá intercambiar información de direccionamiento de áreas con otros direccionadores de áreas. Las áreas se manejan casi de la misma manera que los nodos, salvo que los mensajes dan costos a las áreas, pero no a los nodos.

El concepto de áreas da como resultado dos tipos de nodos de direccionamientos:

- Un direccionador de nivel 1 sólo conoce un área, por lo que mantiene un seguimiento de los nodos del área. Además, no tiene en cuenta las adyacencias a través de las áreas.
- Un direccionador de nivel 2 mantiene una base de datos de direccionamientos de áreas y puede tener adyacencias a través de áreas. Los direccionadores de nivel 2 anuncian rutas al resto de las áreas, por lo que los direccionadores de nivel 1 envían todo el tráfico de áreas externas a los direccionadores de nivel 2.

Los nodos finales pasan simplemente paquetes a un direccionador.

Un direccionador de nivel 2 que puede alcanzar otras áreas anuncia una ruta a un nodo 0 dentro de su área. Cuando los direccionadores de nivel 1 necesitan enviar un paquete a otra área, lo direccionan hacia el nodo 0 más cercano. Esto no significa que sea la mejor ruta a dicha área. Desde ahí, el algoritmo de direccionamiento de nivel 2 envía el paquete a su área de destino.

Configuración de los parámetros de direccionamiento

En cada sistema puede establecer los parámetros de direccionamiento siguientes:

- Número máximo de nodos en el área
- Número máximo de direccionadores adyacentes a este direccionador
- Número máximo de redes en cualquier nodo determinado

- Número máximo de nodos finales que están a un salto de este nodo final
- Costo de un salto en cada red a la que está conectado este nodo
- Valores de varios temporizadores implicados en enviar mensajes hello y que los esperan de otros nodos

Implementación de DNA IV efectuada por IMB

El principal programa de interfaz de usuario para la implementación de direccionador de DNA IV se llama NCP. El NCP del direccionador es un subconjunto limitado de mandatos de DECnet Network Control Program (NCP). El NCP del direccionador habilita al usuario para visualizar y modificar los diversos argumentos de funcionamiento de DNA IV y leer diversos contadores específicos de DNA.

Algunas de las características del NCP del direccionador incluyen:

- NCP implementa entidades nuevas: control de acceso de módulos y filtro de direccionamiento de módulos.
- NCP no tiene mandato **set executor buffer size** ya que el direccionador no origina tráfico DECnet. El direccionador puede reenviar el paquete más grande que cualquier implementador DECnet puede generar. Cumple las restricciones de tamaño del almacenamiento intermedio en todos los nodos adyacentes.
- NCP permite un calificador **all** en los submandatos **node**, **area** y **circuit**.

El NCP del direccionador es similar al NCP de DECnet-VAX, con las diferencias siguientes:

- El NCP del direccionador no incluye el mandato **set node name** y, por consiguiente, no puede asignar nombres a nodos o visualizar nombres de nodos con direcciones.
- El NCP del direccionador no incluye los mandatos **clear** o **purge** ni los mandatos **set** tienen un argumento **all**. La base de datos permanente siempre se copia en la base de datos volátil cuando se inicia, reinicia o arranca el direccionador.
- Un mandato del NCP del direccionador puede tener únicamente un argumento.
- NCP no tiene el concepto de líneas. Para ver los datos que un mandato **show line** del NCP DECnet-VAX muestra, use los mandatos **interface** y **network** de GWCON.
- El NCP del direccionador no da soporte a mandatos entre redes:
  - El NCP del direccionador no incluye el mandato **tell**, el cual solicita mandatos de NCP en otros nodos.
  - Asimismo, el NCP del direccionador no da soporte a solicitudes de protocolo de soporte de otros direccionadores DNA para ejecutar mandatos del NCP en el direccionador en su nombre.

Importante

Antes de configurar DNA IV, es necesario que sea consciente de las características de seguridad opcionales tratadas en:

- “Gestión de tráfico utilizando el control de acceso” en la página 264
  - Proporciona seguridad limitando el acceso en los direccionadores de la red.
- “Gestión del tráfico con filtros de direccionamiento de áreas” en la página 267
  - Limita el acceso a grupos de áreas de otras áreas
  - Permite la fusión de dos espacios de direcciones de DECnet

Si ya está familiarizado con estos temas, salte las dos secciones mencionadas y empiece a leer en “Configuración de DNA IV” en la página 272.

Gestión de tráfico utilizando el control de acceso

El control de acceso protege a un grupo de nodos de otros nodos de la red. Los direccionadores hacen que todos los nodos de una red sean accesibles entre sí. Por lo general, las principales formas de seguridad son las contraseñas y el uso conservador del acceso proxy de DNA IV en el nivel del sistema principal.

No obstante, debido a diferencias en el nivel de seguridad de las máquinas, es posible que deba proveer seguridad adicional limitando el acceso dentro de los direccionadores de la red. El reenviador de DNA le habilita para ello mediante los controles de acceso.

Por lo general, no se recomienda los controles de acceso debido a:

- Los controles de acceso influyen en el rendimiento de un direccionador ya que se prueba cada paquete. Cuanto más complicada sea la configuración del control de acceso, mayor influencia tendrá en el rendimiento.
- Los controles de acceso son difíciles de configurar y los errores de configuración difíciles de diagnosticar.
- Los controles de acceso no pueden ocultar un nodo a los protocolos de direccionamiento. El nodo sigue estando visible para todos los direccionadores de su área.

  Nota: Los controles de acceso no garantizan la seguridad; sólo dificultan las intrusiones. Los protocolos de direccionamiento DNA IV usados en Ethernet y otros soportes de difusión no tienen características de seguridad incorporadas.

El control de acceso evita el reenvío de paquetes de datos de DNA IV (formato largo) basándose en la dirección de origen, dirección de destino e interfaz. Este control no influye en los paquetes de direccionamiento, ya que usan un formato de paquete diferente. Esto da mayor seguridad a la configuración del control de acceso, ya que no puede interrumpir el protocolo de direccionamiento.

Para implementar el control de acceso, las direcciones se enmascaran y comparan. Es decir, se pone una máscara a la dirección en cuestión con 1 en las posiciones de los bits que deben probarse y 0 en el área libre. A continuación, la

dirección se compara con un valor fijado. Por ejemplo, puede usar una máscara de 63.1023 (todo 1) y compararla con un resultado de 6.23, lo cual es cierto únicamente para el nodo 6.23. Puede usar una máscara de 63.0 y un resultado de 9.0, lo cual es cierto para cualquier nodo del área 9.

Esta máscara y los valores de comparación vienen en pares para la dirección de origen y la destino. A continuación, se forman en listas para una interfaz. Cada interfaz tiene una lista de control de acceso, la cual aplica a los paquetes que recibe. La lista puede ser incluyente o excluyente. Una lista incluyente es un conjunto de pares de direcciones que designan un corredor para el flujo de tráfico. Una lista excluyente es un conjunto de pares de direcciones que no permiten el flujo de tráfico.

En una lista incluyente, las direcciones de origen y de destino se prueban usando la máscara y los valores de comparación. Si el origen y el destino de una entrada coinciden, se reenviará el paquete. En una lista excluyente, las direcciones de origen y de destino se prueban usando la máscara y los valores de comparación. Si el origen y el destino de una entrada coinciden, se eliminará el paquete. La elección entre incluyente y excluyente debe realizarse basándose en qué lista será más corta. No obstante, el control de acceso excluyente es, por lo general, más fácil de configurar.

Cuando se eliminan paquetes debido a controles de acceso, se establece el bit Return to Sender Request (Solicitud de retorno a transmisor - RQR) en la cabecera del paquete de datos de formato largo y se devuelve el paquete. A continuación, la solicitud de conexión falla inmediatamente ya que normalmente se envían los paquetes NSP Connect Initiate (iniciación de conexión NSP) con el bit RQR establecido.

Configuración del control de acceso

El control de acceso limita el acceso a un sistema principal o un grupo de sistemas principales determinados. Debe asignar el control de acceso a todos los direccionadores a dicho sistema principal y no sólo al direccionador preferido. De lo contrario, el control de acceso funcionará cuando la ruta primaria esté activada pero fallará cuando se use la secundaria.

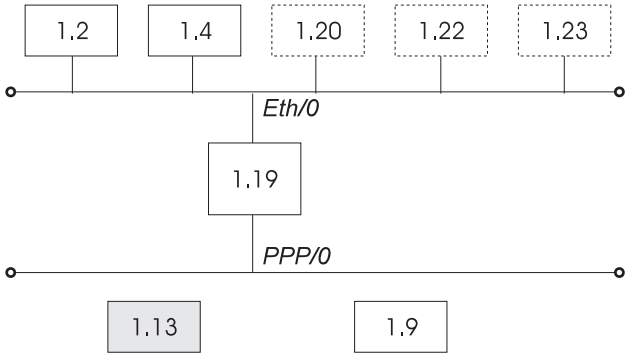
En el mapa de la red, trace una línea para aislar la región fiable del resto de la red. La línea ideal debería cruzar el conjunto de adyacencias menor posible para que se ejecute el menor número posible de interfaces con control de acceso. En el caso de las redes de difusión (Ethernet y red en anillo), trace la línea a través del cable de interconexión al nodo para identificar la interfaz con el filtro. Por cada interfaz que la línea de control de acceso cruce, use NCP para definir la misma lista de control de acceso.

Nota: Dado que todas las aplicaciones DECnet usan el protocolo NSP, el cual necesita una conectividad bidireccional, no es necesario definir el control de acceso en ambas direcciones.

Control de acceso incluyente

En la Figura 16 en la página 266, el nodo 1.13 desea comunicarse únicamente con los nodos 1.2 y 1.4. El control de acceso le permite dar fiabilidad a algunos nodos entre todos los nodos que tienen conexión de direccionadores. Por consiguiente, en la Figura 16 en la página 266 puede proteger el nodo 1.13 de todos los nodos salvo del nodo 1.9 ya que ambos nodos comparten la misma red física.

Para configurar el control de acceso deseado para este ejemplo, cree un filtro incluyente en la interfaz Eth/0 del direccionador 1.19, tal como se muestra en la parte inferior de la Figura 16 en la página 266



Información del filtro incluyente

Resultado de origen	Máscara de origen	Resultado de destino	Máscara de destino
1.2	63.1023	1.13	63.1023
1.4	63.1023	1.13	63.1023
0.0	0.0	1.9	63.1023

Figura 16. Ejemplo de un control de acceso incluyente

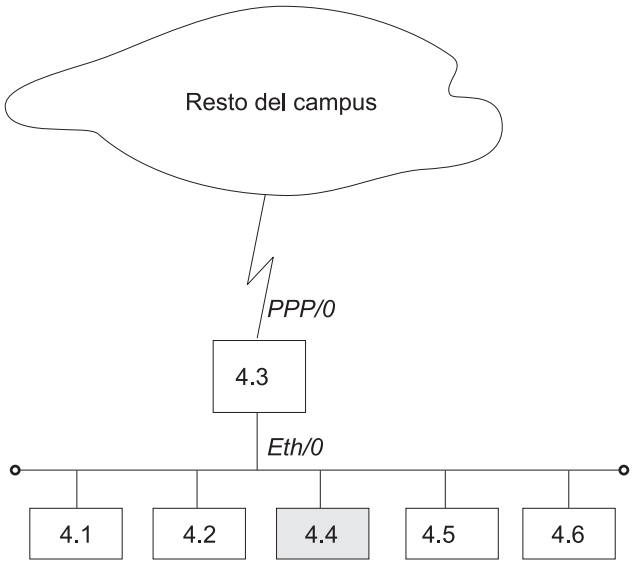
La primera y la segunda entradas de la información del filtro incluyente que aparecen en la Figura 16 permiten a los nodos 1.2 y 1.4 enviar paquetes al nodo 1.13. La tercera entrada permite que todos los nodos hagan envíos al nodo 1.9 (no está intentando dar fiabilidad al nodo 1.9).

Para configurar el ejemplo indicado para el direccionador 1.19, entre los parámetros y mandatos de NCP siguientes:

```
NCP> def mod access-cont circ eth/0 type inclusive
NCP> def mod access-cont circ eth/0 filter 1.2 63.1023 1.13 63.1023
NCP> def mod access-cont circ eth/0 filter 1.4 63.1023 1.13 63.1023
NCP> def mod access-cont circ eth/0 filter 0.0 0.0 1.9 63.1023
NCP> def mod access-cont circ eth/0 state on
```

Control de acceso excluyente

La Figura 17 en la página 267 muestra cómo el control de acceso excluyente aísla el nodo 4.4 del resto del campus.



Información del filtro excluyente

Resultado de origen	Máscara de origen	Resultado de destino	Máscara de destino
0.0	0.0	4.4	63.1023

Figura 17. Ejemplo de control de acceso excluyente

Configure el control de acceso deseado para este ejemplo creando un filtro excluyente en la interfaz PPP/0 del direccionador 4.3, tal como se muestra en la Figura 17. Para configurar el ejemplo indicado para el direccionador 4.3 en la Figura 17, entre los parámetros y mandatos de NCP siguientes:

```
NCP> def mod access-cont circ ppp/0 type exclusive
NCP> def mod access-cont circ ppp/0 filter 0.0 0.0 4.4 63.1023
NCP> def mod access-cont circ ppp/0 state on
```

Gestión del tráfico con filtros de direccionamiento de áreas

Los filtros de direccionamiento de áreas permiten efectuar configuraciones especiales de la red DNA. Dado que se trata de un tema avanzado, muy pocas redes DNA IV necesitan filtros de direccionamiento. En DNA IV existen dos aplicaciones primarias para el filtro de áreas:

- Seguridad; se limita el acceso a algunos grupos de áreas de otras áreas.
- Se permite la fusión de dos espacios de direcciones de DECnet.

Nota: La configuración de los filtros de direccionamiento de áreas es muy delicada y está plagada de dificultades. Es muy fácil romper totalmente el direccionamiento de áreas. Si no comprende cómo funciona el direccionamiento de DECnet, especialmente en el nivel de las áreas, no intente usar filtros de direccionamiento. Puede encontrar documentación sobre el protocolo de direccionamiento DECnet en *DECnet Digital Network Architecture Phase-IV Routing Layer Functional*

Description, número de pedido AAX435ATK, Diciembre de 1983, Digital Equipment Corporation, Maynard, Massachusetts.

Los filtros de direccionamiento de áreas le permiten configurar un direccionador para controlar la información sobre áreas DECnet que se envían o aceptan en los mensajes de direccionamiento de nivel 2. Por cada interfaz, puede configurar varios filtros separados de entrada o salida. Cada filtro especifica qué información de direccionamiento de áreas se pasará o aceptará.

Cuando una red envía una actualización de direccionamiento de nivel 2 y hay un filtro de direccionamiento, la entrada (RTGINFO) de cualquier área que no esté en el filtro tendrá el costo de 1023 y una cuenta de saltos de 63. Cada área del filtro tiene el costo y los saltos correctos en la entrada.

Cuando la red recibe un mensaje de direccionamiento de nivel 2 y hay un filtro de direccionamiento, las entradas de un área que no esté en el filtro se tratarán como si el costo fuese 1023 y la cuenta de saltos 63 (imposible de alcanzar). Cualquier entrada de direccionamiento del paquete que esté en el filtro se procesará normalmente.

Los filtros de direccionamiento únicamente influyen en el proceso de los mensajes de direccionamiento de nivel 2. No hay filtros para los mensajes de direccionamiento de nivel 1. Los filtros de direccionamiento no influyen en el proceso de hello del direccionador y no evitan que los direccionadores de áreas desarrollen adyacencias. Sí, influyen, por el contrario, en la base de datos de direccionamientos de áreas. Si los filtros evitan que un direccionador de áreas obtenga conocimientos de otra área, evitarán que el direccionador se conecte y, por consiguiente, éste no podrá anunciarse como direccionador de áreas.

Seguridad mediante filtro de áreas

Al igual que los controles de acceso, los filtros de direccionamiento proporcionan seguridad. No obstante, los filtros de direccionamiento tienen algunos inconvenientes si se comparan con los controles de acceso:

- El filtro de áreas es menos flexible que los accesos de control ya que requieren que la asignación de áreas corresponda con la arquitectura de seguridad deseada.
- El filtro de áreas es más difícil de comprender y configurar.
- El nivel de seguridad es inferior ya que, de todas formas, un sistema principal que no tenga en cuenta la información de direccionamiento puede enviar los paquetes al direccionador correcto.

No obstante, el filtro de áreas es más eficaz ya que no es necesario comprobar cada paquete. En el ejemplo siguiente, el filtro de áreas se produce en un área que contiene estaciones de trabajo que forman parte de una red grande que contiene máquinas con información confidencial. Puede darse el caso de que las máquinas confidenciales deban ponerse en contacto con una máquina de fuera del área para obtener información.

En la Figura 18 en la página 269, el área 13 contiene estaciones de trabajo que deben poder llegar al área 1. El nodo 13.1 es el direccionador y los otros nodos son las estaciones de trabajo. El nodo 13.1 tiene un filtro que sólo acepta rutas al área 7. Por consiguiente, si el nodo 13.1 recibe un paquete de cualquier nodo del

área 13 que no esté destinado al área 7, no podrá reenviar el paquete y enviará al nodo de envío un mensaje de error.

Para configurar el direccionador 13.1 de la Figura 18, entre los parámetros y mandatos siguientes de NCP:

```
NCP> def mod routing-filter circ eth/1 incoming area 7
NCP> def mod routing-filter circ eth/1 incoming state on
```

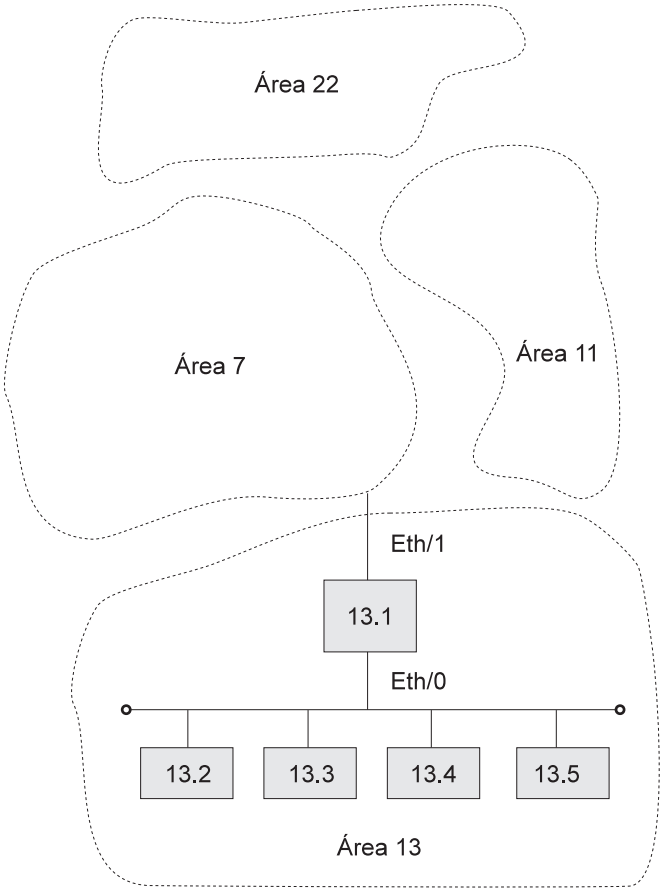


Figura 18. Ejemplo de filtro de direccionamiento de áreas para seguridad

Fusión de dominios DECnet

DECnet tiene un espacio de dirección de nodo de 16 bits con una jerarquía fijada de 6 bits de área y 10 bits de nodo. En comparación, IP tiene un espacio de dirección de nodo de 32 bits con una jerarquía multinivel flexible. Ahora, varias redes establecidas han crecido hasta el punto de usar las 63 áreas. El problema que se plantea es que, a medida que se conectan diferentes recursos entre sí, éstos desean conectar sus redes DECnet pero no es posible debido a conflictos de número de área.

La única solución consiste en volver a diseñar la arquitectura de DECnet. (DECnet Phase V trata esta cuestión). No obstante, al usar filtros de direccionamiento de áreas, es posible permitir un cierto solapamiento entre dos dominios DECnet.

Dominio no es un término estándar de DECnet, lo utilizamos aquí como nombre de una red de área amplia DECnet, presumiblemente una red con varias áreas. El objetivo es fusionar dos de estos dominios para que haya un área común que

pueda llegar a partes de ambos dominios. No obstante, en la unión de dos dominios hay más de 63 áreas. Dado que el filtro de áreas no es fácil de administrar y es restrictivo, no lo use si tiene suficientes números de área disponibles para la unión de los dominios.

Para configurar la solapación de dos dominios, primero deberá decidir qué áreas harán intersección. Dichas áreas serán las que podrán participar en ambos dominios. Los números de esas áreas no se usarán en ningún otro lugar de los dos dominios.

La Figura 19 en la página 272 muestra que las áreas de intersección son las áreas 1 y 2. El resto de las áreas puede duplicarse en los dos dominios. En el ejemplo, hay dos áreas 3, 4 y 5 en cada dominio. Tenga en cuenta que nunca será posible permitir una conexión directa entre un nodo del área 3 del dominio A y uno del área 3 del dominio B. Lo mejor que puede hacer es dar a las áreas de intersección la posibilidad de hablar con partes de cada dominio.

Al diseñar la intersección, compruebe que ninguno de los dominios dependa de las rutas que atraviesan la intersección para mantener la conectividad entre áreas que no están en ésta. Como las rutas que entran y salen de la intersección se filtran, es probable que no tengan una posibilidad de alcance normal entre todas las áreas del dominio.

Para decidir cómo configurar los filtros de direccionamiento, establezca un mapa conciso de la configuración. En este mapa localice todas las áreas y trace el contorno de los dos dominios. A continuación, decida sobre la barrera de filtro que necesita establecer. Vaya siguiendo cuidadosamente la intersección de los dos dominios y localice todas las adyacencias de nivel 2 que atraviesan la barrera de filtro. Las adyacencias son vías de comunicaciones de un salto entre direccionadores de nivel 2 que cruzan entre áreas.

En el ejemplo hay seis adyacencias que cruzan la barrera, de 1.18 a 5.7, de 1.18 a 5.8, de 1.18 a 8.3, de 2.17 a 3.12, de 2.21 a 4.7 y de 2.21 a 4.9.

El primer paso para designar los filtros de áreas consiste en establecer filtros que eviten que las áreas de un dominio se propaguen al otro dominio. Las únicas rutas de áreas que deben dejar la intersección son aquellas que van a áreas de la intersección. En el ejemplo, son las áreas 1 y 2. Por consiguiente, sólo las rutas para las áreas 1 y 2 deben enviarse desde nodos como el 2.17 y el 3.12.

En los enlaces de punto a punto como 2.17 y 3.12, no es importante el punto que filtra, pero es probablemente más seguro filtrar en el punto de envío. Por consiguiente, habrá un filtro en la interfaz 2.17 que permita el reenvío únicamente de rutas de las áreas 1 y 2. Lo mismo se produce en las dos interfaces de 2.21 y el enlace entre 1.18 y 8.3.

Cuando el salto entre dos áreas sea una red Ethernet u otro soporte de difusión como 1.18 a 5.7 y 5.8, deberá tomar la decisión basándose en otras cuestiones. La mayoría de las redes Ethernet tienen la mayor parte de los nodos de direccionamiento de nivel 2 en un área y unos cuantos en la segunda área. En este caso, el filtro deberá estar en el área que tiene unos cuantos y no en la que tiene la mayoría. En el ejemplo, el nodo 1.18 es el agente foráneo de la red Ethernet en el área 5, por lo que debe filtrar. El nodo 1.18 debe enviar direccionadores únicamente para las áreas 1 y 2 de la red Ethernet.

Se puede filtrar en ambos extremos de una adyacencia. Esto permite añadir una capa adicional de seguridad contra las reconfiguraciones accidentales. No obstante, si sólo establece el filtro en un extremo, sólo dicho extremo filtrará.

Teniendo en cuenta estos filtros, los dos dominios no podrán contaminarse entre sí. No obstante, en el caso de un nodo de la intersección, no queda claro qué área 3 se alcanzará cuando intente establecerse una conexión con el nodo 3.4. Dependerá de la ruta actual y de los costos de circuito. Está claro que no se trata de una situación ideal. No importa que sólo haya un nodo 3.4 en el dominio A y ninguno en el dominio B. El direccionamiento entre áreas se efectúa únicamente basándose en el área; sólo los direccionadores de un área saben las rutas a los nodos de dicha área.

Por consiguiente, es necesario establecer otro conjunto de filtros para decidir qué instancia de un área (dominio A o B) podrá alcanzarse desde la intersección para cada área que no esté en la mencionada intersección. Puede decidir, por lo tanto, que los nodos de la intersección pueden llegar a las áreas 3 y 4 del dominio A y al área 5 del dominio B. En el ejemplo, esto puede efectuarse configurando los direccionadores 1.18 y 2.21 para que sólo acepten rutas a las áreas 3, 4, 6 y 8 del dominio A. Los direccionadores 2.17 y 2.21 sólo aceptarán rutas para las áreas 5 y 9 del dominio B.

Por consiguiente, los nodos de la intersección ven un universo que contiene las áreas 1 y 2 de la intersección, las áreas 3, 4, 6 y 8 del dominio A y las áreas 5 y 9 del dominio B.

Para configurar el direccionador 1.18 de la Figura 19 en la página 272, entre los parámetros y mandatos de NCP siguientes:

```
NCP> def mod routing-filter circ eth/0 outgoing area 1,2
NCP> def mod routing-filter circ eth/0 outgoing state on
NCP> def mod routing-filter circ eth/0 incoming area 3,4,6,8
NCP> def mod routing-filter circ eth/0 incoming state on
NCP> def mod routing-filter circ ppp/0 outgoing area 1,2
NCP> def mod routing-filter circ ppp/0 outgoing state on
NCP> def mod routing-filter circ ppp/0 incoming area 3,4,6,8
NCP> def mod routing-filter circ ppp/0 incoming state on
```

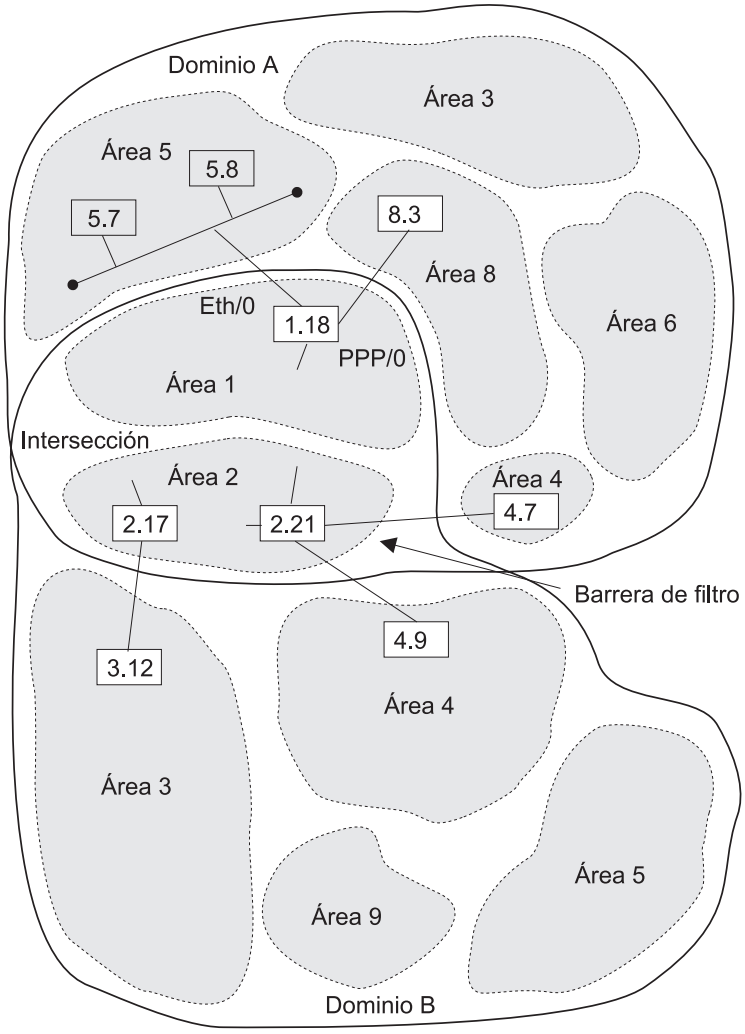


Figura 19. Ejemplo de fusión de dominios de DECnet

Sigue sin haber manera de que un nodo del dominio A área 5 pueda comunicarse directamente con un nodo del dominio B área 5. Para que los nodos de ambas áreas se comuniquen, deberá efectuar una serie de retardos de nivel de aplicación usando el mandato **set host**. Por ejemplo:

- Ejecute el mandato set host para iniciar sesión de forma remota desde un nodo del dominio A área 5 a otro nodo del dominio A área 8.
- Ejecute el mandato set host para iniciar sesión de forma remota desde un nodo del dominio A área 8 a otro nodo del área 1 ó 2.
- Ejecute el mandato set host para iniciar sesión de forma remota desde un nodo del área 1 ó 2 a otro nodo del dominio B área 5.

Configuración de DNA IV

El protocolo DNA IV se ejecuta sobre interfaces de red en anillo, Frame Relay, Ethernet, PPP, clientes de Token-Ring ATM LAN Emulation, clientes de Ethernet LAN Emulation clients y X.25. Las secciones siguientes describen los procedimientos para configurar el protocolo DNA IV para que funcione sobre interfaces de red en anillo y X.25.

Nota: Cuando se trabaje en redes DNA IV y DNA V mezcladas, toda la configuración y supervisión de DNA IV debe efectuarse en el proceso descrito en el presente capítulo.

Consideraciones del algoritmo de DNA IV y DNA V

DNA IV usa un algoritmo de direccionamiento de vector de distancia. DNA V puede usar un algoritmo de vector de distancia o bien un algoritmo de direccionamiento de estado de enlace. El algoritmo seleccionado por el direccionador de puenteo se establece de acuerdo con qué protocolo está habilitado o inhabilitado y las combinaciones que pueden producirse con estos dos protocolos. (Consulte la Tabla 58).

Tabla 58. Consideraciones de algoritmo de DNA IV y DNA V

Estado de DECnet IV	Estado de OSI/DNA V	Algoritmo seleccionado
Habilitado	Inhabilitado	Vector de distancia (automáticamente)
Inhabilitado	Habilitado	Estado de enlace (automáticamente)
Habilitado	Habilitado	Use el mandato **set algorithm** para configurar esta información en la SRAM.

Configuración de DNA IV para red en anillo

El procedimiento para ejecutar el protocolo DNA IV sobre 802.5 Token Ring (TR) implica a mandatos de los procesos de configuración de DNA IV y la red en anillo.

1. Desde el indicador OPCON (*) entre en el proceso de configuración.

```
* talk 6
Config>
```

2. Entre **list device** para ver los números de interfaces para las interfaces de la red en anillo. Apunte el número de interfaz de cada interfaz de la red en anillo.

```
Config> list device
```

3. Use el mandato **network** con el número de la interfaz de la red en anillo que desee configurar. Esto lo situará en el proceso de configuración de la red en anillo.

```
Config> network 0
TKR config>
```

4. Use el mandato **list** para verificar la información de configuración de la red en anillo.

```
TKR config> list

Token-Ring configuration:

Packet size (INFO field):    2052
Speed:                       4 Mb/sec
Media:                       Shielded

RIF Aging Timer:             120
Source Routing:              Enabled
Mac Address    000000000000
```

5. Salga del proceso de configuración de la red en anillo y entre en el de configuración de DNA NCP.

```
TKR config> exit
Config> protocol DN
NCP>
```

6. Use el mandato **define** para definir un circuito DNA en la interfaz de la red en anillo.

   ```
   NCP> define circuit tkr/0 state on
   ```

7. Opcionalmente, use el mandato **define** para establecer el tipo de direccionamiento para el circuito. Para el soporte bilingüe o de Phase IV, deberá cambiar el tipo de direccionamiento y pasar del valor por omisión (estándar) a bilingüe o AMA.

   ```
   NCP> define circuit tkr/0 router type bilingual

                      o-

   NCP> define circuit tkr/0 router type AMA
   ```

8. Use el mandato **list** para comprobar los parámetros.

   ```
   NCP> list circuit tkr/0 characteristics
   Circuit Permanent Characteristics
   Circuit             = TKR/0
   State               = On
   Cost                = 4
   Router priority     = 64
   Hello timer         = 15
   Max routers         = 16
   Router type         = Standard
   ```

9. Reinicie el direccionador para que todos los parámetros configurados entren en vigor.

Nota: Si desea inhabilitar el direccionamiento de origen o establecer el temporizador RIF en un valor que no sea el valor por omisión, use los mandatos **source-routing** y **set RIF-timer** en el proceso de configuración de la red en anillo.

Configuración de DNA IV para X.25

El procedimiento para ejecutar el protocolo DNA IV sobre circuitos X.25 implica a mandatos de los procesos de configuración de X.25 y DNA IV .

1. Desde el indicador OPCON (*) entre en el proceso de configuración. Vaya a "t 6" y entre X.25 config (# red). Si es la primera vez que configura X.25 haga lo siguiente:

   a. DEFINA la dirección DTE del direccionador.

      ```
      X.25 Config> set address
      ```

   b. DEFINA cada protocolo que tendrá soporte sobre X.25:

      ```
      X.25 Config> add protocol
      ```

      IP Por lo general es buena idea añadir este protocolo para poder verificar si la configuración de X.25 general es correcta

      DN

      Nota: Permita que los parámetros del protocolo tomen los valores por omisión.

   c. DEFINA la correlación de la dirección remota del protocolo con la dirección X.25 remota para los protocolos que así lo requieran:

      ```
      X.25 Config> add address
      ```

      para IP:

      - Dirección IP = 128.185.247.22
      - Dirección X.25 = 22

para DN:

- Dirección DN = 5.22
- Dirección X.25 = 22

d. VERIFIQUE que un extremo del circuito X.25 es un DTE y que el otro extremo es DCE.

```
X.25 Config> list all
```

Compruebe en el campo National Personality (Personalidad nacional) el tipo de dispositivo. En el caso del tipo de personalidad nacional de GTE-Telenet, verá:

```
National Personality: GTE Telenet (DTE)

                -o-

National Personality: GTE Telenet (DCE)
```

Para cambiar el tipo de dispositivo a DCE, entre:

```
X.25 Config> set equipment-type dce
```

Listará todos los parámetros configurados para X.25

National Personality: GTE Telenet (DTE) National Personality: GTE Telenet (DCE)

Si no es así, elija un direccionador para que actúe como DCE y modifíquelo como tal,

```
X.25 Config> set national-personality dce
```

e. REINICIE el direccionador para que todos los parámetros configurados entren en vigor.

f. Para VERIFICAR que la configuración es válida después de un reinicio, vaya al lado del monitor y observe si el enlace se está activando.

```
* t
5
+ c
```

Esto le indicará el estado del enlace en ese momento. Si ve que el estado del enlace de X.25 pasa de “testing” a “down”, vaya a los mensajes ELS y compruebe si se ha producido un error evidente. Si el estado del enlace de X.25 pasa de “testing” a “up”, es muy posible que la configuración de X.25 sea válida.

2. Para VERIFICAR que el enlace de X.25 es operativo:

a. INTENTE ejecutar un PING en cada extremo del enlace de X.25 desde el monitor de IP:

```
IP> interface
```

Verifique que se hayan configurado las direcciones de X.25 correctas en el protocolo IP.

IP> **ping** *dirección IP del enlace de X.25 remoto*

3. Para CONFIGURAR DECnet PhaseIV en el direccionador:

a. DEFINA los parámetros de DECnet Executor:

NCP> **define exec address** *área.nodo* Dirección DECnet del direccionador

NCP> **define exec type DEC-ROUTING-IV** Configura el direccionador como un direccionador de tipo LEVEL 1 DEC

Nota: Este ejemplo sirve para configurar un direccionador para que trabaje con otros direccionadores que dan soporte al estándar de direccionamiento DEC sobre redes X.25. Un direccionador que dé soporte al estándar debe definirse como tipo DEC-ROUTING-IV (nivel 1) o DEC-AREA (nivel 2). El tipo de direccionamiento por omisión es ROUTING-IV y AREA, lo que permite trabajar con varios IBM 2210 existentes y otros direccionadores compatibles.

NCP> **define exec state on**

Reinicie el direccionador para que cuando configure el circuito X.25, todos los parámetros específicos de DEC sean visibles. Para verificar la configuración del ejecutar, NCP> **show executor characteristics**

b. DEFINA circuitos de PhaseIV X.25.

Debe configurar el circuito X.25 como PVC o SVC. Si se configura este circuito como PVC, el otro extremo también tendrá que ser un PVC. Si se configura este circuito como un IN-SVC, el otro extremo deberá configurarse como un OUT-SVC

```
NCP>  define cir x25/0 usage IN-SVC
NCP> define cir x25/0 DTE-address "remote X.25 DTE"
NCP> define cir x25/0 call-data
NCP> define cir x25/0 verification enabled
```

La habilitación de la verificación es opcional.

c. DEFINA circuitos en el estado activo:

- para la red en anillo

  NCP> **define cir TKR/0 router type bilingual**

- para TODOS los circuitos

  NCP> **define cir** *xxx* **state on**

Reinicie el direccionador para que todos los parámetros de DECnet entren en vigor, VERIFIQUE que la configuración de X.25 en el protocolo DECnet es tal como la desea.

```
NCP> list circuit x25/0 characteristics
```

Configuración y supervisión de DNA IV

Mandatos de configuración y supervisión de DNA IV

Esta sección describe los mandatos de supervisión y configuración de NCP. Entre los mandatos en el indicador NCP>. Puede accederse a ***todos*** los mandatos de NCP desde los entornos de configuración o de supervisión.

Tabla 59. Mandatos de configuración y supervisión de NCP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxv.
define	Define elementos de la base de datos no volátil (permanente), incluidos: • Listas de control de acceso y filtros de direccionamiento • Elementos de circuitos • Argumentos globales para DNA • Datos de configuración de los nodos
purge module	Elimina listas de control de acceso y filtros de direccionamiento de la base de datos permanente.
set	Establece o cambia elementos de la base de datos volátil, incluidos: • Elementos de circuitos • Argumentos globales para DNA • Datos de configuración de los nodos
show	Muestra el estado de la base de datos volátil y nodos volátiles de la base de datos de direccionamientos.
show/list	Muestra elementos de la base de datos volátil (show) o permanente (list), incluyendo: • El estado actual de los circuitos especificados • El estado actual de la base de datos volátil/permanente para DNA • Las listas de control de acceso de DECnet que se han definido en la base de datos permanente para el direccionador • Los filtros de direccionamiento de áreas de DECnet que se han definido en la base de datos permanente para el direccionador
zero	Borra los contadores de circuito de la base de datos volátil, los contadores globales de la base de datos volátil y los contadores del módulo de la lista de control de acceso. *No* borra los valores de los argumentos establecidos con los mandatos **set** o **define**.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxvi.

Tenga en cuenta la información siguiente sobre los mandatos:

1. Los mandatos **define** no entran en vigor hasta la siguiente vez que se inicia el direccionador.
2. Los mandatos **list, define** y **purge** modifican o muestran datos en la base de datos permanente (RAM estática del direccionador). La base de datos permanente se almacena en la configuración y se aplica en todos los reinicios, cargas de software y ciclos de alimentación.
3. Los mandatos **show** y **list** son los más útiles para supervisar el protocolo DNA IV.
4. Use **set, show** y **zero** para modificar, visualizar o borrar datos de la base de datos volátil.
5. El mandato **zero** borra las estadísticas guardadas en la base de datos volátil, pero ***no*** borra los valores de argumento establecidos con los mandatos set o define.

Define/Set

Esta sección explica los mandatos **define** y **set**.

Use el mandato **define** para definir listas de control de accesos y filtros de direccionamiento y para definir parámetros de circuito, ejecutor y nodo. **Define** se usa para establecer la SRAM (necesita un reinicio).

Sintaxis:

d**efine**	circuit-specifier . . .
	executor . . .
	module access-control . . .
	module routing-filter . . .
	node . . .

Set puede usarse para la RAM volátil (cambio inmediato, no es necesario un reinicio).

Sintaxis:

s**et**	circuit-specifier . . .
	executor . . .
	node . . .

circuit-specifier *argumento*

Las opciones de *circuit-specifier* incluyen:

active circuits
Especifica todos los circuitos que están activos y cuyo estado sea on (activo) (únicamente para set).

all circuits
Especifica todos los circuitos del direccionador.

circuit name
El nombre del circuito. Por ejemplo: Eth/0, TKR/0, PPP/1.

known circuits
(únicamente **set**) Especifica todos los circuitos del direccionador.

Los *argumentos* incluyen:

call-userdata
Se usa durante la inicialización de los circuitos X.25 estáticos. Cuando se define un circuito como SVC de salida, las solicitudes de llamada inicial y posteriores contienen los datos de usuario de llamada definidos al habilitar el circuito. Cuando se define un circuito como SVC de entrada, uno de los criterios seguidos para aceptar una solicitud de llamada de entrada es una coincidencia de los datos del usuario de llamada definidos.

Actualmente los datos del usuario de llamada deben establecerse en el DTE del direccionador local para los SVC de llegada y de salida.

Entre un número par de caracteres hexadecimales (octetos) que tenga un máximo de 14 caracteres.

cost [rango]
Establece el coste de la recepción de un paquete en este circuito. Lo usa el algoritmo de direccionamiento para determinar el coste de un circuito al elegir rutas (el coste no es lo mismo que una métrica de IP). Rango: De 1 a 25. Valor por omisión: 4.

Los valores siguientes son puntos de inicio sugeridos:

Tipo de circuito	*Coste*
Ethernet	4
Red en anillo 4/16	4
Sync 56 Kb	6
Sync T1	5
X.25	25

Ejemplo:

```
define circuit tkr/0 cost 5
```

DTE Address
Especifica la dirección del DTE remoto del circuito X.25. Se trata siempre de la dirección del sistema remoto. Es un número decimal con un máximo de 14 caracteres.

hello timer [rango]
Especifica la frecuencia (en segundos) con la que se envían hellos del direccionador en este circuito. Rango: De 1 a 8191 segundos. Valor por omisión: 15 segundos (recomendado).

maximum recalls
(sólo **define**) Especifica cuántos intentos debe hacer el direccionador para volver a establecer una llamada de un SVC estático de salida después de un fallo inicial de la

llamada. Después de alcanzar el número máximo de rellamadas, el direccionador ya no efectúa ningún intento de establecer el SVC sin la intervención del usuario. Los valores válidos están en el rango incluido entre 1 y 20; el valor por omisión es 1. Consulte también el argumento recall timer.

maximum routers [rango]

(sólo **define**) Especifica cuántos direccionadores más puede haber en este circuito. Rango: De 1 a 33. Valor por omisión: 16.

Nota: El usuario no puede configurar este parámetro en un circuito X.25 cuando el *tipo* de ejecutor se establece en DEC-routing-IV o DEC-area. En dicho caso, el número máximo de direccionadores es 1.

Si se trata de un direccionador de nivel 1, sólo cuentan los direccionadores de este circuito de la misma área. Si se trata de un direccionador de nivel 2, cuentan todos los direccionadores de este circuito. El direccionador local no cuenta en relación con el límite.

Los requisitos de memoria y eficacia del direccionador mejoran manteniendo bajo este número. Establezca este argumento en valor algo superior al número total de direccionadores adyacentes en el circuito. No lo establezca en un valor inferior al número de direccionadores del circuito; pueden producirse anomalías en el direccionamiento.

Nota: En el caso de un circuito de punto a punto (línea síncrona), establezca este argumento en 1. Conseguirá obtener ahorros significativos de memoria en un direccionador con varias líneas de punto a punto.

La suma del número máximo de direccionadores sobre los circuitos debe ser inferior al argumento del número máximo de los direccionadores de difusión, aunque este límite no se aplica con rigurosidad.

recall timer

Determina el retardo, en segundos, entre los intentos de llamada para establecer un circuito estático de salida X.25.

Para **define**, los valores válidos están en el rango incluido entre 1 y 60 segundos. El valor por omisión es 1 segundo. Consulte también el argumento maximum recalls.

Para **set**, los valores válidos están en el rango incluido entre 0 y 65595. El valor por omisión es 60 segundos.

router priority [rango]

Especifica la prioridad del direccionador en las solicitudes para convertirse en el direccionador de los nodos finales de este circuito. Rango: De 1 a 127, donde 127 es la mayor prioridad. Valor por omisión: 64.

Si dos direccionadores tienen la misma prioridad, aquel que tenga la dirección de nodo más elevada ganará. La prioridad de direccionador no influye en las decisiones de

direccionamiento de área o cuando se intenta alcanzar el direccionador de nivel 2 conectado más cercano.

Utilice la prioridad de direccionador para elegir el direccionador designado para que sea el que tenga más probabilidades de convertirse en el mejor salto siguiente de los nodos finales del circuito. Si un circuito tiene dos direccionadores, uno de ellos con 500 nodos tras él y el otro con 20, el que tenga los 500 nodos deberá tener mayor prioridad de direccionador. No obstante, esto no es obligatorio, ya que una vez que un paquete de un nodo final alcance un direccionador, será reenviado a su destino.

Este argumento es irrelevante en las líneas de punto a punto, donde no hay nodos finales. (De todas maneras se selecciona un direccionador designado).

router type

Especifica el tipo de direccionamiento que debe efectuar el direccionador: standard (estándar), AMA o bilingual (bilingüe).

- *Standard*. Especifica que el direccionador está usando el direccionamiento phase IV convencional donde la dirección del MAC se crea a partir del número de nodo y de área. El direccionador tiene como valor por omisión este tipo.

- *AMA*. Especifica que el direccionador puede direccionar paquetes que usan el direccionamiento phase IV donde la dirección del MAC es arbitraria y se sabe por la capa de enlace de datos.

- *Bilingual*. Especifica que el direccionador puede direccionar paquetes que usan el direccionamiento convencional y phase IV con AMA.

state Cuando se establece en **on**, especifica que el circuito está habilitado para que lo use DNA. Cuando se establece en **off**, especifica que el circuito está inhabilitado para que lo use DNA. **off** es el valor por omisión.

usage Especifica si un circuito X.25 es:

- PVC: Un circuito virtual permanente
- OUT-SVC: Un circuito estático de salida
- IN-SVC: Un circuito estático de entrada

  Este parámetro se aplica cuando el tipo de ejecutor está establecido en *DEC-routing-IV* o *DEC-area*. (Consulte **circuit executor type** para obtener más información).

verification

Especifica si el direccionador compara una serie de caracteres de verificación en el direccionador, en los datos de verificación de un mensaje de inicialización de entrada. Si no coinciden, deberá reinicializarse el circuito X.25. Debe especificar enabled (habilitado) o disabled (inhabilitado).

executor *argumento*

Define o establece argumentos (es decir, el ejecutor) globales para DNA en la base de datos permanente (**define**) o volátil (**set**).

La mayoría de estos argumentos reducen la eficacia del direccionador y aumentan la carga en los circuitos, ya que se amplían. También pueden aumentar los requisitos de memoria. No deben exceder los valores necesarios para la configuración de red actual.

Para **set**, el ejecutor debe estar desactivado para modificar los argumentos numéricos o escribir en la base de datos volátil. (A diferencia de DECnet-VMS, el mandato **set executor state on** es válido cuando el estado del ejecutor esté desactivado). Estos cambios se producen inmediatamente sin que sea necesario reiniciar el direccionador.

address [área.nodo]

Establece la dirección de nodo del ejecutor, el ID de nodo de este direccionador. Rango de área: De 1 a 63. El área y el nodo deben ser inferiores al área máxima del ejecutor. El rango de nodo está incluido entre 1 y 1023. El valor por omisión 0.0 es ilegal.

Nota: DNA no se habilitará si la dirección del ejecutor no se establece en un valor legal.

area maximum cost [número]

El costo máximo permitido entre este direccionador de nivel 2 y cualquier otro direccionador de nivel 2. Si la mejor ruta a un área es más costosa que este valor, se considerará que dicha área no se puede alcanzar. Máximo: 1022. Valor por omisión: 1022. Este argumento no se aplica a los direccionadores de nivel 1. Debería ser superior al costo legal máximo al área más distante. Se sugiere el valor “area maximum hops” multiplicado por 25.

area maximum hops [número]

Número máximo de saltos permitidos entre este direccionador de nivel 2 y cualquier otro direccionador de nivel 2. Si la mejor ruta a un área requiere más saltos que los indicados, se considerará que dicha área no se puede alcanzar. Máximo: 30. Valor por omisión: 30. Este argumento no se aplica a los direccionadores de nivel 1. Debería ser el doble de la longitud de vía de acceso más larga (en saltos) de lo que se espera.

El direccionamiento usa la cuenta de saltos únicamente para acelerar el abandono de rutas a las áreas que son inaccesibles. Area maximum hops puede reducirse para que las áreas que no son accesibles se conviertan en inaccesibles con mayor rapidez.

broadcast routing timer [rango]

Especifica la frecuencia de envío, en segundos, de los mensajes de nivel 1 (y 2 en un direccionador de nivel 2). Indica la frecuencia con la que se enviarán en ausencia de cualquier cambio de costo o adyacencia. Este parámetro sirve para proteger la base de datos de direccionamientos contra la corrupción. Si algún costo o adyacencia cambia, se envían

automáticamente, como mínimo, actualizaciones parciales de direccionamiento. Rango: De 1 a 65535. Valor por omisión: 180. Los valores inferiores aumentan la actividad general de este direccionador así como la del resto de los direccionadores adyacentes. Los valores más grandes aumentan el tiempo necesario para corregir la base de datos de direccionamientos si se pierde un mensaje de actualización parcial de direccionamientos.

maximum address number [rango]
(sólo **define**) La dirección de nodo más grande (dentro de esta área) para la que este direccionador mantendrá rutas. La base de datos de direccionamientos no incluirá rutas a nodos de esta área cuya parte de nodo sea superior a la dirección. Rango: De 1 a 1023. Valor por omisión: 32. Debe ser superior a la dirección de nodo más grande del área del direccionador. Si el valor que establece es demasiado grande, esto influirá en la eficacia del direccionador y utilizará una cantidad excesiva de memoria. Este argumento no entrará en vigor hasta que se reinicie el direccionador.

maximum area number [número]
(sólo **define**) El área superior para las que se mantendrán rutas, si se trata de un direccionador de nivel 2. La base de datos de direccionamientos no incluirá rutas a áreas superiores a esta. Máximo: 63. Valor por omisión: 63. Debe ser superior al número de área superior de toda la red. Este argumento no entrará en vigor hasta que se reinicie el direccionador.

maximum broadcast nonrouters [número]
(sólo **define**) Número máximo de nodos finales que pueden ser adyacentes (a un salto) de este direccionador. Se trata de la suma de todos los circuitos de difusión. Si hay más nodos finales, este direccionador no podrá alcanzar algunos de ellos, lo cual puede provocar problemas de direccionamiento imprevisibles. Este argumento no entrará en vigor hasta que se reinicie el direccionador. Rango: De 1 a 1023. Valor por omisión: 63.

maximum broadcast routers [número]
(sólo **define**) Número máximo de direccionadores que pueden ser adyacentes (a un salto) de este direccionador. Se trata de la suma de todos los circuitos de difusión. Si hay más direccionadores, no se aceptarán las rutas de los direccionadores sobrantes. Esto puede provocar problemas de direccionamiento imprevisibles. Este argumento no entrará en vigor hasta que se reinicie el direccionador. Valor por omisión: 32. Máximo: el número de circuitos multiplicado por 33. Este valor debe ser superior o igual a la suma de "circuit maximum routers" de todos los circuitos, aunque este punto no se aplique con rigurosidad. Este parámetro tiene una gran influencia en la utilización de la memoria y no debe establecerse en un valor que sea demasiado superior al necesario. Dado que el valor por omisión es bastante alto, es

posible que tenga que reducirlo si ha establecido el parámetro “maximum address” en un valor también alto.

maximum cost [número]
El costo máximo permitido entre este direccionador y cualquier otro nodo del área. Si la mejor ruta a un nodo es más costosa que este valor, se considerará que dicho nodo no se puede alcanzar. Máximo: 1022. Valor por omisión: 1022. Debería ser superior al costo legal máximo al nodo más distante. Se sugiere el valor del parámetro “maximum hops” multiplicado por 25.

maximum hops [número]
Número máximo de saltos permitidos entre este direccionador y cualquier nodo del área. Si la mejor ruta a un nodo requiere más saltos que los indicados, se considerará que dicho nodo no se puede alcanzar. Máximo: 30. Valor por omisión: 30. Debería ser el doble de la longitud de vía de acceso más larga (en saltos) de lo que se espera. El direccionamiento usa la cuenta de saltos únicamente para acelerar el abandono de rutas a nodos que son inaccesibles. El parámetro maximum number of hops puede reducirse para que los nodos que son inaccesibles se conviertan en inaccesibles con mayor rapidez.

maximum visits [número]
Especifica que cualquier paquete que este direccionador reenvíe y que se haya reenviado más veces de las indicadas en el parámetro de los direccionadores de número máximo de visitas, se eliminará. Se usa para detectar paquetes que están en bucles de direccionamiento, lo que se produce cuando las rutas se abandonan. El número máximo de visitas es 63. Este es el valor por omisión. Este argumento debe ser superior, en un valor al cuadrado, a los parámetros maximum hops y area maximum hops.

state on Habilita DNA. Puede emitirse en cualquier momento, siempre y cuando el direccionador tenga una dirección de nodo válida.

state off Inhabilita DNA. Puede emitirse en cualquier momento. El estado por omisión es off (desactivado).

En el caso de **set**, **set executor** se inhibirá si la inicialización de DNA falló debido a falta de memoria disponible para las tablas de direccionamientos.

type (sólo **define**) En los circuitos X.25, provoca que el direccionador actúe según una de las cuatro maneras siguientes, según el valor seleccionado. Las opciones son:

DEC-routing-iv
configura el direccionador como un direccionador de nivel 1 compatible con DEC.

DEC-area
configura el direccionador como un direccionador de nivel 2 (área) compatible con DEC.

Routing-iv
configura el direccionador como un direccionador de nivel 1 sin compatibilidad con DEC en los circuitos X.25. Este es el valor por omisión.

Area configura el direccionador como un direccionador (área) de nivel 2 sin compatibilidad con DEC en los circuitos X.25.

Un direccionador de nivel 2 acepta las adyacencias con direccionadores de otras áreas y mantiene rutas a todas las áreas. Si puede llegar a otras áreas, también se anuncia a los direccionadores de nivel 1 como una ruta a otras áreas.

En el caso de los direccionadores de nivel 1, se aceptan únicamente las adyacencias con otros direccionadores de la misma área.

Ejemplo:
```
define executor state on
define executor type DEC-area
define executor maximum broadcast routers 10
```

type area (sólo **set**) Hace que el direccionador actúe como un direccionador de nivel 2. Este direccionador aceptará las adyacencias con direccionadores de otras áreas y mantendrá rutas a todas las áreas. Si puede llegar a otras áreas, también se anunciará como ruta a otras áreas a los direccionadores de nivel 1.

El estado de DNA debe estar establecido en *off* antes de cambiar el *tipo*.

type routing-IV
(sólo **set**) Hace que el direccionador actúe como un direccionador de nivel 1, que es el valor por omisión. Las adyacencias sólo se aceptarán para las rutas de la misma área.

El estado de DNA debe estar establecido en *off* antes de cambiar el *tipo*.

Ejemplo:
```
set executor state on
set executor maximum broadcast routers 10
```

m**odule access-control** *argumento especificador de circuito*
(sólo **define**) Define las listas de control de acceso que se usan para restringir el reenvío de paquetes entre algunos orígenes y destinos. Cada lista de acceso se asocia a un circuito y se aplica a los paquetes de datos de formato largo de DECnet recibidos en dicho circuito. El control de acceso no se aplica a ningún paquete hello o de direccionamiento.

Los argumentos para los especificadores de circuitos incluyen:

all circuits
Especifica todos los circuitos del direccionador.

circuit name
Especifica el circuito nombrado.

known circuits
Especifica todos los circuitos del direccionador.

Los elementos siguientes son argumentos que puede seleccionar después de entrar el mandato **define module access-control** y el especificador de circuito:

state on Habilita la lista de control de acceso en este circuito.

state off Inhabilita la lista de control de acceso en este circuito.

type exclusive
Especifica que los paquetes que coincidan con uno o varios filtros de la lista de control de acceso de esta interfaz se eliminarán.

type inclusive
Especifica que sólo los paquetes que coincidan con uno o varios filtros de la lista de control de acceso de esta interfaz se reenviarán.

filter [resultado-origen máscara-origen resultado-destino máscara-destino]
Añade un filtro a la lista del circuito especificado. Se añade el filtro al final de la lista existente.

Se enmascara la dirección de origen con la máscara de origen y se compara con el resultado del origen. Lo mismo se hace con la máscara de destino y el resultado de destino. La acción dependerá del tipo de control de acceso que se use en el circuito.

Los elementos siguientes son las opciones en las que selecciona después de entrar el mandato **define module access-control** y el especificador de circuitos **filter**:

source-result
Dirección con la que se compara la dirección de origen después de enmascararla.

source-mask
Máscara usada para la dirección de origen.

dest-result
Dirección con la que se compara la dirección de destino después de enmascararla.

dest-mask
Máscara usada para la dirección de destino.

Ejemplo: `define module access-control circuit eth/0 state on`

m**odule** r**outing-filter** *argumento especificador de circuito*
(sólo **define**) Define los filtros de direccionamiento que se usan para restringir el envío de rutas de área por direccionadores de nivel 2 (Executor Type Area).

all circuits
Especifica todos los circuitos del direccionador.

circuit name
Especifica el circuito nombrado.

known circuits
Especifica todos los circuitos del direccionador.

Los elementos siguientes son las opciones de dirección que selecciona después de entrar el mandato **define module routing-filter** y el especificador de circuitos:

incoming Influye en el filtro de información de direccionamiento recibido en este circuito.

outgoing Influye en el filtro de información de direccionamiento enviado en este circuito.

Los elementos siguientes son los argumentos que selecciona después de entrar el mandato **define module routing-filter** y el especificador de circuitos:

area [lista áreas]
Especifica que el filtro permite que la información de direccionamiento pase por el conjunto de áreas establecido en la lista de áreas. La lista de áreas es un lista de áreas o rangos de áreas separadas por comas. Los rangos se especifican con dos números de área separados por un guión. La lista de áreas puede no tener ningún contenido, con lo que se especifica que la información no se pasará a ninguna área. A continuación se muestran ejemplos de listas de áreas:

1,4,9,60 Áreas 1, 4, 9 y 60

1-7,9-13,23
Áreas 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13 y 23

state on Especifica que el filtro está activo.

state off Especifica que se ha inhabilitado el filtro pero que continúa almacenado en la base de datos permanente. La única forma de sacar el filtro consiste en usar el mandato **purge**.

Ejemplo: **`define module routing-filter circuit eth/0 state on`**

node *argumento*
Permite definir o establecer información de configuración en nodos de la base de datos volátil (**set**) o permanente (**define**). El único nodo del que se mantiene información es el nodo ejecutor, ya que los nombres de nodo no se almacenan. El nodo especifica la dirección de nodo del direccionador (del ejecutor). Consulte la descripción del mandato **define executor**.

Ejemplo: **`define node state on`**

Ejemplo: **`set node state on`**

Purge

Use el mandato purge para eliminar listas de control de acceso y filtros de direccionamiento de la base de datos permanente.

Sintaxis:

p**urge** module access-control . . .

module routing-filter . .

module access-control *especificador de circuito*
Elimina listas de control de acceso de la base de datos permanente. Puede suprimir una lista de control de acceso completa; no se puede suprimir un filtro.

all circuits
Especifica todos los circuitos del direccionador.

circuit name
Especifica el circuito nombrado.

Ejemplo: `purge module access-control all circuits`

module routing-filter *especificador de circuito*
Elimina filtros de direccionamiento de la base de datos permanente. Puede depurar un filtro especificado o bien depurarlos todos.

Las opciones para los especificadores de circuitos son las siguientes:

all Especifica todos los filtros de direccionamiento de la memoria de configuración.

circuit name
(Nombre circuito) Especifica el filtro de direccionamiento del circuito nombrado.

Ejemplo: `purge module routing-filter all`

Set

Use el mandato **set** para añadir, establecer o modificar especificadores de circuito, argumentos globales, módulos de enlace de datos o nodos de la base de datos DNA volátil.

Sintaxis:

set circuit . . .
executor . . .
node . . .

Para leer una descripción de estas opciones, consulte “Define/Set” en la página 278.

Show

Use el mandato show para mostrar el estado de la base de datos volátil y los nodos volátiles de la base de datos de direccionamientos.

Sintaxis:

show area-specifier . . .
node-specifier . . .

area-specifier *argumento*
Examina el estado de la base de datos de direccionamientos de área volátil. Esto le permite saber qué áreas puede alcanzar y qué rutas hay para las diferentes áreas.

Las opciones para los especificadores de área son las siguientes:

active areas
Proporciona información sobre las áreas que se pueden alcanzar actualmente.

all areas Proporciona información sobre todas las áreas (hasta el área máxima del ejecutor).

area Proporciona información sobre el área especificada. Si no indica el área, se le solicitará que la indique.

known areas
Proporciona información sobre las áreas que se pueden alcanzar actualmente.

Los elementos siguientes son las opciones de submandato que puede seleccionar después de entrar el mandato **show** y el especificador de área:

characteristics
Muestra el estado actual del área especificada. (Lo mismo que summary).

status Proporciona información detallada sobre las áreas especificadas, incluyendo el costo y los saltos.

summary Muestra el estado actual de las áreas especificadas. Este es el valor por omisión.

Ejemplo.: **`show active areas`**

```
Active Area Volatile Summary
Area State       Circuit Next
                         Node
1    reachable    Eth/0  1.22
2    reachable           2.26
3    reachable    X25/0  2.30
```

Ejemplo: **`show active areas status`**

```
Active Area Volatile Status
Area State       Cost Hops Circuit Next
                                   Node
1    reachable   3    1     Eth/0  1.22
2    reachable   0    0           2.26
3    reachable   2    1     PPP/0  3.9
6    reachable   12   3     PPP/0  3.9
3    reachable   11   1     X25/0  2.30

Area Volatile Status
Area State       Cost Hops Circuit Next
                                   Node
5    unreachable 1023  31
```

Los elementos siguientes definen la información que aparece cuando usa el mandato **show**.

area (área) Indica el área de esta línea de la pantalla.

circuit (Circuito) Indica a qué circuito irá el salto siguiente a este nodo. No se da ningún circuito para el área propia del direccionador.

cost (Costo) Indica el costo a esta área.

hops (Saltos) Indica los saltos a esta área.

next node
(nodo siguiente) Indica qué direccionador será el salto siguiente (destino intermedio) al área especificada.

state (estado) Indica que se podrá alcanzar o no.

node-specifier *argumento*

Muestra el estado de la base de datos de direccionamientos de nodos volátil; se incluye información sobre los nodos que pueden alcanzarse y cuáles son las rutas que llevan hacia ellos.

Los especificadores de nodo pueden ser uno de los especificadores siguientes:

active nodes
Proporciona información sobre todos los nodos que pueden alcanzarse actualmente.

all nodes Proporciona información sobre todos los nodos (hasta la dirección máxima del ejecutor). Una visualización de todos los nodos incluye información sobre el área.0 de la "pseudomodalidad". Cualquier direccionador de nivel dos que alcance otras áreas anunciará la ruta al área.0 de nodo. Los direccionadores de nivel uno usan estas rutas para reenviar todos los paquetes al direccionador de nivel uno más cercano que sepa cómo llevar el paquete al área correcta. No existe otra manera de examinar el nodo 0, ya que no se trata de una dirección de nodo legal.

node node
Proporciona información sobre el nodo especificado. Si no se indica el nodo, se le solicitará que lo indique.

known nodes
Proporciona información en los nodos que se pueden alcanzar en la actualidad.

Los argumentos incluyen:

characteristics/ summary
Ambas opciones de submandatos muestran el estado actual de los nodos especificados.

status Proporciona información detallada sobre los nodos especificados, incluyendo el costo y los saltos.

Ejemplo: **`show node status`**

Este ejemplo muestra el estado detallado de un nodo específico.

```
Which node [1.9]? 2.26
Node Volatile Status
Executor node            = 2.26 (gato)
State                    = on
Physical address         = AA-00-04-00-1A-08
Type                     = DEC-area
```

Ejemplo: **`show active nodes`**

Este ejemplo muestra los nodos que se pueden alcanzar.

```
Active Node Volatile Summary
Executor node            = 2.26 (gato)
State                    = on
Identification           = DECnet-MC68360 V1 R2.0 NP00523
[P10]

Node    State      Circuit Next
Address                    Node
2.14   reachable    Eth/0  2.14
2.34   reachable    PPP/0  2.34
2.37   reachable    PPP/0  2.34
1.22   reachable    Eth/0  1.22
```

Ejemplo: **`show adjacent nodes status`**

Este ejemplo muestra información de direccionamiento detallada sobre todos los nodos adyacentes. Sólo se mostrarán los nodos que tengan un salto. Sólo se sabe y se muestra el tipo de nodo de los nodos adya-

centes ya que esta información sólo está contenida en los mensajes hello.

```
Adjacent Node Volatile Status

Executor node            = 2.26 (gato)
State                    = on
Physical address         = AA-00-04-00-1A-08
Type                     = DEC-area
Node    State       Type       Cost  Hops Circuit  Next
Addr                                             Node
2.14  reachable  routing IV     3    1    Eth/0   2.14
2.34  reachable  routing IV     2    1    PPP/0   2.34
2.42  reachable  nonrouting IV  2    1    PPP/0   2.42
1.22  reachable  area           3    1    Eth/0   1.22
```

Show/List

Use el mandato **show circuit** para recuperar información sobre el estado actual de los circuitos especificados de la base de datos volátil. El mandato **list circuit** recupera los datos almacenados en la base de datos permanente para los circuitos.

Sintaxis:

show
- all
- area
- circuit . . .
- executor . . .
- known *argumento*
- module *argumento*
- node *argumento*

Sintaxis:

list
- all
- area
- circuit *argumento*
- executor *argumento*
- module
- node *argumento*

circuit-specifier *argumento*

Las opciones de los especificadores de circuito son las siguientes:

active circuits
: Especifica todos los circuitos que están actualmente activados (por base de datos volátil).

all circuits
: Especifica todos los circuitos del direccionador.

circuit name
: (nombre circuito) Especifica el circuito nombrado.

known circuits
: Especifica todos los circuitos del direccionador.

Los elementos siguientes son las opciones de submandato que selecciona después de entrar el mandato y el especificador de circuito:

characteristics
Proporciona información detallada sobre todos los valores de argumentos para el circuito.

counters Muestra los contadores del circuito.

status Muestra información detallada sobre el circuito de la base de datos volátil.

summary Muestra información resumida sobre el circuito de la base de datos volátil. Se trata del valor por omisión si no se proporciona ningún argumento.

Ejemplo: `show all circuits`

```
Circuit Volatile Summary

Circuit State       Adjacent
                      Node

X25/0   on           5.25
Eth/0   on           1.22
Eth/0                2.14
Eth/0                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                2.14     1498
Eth/0                1.13     1498
X25/0   on           5.25     1498
```

Ejemplo: `show all circuits characteristics`

Este ejemplo muestra las características actuales de los circuitos de esta máquina. Esto incluye todos los argumentos de la configuración, así como las adyacencias actuales y el temporizador de escucha (el temporizador hello de la adyacencia multiplicado por tres).

```
Circuit Volatile Characteristics

Circuit           = Eth/0

State                   = on
Designated router  = 2.26
Cost               = 4
Router priority    = 64
Hello timer        = 15
Maximum routers    = 16
Adjacent node      = 1.22
  Listen timer     = 45
Adjacent node      = 2.14
  Listen timer     = 45
Adjacent node      = 2.39
  Listen timer     = 90

Circuit           = PPP/0

State             = off
Designated router  =
Cost               = 4
Router priority    = 64
Hello timer        = 15
Maximum routers    = 8
```

Ejemplo: `show circuit eth/0 counters`

Este ejemplo muestra los contadores que existen para los circuitos. Tenga en cuenta que algunos de los contadores que DECnet-VAX lleva no están aquí, sino que se leen con el mandato **network** de GWCON.

```
Circuit Volatile Counters

Circuit = Eth/0

525249  Seconds since last zeroed
     0  Terminating packets received
     0  Originating packets sent
  3693  Transit packets received
  4723  Transit packets sent
     0  Transit congestion loss
     0  Circuit down
     0  Initialization failure
     0  Packet corruption loss
```

adjacent node
ID de un nodo con una adyacencia con este nodo en el circuito que se está mostrando. Mientras que las adyacencias con nodos finales convierten a dicho nodo en automáticamente accesible, una adyacencia de direccionador no convierte automáticamente en accesible a dicho nodo. No se considera que un direccionador es accesible a menos que se haya recibido un mensaje de direccionamiento sobre una adyacencia activa del direccionador. Por consiguiente, los nodos pueden aparecer como adyacentes en la base de datos de circuitos pero no estarán en la base de datos de nodos accesible (show active nodes).

block size
Tamaño máximo del bloque de datos que está dispuesto a recibir el nodo adyacente asociado. Por lo general, el tamaño es de 1498 bytes, que es el estándar de 1500 bytes de un paquete Ethernet, menos el campo de longitud de 2 bytes usado con DECnet.

circuit Circuitos en los que se aplican estos datos.

designated router
Muestra cuál cree, este nodo, que es el direccionador designado para esta área en este circuito. (Puede haber algunos desacuerdos temporales cuando se inicia un direccionador nuevo). Por lo general será el mismo para todos los direccionadores del circuito. Los nodos finales envían todos los paquetes que van a destinos que no están en el circuito local al direccionador designado.

hello timer
Temporizador hello de este circuito. Los mensajes hello del direccionador se envían a menudo al circuito.

listen timer
Período de tiempo que designa la frecuencia con que deben recibirse los hellos de nodos finales o de direccionadores de esta adyacencia en este circuito. El valor será el tiempo establecido para el temporizador hello para este circuito en la máquina adyacente, multiplicado por tres.

router priority
Prioridad de direccionador para este circuito, que se usa para conseguir el estado de direccionador designado.

router type
Tipo de direccionador para este circuito - standard (estándar), phase IV con AMA o Bilingual (bilingüe).

maximum routers
Número máximo de direccionadores permitido en este circuito.

state ON u OFF. En la base de datos volátil, el estado será ON si se habilita el circuito y está pasando una autoprueba. Si el circuito ha fallado en la autoprueba o el dispositivo no está presente, el estado será OFF.

En la base de datos permanente, indica si DNA intentará habilitar el circuito.

executor *argumento*
Recupera información sobre el estado actual de la base de datos volátil para DNA con el mandato show executor. El mandato **list executor** recupera los datos almacenados en la base de datos permanente para DNA.

A continuación, se muestra una lista de las opciones de submandato o argumentos que puede seleccionar después de entrar el mandato show/list executor:

characteristics
Información detallada sobre los valores de todos los argumentos ajustables de la base de datos de direccionamientos.

counters Indica los contadores de errores y de sucesos globales para DNA. No hay contadores permanentes, por lo que el mandato **list executor counters** es irrelevante.

status Da información clave sobre el estado de DNA.

summary Presenta un breve resumen sobre el estado de DNA. Este es el valor por omisión.

Ejemplo: **`show executor`**

```
Node Volatile Summary
Executor node            = 2.26 (gato)
State                    = on
Identification           = DECnet-MC68360 V1 R2.0 NP00523 [P10]
```

Ejemplo: **`show executor characteristics`**

Este ejemplo muestra la configuración completa de la base de datos del direccionador. El mandato **list executor characteristics** presenta, básicamente, la misma pantalla.

```
Node Volatile Characteristics
Executor node            = 2.26 (gato)
State                    = on
Identification           = DECnet-MC68360 V1 R2.0 NP00523 [P10]
Physical address         = AA-00-04-00-1A-08
Type                     = DEC-area
Routing version          = V2.0.0
Broadcast routing timer  = 180
Maximum address          = 64
Maximum cost             = 1022
Maximum hops             = 30
Maximum visits           = 63
Maximum area             = 63
Max broadcast nonrouters = 64
Max broadcast routers    = 32
Area maximum cost        = 1022
Area maximum hops        = 30
Maximum buffers          = 103
Buffer size              = 2038
```

Ejemplo: **`list executor status`**
Este ejemplo muestra el estado del direccionador en la base de datos permanente:

```
Node Permanent Status
Executor node            = 2.26 (gato)
State                    = on
Type                     = DEC-area
```

Ejemplo: **`show executor counters`**

Este ejemplo muestra los contadores que lleva 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 muestran cuando usa el mandato **show/list executor**.

area maximum cost
Costo máximo permitido a un área.

area maximum hops
Número máximo de saltos permitidos a un área.

broadcast routing timer
Frecuencia de envío de mensajes de direccionamiento en caso de que no haya ningún cambio.

buffer size
Tamaño del almacenamiento intermedio para el direccionador.

executor node
Dirección del nodo y nombre del nodo. El nombre del nodo es el nombre establecido por el mandato **set hostname** de CONFIG.

identification
Identificación del software del direccionador, tal como la envían los mensajes de ID del sistema MOP.

maximum area
Área más alta para la que se mantienen rutas.

maximum broadcast nonrouters
Número máximo de nodos finales que pueden ser adyacentes de este direccionador.

maximum broadcast routers
Número máximo de direccionadores que pueden ser adyacentes de este direccionador.

maximum buffers
Número máximo de almacenamientos intermedios de paquetes del direccionador.

maximum cost
Costo máximo permitido a un nodo.

maximum hops
Número máximo de saltos permitidos a un nodo.

maximum visits
Número máximo de direccionadores por los que un paquete puede direccionarse entre origen y destino.

physical address
Dirección de Ethernet física establecida en todos los circuitos de Ethernet cuando se inicia DNA. Se deriva del ID de nodo.

routing version
La versión siempre es Versión 2.0.0.

state El estado de DNA, on (activado) u off (desactivado).

type ROUTING IV o AREA, que corresponden a nivel 1 y nivel 2.

module access-control circuit-specifier *argumento*
Establece una lista de las listas de control de acceso de DECnet que se han definido en la base de datos permanente para el direccionador, así como los contadores de su uso. Las opciones para los especificadores de circuitos son las siguientes:

all circuits
Especifica todos los circuitos del direccionador.

circuit [nombre]
Especifica el circuito nombrado.

known circuits
Especifica todos los circuitos del direccionador.

Los elementos siguientes son los argumentos que puede seleccionar después de entrar el mandato **show/list module access-control** y el especificador de circuito:

counters Indica los contadores de uso de las listas de control de acceso.

status Muestra información detallada sobre las listas de control de acceso, incluyendo los filtros de las mencionadas listas.

summary Muestra información resumida sobre el estado de las listas de control de acceso. Este es el valor por omisión.

Ejemplo: **`show module access-control circuit eth/0 counters`**
Ejemplo: **`list module access-control circuit eth/0 counters`**

```
Module Access-Control Volatile Counters

Circuit = Eth/0

6337          Seconds since last zeroed
   0          Packets processed
   0          Packets rejected
   0          Access control loop iterations
```

module routing-filter circuit-specifier *argumento*
Establece una lista de los filtros de direccionamiento de áreas de DECnet que se han definido en la base de datos permanente para el direccionador.

all circuits
Especifica todos los circuitos del direccionador.

circuit [nombre]
Especifica el circuito nombrado.

known circuits
Especifica todos los circuitos del direccionador.

Los elementos siguientes son los argumentos que puede seleccionar después de entrar el mandato **show/list module routing-filter** y el especificador de circuito:

status Muestra información detallada sobre los filtros de direccionamiento, incluyendo la lista de áreas.

summary Muestra información de resumen sobre el estado de los filtros de direccionamiento. Este es el valor por omisión.

Ejemplo: `show module routing-filter circuit eth/0 status`

Ejemplo: `list module routing-filter circuit eth/0 status`

Zero

Use el mandato **zero** para borrar los contadores del circuito de la base de datos volátil, los contadores globales de dicha base de datos y los contadores del módulo de listas de control de acceso.

Sintaxis:

z**ero** circuit-specifier

executor

module access-control circuit-specifier

circuit-specifier

all circuits
Especifica todos los circuitos del direccionador.

circuit [nombre]
Especifica el circuito nombrado.

known circuits
Especifica todos los circuitos del direccionador.

Ejemplo: `zero all circuits`

executor Establece todos los contadores globales de la base de datos volátil en cero. No hay opciones.

Ejemplo: `zero executor`

module access-control circuit-specifier

all circuits
Especifica todos los circuitos del direccionador.

circuit [nombre]
Especifica el circuito nombrado.

Ejemplo: `zero module access-control all circuits`

Uso de OSI/DECnet V

Este capítulo describe la implementación que efectúa el direccionador de la capa de red sin conexión de la International Standards Organization's (ISO) Open Systems Interconnection (OSI). DECnet Phase V da soporte a OSI (de ahora en adelante llamado DECnet V/OSI) y los usuarios de redes DNA V pueden consultar este capítulo para obtener información sobre los protocolos ISO OSI. Este capítulo contiene las secciones siguientes:

Visión general de OSI

Una red OSI está formada por varias subredes interconectadas. Una subred consiste en sistemas principales conectados a los que se denomina sistemas finales (ES) y direccionadores denominados sistemas intermedios (IS), tal como se muestra en la Figura 20.

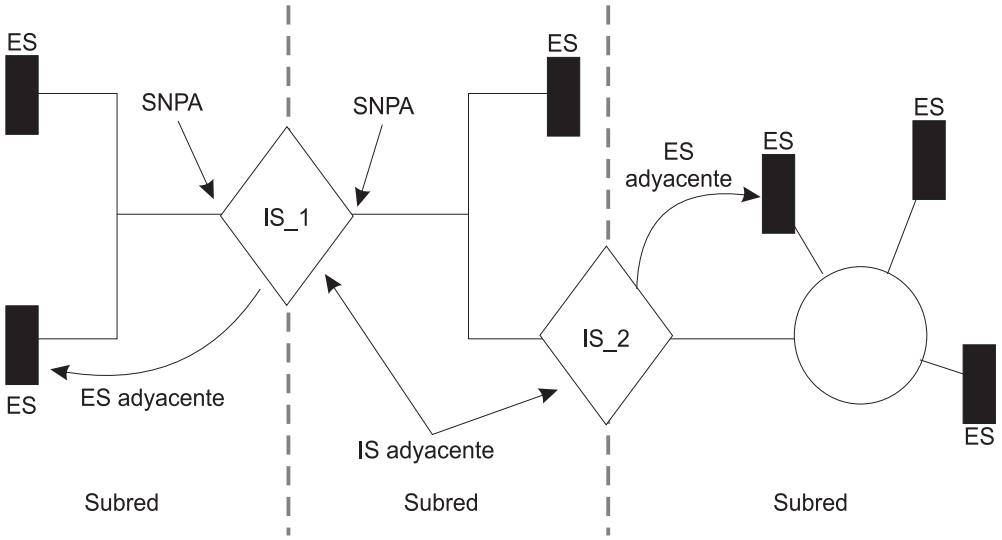


Figura 20. Red OSI

Los ES contienen todas las capas del modelo de referencia OSI y las aplicaciones del sistema principal. Los IS ejecutan las funciones de las tres capas inferiores del modelo de referencia OSI y manejan el direccionamiento de las unidades de datos del protocolo de red (NPDU) entre las subredes. Los IS se conectan lógicamente a la subred en el punto de conexión de ésta (SNPA). El SNPA es el punto de acceso a la capa de enlace de datos.

Según la configuración del IS, cada IS puede ejecutar tres protocolos: ES-IS, IS-IS y Connectionless-Mode Network Protocol (Protocolo de red en modalidad sin conexión - CLNP).

El protocolo ES-IS habilita a los ES e IS conectados a la misma subred para que descubran dinámicamente su respectiva existencia. Un ES conectado a la misma subred que un IS es adyacente de éste. El protocolo de direccionamiento IS-IS habilita a los IS para:

- Descubrir dinámicamente la existencia y disponibilidad de los IS adyacentes.
- Intercambiar información de direccionamiento con otros IS.
- Usar la información de direccionamiento intercambiada para calcular rutas basadas en el recorrido más corto.

El protocolo CLNP es un protocolo de datagramas que transporta paquetes entre IS.

Direccionamiento de NSAP

El NPDU contiene direcciones de red de OSI (también llamadas NSAP). El NSAP se refiere a un punto de la capa de la red donde el usuario accede a dicha capa. Los NSAP son puntos únicos dentro de un sistema que representan puntos finales direccionables de comunicación a través de la capa de red. El número de NSAP puede variar de sistema a sistema.

Una autoridad de direccionamientos como, por ejemplo, el National Institute of Standards and Technology (NIST) del gobierno de los Estados Unidos, administra las direcciones NSAP y determina cómo se asignan e interpretan las direcciones dentro del dominio. Si es necesario, estas autoridades pueden dividir el dominio en subdominios y designar las autoridades correspondientes para administrarlos.

Dentro del NPDU hay dos direcciones NSAP, una dirección de destino y una dirección de origen. La longitud de cada dirección puede variar entre 2 y 20 octetos y, por lo general, se representa en notación hexadecimal. A continuación, se muestra un ejemplo de un NSAP de 6 octetos que puede entrarse en la configuración OSI del direccionador.

```
AA000400080C
```

Dado que la longitud de la dirección es variable, las partes de la cabecera del PDU llamadas indicador de longitud de la dirección de destino e indicador de longitud de la dirección de origen, se usan para indicar la longitud, en octetos, de cada dirección.

Una dirección NSAP está formada por dos partes: una parte de dominio inicial (IDP) y una parte específica de dominio (DSP) tal como se muestra en Figura 21.

Figura 21. Estructura de dirección de NSAP

IDP

La IDP está formada por dos partes, el Authority and Format Identifier (Identificador de formato y autoridad - AFI) y el Initial Domain Identifier (Identificador de dominio inicial - IDI).

El AFI especifica el tipo de IDI y la autoridad de direccionamiento de red responsable de asignar los valores al IDI.

El IDI especifica el dominio de direccionamiento de red del que se asignan los valores de la DSP y la autoridad de direccionamiento de red responsable de asignar valores de la DSP de dicho dominio.

DSP

La autoridad de direccionamiento de la red identificada por el IDI determina la DSP. No obstante, es importante que la DSP incluya información de direccionamiento específica para el dominio.

Formato de direccionamiento IS-IS

El protocolo IS-IS divide la dirección NSAP en tres partes: dirección de área, ID del sistema y selector (consulte la Figura 22). La dirección de área y el ID del sistema junto con un selector con un valor de 0 se denominan Network Entity Title (Título de la entidad de red - NET). NET es la dirección de la capa de red en sí y se asigna cuando se configura un IS en la red OSI.

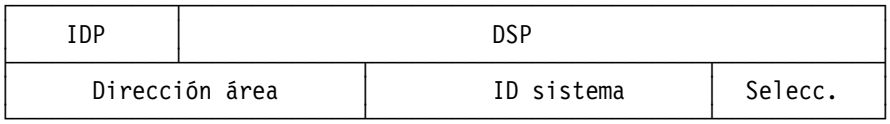


Figura 22. Interpretación de direccionamiento NSAP IS-IS

Dirección de área

En el protocolo IS-IS, la dirección de área es la parte de la NSAP que incluye toda o una parte de la IDP y la parte de la DSP hasta el ID del sistema.

La dirección del área corresponde a la parte de la NSAP que identifica un área específica de un dominio. Esta dirección debe tener, como mínimo, una longitud de 1 octeto y todos los ES e IS de la misma área deben tener la misma dirección de área.

ID del sistema

ID del sistema que corresponde a la parte de la NSAP que identifica un sistema específico de un área. Los ID de sistema deben tener los atributos siguientes:

- De 1 a 8 octetos de longitud.
- La misma longitud en todo el dominio. Los direccionadores usan una longitud de configuración por omisión de 6 octetos.
- Deben ser únicos para cada sistema en todo el dominio.

Selector

El selector es un campo de 1 octeto que actúa como selector para la entidad que va a recibir la PDU, por ejemplo, la capa de transporte o la misma capa de red IS. El direccionador establece este campo en 0.

NSAP de GOSIP Versión 2

Government Open Systems Interconnection Profile (GOSIP) Versión 2 proporciona, para el uso del gobierno, el formato de direccionamiento ilustrado en la Figura 23. Las autoridades responsables de las direcciones han definido claramente los campos y especificado el formato de direccionamiento bajo la DSP establecido por el National Institute of Standards and Technology (NIST).

IDP		DSP						
AFI 47	IDI 0005	Ver 80	Aut.	Reserv.	Dominio (2)	Área (2)	ID. sis (6)	Selecc. (1)

Figura 23. Formato de dirección GOSIP

AFI Este campo de 1 octeto tiene una designación (hexadecimal) de 47. Este valor significa que la dirección está basada en el formato ICD y que la DSP utiliza una sintaxis binaria.

IDI Este campo de 2 octetos tienen una designación (hexadecimal) de 0005. Este valor está asignado al gobierno de los E.E.U.U. y el NIST ha establecido el formato.

VER Este campo de 1 octeto tiene una designación de 80 (hexadecimal). Este valor identifica el formato de la DSP.

Auth. (Authority) Este campo de 3 octetos identifica la autoridad que controla la distribución de las direcciones NSAP.

Reserved Este campo de 2 octetos se proporciona para acomodar un crecimiento futuro.

Domain Este campo de 2 octetos contiene el identificador de dominios de direccionamiento.

Area Este campo de 2 octetos contiene el ID de área.

Sys. ID Este campo de 6 octetos identifica el sistema.

Selector Este campo de 1 octeto selecciona la entidad que recibirá la NPDU.

Direcciones de difusión múltiple

El direccionamiento de difusión múltiple es el método que los IS de nivel 1 (L1) y nivel 2 (L2) usan para distribuir actualizaciones de estado de enlace (LSU) y mensajes hello a otros sistemas o redes LAN. Cuando una LSU o un mensaje hello es de difusión múltiple, un grupo de estaciones de destino recibe el paquete. Por ejemplo, una LSU L1 es de difusión múltiple únicamente con otros IS L1. Un Intermediate System Hello (Hello de sistema intermedio - ISH) es de difusión múltiple únicamente con los ES de la misma subred.

Puede configurar direcciones de difusión múltiple para cada subred con el mandato **set subnet**. La Tabla 60 en la página 303 establece una lista de las direcciones de difusión múltiple de las LAN Ethernet y de red en anillo.

Tabla 60. Direcciones de vertimiento múltiple IS-IS

Destino	Ethernet 802.3	Red en Anillo 802.5	Descripción de la dirección
Todos los ES	09002B000004	C00000004000	Para todos los sistemas finales de la subred.
Todos los IS	09002B000005	C00000008000	Para todos los sistemas intermedios de la subred.
Todos los IS L2	0180C2000015	C00000008000	Para todos los sistemas intermedios L2 de la subred.
Todos los IS L1	0180C2000014	C00000008000	Para todos los sistemas intermedios L1 de la subred.

Direccionamiento OSI

OSI direcciona paquetes con el protocolo IS-IS. El direccionamiento con este protocolo se basa en:

- Un ID de sistema para direccionar dentro de un área
- Una dirección de área para direccionar dentro de un dominio
- El prefijo de dirección accesible para el direccionamiento para fuera del dominio

El protocolo IS-IS utiliza tablas de direccionamientos para reenviar los paquetes a los destinos correctos. Las entradas de dichas tablas se crean a partir de la información contenida en la base de datos de estado de los enlaces o de las direcciones accesibles configuradas por el usuario. La base de datos de estado de los enlaces se crea a partir de la información recibida en la actualización del estado del enlace (LSU). Consulte “Bases de datos de estados de enlaces” en la página 308.

Protocolo IS-IS

El protocolo IS-IS es un protocolo de direccionamiento dinámico del estado de los enlaces que detecta y aprende las mejores rutas a los destinos accesibles. IS-IS puede percibir rápidamente los cambios en la topología de un dominio y, después de un corto período de convergencia, calcular rutas nuevas. Para ello, el IS usa los paquetes siguientes:

- Link State Updates (Actualizaciones del estado de los enlaces - LSU) que el IS usa para mantener actualizada la información de la base de datos de estado de los enlaces.
- Sequence Number PDU (PDU del número de secuencia - SNP) para mantener la base de datos sincronizada y para asegurarse de que cada IS adyacente sabe cuál fue el Link State Packet (paquete de estado del enlace - LSP) más reciente de cada direccionador.
- Mensajes hello que los IS usan para descubrir, inicializar y mantener adyacencias con IS vecinos.

Áreas IS-IS

Un área IS-IS es un conjunto de sistemas en subredes continuas. La topología de cada área queda oculta de las de otras áreas para reducir el tráfico de direccionamiento. Se usa un IS de nivel 1 (L1) para direccionar dentro de un área. Los IS de nivel 2 (L2) se usan para direccionar entre áreas o sobre el troncal. Un IS que encamine dentro de un área o sobre el troncal se considera un IS L1/L2.

Dominio IS-IS

Un dominio IS-IS es un conjunto de normas, administradas por la misma autoridad, que deben seguir todos los ES e IS para asegurar la compatibilidad. Existen dos tipos de dominio que requieren discusión, dominio administrativo y dominio de direccionamiento.

Dominio administrativo

Un dominio administrativo controla la organización de los IS en dominios de direccionamiento así como las direcciones de subred o NSAP que usan dichos dominios de direccionamiento.

Dominio de direccionamiento

Un dominio de direccionamiento es un conjunto de IS y ES gobernados por las normas siguientes:

- Todos los dispositivos usan el mismo tipo de métrica de direccionamiento.
- Todos los dispositivos usan el mismo protocolo de direccionamiento como, por ejemplo, IS-IS.

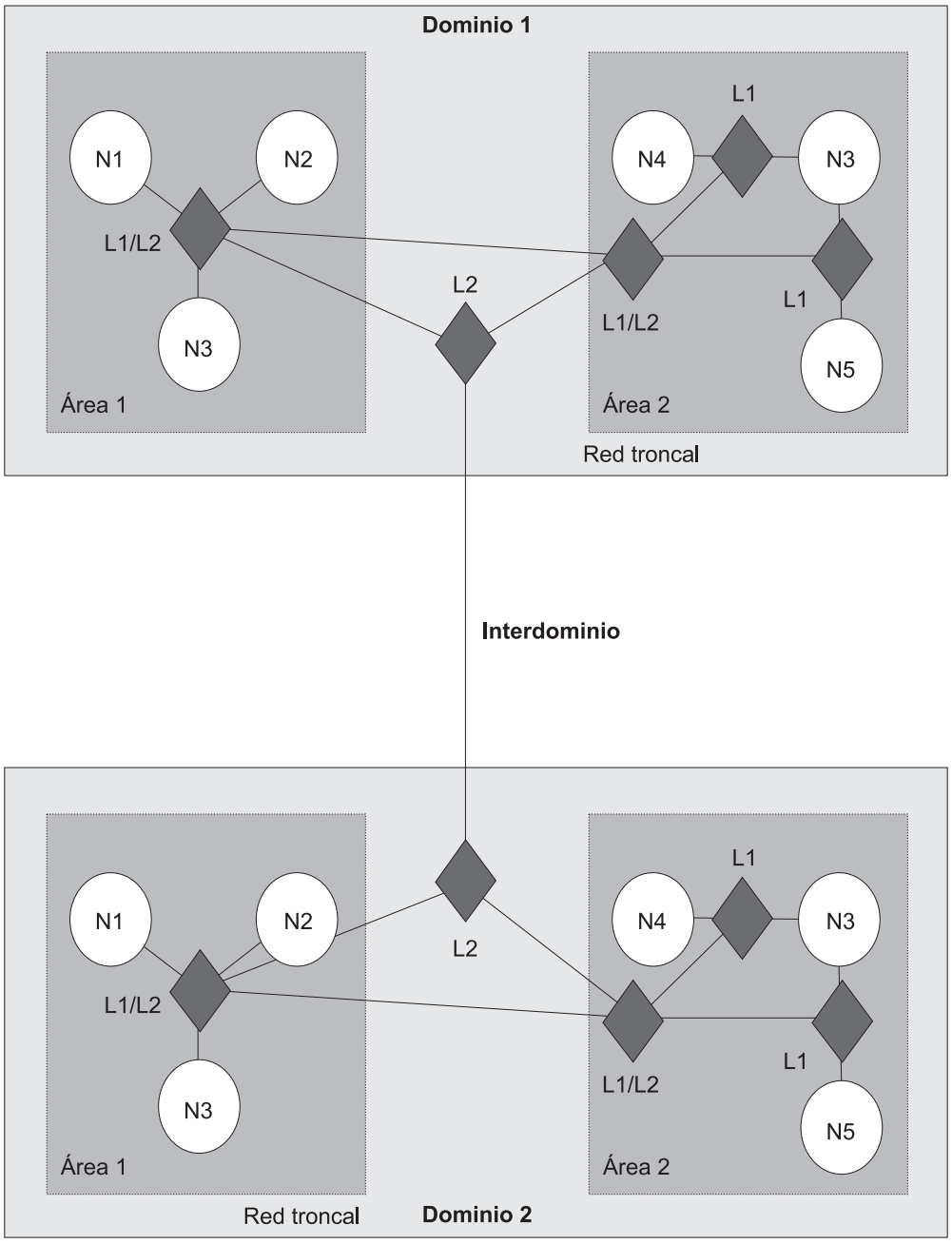


Figura 24. Dominio OSI

Áreas sinónimas

Cuando un IS L1 da servicio a más de un área, las áreas adicionales reciben el nombre de áreas sinónimas. Un direccionador puede dar soporte a cualquier cantidad de dichas áreas, siempre y cuando haya una solapación, como mínimo, de una dirección de área entre direccionadores adyacentes. Por ejemplo, en la Figura 25 en la página 306, el área 1 y el área 2 son sinónimas entre sí y las áreas 3 y 4 también son sinónimas entre sí.

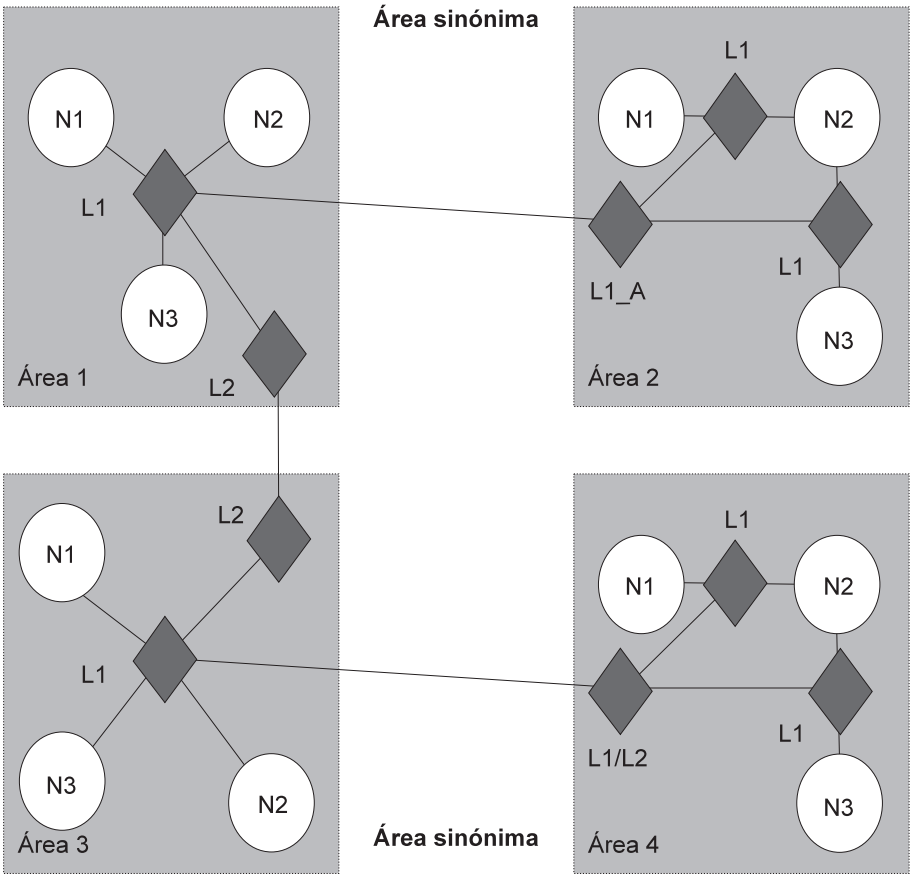


Figura 25. Áreas sinónimas

El L1_A IS del área 2 debe tener la dirección del área 1 añadida en su configuración y el IS L1 del área 1 debe tener la dirección del área 2 añadida en su configuración. Para que las áreas 3 y 4 sean sinónimas, debe añadirse la dirección de cada área a los otros IS L1.

Mensaje hello de IS a IS (IIH)

El mensaje IIH habilita a un IS para que determine la existencia de otros IS y para establecer adyacencias. Existen tres tipos de mensajes IIH: L1, L2 y punto a punto.

Cada IS contiene un temporizador hello local y un temporizador de retención. Cada vez que el temporizador hello expira, se ejecuta un difusión múltiple de un IIH sobre la interfaz del IS a cualquier IS adyacente. Cuando se recibe el mensaje hello, el destinatario establece o actualiza (renueva) la información de adyacencia. Esta información seguirá siendo actual durante el período de tiempo (en segundos) especificado por el temporizador de retención. Si el temporizador de retención se agota, se desactivará la adyacencia.

Mensaje L1 IIH

El mensaje L1 IIH se ejecuta en difusión múltiple sobre la interfaz cuando el temporizador hello local se agota. El IS L1 pone la información siguiente en el IIH:

- ID de origen
- Cualquier dirección de área manual a la que preste servicio
- Tipo de IS (sólo L1 o L1/L2)

- Prioridad
- ID de la LAN
- Si es aplicable, el ID de sistema del IS designado L1 (pseudonodo)

Al recibir este mensaje, el IS L1 adyacente extrae el ID de origen del IS emisor. A continuación, construye su propio mensaje IIH y pone su ID de origen en el campo de ID de origen. El ID de origen del remitente se pone en el campo de IS vecinos. La devolución del ID del remitente sirve a éste de verificación para saber que el IS adyacente es consciente de que existe (adyacencia en 2 sentidos).

Cuando el primer IS recibe el IIH, también extrae el ID de origen y mira en el campo de IS vecino. Al descubrir su propio ID de origen en el campo de IS vecino, este IS establecerá una adyacencia con el otro IS.

Nota: Antes de que el IS L1 adyacente pueda aceptar el paquete, éste deberá tener una dirección de área común y la misma longitud de ID del sistema que el IS adyacente.

Mensaje L2 IIH

El L2 IIH se ejecuta en difusión múltiple sobre sus interfaces con el fin de identificarse ante otros IS L2. El IS L2 tiene la misma función que un L1 IIH. El IS L2 pone la información siguiente en el IIH:

- ID de origen
- Cualquier dirección de área manual a la que preste servicio
- Tipo de IS (sólo L2 o L1/L2)
- Prioridad
- ID de la LAN
- Si es aplicable, el ID del sistema del IS designado L2.

Nota: Antes de que el IS L2 pueda aceptar el paquete, éste deberá tener la misma longitud de ID del sistema que el IS adyacente.

Mensaje IIH de punto a punto

Un mensaje IIH de punto a punto se envía sobre una interfaz de no difusión de IS (Frame Relay o X.25) para identificarse ante otros IS. Este IS da el IIH que contiene la información siguiente:

- ID de origen
- Cualquier dirección de área manual a la que preste servicio
- Tipo de IS (sólo L1, sólo L2 o L1/L2)
- ID del circuito local

IS designado

El IS designado se selecciona entre todos los IS conectados a la misma LAN para ejecutar funciones adicionales. En concreto, genera actualizaciones de estado de enlaces en nombre de la LAN y trata a ésta como si fuera un pseudonodo. Un pseudonodo es un método de modelación de toda la LAN como si fuera un nodo en la red con menos enlaces lógicos. La minimización de los enlaces lógicos en todo el dominio disminuye la complejidad de cálculo del algoritmo del estado del enlace.

Cuando una LAN tiene más de un IS, cada IS compara lo indicado a continuación para determinar qué IS se convertirá en el IS designado:

- Todos los IS comparan sus prioridades. Aquel que tenga la mayor prioridad se convertirá en el IS designado.
- Si los IS tienen la misma prioridad, compararán sus direcciones MAC de origen. Aquel que tenga la dirección de MAC numéricamente mayor se convertirá en el IS designado para la LAN y se indicará mediante el ID LAN.

Bases de datos de estados de enlaces

Cada IS L1 e IS L2 contiene una base de datos de estados de enlaces. El elemento primario de la base de datos es la actualización del estado del enlace (LSU). El direccionador es responsable de crear su propia LSU y de procesar las de otros IS para mantener la base de datos. La base de datos de L1 contiene información sobre ES. Cada base de datos de L1 es idéntica para todos los IS L1 de la misma área. La base de datos de L2 contiene información sobre áreas y direcciones accesibles. Cada base de datos de L2 es idéntica a la de todos los IS L2 configurados en el dominio IS-IS. Gracias a la información obtenida de las bases de datos, el algoritmo de direccionamiento Dijkstra calcula las vías de acceso más cortas a todos los destinos y crea las tablas de direccionamientos.

Inundación del estado de enlace

Para asegurarse de que cada IS L1 y IS L2 mantiene una base de datos idéntica, se inunda toda un área o un troncal con LSU. La inundación es un mecanismo utilizado por un IS L1 o IS L2 para propagar una LSU a todos los IS L1 o IS L2. Un IS L1 sólo inunda con LSU los IS L1. Un IS L2 sólo inunda con LSU los IS L2. Un IS L1/L2 acepta LSU de L1 y L2.

Actualización del estado del enlace de L1 (no pseudonodo)

Todos los IS L1 se inundan con la L1 LSU. El IS L1 da a la LSU la información siguiente:

- ID de origen
- Cualquier dirección de área manual a la que preste servicio
- Tipo de IS (L1)
- ID del sistema y costos de acceder a las adyacencias de IS
- Si es aplicable, los pseudonodos adyacentes del ID de sistema
- Los ID de sistema de cualquier adyacencia ES manual

Actualización del estado del enlace de L1 (pseudonodo)

Todos los IS L1 del área se inundan con la LSU del pseudonodo L1. Cualquier IS L1 situado en la misma LAN que reciba la LSU propagará dicha LSU a todos los IS L1 adyacentes del resto de sus subredes. El IS L1 pone la información siguiente en la LSU:

- ID de origen
- Tipo de IS (L1)
- ID de sistema y costo de acceder a todos los IS que no son pseudonodos situados en la LAN
- Los ID de sistema de cualquier adyacencia ES aprendida mediante un protocolo ES-IS

Actualización del estado de enlace L2 (no pseudonodo)

Todos los IS L2 se inundan con la L2 LSU. La IS L2 pone la información siguiente en su LSU:

- ID de origen
- Conjunto de direcciones de área a las que da servicio
- Tipo de IS (L2)
- ID de sistema y costo de acceder a las adyacencias de IS
- Si es aplicable, el ID de sistema del pseudonodo
- Prefijos de dirección para los IS situados en un dominio externo

Actualización del estado de enlace L2 (pseudonodo)

La LSU del pseudonodo L2 se ejecuta en difusión múltiple sobre la interfaz y se propaga a todos los IS L2 situados fuera de la subred. Cualquier IS no pseudonodo L2 situado en la misma subred que reciba la LSU pasará ésta en relé a todos los L2 situados fuera de la subred. La IS L2 pone la información siguiente en la LSU:

- ID de origen
- Tipo de IS (L2)
- ID de sistema y métricas de los IS no pseudonodos situados en la misma subred

IS L2 conectados y sin conectar

Un IS L2 conectado es un direccionador que tiene conocimiento de otras áreas. Un IS L2 sin conectar es un direccionador que no sabe que existen otras áreas aparte de él mismo.

Al direccionar, un IS L2 desconectado direcciona paquetes al IS L2 conectado más cercano.

Tablas de direccionamientos

Un IS sólo L1 usa una tabla de direccionamientos, la tabla de direccionamientos de nivel 1. Un IS sólo L2 contiene tres tablas de direccionamientos: una tabla de direccionamientos de direcciones de áreas L2, una tabla de direccionamientos de prefijos de direcciones accesibles métrica e internamente y una tabla de direccionamientos de prefijos de direcciones accesibles métrica y externamente. Un IS L1/L2 contiene la tabla de direccionamientos L1 y todas las tablas de direccionamientos L2. Las entradas de la tabla de direccionamientos se crean a partir de la información de la base de datos de estados de enlaces.

Direccionamiento de L1

A continuación, resumimos el direccionamiento de L1:

1. Un IS L1 recibe un paquete y compara la parte correspondiente a la dirección del área de la dirección de destino situada en la cabecera del paquete, con el conjunto de direcciones de áreas del direccionador.
2. Si el paquete está destinado al área del direccionador, éste extraerá el ID del sistema de la dirección. Al buscar una coincidencia, el direccionador comparará el ID del sistema con los ID de sistemas de la tabla de direccionamientos de L1.
3. Si encuentra una coincidencia, el IS direccionará el paquete al ES o al IS del salto siguiente. Si no encuentra ninguna coincidencia, eliminará el paquete.

4. Si el paquete no está destinado a dicha área, L1 reenviará el paquete al IS L2 más cercano o si el direccionador es un IS L1/L2, comprobará las tablas de direccionamientos de L2, tal como describimos en la sección siguiente. Si el L1 no puede determinar a dónde direccionar el paquete, éste se eliminará.

Direccionamiento de L2

Un IS L2 contiene tres tablas de direccionamientos: una tabla de direccionamientos de direcciones de áreas L2, una tabla de prefijos de direcciones accesibles métrica e internamente (interna) y una tabla de prefijos de direcciones accesibles métrica y externamente (externa).

A continuación, resumimos el direccionamiento de L2:

1. Un IS L2 recibe un paquete y compara la parte correspondiente a la dirección de destino de la cabecera con el conjunto de direcciones de áreas de la tabla de direccionamientos de direcciones de áreas. Si encuentra una coincidencia, el paquete se reenviará al direccionador troncal del salto siguiente. Si no encuentra ninguna coincidencia, el direccionador comprobará la tabla de direccionamientos interna.
2. La tabla de direccionamientos interna contiene entradas de prefijos de direcciones accesibles que llevan a otros dominios. Si la tabla de direccionamientos interna contiene una coincidencia, se reenviará el paquete por el troncal al dominio adecuado. Si no se encuentra ninguna coincidencia, el direccionador comprobará la tabla de direccionamientos externa.
3. La tabla de direccionamientos externa contiene entradas de prefijos de direcciones accesibles que también llevan a otros dominios. Si la tabla de direccionamientos externa contiene una coincidencia, se reenviará el paquete por la vía de acceso al dominio adecuado. Si no encuentra ninguna coincidencia, eliminará el paquete.

Consulte “Direccionamiento externo e interno” en la página 311 para obtener una explicación detallada sobre las tablas de direccionamientos internas y externas.

Métrica de direccionamiento

Una métrica de direccionamiento es un valor asociado a una función del circuito para indicar el costo del direccionamiento sobre dicho circuito. Por ejemplo, la métrica de direccionamiento basada en el gasto monetario de un circuito usará un valor bajo para indicar que el gasto monetario es bajo y un valor alto para indicar que el gasto monetario del direccionamiento de un paquete sobre dicho circuito es elevado.

El protocolo de direccionamiento IS-IS usa cuatro métricas de direccionamiento: la métrica por omisión, la métrica de retardo, la métrica de gastos y la métrica de errores.

La implementación actual del modelo OSI usa únicamente la métrica por omisión IS-IS. Por convenio, la métrica por omisión, tiene por objetivo medir la capacidad del circuito para manejar el tráfico. Todos los IS del dominio de direccionamientos deben ser capaces de calcular rutas basadas en la métrica por omisión. El resto de las métricas de direccionamiento son opcionales. Aunque esta implementación del protocolo OSI no las usa, las describimos a continuación por motivos meramente informativos.

- La métrica de retardo mide el retardo de tránsito del circuito asociado.

- La métrica de gastos mide el costo monetario de utilizar el circuito asociado.
- La métrica de errores mide la probabilidad de que se produzcan errores residuales en el circuito asociado.

Direccionamiento externo e interno

Un direccionamiento externo o interno implica que un IS L2 direcciona un paquete entre dos dominios separados. Cuando es necesario direccionar un paquete a otro dominio, el IS L2 intenta que la dirección coincida con un prefijo de dirección accesible de la tabla de direccionamientos externa o interna. Las rutas externas e internas se basan en el costo (métrica de direccionamiento) de llegar al destino. El costo de una ruta interna tiene en cuenta el costo del direccionamiento dentro del dominio y el de direccionamiento al destino. El costo de una ruta externa se basa únicamente en el costo del direccionamiento al destino fuera del dominio de direccionamiento. El IS elige la vía de acceso con el costo más bajo.

Por ejemplo, si un paquete está destinado a ir del nodo A del dominio 1 al nodo D del dominio 2 (Figura 26 en la página 312). El nodo A puede elegir entre dos vías de acceso para enviar el paquete: al nodo B y después al nodo D o bien al nodo C y después al nodo D. La forma en que los nodos B y C anuncien el costo de sus rutas a D determinará cómo el nodo A decidirá direccionar el paquete, ya sea interna o externamente. Existen tres opciones posibles:

- Los nodos B y C anuncian el costo de sus rutas a D como interno. El costo interno de la ruta A-B-D es 35, que es el costo de direccionar de A a B, más el de direccionar de B a D. El costo interno de la ruta A-C-D es 40, que es el costo de direccionar de A a C, más el de direccionar de C a D. En este caso, el nodo A elegirá direccionar sobre la vía de acceso A-B-D ya que el costo es inferior.
- Los nodos B y C anuncian el costo de sus rutas como externo. El costo externo de A-B-D es 30, que es el costo de direccionar de B a D. El costo externo de A-C-D es 20. En este caso, el nodo A elegirá direccionar sobre la vía de acceso A-C-D porque el costo de esta ruta es inferior.
- Los nodos B y C anuncian el costo de sus rutas como interno y externo. El costo interno y externo de las rutas se añade a sus tablas de direccionamientos respectivas. Dado que se prefieren las rutas internas a las externas, el direccionador elegirá la ruta interna A-B-D.

Nota: Dado que no existe un protocolo de direccionamiento externo, todas las rutas de prefijo entre dominios deben configurarse estáticamente.

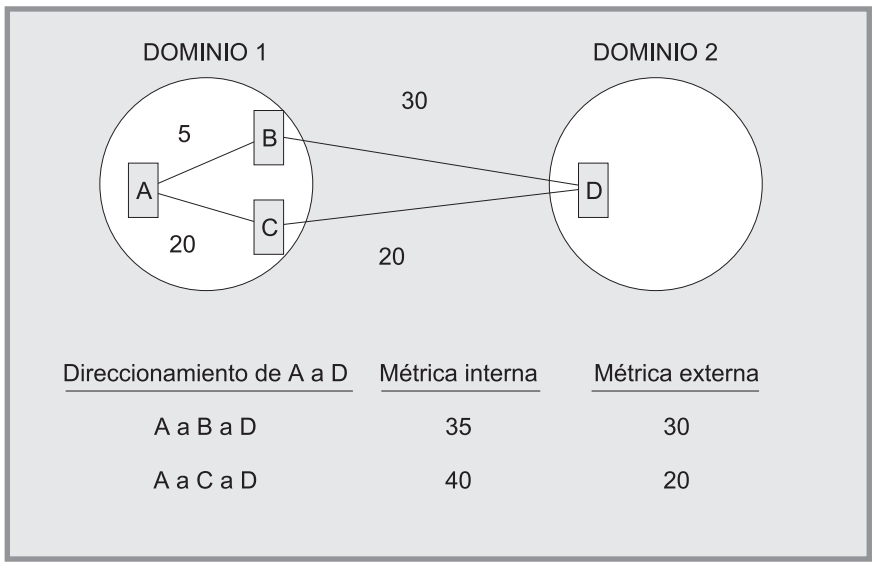


Figura 26. Métricas de direccionamiento externo e interno

Codificación de prefijos de direcciones

Cuando entre rutas de prefijos de direcciones, tenga muy en cuenta la diferencia existente entre las normas de codificación para NSAP y para rutas de prefijos. Los cuatro ejemplos siguientes ilustran la codificación de prefijos de direcciones.

Codificación de un IDI de longitud fija

Para varios prefijos de direcciones, codificar el prefijo y el NSAP correspondiente es lo mismo. Por ejemplo, si está usando la dirección GOSIP 1.0 y desea crear una ruta a una organización de DoD. El IDI de Org es 1234 y el IDI de DoD es 0006. La dirección de NSAP codificada será

```
4700061234CCCC222222222222
```

El prefijo de la dirección codificada es el resultado de truncar el NSAP

```
4700061234
```

Las normas de codificación tratan todos los formatos de NSAP que tengan un IDI de longitud fija y todos los prefijos de dirección que acaban después del IDP.

Codificación de un AFI

Un prefijo de dirección basado completamente en el AFI sólo se codifica en el campo AFI de 1 octeto. Por ejemplo, si necesita un prefijo de dirección para todas las direcciones de formato X.121 (usadas en redes X.25), usará un AFI de X.121 que tenga un valor de 37.

Codificación de un IDI de longitud variable

Las direcciones de NSAP que tienen formatos de IDI de longitud variable como, por ejemplo, X.121, F.69, E.163 y E.164, usan un esquema de codificación más complicado. Cuando los IDI de longitud variable se codifican como un NSAP, la dirección se rellena a la izquierda con ceros; no obstante, cuando se codifica el IDI como un prefijo de dirección, no se rellena en la izquierda.

Por ejemplo, desea que la ruta X.25 llame desde los E.E.U.U. a una portadora X.25 situada en los Países Bajos. Supongamos que la portadora tiene un Data Network Identifier Code (Código identificador de la red de datos - NDIC) 2041. La codificación del prefijo de la dirección será

```
372041
```

Un abonado a X.25 que tenga un número de teléfono nacional (NTN) de 117010 en esta portadora tendrá un NSAP de

```
3700002041117010
```

Observe que el IDI del NSAP se rellena a la izquierda con ceros hasta alcanzar los 14 dígitos ya que el número de datos internacionales resultantes (2041117010) era inferior a 14 dígitos.

No obstante, si desea un prefijo de dirección que apunte únicamente a un abonado de X.25, la codificación será el NSAP (3700002041117010), ya que el prefijo no acaba en el IDP.

Prefijos de dirección por omisión

El prefijo de dirección por omisión se usa cuando desea originar una ruta por omisión a todas las direcciones situadas fuera del dominio. Los prefijos de dirección por omisión tienen una longitud de cero, por lo que no hay que codificar nada.

Contraseñas de autenticación

Para proporcionar una capa mínima de seguridad a la red, OSI tiene una opción de contraseñas de autenticación. Cuando ésta se habilita, el IS no aceptará ningún paquete IS-IS que no contenga la contraseña adecuada. El campo de autenticación de la NPDU contiene las contraseñas de autenticación. Existen dos tipos de estas contraseñas: de transmisión y de recepción.

Se añade una contraseña de transmisión a los paquetes IS-IS que transmite el IS. Una contraseña de recepción es un listado de contraseñas de transmisión que el IS acepta. Por ejemplo, con la autenticación habilitada, si no se añade una contraseña de transmisión al paquete, o no hay un listado de contraseñas de transmisión en la base de datos de contraseñas de recepción, se eliminará el paquete. Existen tres tipos de contraseñas de recepción y transmisión: de dominio, de área y de circuito.

Una contraseña de dominio proporciona seguridad a la información de direccionamiento de L2. Una contraseña de área proporciona seguridad a la información de direccionamiento de L1. Una contraseña de circuito proporciona seguridad a los mensajes hello de IS-IS.

Protocolo ESIS

El protocolo ES-IS habilita a los ES e IS conectados a la misma subred para que descubran dinámicamente su respectiva existencia y disponibilidad. Esta información también permite a los ES obtener información de todos ellos sin que haya un IS disponible.

La información de redirección de ruta habilita a un IS para que informe a un ES de la existencia de una ruta mejor al reenviar NPDU a un destino en concreto. Por

ejemplo, una ruta mejor puede ser otro IS situado en la misma subred que el ES o el ES de destino situado en la misma subred.

Mensaje hello

La información de direccionamiento se pasa a los ES e IS mediante mensajes hello.

Cada ES y cada IS tienen un temporizador de configuración local (CT) y un temporizador de retención (HT). Cada vez que el CT se agota, se envía en difusión múltiple un mensaje hello a la LAN. Cuando este mensaje se recibe, el destinatario establece el valor del HT de acuerdo con el valor transmitido en el campo HT del mensaje. Se espera que el destinatario retenga este información hasta que el HT se agote, para asegurar el funcionamiento correcto del protocolo ES-IS.

Mensaje hello de sistema final (ESH)

El mensaje ESH se envía en difusión múltiple desde el ES a todos los IS L1 cuando el CT local se agota. El ES crea este mensaje para informar a un IS sobre cualquier NSAP al que dé servicio. Al recibir el mensaje, el IS extrae la información SNPA y NSAP y almacena el par en la tabla de direccionamientos L1, sustituyendo cualquier otra información que estuviera almacenada.

Mensajes hello de sistema intermedio (ISH)

El mensaje ISH se envía en difusión múltiple a todos los ES adyacentes cuando el CT local se agota. El IS crea este mensaje para informar al ES de su NET. Al recibir el mensaje, el ES extrae la información SNPA y NET y almacena el par en una de las tablas de direccionamientos locales, sustituyendo cualquier otra información que estuviera almacenada.

Circuitos X.25 para DECnet V/OSI

En el caso de las redes X.25, el direccionador establece circuitos virtuales conmutados (SVC) X.25 en los circuitos de direccionamiento.

Nota: Para habilitar DECnet V/OSI para X.25, debe entrar en el proceso de DECnet IV y definir el direccionador para que sea un direccionador DEC-AREA o DEC-ROUTING-IV. Debe ejecutar esta operación (y reiniciar el direccionador) para habilitar los mandatos para la configuración de DECnet V/OSI. Use el mandato **define executor type**.

Circuitos de direccionamiento

Los circuitos de direccionamiento son conexiones de punto a punto entre nodos que implementan el protocolo ISO CLNS. El direccionador emplea los circuitos de direccionamiento siguientes:

- Circuitos de entrada estáticos
- Circuitos de salida estáticos
- Circuitos asignados dinámicamente

Los circuitos de entrada y de salida estáticos sólo tienen un SVC asociado a ellos y llevan tanto datos del usuario como datos que no son del usuario (como mensajes de protocolo de direccionamiento). Los circuitos estáticos se activan y desactivan explícitamente usando mandatos de configuración DECnet V/OSI. Los

circuitos de direccionamiento asignados dinámicamente se establecen al llegar los datos y se borran cuando no se reciben ni se transmiten datos. Un circuito asignado dinámicamente puede tener varios SVC, pero sólo puede transportar datos del usuario.

DECnet V/OSI controla las llamadas de cada uno de los tipos de circuitos de direccionamiento usando *filtros* y *plantillas*. Los filtros se usan para procesar las llamadas de entrada, mientras que las plantillas se usan para establecer las llamadas de salida.

Filtros

Un *filtro* es un conjunto de parámetros que el usuario puede configurar y que definen los criterios para aceptar las llamadas de entrada destinadas al circuito de direccionamiento X.25 especificado.

Los parámetros definidos en un filtro incluyen la dirección DTE de llamada, una prioridad de filtro y los datos del usuario/llamada.

Filtros y circuitos de direccionamiento

Las llamadas de entrada pueden estar en un circuito de entrada estático o en un circuito asignado dinámicamente (DA). Puede definir uno o varios filtros en el mismo circuito de direccionamiento. Por ejemplo, un circuito DA puede tener varias adyacencias y puede definirse más de un filtro para él.

Prioridades del filtro

Las lista de filtros de los circuitos de entrada estáticos y de los circuitos DA se entremezclan y la mezcla está ordenada por prioridad descendente. Cuando se recibe una llamada de entrada, el direccionador busca primero la mayor prioridad en la lista de filtros. Para evitar que se asigne erróneamente un circuito estático a un circuito DA, se recomienda asignar a los filtros de todos los circuitos estáticos una prioridad superior a la de los filtros de todos los circuitos DA.

Restricciones de los filtros a las llamadas

En el caso de un circuito de entrada estático, el filtro debe especificar una dirección DTE de llamada concreta, pero el primer octeto de los datos de llamada/usuario debe contener el discriminador de protocolos ISO 8473 (129). Para que varios circuitos DA funcionen correctamente, deberán configurarse restricciones adicionales para cada filtro definido. Esto asegurará que los criterios de selección especificados en dichos filtros permitan efectuar la distinción necesaria entre las llamadas de entrada.

Nota: Si un circuito DA se conecta incorrectamente con un circuito estático, la arquitectura no intentará identificar la condición o rectificar el problema. En el lado estático se generará el “fallo de inicialización” usual debido a una falta de respuesta a las consultas de inicialización de enlaces. Por consiguiente, el SVC estático se borrará posteriormente.

Plantillas

Una plantilla es un conjunto de parámetros que el usuario puede configurar para las llamadas de salida. La plantilla establece los parámetros para que el circuito del direccionador remoto acepte las llamadas de entrada. Los parámetros definidos en una plantilla incluyen la dirección DTE de llamada y los datos del usuario/llamada.

Sólo puede definir una plantilla por circuito de direccionamiento estático de salida.

Inicialización de enlaces

La inicialización de enlaces es un procedimiento propiedad de Digital Equipment Corporation (y no forma parte de OSI). Esta inicialización se efectúa inmediatamente después del establecimiento del SVC. Se usa principalmente para establecer la relación de DECnet con un sistema remoto en un enlace de punto a punto.

Al recibir un mensaje de inicialización/XID, puede efectuarse la verificación en dos niveles: basándose en el circuito o bien en el sistema. Básicamente, el proceso de verificación compara los datos de verificación de entrada con datos especificados localmente para el circuito o para el sistema de llamada. Los datos de verificación aparecen en el campo de datos de verificación del mensaje XID.

Nota: Este release del software de direccionador no da soporte a la verificación efectuada por el sistema.

Configuración de OSI/DECnet V

Nota: Cuando trabaje con redes DNA IV mezcladas con redes DNA V, deberá efectuar toda la supervisión y configuración de DNA IV desde el proceso de configuración de DNA IV NCP>. Para obtener información sobre la configuración de DNA IV, consulte “Uso de DNA IV” en la página 259. El uso de “OSI” en este capítulo se refiere a los entornos OSI y DNA V a menos que se indique lo contrario.

Procedimiento de configuración básico

En esta sección se indican los pasos de configuración mínimos necesarios para activar y ejecutar el protocolo OSI/DNA V sobre una LAN (Ethernet o red en anillo), redes de conmutación de paquetes X.25 y Frame Relay. Antes de empezar cualquier procedimiento de configuración, use el mandato **list device** del proceso **config** para establecer una lista de los números de interfaz de los diferentes dispositivos. Si desea obtener más información sobre los mandatos de configuración, consulte los mandatos de configuración descritos en el presente capítulo.

Nota: Para que los cambios de configuración nuevos entren en vigor, deberá reiniciar el direccionador.

Siga el procedimiento de configuración básico siguiente antes de empezar los procedimientos especializados descritos en las secciones siguientes.

Establecimiento del título de la entidad de red (NET)
: Establezca el NET del direccionador usando el mandato set **network-entity-title**. El NET está formado por el ID de sistema del direccionador y su dirección de área. Use el mandato **list globals** para verificar que NET esté configurado correctamente.

Habilitación global de OSI
: Habilite el software de OSI para que se ejecute en el direccionador usando el mandato **enable OSI**. Use el mandato **list globals** para verificar que el protocolo OSI esté habilitado.

Configuración de OSI sobre una LAN Ethernet o red en anillo

Para configurar el protocolo OSI para que se ejecute sobre una LAN Ethernet o red en anillo , establezca la subred. Existe una correspondencia de una a una entre las subredes y las interfaces. Use el mandato **set subnet** para configurar todas las subredes LAN (Ethernet y red en anillo). Use las direcciones de difusión múltiple por omisión para Ethernet. Cuando configure una red en anillo, use las direcciones siguientes:

Parámetro	Dirección funcional 802.5
All ESs (Todos los ES) [09002B000004]	C00000004000
All ISs (Todos los IS) [09002B000005]	C00000008000
All L1 ISs (Todos los IS L1) [0180C2000014]	C00000008000
All L2 ISs (Todos los IS L2) [0180C2000015]	C00000008000

Use el mandato **list subnet detailed** o **list subnet summary** para verificar que haya configurado correctamente las subredes.

Configuración de OSI sobre X.25 o Frame Relay

Para configurar el protocolo OSI para que se ejecute sobre la interfaz de X.25 o Frame Relay, haga lo siguiente:

Establezca la subred Use el mandato **set subnet** para establecer la interfaz en X.25 o FRL (Frame Relay). Use los valores por omisión para toda la información necesaria. Use el mandato **list subnet detailed** o **list subnet summary** para verificar que haya configurado correctamente las subredes.

Establezca el circuito virtual Use el mandato **set virtual-circuit** para configurar un circuito virtual X.25 o Frame Relay.

Nota: El direccionador le solicitará una dirección DTE. Para frame relay, entre el número de DLCI (Data Link Control Identifier - Identificador del control del enlace de datos). Para X.25 entre la dirección DTE de PSN.

Configuración de un direccionador DNA V para un entorno DNA IV

Cuando configure un direccionador DNA V, es posible que deba configurar una interfaz para ejecutar un entorno DNA IV. Por ejemplo, el direccionador se conecta a una red DNA V y DNA IV, o un ES de DNA IV está conectado a un direccionador de DNA V.

Antes de empezar a seguir los pasos que indicamos a continuación, use la sección anterior adecuada para configurar OSI sobre una LAN, X.25 o Frame Relay.

1. Entre en el proceso de configuración de DN. Salga de `OSI config>` y entre `NCP>`. Use el mandato **protocol DN**.
2. Defina la dirección DNA global. Use el mandato **define executor address** para configurar el nodo DNA y el número de área del direccionador.
3. Habilite globalmente DNA. Use el mandato **define executor state** para habilitar el protocolo DNA para que se ejecute en el direccionador.
4. Habilite el direccionamiento entre áreas. Si el algoritmo de direccionamiento L2 es el vector de distancia del nivel 2, use el mandato **define executor type**

area para asegurarse de que este direccionador pueda intercambiar información de direccionamiento de nivel 2 de DNA IV.

5. Habilite el circuito DNA IV. Habilite el circuito que usará el direccionador para intercambiar la información de direccionamiento. Use el mandato **define circuit** *type* **state on**.

Consideraciones de algoritmo de DNA IV y DNA V

DNA IV usa un algoritmo de direccionamiento de vector-distancia. DNA V puede usar un algoritmo de direccionamiento de vector-distancia o de estado-enlace. El algoritmo se selecciona de acuerdo con lo que está habilitado o inhabilitado y las combinaciones que pueden producirse con estos dos protocolos.

DNA IV inhabilitado *y* OSI/DNA V habilitado
: Se considera que esta combinación es un entorno OSI/DNA V puro y se establece el algoritmo automáticamente en estado-enlace en los niveles 1 y 2 sin tener en cuenta cómo está configurado el mandato **set algorithm**.

DNA IV habilitado *y* OSI/DNA V inhabilitado
: Se considera que esta combinación es un entorno DNA IV puro y se establece el algoritmo automáticamente en vector-distancia sin tener en cuenta cómo está configurado el mandato **set algorithm**.

DNA IV habilitado *y* OSI/DNA V habilitado
: Se trata de un entorno mezclado y se lee y configura la información del algoritmo a partir de la SRAM. Use el mandato **set algorithm** para configurar esta información en la SRAM.

Configuración y supervisión de OSI/DECnet V

Este capítulo describe los mandatos de supervisión y configuración de OSI/DECnet V e incluye las secciones siguientes:

Acceso al entorno de configuración de OSI

Para obtener información sobre cómo acceder al entorno de configuración de OSI, consulte "Getting Started (Introduction to the User Interface)" en el manual *Software User's Guide* (Guía del usuario del software).

Mandatos de configuración de OSI/DECnet V

Esta sección resume y después explica los mandatos de configuración de OSI. Estos mandatos le permiten crear o modificar una configuración de OSI. Entre todos los mandatos de configuración de OSI después del indicador `OSI Config>`. Los valores por omisión de los mandatos y sus parámetros se ponen entre corchetes inmediatamente después del indicador.

Los mandatos de configuración manipulan la base de datos de OSI permanente (SRAM).

Tabla 61 (Página 1 de 2). Resumen de mandatos de configuración de OSI

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxv.
Add	Añade áreas a las que da soporte este nodo; recibe contraseñas con objetivos de autenticación; pone prefijos a direccionadores para otros dominios y alias
Change	Modifica algunos parámetros establecidos con el mandato **add**.
Clear	Borra una contraseña recibida, una contraseña de transmisión o una SRAM
Delete	Suprime áreas, PVC, direcciones-prefijo, adyacencias, alias, subredes y parámetros del circuito de direccionamiento X.25.
Disable	Inhabilita una subred, el protocolo OSI o un circuito de direccionamiento X.25.
Enable	Habilita una subred, el protocolo OSI o un circuito de direccionamiento X.25.
List	Muestra la configuración actual de las adyacencias, alias, contraseñas, pvc, direcciones-prefijo, subredes, algoritmo, phaseivpfx, información global o circuitos de direccionamiento X.25.

Tabla 61 (Página 2 de 2). Resumen de mandatos de configuración de OSI	
Mandato	Función
Set	Configura las propiedades asociadas a parámetros OSI (conmutadores, globales, NET, temporizadores, subredes, contraseñas-transmisión, direcciones-prefijo, adyacencias, pvc, algoritmos y phaseivpfx)
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxvi.

Add

Use el mandato **add** para configurar direcciones de prefijo y área, recibir contraseñas y dar alias a direcciones.

Sintaxis:

a**dd** alias

area...

filter...

prefix-address

receive-password

routing-circuit...

template...

alias Añade una serie de caracteres ASCII que designa una dirección de área o un ID de sistema en particular. Esta serie puede utilizar caracteres incluidos entre *a-z, A-Z, 0-–9*, otros caracteres entre los que se incluye el guión (-), la coma (,) y el subrayado (_). No use caracteres de escape.

El desplazamiento indica la posición, en semioctetos (porciones), donde la serie de caracteres empieza dentro de la dirección (alias usados para ID del sistema que tienen un desplazamiento de 1). Esta serie debe tener el mismo tamaño o longitud que el segmento al que designa o recibirá un mensaje indicando `invalid segment length` (longitud de segmento no válida). El alias máximo permitido es de 20 bytes.

Nota: Cuando use una entrada de alias, deberá ponerla entre corchetes. Por ejemplo: **l1_update 47[***nombrenuevo***]99999000012341234.**

Ejemplo:

```
add alias
Alias [ ]:
Segment [ ]:
Offset [1]:
```

Alias La serie de caracteres que desea utilizar

Segment El segmento NSAP al que sustituirá el alias.

Offset La situación del alias (en 4 bits, semioctetos) dentro del NSAP. El desplazamiento se determina desde el principio (izquierda) del NSAP tal como aparece en el terminal.

area *dir-área*

Añade direcciones de área adicionales (máximo de 18 bytes) a las que da soporte el nodo. Un nodo L1 que da soporte a otras áreas considera a éstas sinónimas. Una dirección de área es la parte del área del NET configurado. Si intenta añadir una dirección de área duplicada, el direccionador mostrará un mensaje de error.

Ejemplo:

```
add area 47000580999999000012341234
```

Nota: Cuando añada áreas sinónimas a un nodo L1, use el mandato **set globals** para configurar el número máximo de áreas sinónimas permitidas para este nodo. Todos los direccionadores de un área deben usar el número máximo de áreas sinónimas. No pueden establecerse adyacencias si son diferentes.

filter *nombre-filtro nombre-circuito-direccionamientos DTE-llamada Datos prioridad usuario llamada*

Añade parámetros en los que el direccionador basa su aceptación de las llamadas X.25 de entrada en un circuito de direccionamientos, ya sea un circuito de entrada estático o un circuito asignado dinámicamente (DA).

El *nombre-filtro* es el nombre que da al filtro. El *nombre-circuito-direccionamiento* es el nombre del circuito de direccionamiento con el que está asociado el filtro.

El *DTE-llamada* es la dirección del direccionador que llama.

El direccionador local comprueba la dirección del DTE de una llamada de entrada con una lista de filtros con prioridades para todos los circuitos. Una *prioridad* de filtro superior en la lista significa que primero se establece una conexión con la dirección del DTE de llamada del filtro. Se recomienda que asigne una mayor prioridad a los filtros para los circuitos estáticos que para los circuitos DA. Esto puede evitar que una llamada estática de entrada se asigne a un circuito DA.

El valor *Datos usuario llamada* puede ser uno de los tres valores siguientes: *osi, dec* o *user*.

- En el caso de *osi*, el direccionador configura automáticamente un discriminador de protocolos ISO para los datos de la llamada y ésta debe ser una llamada de un nodo OSI.
- En el caso de *dec*, el direccionador espera que las llamadas de entrada sean de un direccionador Digital Equipment Company (Compañía de equipos digitales).
- En el caso de *user*, se le solicitará una entrada adicional con un máximo de 16 octetos. Entre texto para restringir la aceptación de las llamadas de entrada. El campo *Datos usuario llamada* de la llamada de entrada debe coincidir con el texto especificado.

Ejemplo:

```
add filter
Filter Name [ ]:
Routing Circuit Name [ ]:
DTE Address [ ]:
Call UserData (OSI/DEC/USER)]:
```

Si selecciona **user** aparecerá un indicador adicional para que entre datos del usuario, seguido de un indicador de prioridad:

```
(max 16 octets) [ ]?
Priority (1-10) [5]?
```

prefix-address

Añade rutas estáticas a destinos situados fuera del dominio IS-IS. Este parámetro le solicita información diferente según el tipo de subred (X.25, LAN o FRL) que se configuró usando el mandato **set subnet**.

Nota: Si no se entra ningún prefijo de dirección, se asumirá el prefijo por omisión.

Ejemplo:

Subred LAN:

```
add prefix-address
Interface Number [0]:
Address Prefix [ ]:
MAC Address [ ]:
Default Metric [20]:
Metric Type [Internal]:
State [ON]:
```

Subred X.25:

```
add prefix-address
Interface Number [0]:
Address Prefix [ ]:
Mapping Type[Manual]:
DTE Address[]:
Default Metric[20]:
Metric Type [Internal]:
State [ON]:
```

Subred Frame Relay:

```
add prefix-address
Interface Number [0]:
Address Prefix [ ]:
DTE Address [ ]:
Default Metric [20]:
Metric Type [Internal]:
State [ON]:
```

Nota: Si la subred no existe, recibirá el mensaje de error `Subnet does not exist - cannot define a reachable address` (La subred no existe - no se puede definir una dirección accesible).

Interface Number

Define la interfaz sobre la que se accede a la dirección

Address Prefix

Define el prefijo de NSAP (máximo de 20 bytes).

MAC Address

Define la dirección del MAC de destino. Debe especificar esta dirección si la interfaz corresponde a una subred LAN. Este indicador sólo aparecerá si la interfaz está conectada a una subred LAN.

Mapping Type

Define cómo se determina la dirección física de destino, manual o X.121.

Si es manual, el protocolo le solicitará la dirección del DTE.
Si es X.121, el protocolo no le solicitará la dirección del DTE. En este caso, esta dirección se extraerá del NSAP.

DTE Address
Define la dirección del DTE de destino. Debe especificar esta dirección si la interfaz es X.25 y el tipo de correlación es manual. Este indicador sólo aparece si se configura la interfaz para X.25 y el tipo de correlación es manual.

Default Metric
Define el costo de la dirección.

Metric Type
Define si el costo métrico se usa para el direccionamiento externo (E) o interno (I).

State Cuando se establece en ON (activo), esta dirección-prefijo se anuncia a otros direccionadores de L2. Cuando se establece en OFF (inactivo), se trata de una dirección-prefijo no funcional.

routing-circuit

Añade un canal de comunicaciones para los circuitos virtuales conmutados X.25 (SVC) que la capa de direccionamiento usa para enviar y recibir datos.

El parámetro del circuito de direccionamiento sólo se puede aplicar si configura el direccionador como direccionador de tipo DEC. Puede especificar uno de los tipos de circuito de direccionamiento siguientes:

- estático entrada
- estático salida
- asignado dinámicamente

Un circuito estático de entrada maneja las llamadas X.25 de entrada. Un filtro de llamadas (consulte **add filter**) especifica los datos que usará el direccionador para aceptar o rechazar llamadas de entrada al circuito. Un circuito de salida estático inicia las llamadas X.25 de salida. El direccionador usa una plantilla de llamadas (consulte **add template**) para efectuar llamadas de salida. Un circuito asignado dinámicamente puede tener varios SVC que se ejecuten simultáneamente. A diferencia de los circuitos estáticos, el direccionador usa un circuito asignado dinámicamente únicamente cuando hay tráfico de entrada o salida del direccionador. Cierra el circuito asignado dinámicamente al agotarse el temporizador de desocupación.

El mandato **add routing-circuit** le solicita los valores de sus parámetros.

Ejemplo:

```
add routing-circuit
Interface number  [0]?
Circuit Name  [ ]?
Circuit Type (STATIC/DA)  [STATIC]?
Circuit Direction (OUT/IN)  [OUT]?
```

Si selecciona **STATIC** y **OUT**, aparecerán los indicadores adicionales siguientes:

```
Recall Timer (0-65535)  [60]?
Max Call Attempts (0-255)  [10]?
Initial Min Timer (1-65535)  [55]?
Enable IS-IS [YES]?
Level 2 only [NO]?
External Domain [NO]?
Default Metric  [20]?
ISIS Hello Timer [3]?
Enable DECnetV Link Initialization  [YES]?
Modify Receive Verifier  (YES/NO)  [NO]?
Transmit Verifier (YES/NO)  [NO]?
Explicit Receive Verification (TRUE/FALSE)  [TRUE]?
```

Si selecciona **STATIC** e **IN**, aparecerán los indicadores adicionales siguientes:

```
Initial Min Timer (1-65535)  [55]?
Enable IS-IS [YES]?
Level 2 only [NO]?
External Domain [NO]?
Default Metric [20]?
ISIS Hello Timer [3]?
Enable DECnetV Link Initialization [YES]?
Modify Receive Verifier (YES/NO) [NO]?
Modify Transmit Verifier (YES/NO) [NO]?
Explicit Receive Verification (TRUE/FALSE) [TRUE]?
```

Si selecciona **DA** para el tipo de circuito, aparecerán los indicadores adicionales siguientes:

```
Recall Timer (0-65535) [60]?
Reserve Timer (1-65536) [600]?
Idle Timer (1-65536) [30]?
Max SVCs (1-65535) [1]?
```

Interface Number

Especifica la interfaz X.25 lógica de este circuito de direccionamiento.

Circuit Name

Establece el nombre alfanumérico de este registro de circuito de direccionamiento.

Circuit Type

Especifica si este circuito de direccionamiento es un circuito STATIC (estático) o DYNAMICALLY ALLOCATED (asignado dinámicamente).

Circuit Direction

Especifica IN (entrada) o OUT (salida) para determinar si el SVC del circuito estático se establecerá con una solicitud de llamada de entrada o una solicitud de llamada de salida. En ambos casos, se establece inicialmente el SVC sobre la acción del operador, pero el circuito no se habilita totalmente hasta que ambos extremos del circuito se hayan inicializado satisfactoriamente.

Recall Timer

Define el tiempo, en segundos, que debe esperar un circuito DA o un circuito estático de salida antes de intentar una solicitud de llamada nueva. Esto es el resultado del fallo de la solicitud de llamada inicial o de que una llamada posterior se haya borrado.

Max Call Attempts
Si falla una solicitud de llamada, Max Call Attempts define el número máximo de solicitudes de llamada posteriores que el circuito estático de salida intentará antes de abandonar. Llegado a este punto, el fallo de llamada se anotará cronológicamente y será necesaria la intervención del operador para activar el circuito estático de salida.

Initial Min Timer
Especifica el período de tiempo (en segundos) que esperará un circuito estático de salida para que se inicialice un enlace (recepción de un ESH o un ISH) después de que se haya aceptado la solicitud de llamada. Si el temporizador mín inicial se agota antes de que se haya inicializado completamente el enlace, el SVC se borrará y se generará un suceso que indicará un fallo de la inicialización.

Enable IS-IS
Define si el protocolo IS-IS está habilitado en este circuito de direccionamientos. Cuando se establece en ON, se habilita el protocolo IS-IS; cuando se establece en OFF, este protocolo no se habilita.

Level2 Only
Especifica si este circuito de direccionamientos se usa únicamente para direccionamientos de nivel 2.

External Domain
Especifica si el direccionador transmite y recibe mensajes a un dominio o desde un dominio situado fuera de su dominio de direccionamientos IS-IS.

Default Metric
Define el costo de esta dirección.

ISIS Hello Timer
Define el intervalo de tiempo transcurrido entre la transmisión de hellos ISIS.

Enable DECnetV Link Initialization
Define si la inicialización de enlaces de estilo DEC para este circuito está habilitada (YES) o no (NO).

Modify Receive Verifier
Especifica los datos de verificación que se comprobarán cuando se reciba un XID al verificar por circuito.

Modify Transmit Verifier
Especifica los datos de verificación que se incluirán en el XID.

Explicit Receive Verification
Define si la verificación se efectúa por circuito o por sistema. TRUE (VERDAD) especifica la verificación por circuito y FALSE (MENTIRA) especifica por sistema.

Reserve Timer
Define el tiempo transcurrido después de que el temporizador de desocupación se agote durante el cual el direccionador seguirá considerando un nodo remoto de un

circuito DA como “activo”. El direccionador podrá reenviar datos en el circuito DA hasta que se agote el temporizador de reserva.

Idle Timer

Define el período de tiempo que puede estar desocupada una adyacencia DA (sin transmisión de datos) antes de borrarla.

Max SVCs

Define el número máximo de adyacencias SVC a las que este circuito DA da soporte. Si no puede efectuarse ninguna llamada debido a que se ha alcanzado el número máximo de adyacencias SVC, se generará un suceso "Exceed Max SVC adjacencies" (superado el número máximo de adyacencias SVC).

receive-password

Añade una serie de caracteres ASCII (hasta un máximo de 16 caracteres) que autentifica todos los paquetes de entrada. Un paquete de entrada cuya contraseña coincida con una de las contraseñas de recepción se procesará a través de IS; se eliminarán aquellos paquetes de entrada cuya contraseña no coincida.

Ejemplo:

```
add receive-password
```

Nota: Se obtendrá un mensaje de error si se usa un *tipo de contraseña* no válido.

```
Password type [Domain]:
Password [ ]:
Reenter password:
```

Password type

Designa uno de los dos tipos de contraseñas: *dominio* o *área*.

Las contraseñas de dominio se usan con LSP L2 (paquetes de estado del enlace, nivel 2) y SNP (PDU del número de secuencia).
Las contraseñas de área se usan con LSP L1 y SNP.

Password

Designa la serie de caracteres que se usa para la autenticación. La serie máxima que se permite tiene 16 caracteres.

template *nombre-plantilla nombre-circuito-direccionamiento DTE destino Datos usuario-llamada*

Crea una plantilla a través de la cual el direccionador efectúa llamadas de salida en un circuito de direccionamiento de salida estático. Las plantillas para circuitos de salida estáticos son análogas a los filtros para circuitos de entrada estáticos.

El *nombre-plantilla* es el nombre que da a la plantilla. El *nombre-circuito-direccionamiento* es el nombre del circuito de direccionamiento con el que está asociada la plantilla.

El *DTE-destino* es una dirección para el direccionador remoto que tiene un máximo de 14 dígitos.

Los *Datos usuario-llamada* deben coincidir con los datos de llamada establecidos en un filtro del circuito remoto. *Datos usuario-llamada* puede ser uno de los tres valores siguientes: *osi, dec* o *user*:

- En el caso de *osi*, el direccionador configura automáticamente un discriminador de protocolos ISO para los datos de la llamada y ésta debe ir a un direccionador ISO.
- En el caso de *dec*, los datos del usuario identifican las llamadas de salida como provenientes de un direccionador Digital Equipment Company.
- En el caso de *user*, se le solicitará una entrada adicional con un máximo de 16 octetos. Entre texto para que coincida con los datos de usuario del filtro adecuado en un direccionador remoto.

Ejemplo:

```
add template
      Template Name []?
      Routing Circuit Name []?
      DTE Address []?
      Call UserData (OSI/DEC/USER) ?
```

Si elige **user**, aparecerá este indicador adicional:

```
      (max 16 octets) [] ?
```

Entre un máximo de 16 octetos de texto para los datos del usuario.

Change

Le permite modificar los parámetros de registros ISO/DNV creados en la base de datos permanente.

Sintaxis:

ch**ange** filter
prefix-address
routing-circuit
template

filter *nombre-filtro*

Cambia los valores de los parámetros del filtro del circuito de direccionamiento. Puede entrar un nombre de filtro o dejar que el direccionador le solicite el nombre de filtro.

Los valores indicados entre corchetes [] son los valores actuales de los parámetros; el valor configurado que se lee en la base de datos permanente.

Ejemplo: **change filter**

```
Filter Name [currentvalue]?
DTE Address [currentvalue]?
Call Userdata (OSI/DEC/USER)? [currentvalue]?
```

Si selecciona **user**, aparecerá este indicador adicional para que entre datos del usuario, seguido de un indicador de prioridad:

```
      (max 16 octets) [currentvalue] ?
```

prefix-address

Cambia los datos de dirección para las subredes. El direccionador le solicitará los datos de dirección.

Ejemplo: `change prefix-address`

Subred LAN:

```
Interface Number [0]:
Address Prefix [ ]:
MAC Address [ ]:
Default Metric [20]:
Metric Type [Internal]:
State [ON]?
```

Subred X.25:

```
Interface Number [0]:
Address Prefix [ ]:
Mapping Type [Manual]:
DTE Address [ ]:
Default Metric [20]:
Metric Type [Internal]:
State [ON]?
```

Subred Frame Relay:

```
Interface Number [0]:
Address Prefix [ ]:
DTE Address [ ]:
Default Metric [20]:
Metric Type [Internal]:
State [ON]?
```

Interface Number
Indica la interfaz sobre la que se alcanza la dirección.

Address Prefix
Indica el prefijo del NSAP de destino (máximo de 20 bytes).

MAC Address
Indica la dirección del MAC de destino. Debe especificar esta dirección si la interfaz corresponde a una subred LAN. Este indicador sólo aparecerá si la interfaz está conectada a una subred LAN.

Mapping Type
Indica cómo se determina la dirección física de destino, *manual* o *X.121*.

Si es manual, el protocolo le solicitará la dirección del DTE.
Si es X.121, el protocolo no le solicitará la dirección del DTE. En este caso, esta dirección se extraerá del NSAP.

DTE Address
Define la dirección del DTE de destino. Debe especificar esta dirección si la interfaz es X.25 y el tipo de correlación es manual. Este indicador sólo aparece si se configura la interfaz para X.25 y el tipo de correlación es manual.

Default Metric
Indica el costo de la dirección.

Metric Type
Indica si el costo métrico se usa para el direccionamiento externo (E) o interno (I).

State Cuando se establece en ON (activo), esta dirección recibirá paquetes. Cuando se establece en OFF (inactivo), se trata de una dirección no funcional.

routing-circuit *nombrecircuitodireccionamiento*

Cambia los valores de configuración de un circuito de direccionamiento. Puede entrar un nombre de circuito de direccionamiento o dejar que el direccionador le solicite un nombre. Los valores que están entre corchetes [] son los valores actuales que se leen en la base de datos permanente.

Ejemplo: `change routing-circuit`

```
Routing Circuit Name [currentvalue]?
Recall Timer (0-65535) [currentvalue]?
Max Call Attempts (0-255) [currentvalue]?
Initial Min Timer (1-65535) [currentvalue]?
Enable ES-IS [currentvalue]?
Enable IS-IS [currentvalue]?
Level 2 only [currentvalue]?
External Domain [currentvalue]?
Default Metric [currentvalue]?
ESIS IS Hello Timer [currentvalue]?
ISIS Hello Timer [currentvalue]?
Enable DECnetV Link Initialization [currentvalue]?
Modify Receive Verifier (YES/NO) [currentvalue]?
Modify Transmit Verifier (YES/NO) [currentvalue]?
Explicit Receive Verification (TRUE/FALSE) [currentvalue]?
```

template *nombre-plantilla*

Cambia los valores de la plantilla de un circuito de direccionamiento de salida estático. Puede entrar un nombre de plantilla o dejar que el direccionador le solicite un nombre. Los valores indicados entre corchetes [] corresponden a los valores actuales de los parámetros; los valores configurados que se leen en la base de datos permanente.

Ejemplo: `change template`

```
Template Name [currentvalue]?
DTE Address [currentvalue]?
Call UserData (OSI/DEC/USER)? [currentvalue]
```

Si selecciona **user**, este indicador opcional aparecerá para que entre los datos de usuario; seguido de un indicador de prioridad:

```
(max 16 octets) [currentvalue] ?
Priority (1-10) [currentvalue]?
```

Clear

Use el mandato clear para borrar la SRAM o para eliminar la contraseña de transmisión o recepción.

Sintaxis:

clear receive-password

sram

transmit-password

receive-password

Elimina todas las contraseñas de recepción configuradas anteriormente usando el mandato **add receive-password**.

Nota: Si usa una contraseña no válida recibirá un mensaje de error.

Ejemplo: `clear receive`

```
Password Type [Domain]:
```

Password Type

Especifica el tipo de contraseña que se está usando: *Dominio* o *Área*. Consulte el mandato **add receive-password** para obtener una descripción de estas contraseñas.

SRAM

Use este parámetro para borrar la configuración OSI de la SRAM.

Atención: Use este mandato ***únicamente*** si tiene la intención de borrar la configuración.

Ejemplo:

```
clear sram
Warning:  All OSI SRAM Information will be erased.
Do you want to continue? (Y/N) [N]?
```

Transmit-password

Elimina la contraseña de transmisión previamente configurada usando el mandato **set transmit-password**. El resultado de este parámetro es el mismo que el producido por el parámetro de la contraseña de recepción.

Nota: Si usa una contraseña no válida recibirá un mensaje de error.

Ejemplo:

```
clear password transmit
Password Type [Domain]:
```

Delete

Use el mandato **delete** para eliminar parámetros configurados previamente usando los mandatos **set** o **add**.

Sintaxis:

del**ete**	adjacency
	alias
	area
	filter (sólo configuración DEC)
	prefix-address
	routing-circuit
	subnet
	template (sólo configuración DEC)
	virtual-circuit

adjacency

Elimina una adyacencia de ES configurada estáticamente con el mandato **set adjacency**.

Ejemplo:

```
delete adjacency
Interface Number [0]?
Area Address [ ]?
System ID [ ]?
```

Interface number
Indica la interfaz de la adyacencia.

Area address
Indica la dirección de área de la adyacencia.

System ID
Indica la parte del NET que identifica la adyacencia dentro del área.

alias Elimina la serie de caracteres ASCII que designa una parte de una dirección de área o un ID de sistema.

Ejemplo:

```
delete alias
ALIAS [ ]?
```

area *dirección*
Elimina la dirección de área (*dirección*) configurada previamente con el mandato **add area**.

Ejemplo:

```
delete area 47000580999999000012341234
```

filter *nombre-filtro*
Elimina un registro de filtro de la base de datos permanente.

Ejemplo:

```
delete p_systems
```

prefix-address
Elimina la dirección-prefijo configurada previamente con el mandato **set prefix-address**.

Ejemplo: `delete prefix-address`

```
Interface Number [0]?
Address Prefix [ ]
```

Interface number
Indica el número de interfaz sobre la que está configurada la dirección-prefijo.

Address Prefix
Indica el prefijo del NSAP de destino.

Interface number
Indica el número de la interfaz sobre la que está configurado el PVC.

DTE address
Indica la dirección del DTE de la red X.25 al que se está conectando o el DLCI de la red Frame Relay al que se está conectando.

routing-circuit *nombre-circuito-direccionamiento*
Elimina un circuito de direccionamiento X.25 que se estableció con **add routing-circuit** desde la base de datos permanente.

Ejemplo:

```
delete routing-circuit p_system2
```

subnet *núm.intfz*

Elimina una subred que se configuró previamente con el mandato **set subnet**. *núm.intfz* indica el número de interfaz de la subred configurada.

Ejemplo:

```
delete subnet 1
```

template *nombre-plantilla*

Elimina la plantilla de un circuito de direccionamiento de salida estático mediante el cual el direccionador genera mensajes X.25 de salida a partir de la base de datos permanente.

Ejemplo:

```
delete template x25_5
```

virtual-circuit

Elimina un circuito virtual X.25 o Frame Relay que se configuró previamente con el mandato set virtual-circuit.

Ejemplo:

```
delete virtual-circuit
Interface number [0]?
DTE address []?
```

Interface number

Número de interfaz sobre el que está configurado el circuito virtual.

DTE address

Dirección del DTE de la red X.25 al que se está conectando o el DLCI de la red Frame Relay al que se está conectando.

Disable

Use el mandato **disable** para inhabilitar las funciones habilitadas previamente usando el mandato **enable**.

Sintaxis:

disable osi

routing-circuit

subnet

osi Inhabilita el protocolo OSI en el direccionador.

routing-circuit *nombre-circuito-direccionamiento*

Inhabilita el circuito de direccionamiento especificado.

Use el mandato **add routing-circuit** para establecer circuitos de direccionamiento.

subnet núm.interfaz

Inhabilita el protocolo OSI en la subred especificada (*núm.interfaz*).

Ejemplo:

```
disable subnet 0
```

Enable

Use el mandato **enable** para habilitar el protocolo OSI o una subred OSI.

Sintaxis:

enable osi

routing-circuit...

subnet...

osi Habilita el protocolo OSI en el direccionador.

routing-circuit *nombre-circuito-direccionamiento*
Habilita el circuito de direccionamiento especificado.

Use el mandato **add routing-circuit** para establecer circuitos de direccionamiento.

Ejemplo:

```
enable routing-circuit p_system2
```

subnet núm.interfaz
Habilita el protocolo OSI en la subred especificada (*núm.interfaz*).

Ejemplo:

```
enable subnet 0
```

List

Use el mandato list para visualizar la configuración actual del protocolo OSI.

Sintaxis:

list adjacencies

algorithm

alias

filter (sólo configuración DEC)

globals

password

phaseivpfx

prefix-address

routing-circuits (sólo configuración DEC)

subnets

templates (sólo configuración DEC)

timers

virtual-circuits

adjacencies
Muestra todas las adyacencias de ES configuradas estáticamente.

Ejemplo:

```
list adjacencies
Ifc    Area Address    System ID         MAC Address
 0                     0001-0203-0405    0001-0203-0405
 1                     0002-4000-0000    0000-0019-3004
```

Ifc Indica el número de la interfaz que se conecta con la adyacencia.

Area Address
Indica la dirección de área de esta adyacencia de ES.

System ID
Indica la parte del NET que identifica la adyacencia.

MAC Address
Indica la dirección de MAC (SNPA) de la adyacencia.

algorithm

Muestra el algoritmo de direccionamiento que está configurado en la SRAM para el protocolo DNA V. Si está ejecutando únicamente el protocolo OSI, este parámetro no tendrá soporte.

Ejemplo:

```
list algorithm
Level 1 algorithm  LINK_STATE
Level 2 algorithm  DISTANCE_VECTOR
```

Level 1 Algorithm
Indica la configuración actual del algoritmo de direccionamiento para nivel 1, estado del enlace (valor por omisión) o vector de distancia.

Level 2 Algorithm
Indica la configuración actual del algoritmo de direccionamiento para nivel 2, estado del enlace o vector de distancia (valor por omisión).

Nota: Según si DNA IV está habilitado o inhabilitado, el algoritmo de direccionamiento que se visualiza aquí será diferente de lo que se esté ejecutando en el direccionador.

alias Muestra los alias configurados y los segmentos de dirección correspondientes.

Ejemplo:

```
list aliases
Alias        Segment          Offset

joplin       AA0004000104        1
moon         0000931004F0        1
trane        000093E0107A        1
```

filter Muestra los filtros definidos para circuitos X.25.

Ejemplo:

```
list filters
           Rout Cir Name   Filter Name   DTE Addr   Pri   Call Data
           routeCir2       filter1       25         5     81
```

globals Muestra los parámetros globales de NET, direcciones de área, valores de conmutación y configuración del temporizador actuales del direccionador.

Ejemplo:

```
list globals
DNAV State: Enabled*   Network Entity Title:  4700050001:0000931004F0
Manual Area Addresses:
1. 4700050001    2. 7700050011

Switches:
ESIS Checksum = On              ESIS Init Option = Off
Authentication = Off

Globals:
IS Type = L2                    System ID Length = 6
L1 LSP Size = 1492 bytes        L2 LSP Size = 1492 bytes
Max IS Adjs = 50                Max ES Adjs = 200
Max Areas = 50                  Max ESs per Area = 50
Max Ifc Prefix Adds = 100       Max Ext Prefix Adds = 100
Max Synonymous Areas = 3        Max Link State Updates = 100
```

OSI State or DNAV State
Indica si el protocolo OSI o el DNA V está ejecutándose en el direccionador.

Network Entity Title
Indica la dirección de área y el ID de sistema que forman el NET del direccionador.

Manual Area Addresses
Áreas en las que el direccionador funciona. La primera dirección de área refleja la dirección de área del NET configurado del direccionador. Las direcciones de área adicionales se añadieron con el mandato **add area**.

Globals: Indica los parámetros globales configurados actualmente:

IS Type La designación del direccionador en el entorno OSI: L1 o L2.

Domain ID Length
El tamaño (en bytes) de la parte de ID del sistema de NET.

Nota: Todos los direccionadores del dominio deben estar de acuerdo en la longitud del ID del dominio.

L1 LSP Size/L2 LSP Size
Muestra el tamaño máximo del almacenamiento intermedio de LSP de L1 y L2.

Max IS Adjacencies/Max ES Adjacencies
Muestra el número máximo de adyacencias de IS y ES permitidas para todos los circuitos.

Max Areas
Muestra el número máximo de áreas del dominio de direccionamiento.

Max ESs per Area
Muestra el número máximo de ES permitidos en un área.

Max Int Prefix Adds
Muestra el número máximo de direcciones de prefijo interno.

Max Ext Prefix Adds
Muestra el número máximo de direcciones de prefijo externo.

Max Synonymous Areas
Muestra el número máximo de áreas de nivel 1 a las que da servicio este direccionador.

password

Muestra el número de las contraseñas de transmisión y recepción configuradas para cada dominio y área OSI. Las contraseñas de recepción se configuran con el mandato **add receive-password**. Las contraseñas de transmisión se configuran con el mandato **set transmit-password**.

Ejemplo:

```
list password
  Number of Passwords Configured:
      -- Domain --
  Transmit = 3
  Receive  = 2
      -- Area --
  Transmit = 4
  Receive  = 6
```

phaseivpfx

Muestra el prefijo de dirección de DNA phase IV configurado que está usando el protocolo OSI para direccionar paquetes a una red DNA IV conectada.

Ejemplo:

```
list phaseivpfx
            Local Phase IV Prefix: 49
```

prefix-address

Muestra todas las SNPA de las rutas configuradas estáticamente.

Ejemplo:

```
list prefix:-addresses
Ifc  Type  Metric  State  Address Prefix  Dest Phys Address
 0    INT    20     On        470006        302198112233
 1    EXT    50     OFF       470006        302198223344
```

Ifc Indica el número de la interfaz donde se puede acceder a la dirección.

Type Indica el tipo de métrica, interna (INT) o externa (EXT).

Metric Indica el costo de la dirección accesible.

Address prefix
Indica el prefijo del NSAP de destino. Este prefijo puede tener 20 bytes de longitud.

Dest Phys Address
Indica la dirección del DTE de destino si esta interfaz es X.25 y la correlación configurada es manual.

routing-circuits

Muestra un resumen de todos los circuitos de direccionamiento o detalles de cada circuito de direccionamiento.

Ejemplo:

```
list routing circuits
Summary or Detailed [Summary]? Summary

Ifc   Name        Type                Enabled
0     routecir1   STATIC-OUT          YES
0     routecir2   STATIC-IN           YES
0     routecir3   DA                  YES


Summary or Detailed [Summary]? Detailed

Routing Circuit Name []  routecir2
Interface #:               0
Enabled:                   YES
Type:                      STATIC
Direction:                 Incoming
Initial Minimum Timer:     55
Enable IS-IS:              YES
L2 Only:                   NO
External Domain:           NO
Metric:                    20
IS-IS Hello Timer:         3
DECnetV Link Initialization:   YES
Receive Verifier:
Transmit Verifier:
Explicit Receive Verification: TRUE
```

Interface # / Ifc
Especifica la interfaz X.25 lógica de este circuito de direccionamiento.

Name Establece el nombre alfanumérico de este registro de circuito de direccionamiento.

Enabled Indica el estado del circuito de direccionamiento: YES (SÍ) para habilitado y NO para inhabilitado.

Type Indica si el circuito es STATIC-IN (ESTÁTICO DE ENTRADA), STATIC-OUT (ESTÁTICO DE SALIDA) o DA (asignado dinámicamente).

Direction Indica cómo establece el direccionador un circuito de direccionamiento estático: mediante una solicitud de llamada de entrada (IN) o una solicitud de llamada de salida (OUT).

En ambos casos, el SVC se establece inicialmente mediante una acción del operador, pero el circuito no se habilita completamente hasta que ambos extremos del circuito se hayan inicializado satisfactoriamente.

Initial Min Timer
Especifica el período de tiempo (en segundos) que esperará un circuito estático de salida para que se inicialice un enlace (recepción de un ESH o un ISH) después de que se haya aceptado la solicitud de llamada. Si el temporizador mín inicial se agota antes de que se haya inicializado completamente el enlace, el SVC se borrará y se generará un suceso que indicará un fallo de la inicialización.

Enable IS-IS
Indica si el protocolo IS-IS está habilitado en este circuito.

L2 Only Indica si este circuito de direccionamientos se usa únicamente para direccionamientos de nivel 2.

External Domain
Indica si el direccionador transmite y recibe mensajes a un dominio o desde un dominio situado fuera de su dominio de direccionamientos IS-IS.

Metric Especifica el costo de esta dirección.

ISIS Hello Timer
Indica el intervalo de tiempo transcurrido entre la transmisión de hellos ISIS.

DECnetV Link Initialization
Indica si la inicialización de enlaces de estilo DEC para este circuito está habilitada (YES - SÍ) o no (NO).

Receive Verifier
Muestra los datos de verificación que se comprobarán con un XID recibido al verificar por circuito.

Transmit Verifier
Muestra los datos de verificación que se incluirán en los XID cuando se verifique por circuito.

Explicit Receive Verification
Indica si la verificación la efectúa el circuito o el sistema. TRUE (VERDAD) indica verificación del circuito, FALSE (MENTIRA) indica verificación del sistema.

Subnet *inf.subred núm.intfz*
Muestra información de la subred.

- *Inf.subred* tiene dos opciones: Summary (resumida) o Detailed (detallada).
  - *Summary* muestra información de todas las subredes configuradas.
  - *Detailed* muestra únicamente información de las subredes LAN.
- *núm.Intfz* es la interfaz que se conecta con la subred.

Ejemplo:

```
list subnet summary
Ifc  State  Type  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    Frl
```

Ifc Indica el número de interfaz de la subred.

State Indica el estado de la interfaz, ON (activo) u OFF (inactivo).

Type Indica el tipo de subred: LAN, X25,

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 está funcionando únicamente en el nivel 2, yes (verdad) o no (falso).

Ext Dom Indica si el direccionador está funcionando fuera del dominio de direccionamiento IS-IS (dominio externo).

Metric Indica el costo del uso de esta subred.

EIH Indica el intervalo de envío a la subred de los mensajes hello de ES.

IIH Indica el intervalo de envío de los mensajes hello de IS a la subred.

Ejemplo:

```
list subnet detailed
            Interface Number [0]? 0

            Detailed information for subnet 0:
               ISIS Level 1 Multicast: 018002B000014
               ISIS Level 2 Multicast: 018002B000015
               All ISs Multicast:      009002B000005
               All ESs Multicast:      009002B000004
               Level 1 Priority: 64
               Level 2 Priority: 64
```

ISIS Level 1 Multicast
Indica la dirección de difusión múltiple a usar cuando se transmitan y reciban PDU IS-IS de L1.

ISIS Level 2 Multicast
Indica la dirección de difusión múltiple a usar cuando se transmitan y reciban PDU IS-IS de L2.

All ISs Multicast
Indica la dirección de difusión múltiple a usar cuando se reciban hellos de ES.

All ESs Multicast
Indica la dirección de difusión múltiple a usar cuando se transmitan hellos de IS.

Level 1 Priority/Level 2 Priority
Indica la prioridad del direccionador para convertirse en el direccionador designado de la LAN.

templates
Muestra una lista de las plantillas de este direccionador.

Ejemplo:

```
list template
Route Cir Name      Template Name      DTE Addr      Call UserData
routetest2          temptest2          25            81
```

timers Muestra la configuración del temporizador OSI/DNA V (qué se está ejecutando en el direccionador, OSI o DNA V).

Ejemplo:

```
list timers
            Timers:
            Complete SNP (sec) = 10        Partial SNP (sec) = 2
            Min LSP Gen (sec) = 30         Max LSP Gen (sec) = 900
            Min LSP Xmt (sec) = 30         Min Br LSP Xmt (msec) = 33
            Waiting Time (sec) = 60        DR ISIS Hello (sec) = 1
            ES Config Timer (sec) = 10
```

Timers: Indica la configuración de los temporizadores de OSI salvo los temporizadores por circuito.

Complete SNP
Intervalo entre la generación de SNP completos.

Partial SNP
Intervalo mínimo entre el envío de SNP parciales.

Min LSP Generation/Max LSP Generation
Los intervalos mínimo y máximo entre las generaciones de LSP.

Min LSP Transmission
El intervalo mínimo entre retransmisiones de LSP.

Min Broadcast LSP Transmission
El intervalo mínimo entre retransmisiones LSP en un circuito de difusión.

Waiting Time
Tiempo de retardo del proceso de actualización antes de entrar en el estado ON (activo).

DR ISIS Hello
Intervalo entre generaciones de PDU de hello IS-IS si este direccionador es un direccionador designado.

ES Config Timer
Intervalo mínimo en el que un ES debe enviar un paquete hello cada vez que se activa una interfaz.

virtual-circuits
Muestra información sobre todos los circuitos virtuales X.25.

Ejemplo: `list virtual-circuits`

Set

Use el mandato **set** para configurar el direccionador para que ejecute el protocolo OSI.

Sintaxis:

set
adjacency
algorithm
globals
network-entity-title
phaseivpfx
subnet
switches
timers
transmit-password (sólo configuración DEC)
virtual-circuit (sólo configuración IBM 2210)

adjacency
Añade o cambia una adyacencia ES. Añade una adyacencia ES para todas las LAN ES que no ejecutan el protocolo ES-IS.

Ejemplo:

```
set adjacency
Interface Number [0]:
Area Address [ ]:
System ID [ ]:
MAC Address [ ]:
```

Interface Number
Indica el número de la interfaz que se conecta con la adyacencia.

Area Address
Indica el área donde está situada la adyacencia.

System ID
Indica la parte del ID del sistema del NET que se usa para identificar la adyacencia.

MAC Address
Indica la dirección de MAC (SNPA) de la adyacencia.

algorithm

Nota: Se trata de un mandato de DNA phase V. Este mandato sólo funcionará si se incluye el protocolo DNA phase V en la carga de software. Esto le permitirá seleccionar el tipo de algoritmo de direccionamiento que está usando para el protocolo de direccionamiento de DNA, el estado de enlace (DNA V) o el vector de distancia (DNA IV).

Ejemplo:

```
set algorithm
Level 1 Algorithm [link_state]?
Level 2 Algorithm [distance_vector]?
```

Level 1 Algorithm
Selecciona el tipo de algoritmo de direccionamiento, el link_state (estado_enlace) (para redes DNA V) o el distance_vector (vector_distancia) (para redes DNA IV).

Level 2 Algorithm
Selecciona el tipo de algoritmo de direccionamiento, el link_state (estado_enlace) (para redes DNA V) o el distance_vector (vector_distancia) (para redes DNA IV).

globals Configura los parámetros globales necesarios para el protocolo OSI.

Ejemplo:

```
set globals
IS Type [L2]:
System ID Length [6 bytes]:
Max Synonymous Areas [3]:
L1 LSP Buffer Size :[1492 bytes]:
L2 LSP Buffer Size [1492 bytes]:
Max IS Adjacencies ]50[:
Max ES Adjacencies [200]:
Max Areas in Domain [50]:
Max ESs per Area [500]:
Max Internal Prefix Addresses [100]:
Max External Prefix Addresses [100]:
Max Link State Updates [100]?
```

IS Type (L1 o L2)
Selecciona el nivel del direccionador: nivel 1 o nivel 2.

System ID Length
Selecciona la longitud de la parte del ID de dominio del NET. Esta longitud debe ser la misma para todos los direccionadores del mismo dominio.

Max Synonymous Areas
Selecciona el número máximo de áreas de nivel 1 a las que sirve este direccionador.

L1 LSP Buffer Size
Selecciona el tamaño del almacenamiento intermedio de los SNP y LSP de nivel 1 originados por el direccionador. El rango está entre 512 y 1492. Si el tamaño del paquete de la interfaz es inferior al configurado aquí, OSI no se ejecutará y el direccionador generará el mensaje ELS ISIS.053.

L2 LSP Buffer
Selecciona el tamaño del almacenamiento intermedio de los SNP y los LSP de nivel 2 originados por el direccionador. El rango está entre 512 y 1492. Si el tamaño del paquete de la interfaz es inferior al configurado aquí, OSI no se ejecutará y el direccionador generará el mensaje ELS ISIS.053.

Max IS Adjacencies
Selecciona el número total de las adyacencias IS permitidas para todos los circuitos. Este número se usa para dar tamaño a la agrupación libre de adyacencias IS.

Max ES Adjacencies
Selecciona el número total de las adyacencias ES permitidas para todos los circuitos. Este número se usa para dar tamaño a la agrupación libre de adyacencias ES.

Max Areas in Domain
Selecciona el número total de áreas del dominio de direccionamiento. Este número se usa para dar tamaño a la tabla de direccionamientos L2.

Max ESs per Area
Selecciona el número total de ES en cualquier área. Este número se usa para dar tamaño a la tabla de direccionamientos L1.

Max Internal Reachable Addresses
Selecciona el número que está usando para dar tamaño a la tabla de direccionamientos métricos interna.

Max External Reachable Addresses
Selecciona el número que está usando para dar tamaño a la tabla de direccionamientos métricos externa.

Max Link State Updates
Selecciona el número que está usando para dar tamaño a la base de datos de estados de enlace.

network-entity-title

Configura el NET del direccionador. El NET está formado por el ID de sistema del direccionador y la dirección de área del direccionador.

Ejemplo:

```
set network-entity-title
Area-address [ ]
System-ID [ ]:
```

Area-address

Indica una de las porciones de dirección de área del NET del direccionador. Se incluye como primera dirección en el juego de direcciones de áreas manuales del direccionador. Cada dirección de área puede tener un máximo de 19 bytes.

System-ID

Define la parte del NSAP que identifica este direccionador específico. El ID del sistema puede tener un máximo de 19 bytes, pero la longitud debe estar de acuerdo con la longitud del ID de dominio configurada con el mandato **set globals**.

phaseivpfx

Configura la dirección-prefijo para permitir al protocolo OSI direccionar paquetes a la red DNA IV conectada. El valor por omisión es 49 (hexadecimal).

Ejemplo:

```
set phaseivpfx
Local Phase IV prefix [49]?
```

subnet Añade o cambia una subred. Este parámetro le solicita información diferente, según el tipo de subred que configure. X.25 o LAN.

Ejemplo:

Subred X.25:

```
set subnet
Interface number [0]:
Interface Type [X25]:
```

Subred LAN:

```
Interface number [0]:
Interface Type [LAN]:
Enable ES-IS [N]?
Enable IS-IS [N]?
Level 2 Only [N]?
External Domain [N]?
Default Metric [20]:
ESIS IS Hello Timer [10 sec]:
ISIS Hello Timer [3 sec]:
Modify Transmit password [No]?
Modify the set of receive passwords [No]?
L1 Priority [64]:
L2 Priority [64]:
All ESs [0x09002B000004]:
All ISs [0x09002B000005]:
All L1 ISs [0x0180C2000014]:
All L2 ISs [0x0180C2000015]:
```

Subred Frame Relay:

```
Interface number [0]:
Interface Type [FRL]:
```

Interface number
Enlaza la subred con la interfaz especificada.

Enable ES-IS
Indica si el protocolo ES-IS va a ejecutarse sobre la interfaz, sí (Y) o no (N).

Enable IS-IS
Indica si el protocolo IS-IS va a ejecutarse sobre la interfaz, sí (Y) o no (N).

Interface Type
Indica el tipo de subred: LAN, X.25 y Frame Relay (FRL). LAN incluye Ethernet y red en anillo.

Level 2 Only
Indica si la subred debe ejecutarse sólo en nivel 2, sí (Y) o no (N). Un no permitirá al direccionador direccionar sobre la subred en el nivel 1 y el 2.

External Domain
Indica si el circuito está funcionando fuera del dominio de direccionamiento IS-IS.

Default Metric
Indica el costo de la subred. El costo está en el rango incluido entre 20 y 63.

IS Hello Timer
Indica el período entre transmisiones de PDU de hello de IS.

ISIS Hello Timer
Indica el período de transmisiones de PDU de hello IS-IS de L1 y L2.

Modify Transmit password

Elimina o cambia una contraseña de transmisión de un circuito. Si selecciona yes (sí), esta opción le solicitará:

```
Delete or change the transmit password
[change]?
```

Modify the set of receive passwords

Elimina todo o añade una contraseña de recepción de circuito. Si selecciona yes (sí), esta opción le solicitará:

```
Delete all or add 1 receive password
[add]?
```

L1 Priority/L2 Priority

Indica la prioridad del direccionador para convertirse en el direccionador designado de la LAN.

All ESs Indica la dirección de difusión múltiple a usar cuando se transmitan hellos de IS. La dirección por omisión refleja la dirección de difusión múltiple de ethernet/802.3. Si está conectándose con una 802.5 LAN, use **C00000004000**.

All ISs Indica la dirección de difusión múltiple a usar cuando se reciban hellos de ES. La dirección por omisión refleja la dirección de difusión múltiple de ethernet/802.3. Si está conectándose con una 802.5 LAN, use **C00000008000**.

All L1 ISs

Indica la dirección de difusión múltiple a usar cuando se transmitan y reciban PDU IS-IS de L1. La dirección por omisión refleja la dirección de difusión múltiple de ethernet/802.3. Si está conectándose con una 802.5 LAN, use **C00000008000**.

All L2 ISs

Indica la dirección de difusión múltiple a usar cuando se transmitan y reciban PDU IS-IS de L2. La dirección por omisión refleja la dirección de difusión múltiple de ethernet/802.3. Si está conectándose con una 802.5 LAN, use **C00000008000**.

switches Activa y desactiva las opciones de OSI.

Ejemplo:

```
set switches
ES-IS Checksum Option [OFF]?
ES-IS Init Option [OFF]?
ISIS Authentication [OFF]?
```

IS-IS Checksum Option

Cuando esta opción está activada, el direccionador genera sumas de comprobación para todos los paquetes ES-IS de origen.

ES-IS Init Option

Cuando esta opción está activada, el direccionador envía un hello de IS directo a un vecino ES nuevo.

IS-IS Authentication

Si esta opción está activada, cada paquete IS-IS incluye la contraseña de transmisión configurada para el dominio, el área y los circuitos. Además, no se comprueba con las contraseñas de recepción.

timers Configura los temporizadores de OSI, excluyendo los temporizadores de circuito.

Ejemplo:

```
set timers
Complete SNP [10 sec]:
Partial SNP [2 sec]:
Minimum LSP Generation [30 sec]:
Maximum LSP Generation [900 sec]:
Minimum LSP Transmission [5 sec]:
Minimum Broadcast LSP Transmission [33 msec]:
Waiting Time [60 sec]:
Designated Router ISIS Hello [1 sec]:
Suggested ES Configuration Timer (sec) [10]:
```

Complete SNP
Selecciona el intervalo transcurrido entre la generación de PDU de número de secuencia completos (SNP) por el direccionador designado en un circuito de difusión.

Partial SNP
Selecciona el intervalo mínimo entre el envío de PDU de número de secuencia parciales (SNP).

Minimum LSP Generation
Selecciona el intervalo mínimo entre generaciones sucesivas de paquetes de estado de enlace (LSP) con el mismo ID de LSP generado por el direccionador.

Maximum LSP Generation
Selecciona el intervalo máximo entre LSP generados por el direccionador.

Minimum LSP Transmission
Selecciona el intervalo mínimo entre retransmisiones de un LSP.

Minimum Broadcast LSP Transmission
Selecciona la transmisión mínima, en milisegundos, entre la transmisión de LSP en un circuito de difusión.

Waiting Time
Selecciona la cantidad de segundos que debe retardarse el proceso de actualización en el estado de espera antes de entrar en el estado ON (activo).

Designated Router ISIS Hello
Selecciona el intervalo transcurrido entre la generación de PDU de hello IS-IS por parte del direccionador, si éste es el direccionador designado de una LAN.

Suggested ES Configuration Timer
Establece el campo de opción del mensaje hello de IS que instruye al ES que cambie el ritmo de envío de hellos de ES.

transmit-password

Establece o cambia una contraseña de transmisión.

Ejemplo:

```
set transmit-password
Password type [Domain]:
Password [ ]:
Reenter password:
```

Password type

Selecciona el tipo de contraseña: *dominio* o *área.*

Las contraseñas de dominio se usan con SNP y LSP de L2. Las contraseñas de área se usan con LSP L1 y SNP.

Password

Indica la serie de caracteres que se usa para autenticación. La serie de caracteres máxima permitida puede tener 16 caracteres.

virtual-circuit

Configura un SVC o PVC X.25 o un PVC Frame Relay.

Ejemplo:

```
set virtual-circuit
Interface Number [0]:
DTE Address[]:
Enable ISIS (Y or N) [Y]?
L2 only (Y or N) [N]?
External Domain (Y or N) [N]?
Default Metric [20]:;
ISIS Hello Timer [3 sec]?
Modify transmit password (y or n) [N]?
Modify the set of receive passwords [No]?
```

Interface Number

Indica la interfaz de X.25 o de Frame Relay sobre la que está configurado el circuito virtual.

DTE Address

Indica la dirección del DTE de destino para X.25 o el DLCI (identificador de control del enlace de datos) para Frame Relay. Esta dirección debe ser la misma que la definida para el circuito virtual en la configuración de X.25 o en la de Frame Relay.

Default Metric

Indica el costo del circuito.

Enable IS-IS

Indica si el protocolo IS-IS va a ejecutarse sobre la interfaz, sí (Y) o no (N).

L2 only Indica si el circuito debe ejecutarse sólo en el nivel 2, yes (Y) o no (N). Un no permitirá al direccionador direccionar en el nivel 1 y el nivel 2.

External Domain

Indica si el circuito está funcionando fuera del dominio de direccionamiento IS-IS.

Acceso al entorno de supervisión de OSI/DECnet V

Para obtener información sobre cómo acceder al entorno de supervisión de OSI/DECnet V, consulte *Getting Started (Introduction to the User Interface)* en el manual *Software User's Guide* (Guía del usuario del software).

Mandatos de supervisión de OSI/DECnet V

Esta sección describe los mandatos de supervisión de OSI/DECnet V. Use estos mandatos para reunir información de la base de datos.

Los mandatos de supervisión muestran o modifican la base de datos volátil.

Tabla 62 (Página 1 de 2). Resumen de los mandatos de supervisión de OSI/DECnet V

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 xxv.
Addresses	Muestra las direcciones de área y NET del direccionador.
Change Metric	Modifica el costo de un circuito.
CLNP-Stats	Muestra estadísticas OSI CLNP.
DNAV-info	Muestra el algoritmo de direccionamiento de nivel 1 y nivel 2 que actualmente está en vigor.
Designated-router	Muestra el direccionador designado de la LAN.
ES-adjacencies	Muestra todas las adyacencias de ES de la base de datos de adyacencias.
ES-IS-Stats	Muestra las estadísticas asociadas al protocolo ESIS.
IS-adjacencies	Muestra todas las adyacencias IS de la base de datos de adyacencias.
IS-IS-Stats	Muestra las estadísticas asociadas al protocolo ISIS.
L1-routes	Muestra todas las rutas de L1 de la base de datos de nivel 1.
L2-route	Muestra todas las rutas de L2 de la base de datos de nivel 2.
L1-summary	Muestra un resumen de la base de datos de enlaces de nivel 1.
L2-summary	Muestra un resumen de la base de datos de enlaces de nivel 2.
L1-update	Muestra la información contenida en el paquete de actualización de estado de enlace de L1.
L2-update	Muestra la información contenida en el paquete de actualización de estado de enlace de L2.
Ping-1139	Hace que el direccionador envíe una solicitud de eco a un destino y espere una respuesta.
Route	Muestra la ruta que sigue un paquete hasta un destino especificado.
Send echo packet	Codifica un mensaje de solicitud de eco en el paquete CLNP.

Tabla 62 (Página 2 de 2). Resumen de los mandatos de supervisión de OSI/DECnet V

Mandato	Función
Show routing circuits	Muestra el estado de los circuitos de direccionamiento definidos por el usuario para una interfaz especificada. Se aplica cuando el direccionador está configurado como un direccionador de estilo DEC.
Subnets	Muestra todas las subredes definidas por el usuario.
Toggle	Habilita o inhabilita la función de sustitución de alias NSAP.
Traceroute	Muestra la ruta que sigue un paquete hasta su destino.
Virtual-circuits	Muestra todos los circuitos virtuales definidos por el usuario. Se aplica cuando el direccionador está configurado como un direccionador de estilo IBM 2210.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxvi.

Addresses

Use el mandato **addresses** para establecer una lista de las direcciones de área y NET del direccionador que están configuradas.

Sintaxis:

a**ddresses**

Ejemplo:

```
addresses
Network Entity Title:
4700-0500-01  000-9310-04F0
Area Addresses:
4700-0500-01
4900-02
```

Network Entity Title
Identifica al direccionador. El NET está formado por una dirección de área y un ID de sistema.

Area Address
Indica las direcciones dentro del dominio de direccionamientos. El direccionador puede tener un máximo de tres direcciones de área configuradas al mismo tiempo.

Change Metric

Use el mandato **change metric** para modificar el costo de un circuito.

Sintaxis:

ch**ange metric**

Ejemplo:

```
change metric
Circuit [0]?
New Cost [0]?
```

Circuit Indica el número del circuito que desea cambiar.

New Cost
Indica el costo nuevo del circuito. Rango: De 1 a 63.

CLNP-Stats

Use el mandato **clnp-stats** para visualizar las estadísticas de OSI Connectionless Layer Network Protocol (CLNP).

Sintaxis:

c**lnp-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
IS0 unknown initial protocol ID                 0
Received error packet                           0
Received local data packet                      0
Sent error packet                               0
received echo packet - destination unknown      0
cannot send an echo packet, handler error       0
sent ECHO reply packet                          0
sent ECHO request packet                        0
received ECHO Request                           0
received ECHO reply                             0
Error PDU dropped - SP, MS or E/R flag set      0
```

Received incomplete packet
Indica que se ha recibido un fragmento de un paquete de datos que se ha reconocido como un paquete de datos ISO CLNP.

Received packet with bad NSAP length
Indica que se ha recibido un paquete de datos ISO CLNP con una longitud NSAP incorrecta.

Received packet with bad checksum
Indica que se ha recibido un paquete de datos ISO CLNP con una suma de comprobación errónea.

Received packet with bad version number
Indica que se ha recibido un paquete de datos ISO CLNP con un número de versión sin soporte o incorrecto.

Received packet with bad type
Indica que se ha recibido un paquete de datos ISO CLNP con un campo de tipo sin soporte o incorrecto.

Received packet with expired lifetime
Indica que se ha recibido un paquete de datos ISO CLNP con un tiempo de vida agotado.

Received packet with bad option
Indica que se ha recibido un paquete de datos ISO CLNP con un parámetro opcional erróneo.

Received packet with unknown destination
Indica que se ha recibido un paquete de datos ISO CLNP pero que no se ha podido direccionar. La tabla de direccionamientos no contiene una entrada para el destino.

Received packet with no segmentation permitted
Indica que se ha recibido un paquete de datos ISO CLNP que necesitaba segmentación. El distintivo de segmentación permitido no está establecido.

Received data packet cannot be forwarded
Indica que se ha recibido un paquete de datos ISO CLNP pero que no se ha podido direccionar debido a un error del manejador.

No buffer available to send error packet
Ha fallado un intento de enviar un paquete de error ISO CLNP debido a una falta de almacenamientos intermedios de E/S del sistema.

No route to send error packet
Ha fallado un intento de enviar un paquete de error ISO CLNP porque no se ha podido direccionar.

Received OK CLNP packet
Indica que se ha recibido un paquete de datos ISO CLNP y que éste ha pasado la comprobación de errores.

Cannot forward error packet
Indica que no se ha podido direccionar un paquete de error ISO CLNP debido a un error del manejador.

ISO unknown initial protocol ID
Indica que se ha recibido un paquete ISO CLNP con un identificador de protocolo inicial sin soporte o desconocido.

Received error packet
Indica que se ha recibido un paquete de error ISO CLNP para este direccionador.

Received local data packet
Indica que se ha recibido un paquete de datos ISO CLNP con un NSAP de destino que indica uno de los NSAP del direccionador.

Sent error packet
Indica que se ha enviado un paquete de error ISO CLNP al recibir un paquete anómalo.

Designated-router

Use el mandato **designated-router** para visualizar el direccionador designado para las subredes LAN que están conectadas físicamente a este direccionador y ejecutan activamente IS-IS.

Sintaxis:

de**signated-router**

Ejemplo:

```
designated-router
Designated Router Information:
Hdw   Int#   Circ       L1DR                L2DR
Eth/1  1      2         0000931004F002      0000931004F002
TKR/0  0      1         Elvis-01            Elvis-01
```

Hdw Indica el tipo e instancia de la LAN conectada a este direccionador.

Intnúm. Indica el número de la interfaz de este direccionador que establece una conexión con la LAN.

Circ Indica el número de circuito asignado por el direccionador. Este valor siempre es un número más que el número asignado a la interfaz para las subredes de la LAN.

L1DR Indica el ID de LAN del direccionador designado. Si está habilitado el uso de un alias, este mandato visualizará el alias del segmento en concreto. El ID de LAN es el ID del sistema del direccionador designado concatenado con un ID de circuito asignado localmente de 1 byte.

L2DR La descripción de este parámetro es la misma que para el parámetro L1DR anterior.

Nota: Si todavía no se ha elegido el direccionador designado, aparecerá “Not Elected” (Sin elegir) en vez de un ID de LAN.

DNAV-info

Use el mandato **dnav-info** para visualizar el algoritmo de direccionamiento que está ejecutándose actualmente en el direccionador.

Sintaxis:

dn**av-info**

Ejemplo:

```
dnav-info
DNA V Level 1 Routing Algorithm: Distance-vector
DNA V Level 2 Routing algorithm: Distance-vector
```

Nota: Según si DNA IV está habilitado o no, el algoritmo que aparezca aquí puede diferir de lo que se haya configurado en memoria con el mandato **set algorithm** en el indicador `config>` de OSI/DECnet V.

Si DNA IV está habilitado - el algoritmo de direccionamiento será el que esté configurado en memoria.

Si DNA IV está inhabilitado - el algoritmo de direccionamiento se establecerá en estado de enlace y puede ser diferente del que se haya establecido en memoria.

ES-Adjacencies

Use el mandato **es-adjacencies** para visualizar todas las adyacencias del sistema final (ES) que estén configuradas o se hayan sabido a través del protocolo ESIS.

Sintaxis:

es-ad**jacencies**

Ejemplo:

```
es-adjacencies
End System Adjacencies
System ID       MAC Address      Interface    Lifetime   Type
6666-6666-6666  1234-FEAA-041C       0        50         DNAIV
```

System ID
ID del sistema de la adyacencia ES.

MAC Address
Indica la dirección del MAC del ES de la subred.

Interface Indica el número de la interfaz del direccionador donde se tuvo conocimiento de la adyacencia ES.

Lifetime Indica el período de tiempo, en segundos, que el direccionador ha dejado antes de que se descarte la información recibida en el último mensaje ES Hello. En el caso de una ES-Adjacency (adyacencia ES) configurada estática o manualmente, este campo lee **Static**.

Type Indica el tipo de adyacencia ES, OSI DNAIV, DNAIV' y MANUAL para las adyacencias configuradas estáticamente.

ES-IS-Stats

Use el mandato **es-is-stats** para visualizar las estadísticas del protocolo ESIS.

Sintaxis:

es-is**-stats**

Ejemplo:

```
es-is-stats

ESIS input queue overflow                       0
Received incomplete packet                      0
Received packet with bad checksum               0
Received packet with bad version                0
Received packet with bad type                   0
No iob available to send hello                  0
Cannot send hello due to packet handler error   0
Sent hello                                      3672
Received packet with bad header                 0
Received hello with bad nsap                    0
Received hello packet with bad option           0
Received hello                                  0
Received hello with unsupported domain source   0
No resources to install route                   0
Received hello with conflicting route           0
Timed out route reactivated                     0
No resources to send redirect                   0
Redirect not sent - handler error               0
Sent redirect                                   0
Timed out route                                 0
Timed out route                                0
Unable to  allocate resources for a new ES adjacency 0
hello PDU dropped, received over point-to-point circ 0
ESIS hello PPDU dropped, no matching area address 0
dropped hello packet - manual ES adjacency exists 0
```

ESIS input queue overflow
El paquete ESIS se ha eliminado debido a que se ha desbordado una cola de entrada de tareas.

Received incomplete packet
Se ha recibido un fragmento de paquete reconocido como un paquete ESIS.

Received packet with bad checksum
Se ha recibido un paquete ESIS con una suma de comprobación errónea.

Received packet with bad version
Se ha recibido un paquete ESIS con una versión sin soporte o errónea.

Received packet with bad type
Se ha recibido un paquete ESIS con un campo de tipo sin soporte o erróneo.

No iob available to send hello
Ha fallado un intento de enviar un paquete hello de ESIS debido a una falta de almacenamientos intermedios de E/S del sistema.

Cannot send hello due to packet handler error
No se ha podido enviar un hello de ESIS debido a un error del manejador.

Sent hello
Se ha enviado un hello de ESIS a una interfaz.

Received packet with bad header
Se ha recibido un paquete hello de ESIS con un tiempo de retención o un campo recibido erróneo.

Received hello with nsap
Se ha recibido un paquete hello de ESIS con un NSAP erróneo o un NSAP que desborda el campo.

Received hello packet with bad option
Se ha recibido un paquete de datos ESIS CLNP con un parámetro de opción erróneo.

Received hello
Se ha recibido en la interfaz un paquete hello de ESIS.

Received hello with unsupported domain source
Se ha recibido un paquete hello de ESIS proveniente de una fuente de dominio sin especificar.

No resources to install route
Se ha recibido un paquete hello de ESIS, pero no había recursos para instalar el direccionador.

Received hello with conflicting route
Se ha recibido un paquete hello de ESIS, pero no se ha podido entrar en la base de datos. Una ruta dinámica o estática definida anteriormente en la base de datos entra en conflicto con la ruta del hello.

Timed out route reactivated
Se ha recibido un paquete hello de ESIS con una ruta con tiempo excedido previamente.

No resources to send redirect
No se ha podido enviar un paquete de redirección ESIS debido a falta de recursos.

Redirect not sent handler error
No se ha podido enviar un paquete de redirección ESIS debido a un error del manejador.

Sent redirect
Se ha enviado a la interfaz un paquete de redirección de ESIS.

Timed out route
Una ruta hello de ESIS ha excedido el tiempo.

Unable to allocate resources for a new ES adjacency
Se ha recibido un paquete hello de ES-IS pero el direccionador no tiene los recursos suficientes para establecer una adyacencia de ES con el nodo transmisor.

hello PDU dropped, received over point-to-point circ
Se ha eliminado un paquete hello de ES-IS debido a que el circuito implicado es un circuito de punto a punto.

ESIS hello PPDU dropped, no matching area address
Se ha eliminado un paquete hello de ES-IS debido a que el área no coincidía con la dirección de área del direccionador. El protocolo ES-IS sólo se aplica a un área.

dropped hello packet-manual ES adjacency exists.
Se ha eliminado un paquete hello de ES-IS debido a que existe una adyacencia de ES estática con el nodo transmisor.

IS-Adjacencies

Use el mandato **IS-adjacencies** para establecer una lista de todas las adyacencias IS de las que se tiene conocimiento a través del protocolo ISIS.

Sintaxis:

is-ad**jacencies**

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           OSI
0000-9310-04C8   AA00-0400-EF04   0     L2   L1/L2   DOWN         DNAIV
AA00-0400-0504   AA00-0400-0504   1     L2     L2     UP     5390    OSI
```

System ID
EL ID del sistema de la adyacencia IS.

MAC Address
Indica la dirección del MAC de la adyacencia IS.

Int Indica el número de la interfaz del direccionador que establece la conexión con la adyacencia IS.

Level En el caso de las LAN, este parámetro indica el nivel del sistema vecino a partir del tipo de mensaje hello, L1 o L2. Para punto a punto, indica sólo el tipo de sistema vecino L1, de lo contrario L2.

Usage Indica, a partir del tipo de circuito del paquete hello, sólo L1, sólo L2 o L1 y L2.

State Indica el estado operacional de la adyacencia IS, activa o inactiva.

Life Indica el período de tiempo, en segundos, que tiene que transcurrir para descartar el último mensaje hello de IS.

Type Indica el tipo de protocolo de direccionamiento de la adyacencia IS, OSI o DNA IV.

IS-IS-Stats

Use el mandato **is-is-stats** para visualizar la información asociada al protocolo ISIS.

Sintaxis:

is-is**-stats**

Ejemplo:

```
is-is-stats
Link State Database Information

no. of level 1 LSPs       1      no. of level 2 LSPs       0
no. of L1 Dijkstra runs   21     no. of L2 Dijkstra runs   0
no. of L1 LSPs deleted    0      no. of L2 LSPs deleted    0
no. of routing table entries allocated   6

Packet Information

level 1 lan hellos rcvd  0      level 1 lan hellos sent   10967
level 2 lan hellos rcvd  0      level 2 lan hellos sent   10967
pnt to pnt  hellos rcvd  0      pnt to pnt  hellos sent   0
level 1 LSPs rcvd        0      level 1 LSPs sent         40
level 2 LSPs rcvd        0      level 2 LSPs sent         0
level 1 CSNPs rcvd       0      level 1 CSNPs sent        0
level 2 CSNPs rcvd       0      level 2 CSNPs sent        0
level 1 PSNPs rcvd       0      level 1 PSNPs sent        0
level 2 PSNPs rcvd       0      level 2 PSNPs sent        0
```

no. of level 1/level 2 LSPs
Indica el número de paquetes de estado de enlace L1 y L2 que hay en la base de datos.

no. of L1/L2 Dijkstra runs
Indica el número de veces que el direccionador calculó las tablas de direccionamientos L1 y L2.

no. of L1/L2 LSPs deleted
Indica el número de paquetes de estado de enlace L1 y L2 que se suprimieron de la base de datos.

no. of routing table entries allocated
Indica el número de entradas que contiene actualmente la tabla de direccionamientos.

level 1/level 2 lan hellos rcvd
Indica el número de hellos de LAN que el direccionador ha recibido.

level 1/level 2 hellos sent
Indica el número de hellos de LAN que el direccionador ha enviado.

pnt to pnt hellos rcvd
Indica el número de hellos de punto a punto que el direccionador ha recibido.

pnt to pnt hellos sent
Indica el número de hellos de punto a punto que el direccionador ha enviado.

level 1/level 2 LSPs rcvd
Indica el número de paquetes de estado de enlace (LSP) L1 y L2 que el direccionador ha recibido.

level 1/level 2 LSPs sent
Indica el número de LSP L1 y L2 que el direccionador ha enviado.

level 1/level 2 CSNPs rcvd
Indica el número de PDU de número de secuencia completa (CSNP) L1 y L2 que ha recibido el direccionador.

level 1/level 2 CSNPs sent
Indica el número de CSNP L1 y L2 que el direccionador ha enviado.

level 1/level 2 PSNPs rcvd
Indica el número de PDU de número de secuencia parcial L1 y L2 (PSNP) que ha recibido el direccionador.

level 1/level 2 PSNPs sent
Indica el número de PSNP L1 y L2 que el direccionador ha enviado.

L1-Routes

Use el mandato **l1-routes** para visualizar todas las rutas de nivel 1 que están en la base de direccionamientos L1.

Sintaxis:

l1-r**outes**

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 costo de esta ruta.

Source Indica uno de los tres orígenes donde el direccionador tuvo conocimiento de la ruta: LOCAREA, ESIS o ISIS.

Next Hop Indica el salto siguiente que daría un paquete en su ruta. Una designación efectuada con un asterisco (*) se refiere al mismo direccionador como el destino del paquete. Una dirección con un número de interfaz es la dirección del MAC de un ES conectado directamente o la dirección del DTE si el salto siguiente es una conmutación X.25 o un DLCI si el salto siguiente es una conmutación Frame Relay. Un ID de sistema (34555372215) se refiere al salto siguiente hacia el destino.

L2-Routes

Use el mandato **l2-routes** para visualizar todas las rutas de nivel 2 de la base de datos de L2.

Sintaxis:

l2-r**outes**

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 la dirección a alcanzar.

Cost Indica el costo de esta ruta.

Type Indica los cuatro tipos de rutas: área-LOC (local), prefijo-LOC, área, prefijo/I y prefijo/E. Área-LOC es un área conectada directamente; un prefijo-LOC es un prefijo que anuncia este direccionador; prefijo/I y prefijo/E son rutas que requieren otro salto para alcanzar su destino.

Next Hop Indica el salto siguiente que daría un paquete en su ruta. Una designación * o una designación directa, se refiere a un sistema principal conectado directamente fuera del direccionador. Un ID del sistema se refiere al siguiente direccionador por el que deberá pasar un paquete para alcanzar su destino.

L1-Summary

Use el mandato **l1-summary** para mostrar un resumen de la base de datos de estados de enlaces de nivel 1.

Sintaxis:

l1-s**ummary**

Ejemplo:

```
l1-summary
Link State Database Summary - Level One

LSP ID               Lifetime   Sequence #   Checksum   Flags   Cost
0000-9300-40B0-0000    0           0            0        0     1024
0000-93E0-107A-0000    384         CE           3CC9     1     0
AA00-0400-0504-0000    298         8E           40F1     B     20
AA00-0400-0504-0100    4           B8           A812     3     20

Total Checksum 25CC
```

LSP ID Representa el ID del sistema de origen de la PDU del estado de enlace más dos bytes adicionales. El primer byte adicional designa el tipo de actualización. 00 representa una actualización que no es un pseudonodo. 01–FF representa una actualización de pseudonodo para el número del circuito. El segundo byte representa el número de LSP. Este número se asigna al paquete cuando los datos están contenidos en más de un paquete.

Lifetime Indica el período de tiempo, en segundos, durante el cual el direccionador mantendrá el LSP.

Sequence #
Indica el número de secuencia del LSP.

Checksum
Indica el valor de la suma de comprobación del LSP.

Flags Indica un valor de un octeto que refleja el campo del distintivo del LSP. Los ocho bits se desglosan como indicamos a continuación:

Bit 8 Indica el distintivo P. Cuando está establecido (1), el IS de emisión da soporte a la función Partition Repair (reparación de partición) opcional.

Bits 7-4 Indica el distintivo ATT. Cuando está establecido (1), el IS de emisión está conectado a otras áreas con una de las opciones siguientes: Default Metric (Métrica por omisión) (bit 4), Delay Metric (Métrica de retardo) (bit 5), Expense Metric (Métrica de gastos) (bit 6) o Error Metric (Métrica de errores) (bit 7).

Bit 3 Indica el distintivo LSPDBOL. Cuando está establecido (1), se ha producido una sobrecarga de la base de datos de LSP. El proceso de decisión no usará el LSP que tenga este bit establecido para calcular rutas a otro l a través del sistema de origen.

Bits 2-1 Indica el distintivo del tipo de IS. Cuando se establece en los valores siguientes, designa el tipo de direccionador IS, nivel 1 o nivel 2.

Valor	Descripción
0	Sin usar.
1	Bit 1 establecido. IS de nivel 1.
2	Sin usar.
3	Bits 1 y 2 establecidos. IS de nivel 2.

Cost Indica el costo de direccionar a dicho vecino.

L2-Summary

Use el mandato **l2-summary** para visualizar un resumen de la base de datos de estados de enlace de nivel 2.

Sintaxis:

l2-s**ummary**

Ejemplo:

```
l2-summary
Link State Database Summary - Level Two

LSP ID               Lifetime   Sequence #   Checksum   Flags   Cost
0000-9310-04F0-0000      33E     12             EF19       3       0
0000-5000-FB06-0000      455      4             2BB1       3      20
0000-5000-FB06-0100      469     12             DE32       3      20

Total Checksum 0
```

La descripción de la producción de L2-summary es la misma que la del mandato l1-summary.

L1-Update

Use el mandato **l1-update** para visualizar una actualización del estado de enlace para el IS de nivel 1 especificado.

Sintaxis:

l1-u**pdate**

Ejemplo:

```
l1-update
LSP ID []? 0000931004F0000

Link State Update For ID 0000931004F00000

Area Addresses

470005001

Intermediate System Neighbors     Metric      Two Way

0000931004F002                      20           N
0000931004F001                      20           Y

End System Neighbors              Metric

00009310004F0                       *
```

LSP ID Indica el ID del sistema de origen de la PDU del estado de enlace más dos bytes adicionales. El primer byte designa el tipo de actualización. 00 representa una actualización que no es pseudonodo. 01–FF representa una actualización de pseudonodo. El segundo byte representa el número de LSP. Este número se asigna al paquete cuando los datos están contenidos en más de un paquete.

Area Addresses
Indica las direcciones del área donde este direccionador está configurado para direccionar paquetes.

Intermediate System Neighbors
Indica los IS vecinos adyacentes.

Metric Indica el costo del IS vecino.

Two Way Indica si el direccionador recibe actualizaciones del vecino.

End System Neighbors
Indica los ES conectados directamente.

L2-Update

Use el mandato l2-update para visualizar la actualización del estado del enlace para el IS de nivel 2 especificado.

Sintaxis:

l2-u**pdate**

Ejemplo:

```
l2-update
LSP ID []? 0000931004F0000

Link State Update For ID 0000931004F00000

INTERMEDIATE SYSTEM NEIGHBORS    METRIC   TWO WAY
   0000931004F002                  20        N
   0000931004F001                  20        N
   55002000182000                  20        N
```

Intermediate System Neighbors
Indica otros IS conectados directamente.

Metric Indica el costo hasta el IS.

Two Way Indica si el direccionador recibe actualizaciones del vecino.

Ping-1139

Hace que el direccionador envíe una solicitud de eco a un destino y espere una respuesta, tal como se recomienda en RFC 1139. RFC 1139 especifica que esto es una función de OSI y no de DECnet. **Ping-1139** da soporte a ecos de corto y largo plazo. Los ecos de corto plazo usan paquetes de datos CLNP normales, lo que los convierte en transparentes para los sistemas intermedios que no dan soporte a RFC1139. Los ecos de largo plazo usan paquetes de solicitud/respuesta PING.

La longitud de los datos por omisión del paquete de solicitud de eco es de 16 bytes. Puede establecer la longitud de los datos hasta un máximo de 64 bytes.

Cuando entre el mandato **ping-1139**, las solicitudes de eco se enviarán continuamente hasta que pulse cualquier tecla. En ese momento, se visualizarán estadísticas en las que se verá el número de solicitudes transmitidas y el de respuestas recibidas.

Sintaxis:

ping-1139

Ejemplo:

```
ping-1139
Long-term/Short-term [LONG-TERM]?
Destination NSAP:  []? AA0003000A14
Data Length [16]?

PINGing AA0003000A14

---- PING Statistics ----
 8 requests transmitted, 8 replies received
```

Route

Use el mandato **route** para visualizar el salto siguiente del paquete a un destino especificado (destnsap).

Sintaxis:

route *dest-nsap*

Ejemplo:

```
route 490002aa0004000e08
Destination System: 0000-9310-04C9
Destination MAC Address: AA00-0400-1408
Interface: 0
```

Destination System
Indica el ID del sistema del IS del salto siguiente. En el caso de un ES conectado directamente, este valor estará en blanco.

Destination MAC Address
Indica la dirección del MAC del IS del salto siguiente o el ES conectado directamente.

Interface Indica la interfaz que atravesará un paquete para llegar al IS del salto siguiente o al ES conectado directamente.

Send (Echo Packet)

Use el mandato **send echo packet** para codificar un mensaje de solicitud de eco en el paquete CLNP al nsap de destino especificado. Durante este mandato, el sistema no interactúa con la supervisión de OSI. Para verificar que se envió la solicitud de eco y que se recibió una respuesta de eco, compruebe el ELS (Sistema de anotación cronológica de sucesos).

Nota: No puede enviarse a sí mismo un paquete eco. Si lo intenta, recibirá un mensaje CLNP.004 ELS.

Sintaxis:

se**nd**

Ejemplo:

```
send
Destination NSAP: []?
```

Subnets

Use el mandato **subnets** para visualizar información sobre todas las subredes operacionales. Las subredes desactivadas o inhabilitadas no estarán en la lista.

Sintaxis:

su**bnets**

Ejemplo:

```
subnets
L2
 Hdw   Int #  Circ  Only  ES-IS IS-IS  L1DR  L1Pri  L2DR   L2pri  Cost   Ext
 PPP/2 2       3     N     N     Y
 Eth/0 0       1     N     Y     Y      Y     64    N      64     20    N
```

Hdw El tipo e instancia de la red que conecta con la subred.

Int # El número de interfaz del direccionador que establece la conexión con la subred.

Circ El ID asignado al circuito para el protocolo ISIS.

L2 only Indica si este direccionador es sólo de nivel 2, Y (sí) o N (no).

ES-IS El protocolo ES-IS está habilitado en la subred, Y o N.

IS-IS El protocolo IS-IS está habilitado en la subred, Y o N.

L1DR Este direccionador es el direccionador designado de nivel 1 para esta subred, Y o N.

L1Pri La prioridad de nivel 1 de la subred de LAN para convertirse en el direccionador designado.

L2DR Este direccionador es el direccionador designado de nivel 2 para esta subred, Y o N.

L2Pri La prioridad de nivel 2 de la subred para convertirse en el direccionador designado.

Cost El costo del circuito.

Ext Indica si la subred trabaja fuera del dominio de direccionamiento IS-IS (externo).

Toggle (Alias/No Alias)

Use el mandato **toggle** alias/no alias para habilitar o inhabilitar la función de visualización del alias del NSAP para el protocolo OSI.

Sintaxis:

t**oggle**

Ejemplo:

```
toggle
Alias substitution is ON
```

Traceroute

Use el mandato **traceroute** para rastrear la vía de acceso que sigue un paquete OSI hasta un destino.

Nota: No puede ejecutar un mandato traceroute hacia sí mismo, de lo contrario recibirá el mensaje de error siguiente:

```
Sorry, can't traceroute to this router. (No se
puede ejecutar un traceroute a este direccionador).
```

Sintaxis:

tr**aceroute** *dirección*

Ejemplo:

```
traceroute 490002aa0004000e08
Successful trace:

TRACEROUTE 470007: 56 databytes

1          490002aa0004000e08      32ms       5ms       5ms

Destination unreachable response:

Destination unreachable

No response:

1 * * *
2 * * *
```

TRACEROUTE
Muestra la dirección del área de destino y el tamaño del paquete que se envía a dicha dirección.

1 El primer rastreo que muestra el NSAP de destino y el tiempo que ha sido necesario para que el paquete llegase a su destino. El paquete se rastrea tres veces.

Destination unreachable
Indica que no hay ninguna ruta disponible al destino.

1 * * *

2 * * * Indica que el direccionador está esperando algún tipo de respuesta del destino, pero que éste no responde. El direccionador esperará 32 saltos antes de considerar la condición de tiempo excedido. Vaya al ELS y active los mensajes OSI CLNP para determinar por qué el sistema principal no responde.

Utilización de NHRP

Este capítulo describe cómo usar:

- Next Hop Resolution Protocol (NHRP) tal como se especifica en el Internet Draft Version 13, que se ha presentado para obtener el estado de RFC.

Visión general de Next Hop Resolution Protocol (NHRP)

Next Hop Resolution Protocol (NHRP) define un método para que una estación de origen determine la dirección de acceso múltiple sin difusión (NBMA) del “salto siguiente” hacia el destino. El siguiente salto NBMA puede ser el mismo destino o el direccionador de salida de la red NBMA “más cercana” a la estación de destino. Esta información del “salto siguiente” se llama ruta de atajo (“cut-through”) o VC en la especificación NHRP; el direccionador usa el término “shortcut” en vez de “cut-through”. La estación de origen puede establecer el circuito virtual NBMA directamente con el destino o el direccionador de salida y reducir el número de saltos en la red.

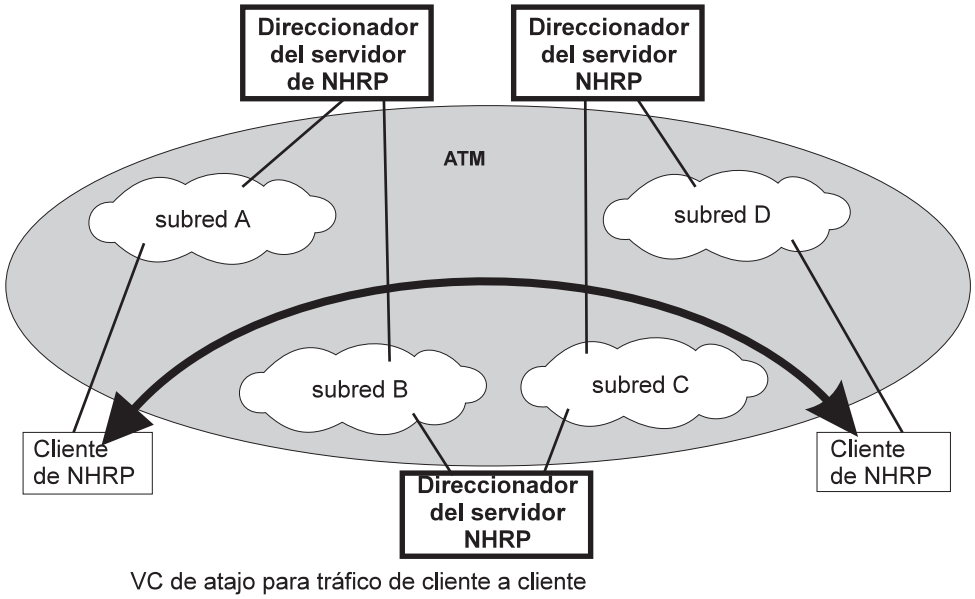


Figura 27. Visión general de Next Hop Resolution Protocol (NHRP)

El 2210 puede usar NHRP para establecer atajos para tráfico IP sobre la red ATM NBMA para interfaces RFC 1483 y Emulated LAN (ELAN). El borrador de Internet no trata el uso de NHRP en el entorno ELAN, pero el 2210 incluye mejoras para permitir usar LAN. Estas mejoras se implementan actualmente usando las extensiones propias de cada proveedor incluidas en la definición del protocolo NHRP.

El borrador de NHRP describe el flujo de protocolo básico como sigue: los clientes de NHRP registran sus direcciones de protocolo y las direcciones de NBMA en uno o varios servidores de NHRP. Por lo general, los servidores son direccionadores de la vía de acceso direccionada a través de la red NBMA a los clientes. Cuando un cliente desea establecer un atajo a un destino, envía un paquete Next Hop Resolution Request (Solicitud de resolución de salto siguiente) por la vía de acceso direccionada. La solicitud incluye la dirección del protocolo de destino. Los

direccionadores (que también son servidores de NHRP) situados en la vía de acceso direccionada comprueban si la dirección del protocolo de destino es una dirección a la que pueden servir.

Si el direccionador puede satisfacer la solicitud, devolverá una Next Hop Resolution Reply (Respuesta de resolución del salto siguiente) con la dirección NBMA de la estación de destino. El originador podrá entonces establecer un circuito virtual directo con el destino. Si no puede satisfacer esta solicitud, el direccionador la reenviará al direccionador del salto siguiente. Este reenvío proseguirá hasta que se satisfaga la solicitud o se determine que no se puede acceder al destino.

Para utilizar terminología de cliente/servidor, un dispositivo puede ser al mismo tiempo cliente y servidor. Cliente es el dispositivo que origina Next Hop Resolution Requests y servidor el que proporciona Next Hop Resolution Replies con información de la dirección NBMA. El 2210 es un dispositivo de este estilo; el cliente se "registra" conceptualmente en la función del servidor en la misma máquina, aunque en realidad no fluye ninguna Registration Requests (Solicitud de registro). El servidor también da soporte a registros NHRP de clientes de NHRP remotos.

La información que proporcionan los clientes a su servidor y los servidores a los peticionarios, debe renovarse periódicamente y puede depurarse si así lo dictan las condiciones. Clientes y servidores mantienen antememorias de información de resolución que han enviado y recibido; se usan períodos de tiempo de retención para asignar una edad a las entradas o ejecutar renovaciones.

Beneficios de la implementación de IBM y NHRP

Por lo general, el uso de atajos de NHRP puede:

- Mejorar el rendimiento de extremo a extremo eliminando saltos entre direccionadores cuando el origen y el destino están en la misma red NBMA y pueden comunicarse directamente.
- Reducir la carga de los direccionadores de red, ya que estos no tratan tráfico que, sin NHRP tendrían que manejar. Esto puede reducir los costos generales ya que son necesarios menos direccionadores o menos anchura de banda.

La implementación ejecutada por IBM de NHRP proporciona los beneficios adicionales siguientes:

- El borrador de NHRP no trata el uso de protocolos en un entorno Emulated LAN. No obstante, la implementación ejecutada por IBM de NHRP incluye consideraciones para tales tipos de entornos; los paquetes de NHRP pueden fluir entre direccionadores sobre conexiones ELAN y pueden establecerse VC de atajo.
- Direccionamiento de un salto: los dispositivos ATM que no dan soporte a NHRP pueden ser el destino de los atajos, eliminando otro salto de direccionador para el tráfico, al ampliar la definición de los dispositivos que reciben "servicios" para incluir atajos que comparten una subred de protocolo con el servidor. Por ejemplo, todas las direcciones IP de una subred classical IP de la cual forma parte un servidor, reciben "servicios" del mencionado servidor. La función NHRP actúa de interfaz con los componentes classical IP 1577 y LAN Emulation para usar las posibilidades de resolución de dirección ATM y aplicarlas a las solicitudes de NHRP. Esta mejora puede incluso usarse para el tráfico con los dispositivos conectados a LAN de legado que se conectan a ATM mediante conmutadores de LAN; el servidor de NHRP en el

direccionador responde al cliente con información de direccionamiento ATM para el conmutador de la LAN, lo que permite al cliente ir directamente por atajo a dicho conmutador. Para consultar ejemplos de estos casos de "direccionamiento de un salto", consulte la Figura 27 en la página 367 y la Figura 28 en la página 370

Nota: Un salto es una operación efectuada por un direccionador tradicional cuando reenvía paquetes de una subred a otra. En particular, dichas operaciones están (1) efectuando una búsqueda en un identificador de subred de la capa 3 (2) determinando el "salto siguiente" de salida del paquete (3) desmantelando y sustituyendo la cabecera de paquete de la capa 2, eliminando información de enlace de ingreso y añadiendo información de enlace de salida. Por lo tanto, en el caso del direccionamiento de "un salto", esta operación se produce una vez durante la transferencia de un paquete desde su origen a su destino.

- La implementación de IBM puede funcionar en redes donde algunos direccionadores no den soporte a NHRP. Si el direccionador de salto siguiente no puede dar soporte a NHRP, puede establecerse un VC de atajo hacia el "último" servidor de la vía de acceso. Consulte "atajos de direccionador a direccionador no permitidos" en la página 379 y "Listas de exclusiones" en la página 377.
- El cliente puede configurar el 2210 para que establezca atajos sólo cuando el tráfico a un destino sea superior a un ritmo de datos determinado. Esto puede eliminar la creación de VC para tráfico de bajo volumen o de una vez (por ejemplo, detecciones de condiciones de excepción de SNMP). Consulte el "parámetro data-rate" en la página 391 y el "parámetro attempt shortcuts?" en la página 390.
- El direccionador proporciona soluciones para el efecto "dominó" que se describe en el borrador de NHRP. Consulte el "parámetro attempt shortcuts?" en la página 390.
- Todos los direccionadores conectados a ATM de la vía de acceso direccionada deben dar soporte a NHRP para obtener beneficios óptimos, aunque 2210 puede seguir funcionando y proporcionando atajos en una red mixta.

Características de rendimiento

NHRP se usa durante el contacto inicial de un dispositivo de origen con un destino. Una vez se haya establecido un VC de atajo, NHRP ya no participará en la transferencia real de los datos. Las salvaguardas aseguran que el tráfico NHRP no se vuelva a intentar para cada paquete. Asimismo, la implementación que efectúa IBM proporciona una opción para que los atajos de NHRP sólo se soliciten cuando el tráfico para un destino determinado supere un umbral de velocidad de datos configurable. Esto puede evitar, por ejemplo, el establecimiento de circuitos virtuales que sólo se usen para una trama de detección de condición de excepción SNMP generada por un sistema principal IP.

El funcionamiento de NHRP no influye en el rendimiento de la vía de acceso rápida del direccionador y no influirá significativamente en la vía lenta. Cuando hay atajos disponibles, el rendimiento mejora eliminando los saltos extraños sobre la red ATM. Además, el rendimiento de los direccionadores intermedios eludidos por los atajos de NHRP mejora, ya que estos direccionadores manejan menos tráfico.

Nota: Si una configuración no incluye una interfaz 1577 (es decir, sólo se configura el direccionador para ELAN), sólo podrán establecerse VC de atajo

para el direccionador desde clientes que den soporte a las extensiones de IBM. Esta limitación puede evitarse definiendo simplemente una interfaz 1577 en el direccionador.

Ejemplos de configuraciones de NHRP

Los párrafos siguientes presentan ejemplos de configuraciones de NHRP.

NHRP en un entorno RFC 1577 Classic IP con todos los dispositivos capacitados para NHRP

En esta imagen, los clientes de NHRP usan conexiones RFC 1577 para comunicarse con el direccionador. Usan protocolo NHRP para informarse en el servidor de NHRP sobre sus respectivas direcciones ATM. A continuación, establecer un circuito virtual directo entre sí para el tráfico IP.

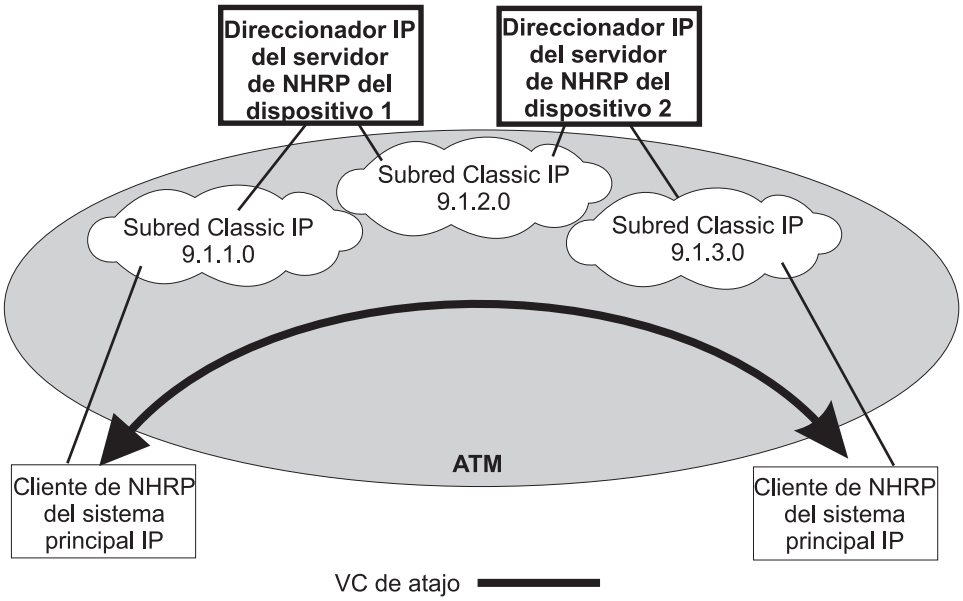


Figura 28. NHRP en un entorno Classic IP

NHRP en un entorno Classic IP con dispositivos no capacitados para NHRP

Este ejemplo muestra cómo puede usarse NHRP entre dos dispositivos 1577 cuando uno de ellos no da soporte a NHRP. En este caso, el dispositivo 2 proporciona al cliente de NHRP la dirección ATM del dispositivo no capacitado para NHRP y el cliente puede establecer un atajo para el tráfico destinado al sistema principal no capacitado para NHRP. No obstante, cuando el tráfico fluye del dispositivo no capacitado para NHRP, lo hace en la vía de acceso direccionada al dispositivo 2; a continuación, este dispositivo actúa como un cliente de NHRP y establece un atajo al destino.

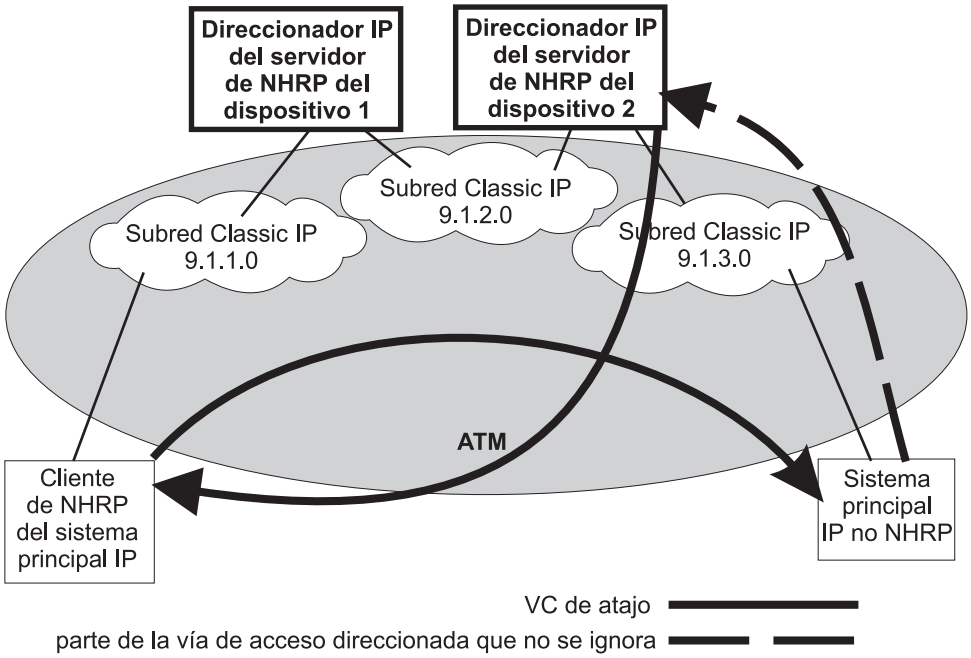


Figura 29. NHRP en un entorno Classic IP con dispositivos no capacitados para NHRP

NHRP en un entorno de LAN Emulation puro

En el caso de la emulación de LAN, los direccionadores usan las extensiones de IBM para proporcionar información de NBMA para dispositivos en las ELAN. Cuando el dispositivo 1 recibe tráfico del sistema principal A destinado al sistema principal B, origina una Next Hop Resolution Request y la envía por la vía de acceso direccionada. El dispositivo 2 responde a la solicitud con información de NBMA sobre el sistema principal B, una de las estaciones a la que sirve ya que están en la misma ELAN. A continuación, el dispositivo 1 establece un VCC directo de datos al sistema principal B incluso aunque éste no participe o dé soporte a los intercambios de NHRP. Tenga en cuenta que este VCC sólo se usará para el tráfico cuya dirección sea de A a B. Asimismo, cuando el sistema principal B envíe tráfico al sistema principal A, el dispositivo 2 generará una Next Hop Resolution Request, el dispositivo 1 responderá con información de direccionamiento sobre el sistema principal A y el dispositivo 2 establecerá un VCC directo de datos a A para el tráfico que vaya de B a A.

Los LEC de este ejemplo son dispositivos que cumplen el estándar sin soporte de NHRP. Deben satisfacer los requisitos de LEC descritos en “Implementación de NHRP” en la página 374.

No debe configurarse nada en especial en estos dispositivos o en los servidores de NHRP. El tráfico de NHRP fluye sobre la subred ELAN sin VC adicionales.

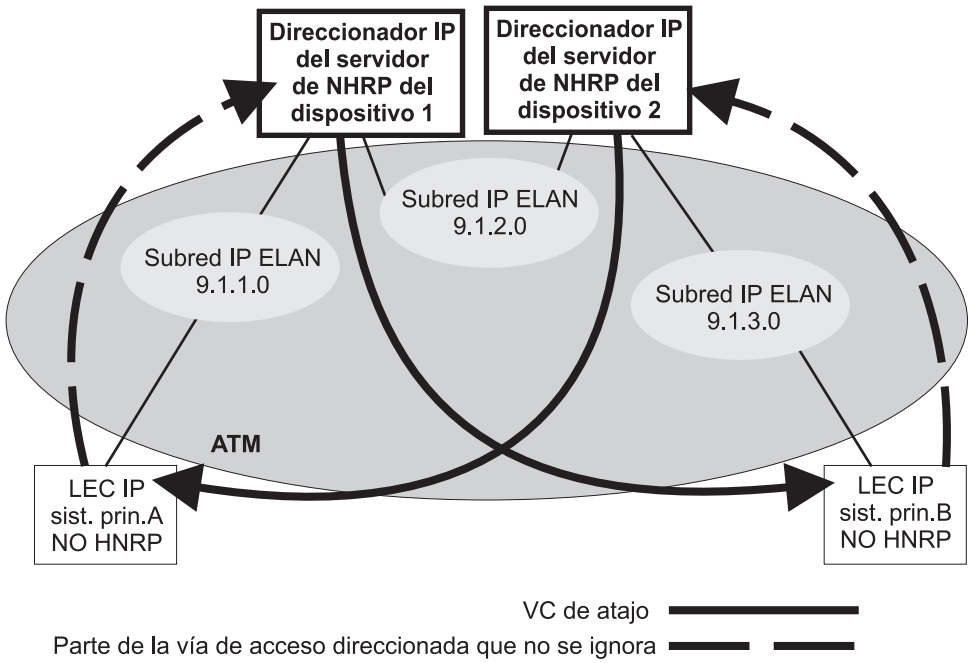


Figura 30. NHRP en un entorno ELAN

NHRP en un entorno de LAN Emulation con conmutadores de LAN

En este ejemplo, las estaciones de origen y de destino están conectadas a LAN legales y no están conectadas a la red ATM. Los conmutadores de LAN que funcionan como clientes de LAN Emulation dan conectividad ATM a los dispositivos LAN legales. Las mejoras efectuadas a NHRP y las extensiones de IBM permiten el mismo tipo de “direccionamiento de un salto” en este entorno que el descrito en el ejemplo anterior. Gracias a las mejoras, los servidores intercambian las direcciones MAC reales y la información de direccionamiento de los dispositivos LAN legales. A continuación, los 2210 pueden establecer VCC directos de datos con los conmutadores y pasar el tráfico directamente. En la vía de acceso sólo hay un “salto” de direccionador, aunque el tráfico pase a través de dos conmutadores de LAN.

Este ejemplo también ilustra que el entorno ELAN puede ser de red en anillo o Ethernet o cualquier mezcla de tipos de LAN.

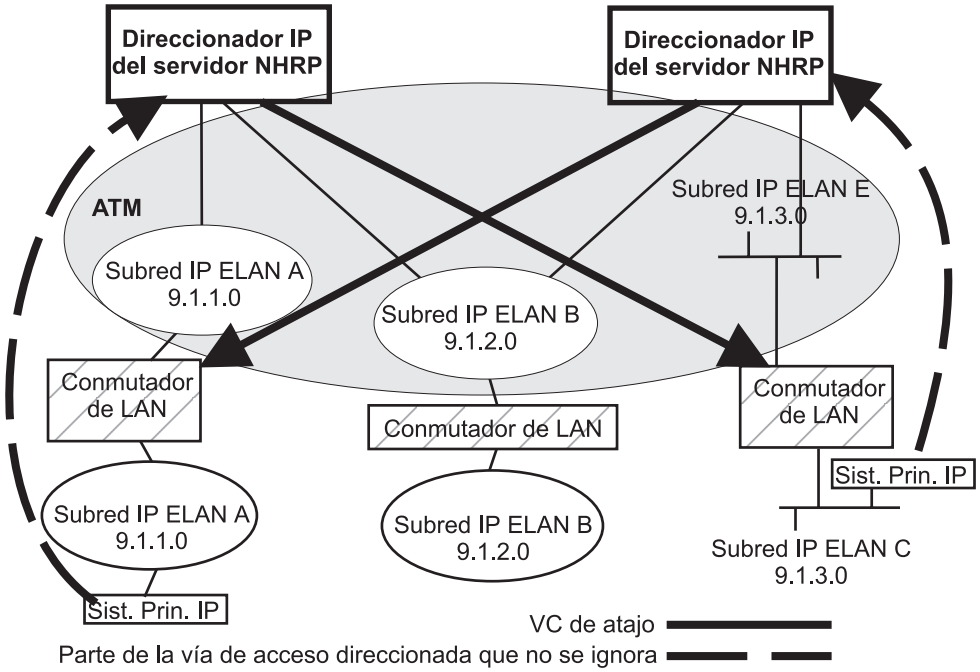


Figura 31. NHRP en un entorno ELAN con conmutadores de LAN

NHRP en un entorno ELAN o classical IP mixto

La función NHRP en el direccionador puede funcionar con interfaces Classic IP y ELAN en la misma red. En este ejemplo, el cliente de NHRP da soporte a las extensiones de IBM y puede atajar directamente al destino LEC en el caso del tráfico que siga dicha dirección.

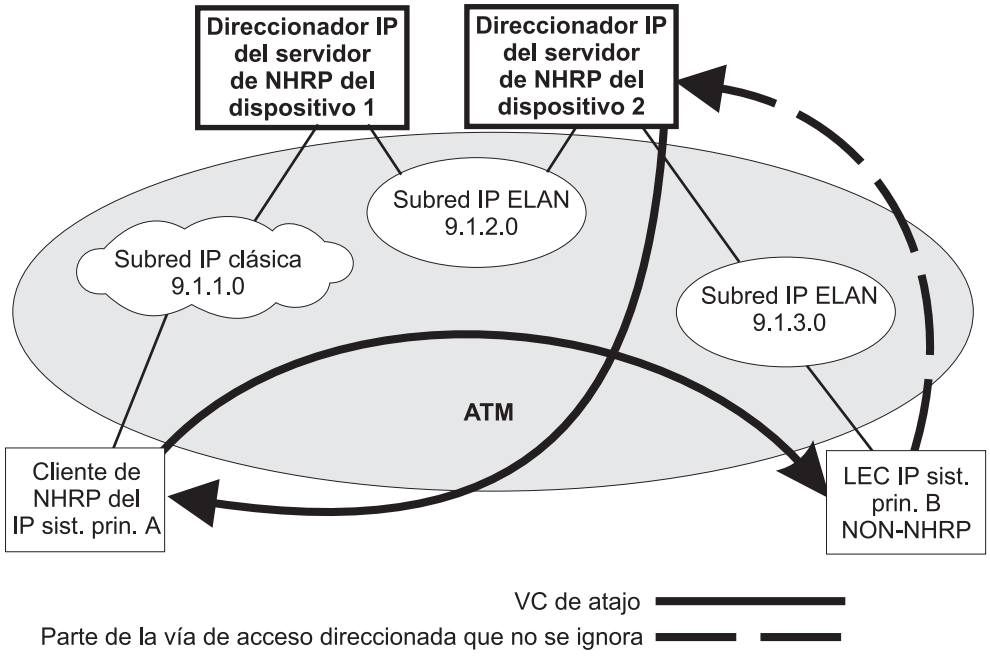


Figura 32. NHRP en un entorno ELAN o classical IP mixto

NHRP a un direccionador de salida

No es necesario que las estaciones de origen o las de destino del tráfico de protocolo pertenezcan a subredes servidas por participantes de NHRP. Pueden acceder a la red ATM a través de direccionadores que se comuniquen con los dispositivos NHRP. En dicho caso, 2210 proporciona atajos a través de la red ATM para eliminar la mayor cantidad posible de saltos.

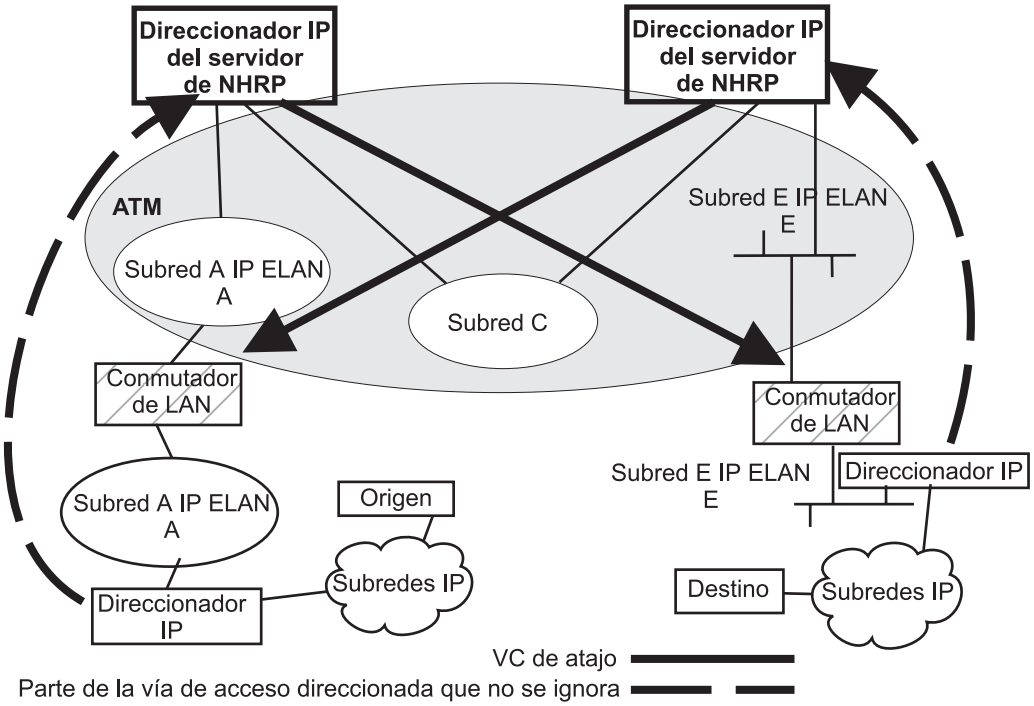


Figura 33. NHRP a un direccionador de salida

Implementación de NHRP

NHRP interactúa con la función de direccionador del direccionador. Cuando esta función está reenviando paquetes por la vía de acceso direccionada y NHRP obtiene satisfactoriamente un VC de atajo, NHRP actualizará la función de direccionador para enviar el paquete directamente por el VC de atajo.

NHRP actualiza la tabla de reenvíos de la función de direccionamiento después de que se active el VC. Esto permite que se produzca la conmutación de la vía de acceso direccionada a la vía de acceso de atajo, sin que se produzcan pérdidas de paquetes.

Cuando se usa un atajo de NHRP, el direccionador transmite tramas a una dirección de salto siguiente de una subred a la que el mismo direccionador no pertenece. Por ello, el NET o interfaz que proporciona la vía de acceso de salida al tráfico se llama “virtual” network interfaz (interfaz de red virtual).

Virtual Network Interface (VNI)

Por lo general, el flujo de paquetes de salida de un direccionador tiene las restricciones siguientes:

- Incapacidad de enviar paquetes directamente a direcciones de red que no estén definidas en una interfaz de red.
- Incapacidad de enviar paquetes a tipos de red (por ejemplo, ELAN de red en anillo) a menos que dicho tipo de red esté definido en una interfaz de red.

El manejador de red Virtual Network Interface (VNI) elimina estas restricciones, lo que permite al direccionador reenviar paquetes directamente a saltos siguientes obtenidos a través de NHRP (rutas atajo). Permite el direccionamiento de un salto, en el que las rutas de atajo de NHRP pueden establecerse directamente con dispositivos que no dan soporte a NHRP.

VNI da soporte a interfaces de red de redes en anillo, Ethernet V2 y Ethernet DIX ELAN e interfaces de red classic IP. Cuando la vía de acceso de salida va a usar una interfaz classic IP (1577), la implementación utilizará, en realidad, la interfaz del manejador de red 1577 para VNI existente. No obstante, cuando esta vía de acceso deba utilizar un atajo LANE, accederá a una interfaz única. Esto recibe el nombre de Interfaz de atajos LANE (LSI). LSI es diferente de la interfaz LEC tradicional ya que proporciona más de un tipo de encapsulación de LAN; es decir, puede establecerse un VC usando la encapsulación de red en anillo mientras que otro usa Ethernet V2. Además, LSI proporciona conexiones a más de una Emulated LAN, mientras que una interfaz LEC tradicional se conecta únicamente con una ELAN.

Cuando habilita NHRP, se crea una LSI por cada adaptador ATM. A esta LSI se le asigna el número de interfaz disponible siguiente y se listará cuando invoque funciones de consola que muestren información sobre las interfaces del direccionador.

Interfaz de atajos LANE (LSI)

Los atajos LANE proporcionados por las extensiones IBM a NHRP no son compatibles con algunas implementaciones en pila de protocolos de estación final y de LAN Emulation Client (LEC). En esta sección describimos cómo pueden surgir estas incompatibilidades y, en algunos casos, cómo pueden superarse usando opciones de configuración.

Los LEC paranoides son dispositivos que usan el LAN Emulation Flush Protocol para verificar que los clientes que establezcan VCC directos de datos con ellos sean miembros de su ELAN. Estos dispositivos no funcionarán con atajos NHRP generados por LSI dado que la LSI no forma parte del ELAN de destino.

Nota: La opción de configuración “Exclude List” (lista de exclusiones) puede usarse para evitar atajos a LEC paranoides, tal como se describe en “Listas de exclusiones” en la página 377.

Por omisión, la LSI usará la dirección del MAC incorporada en el adaptador ATM asociado como dirección del MAC de origen de las tramas transmitidas por los VCC de atajo LANE. Es posible, aunque poco probable, que esto pueda confundir a alguna implementación en pila de protocolo de estación final, ya que la dirección del MAC no coincidirá con la del direccionador que use la estación final como pasarela para transmitir paquetes a la dirección IP asociada.

Para que ello ocurra, la estación final debería informarse de las direcciones del MAC del direccionador en tramas IP de una difusión individual, lo que no es normal (por lo general, las correlaciones de IP a MAC se saben a partir de paquetes ARP). No obstante, si esto se produce, la estación final puede usar la dirección del MAC obtenida como dirección del MAC de destino de las tramas que transmite al destino IP asociado en vez de usar la dirección del MAC del direccionador. Tales tramas se eliminan o bien se reenvían sobre VCC de métodos abreviado LANE. El reenvío sólo se produce si el LEC se entera de la vinculación de la dirección MAC a ATM en las tramas recibidas (lo cual es una elección de implementación opcional).

En ambos casos, las tramas no llegarán a destino ya que la LSI descarta las tramas recibidas en un VCC de atajo LANE. Además, la LSI libera el VCC de atajo LANE y no se establecerán más atajos con la dirección ATM asociada. A partir de ese momento, el tráfico para los destinos asociados con la dirección ATM seguirá la vía de acceso direccionada. Tenga en cuenta que los mensajes ELS y la visualización de consola de los atajos LANE ayudan a identificar estos destinos.

Puede configurarse la LSI para que no use la dirección del MAC administrada universalmente como dirección del MAC de origen. Con esta opción, tiene dos posibilidades de elección para la dirección del MAC de origen:

1. Puede usar la dirección del MAC del direccionador del último salto, proporcionada en el paquete de respuesta de resolución de NHRP, como la dirección del MAC de origen.

   El uso de la dirección del MAC del direccionador del último salto como dirección del MAC de origen resuelve el problema de la confusión de apilamiento del protocolo de la estación final pero introduce otro problema potencial. Puede provocar confusión en los LEC que se enteren de la vinculación de la dirección del MAC a ATM a partir de las tramas recibidas y, por consiguiente, no debe usarse con LEC que tengan este tipo de aprendizaje. Por ejemplo, el LEC del puente 8281 ATM-LAN de IBM tiene este tipo de aprendizaje.

2. Puede configurar la dirección del MAC de origen.

   Esta dirección puede configurarse para evitar el problema de las direcciones del MAC duplicadas observado en una ELAN, que se produce debido a atajos entre ELAN. La dirección del MAC debe configurarse para esta red LSI cuando hay entradas de atajos LANE no permitidas. Consulte “Métodos abreviados LANE” en la página 397 para obtener detalles sobre cómo visualizar entradas de atajos LANE no permitidas.

Estas opciones de configuración se proporcionan para maximizar la flexibilidad en la consecución de compatibilidad con el mayor conjunto posible de destinos en una instalación determinada. Consulte “Configuración de la interfaz de atajos LANE (LSI)” en la página 381 para obtener información detallada y “Change” en la página 388 para obtener una descripción del mandato **change**.

Parámetros de configuración

Esta sección describe algunos parámetros de configuración relacionados con NHRP y el uso que se recomienda. Consulte “Mandatos de configuración de NHRP” en la página 383 para obtener información sobre la sintaxis del mandato, sus parámetros, los valores válidos y los valores por omisión.

Configuración automática de NHRP

NHRP se habilita por omisión si IP está presente en la entrega. Puede inhabilitarse entrando el mandato **disable NHRP** desde el indicador `NHRP config>`. Consulte “Acceso al proceso de configuración de NHRP” en la página 383 para obtener información adicional.

Cuando use un archivo de configuración existente, NHRP se habilitará por omisión si no se configuró previamente. El archivo de configuración se actualizará automáticamente en el momento de ejecución para crear interfaces de atajos de NHRP. Deberá guardar este archivo de configuración actualizado y reiniciar el sistema para que el cliente de NHRP use los atajos LANE.

Listas de exclusiones

La configuración le permite crear una lista de direcciones de protocolo (y máscaras asociadas) que representan dos tipos de dispositivos:

- Direccionadores de salto siguiente que no contienen una función de servidor de NHRP
- Dispositivos de destino a los que no deben permitirse los VC de atajo

Direccionadores del salto siguiente: La lista de exclusiones puede usarse para identificar direccionadores que estén en la vía de acceso direccionada pero que no den soporte a la función de servidor de NHRP.

El servidor responde a una Next Hop Resolution Request proporcionando la dirección ATM del direccionador del salto siguiente cuando todo lo indicado a continuación sea verdadero:

- La dirección del salto siguiente es diferente de la dirección de destino.
- La interfaz del direccionador con el direccionador del salto siguiente es una ATM classical IP o una subred ELAN.
- La dirección del salto siguiente está en la lista de exclusiones.

Al procesar la solicitud, el direccionador no reenvía la Resolution Request a la dirección del salto siguiente, pero responde al cliente con información de direccionamiento que permite a éste establecer un VC de atajo al direccionador del salto siguiente.

Nota: Si el direccionador del salto siguiente es uno de los Disallowed R2R Shortcuts (atajos R2R no permitidos), el direccionador enviará un NAK a la Resolution Request en vez de una respuesta positiva.

Por lo general, si el direccionador del salto siguiente está en la lista de exclusiones, no deberá enviar ningún paquete NHRP que sólo manejaría un servidor de NHRP.

Dispositivos de destino: La lista de exclusiones también puede usarse para evitar VC de atajos a una dirección de protocolo determinada (por ejemplo, un dispositivo de una subred ELAN o CIP que sólo pueda dar soporte a un número pequeño de VC).

Al procesar una Next Hop Resolution Request para un dispositivo de destino, el servidor responde al cliente con información de direccionamiento que permite a

éste establecer un VC de atajo al mismo direccionador, cuando el resto de lo que indicamos a continuación es verdad:

- La dirección del salto siguiente es la misma que la dirección de destino.
- La interfaz del direccionador con el destino es una ATM classical IP o una subred ELAN.
- La dirección de destino está en la lista de exclusiones.

Extensiones

El protocolo NHRP incluye **Extensions** (extensiones). Las extensiones se añaden a paquetes NHRP. Se usan para solicitar funciones adicionales a participantes de NHRP. El uso del parámetro **extensions** le permite determinar si el direccionador envía algunas extensiones:

- extensiones de información de la vía de acceso
- extensiones IBM privadas del proveedor

Extensiones de información de la vía de acceso: Hay tres extensiones definidas en NHRP para proporcionar información de vía de acceso. Estas extensiones pueden usarse para ayudar a supervisar la misma solicitud, determinar la vía de acceso seguida por ésta, determinar quién generó la respuesta y la vía de acceso que siguió ésta. Las extensiones de información de la vía de acceso son:

- Forward Transmit - (Transmisión de reenvío) Cada servidor del salto siguiente (NHS) que reenvía la solicitud a lo largo del recorrido debe añadir información sobre sí mismo.
- Responder Address - (Dirección del emisor de la respuesta) El servidor del salto siguiente (NHS) que genera la respuesta debe añadir información sobre sí mismo.
- Reverse Transmit - (Transmisión inversa) Cada servidor del salto siguiente (NHS) que reenvía la respuesta a lo largo del recorrido debe añadir información sobre sí mismo.

Puede configurarse el direccionador para que envíe una de estas extensiones o todas en los paquetes Next Hop Resolution Request que genere. La información recibida en los paquetes de respuesta se visualizará en los mensajes NHRP ELS del direccionador.

Extensiones IBM privadas del proveedor: Para dar soporte a NHRP en un entorno Emulated LAN, el servidor añade extensiones únicas del proveedor a paquetes de NHRP. Estas extensiones actúan como “consultas”; el cliente de NHRP las pone en la Next Hop Resolution Request. Si el servidor da soporte a esta función, responderá con tres extensiones correspondientes que contengan la información de dirección ELAN (dirección del MAC, dirección ATM e información de direccionamiento); estas extensiones se incluyen en la Next Hop Resolution Reply.

Puede configurarse el direccionador para que no dé soporte a las extensiones específicas de IBM. Si estas extensiones no se usan, no serán posibles los atajos directos a dispositivos de ELAN. Use la opción “Exclude List” para inhabilitar selectivamente atajos a algunos dispositivos ELAN.

atajos de direccionador a direccionador no permitidos

El funcionamiento de NHRP puede producir el establecimiento de vías de acceso de tránsito a través de red NBMA entre direccionadores. No obstante, el establecimiento de un atajo NHRP que atraviese un límite donde la información usada en la selección de rutas se pierde, puede producir un bucle de direccionamiento. Tales situaciones incluyen la pérdida de información de vector de vía de acceso BGP y el interfuncionamiento de protocolos de direccionamiento múltiple con métricas disimilares. En tales circunstancias, los atajos NHRP entre direccionadores no deben permitirse. Esta situación puede evitarse si no hay vías de acceso “back door” (traseras) entre la entrada y el direccionador de salida fuera de la red NBMA.

El servidor permite atajos de direccionador a direccionador (R2R) por omisión. No obstante, al configurar atajos R2R no permitidos, puede crear una lista de direcciones de destino o de direccionador para la que el direccionador no permita atajos.

Para crear un atajo R2R no permitido, debe especificar una dirección de protocolo y una máscara. La dirección de protocolo es el destino o un direccionador y la máscara permite un rango de direcciones.

Para ilustrar cómo especificar atajos R2R no permitidos usando direcciones de protocolo y máscaras, observe el diagrama de red siguiente:

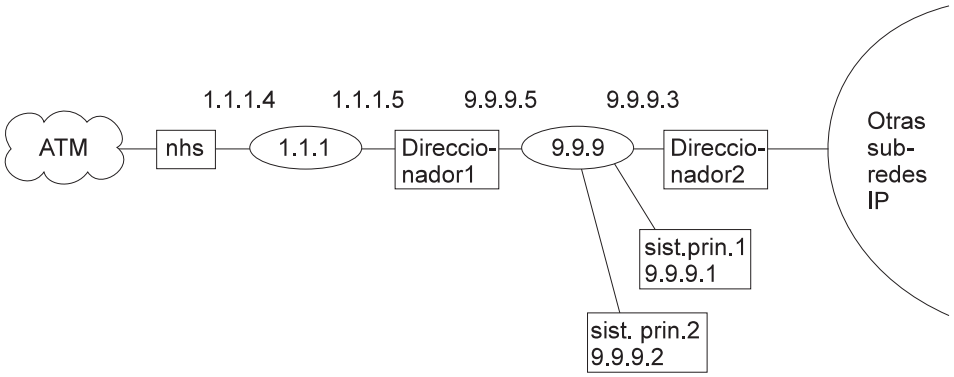


Figura 34. Uso de atajos de direccionador a direccionador no permitidos

Ejemplo 1: Una entrada que tenga la *dirección=9.9.9.1 máscara=255.255.255.255* provocaría que el NHS enviase un NAK al remitente de una Next Hop Resolution Request con la dirección del protocolo de destino 9.9.9.1 (HOST1). Dado que 9.9.9.1 no está conectada directamente a una de las subredes de dispositivo, pero se puede acceder a ella mediante otro direccionador, el direccionador comprobará la lista de atajos R2R no permitidos.

Ejemplo 2: Una entrada con *dirección=9.9.9.0 máscara=255.255.255.0* provocará que el direccionador envíe un NAK a todas las direcciones de destino entre 9.9.9.1 y 9.9.9.255. No será posible acceder a Sist.princ.1, Sist.princ.2 y Direccionador2 usando atajos al direccionador pero sí que será posible acceder a dispositivos situados en otras subredes servidas por Direccionador2.

Ejemplo 3: Una entrada con *dirección=1.1.1.5 máscara=255.255.255.255* provocará que el direccionador responda negativamente a cualquier destino cuyo

direccionador de salto siguiente sea 1.1.1.5, Direccionador1. El direccionador responderá negativamente a cualquier dirección de la subred 9.9.9 y a cualquier dirección de las otras subredes IP a las que se acceda a través del direccionador 9.9.9.3 ya que el salto siguiente es 1.1.1.5.

Ejemplo 4: Una entrada con *dirección=cualquier máscara=0.0.0.0* inhabilitará los atajos R2R para todas las direcciones.

Uso del control de acceso de protocolos

Este parámetro determina si los controles de acceso a la capa de protocolo se comprobarán y, si se comprueban, cómo se aplicarán los controles a los paquetes NHRP.

Si este parámetro de configuración se establece en el valor por omisión *none* (ninguno), los controles de acceso de la capa de protocolo no se comprobarán.

Con el valor *source and destination* (origen y destino), cuando el peticionario de NHRP no sea un direccionador, se asumirá que la dirección IP del cliente de NHRP es el origen de todos los paquetes IP que transmitirá el cliente usando la ruta de atajo NHRP. El direccionador negará solicitudes de atajo NHRP a los clientes de NHRP que no sean direccionadores si se están filtrando paquetes IP para el par de direcciones origen/destino IP, en la que el origen es la dirección del cliente de NHRP.

Si selecciona la opción *destination only* (sólo destino) el direccionador negará solicitudes de atajo a cualquier cliente de NHRP si se están filtrando paquetes IP a la dirección de destino. Si los clientes de NHRP no son fiables, deberá seleccionarse *destination only.destination only* puede ser la mejor opción cuando los clientes de NHRP no son direccionadores y tienen varias direcciones IP o son clientes que no son direccionadores y que transmiten paquetes que provienen de otros orígenes.

Los clientes de NHRP que residen en los direccionadores usan las rutas de atajo NHRP para reenviar paquetes de otros orígenes: por consiguiente, si *source and destination* está configurado y el direccionador recibe una solicitud de atajo de otro direccionador, el direccionador aplicará los filtros IP igual que cuando se selecciona *destination only*.

Controles de acceso NHRP

Los controles de acceso de NHRP para denegar atajos a algunas direcciones IP pueden definirse añadiendo estas direcciones a la lista de exclusiones y los atajos de direccionador a direccionador no permitidos.

ID de la red ATM

Dado que un servidor puede tener más de un adaptador ATM, puede estar conectado a dos redes diferentes o no asociadas. Debe tenerse en cuenta esta posibilidad al decidir cuándo deben permitirse VC de atajo.

Puede determinarse qué interfaces deben tratarse como si estuvieran conectadas a la misma red ATM física asignando a cada interfaz ATM un ID de red usando el mandato **set** en el indicador `ATM Interface Config>`, tal como se describe en el capítulo “Using and Configuring ATM” (Uso y configuración de ATM) en el manual *Software User’s Guide*

Se considera que las interfaces ATM que tienen el mismo ID de red pertenecen a la misma red. Por omisión, se asigna a todas las interfaces ATM el ID de red 0.

Configuración de la interfaz de atajos LANE (LSI)

La interfaz de atajos LANE (LSI) de NHRP se crea automáticamente para cada adaptador ATM cuando se habilita NHRP para el direccionador. LSI usa valores por omisión para los parámetros siguientes.

- ESI
- Selector
- Use Best Effort Service for Data VCCs
- Peak Cell Rate of outbound Data VCCs
- Sustained Cell Rate of outbound VCCs
- Use ATM adapter's universally administered MAC address for source

Los valores por omisión pueden modificarse usando el mandato **change** en el indicador `NHRP Advanced config>`. Consulte "Change" en la página 388.

Configuración de dispositivos en una red ATM

Si tiene un cliente/servidor de NHRP y su configuración necesita que dé una dirección ATM del servidor de NHRP del direccionador, deberá seleccionar la dirección ATM adecuada. Deberá usar una dirección asociada a una "interfaz ATM" en el dispositivo y deberá asignar una dirección IP a esta interfaz. Los dos últimos dígitos de la dirección ATM del direccionador, el selector, se asignan dinámicamente después de activar el direccionador (y pueden cambiar si la configuración del direccionador cambia), a menos que haya configurado un selector específico.

Puede especificar la dirección ATM, incluyendo el selector, entrando **prot arp** en el indicador talk 6 Config>, seguido de **add atm**, que da la dirección IP deseada, y especificando un selector. Es el mismo procedimiento que el usado para definir un cliente de ATMARP.

Uso de NHRP con LAN Emulation

Si desea usar NHRP en el dispositivo, deberá configurar todos los LEC con una dirección del MAC exclusiva administrada localmente (LAA). Si no configura los LEC con una LAA exclusiva, la función de atajo de NHRP al conmutador o dispositivo correspondiente no funcionará porque:

- El tráfico enviado en un VCC de atajo NHRP LANE contendrá la dirección del MAC Universally Administered (universalmente administrado) como la dirección del MAC de origen.
- Algunos dispositivos de red tendrán conocimiento de la asociación entre la dirección del MAC y el VCC a partir del tráfico que haya recibido el dispositivo. Estos dispositivos usarán el NHRP VCC para transmitir datos.
- Si el direccionador detecta tráfico de entrada en un NHRP VCC, asumirá que se ha producido un estado de error y cerrará el VCC, y evitará nuevos atajos al dispositivo de red.

Nota: Por omisión, el direccionador habilita las IBM LAN Emulation Extensions (extensiones IBM LAN Emulation) en NHRP, por lo que podrá inhabilitar las extensiones o configurar la dirección del MAC administrada localmente única para cada LEC.

Configuración y supervisión de NHRP

Este capítulo describe cómo configurar y supervisar Next Hop Resolution Protocol (NHRP). Para obtener una descripción de este protocolo, consulte “Visión general de Next Hop Resolution Protocol (NHRP)” en la página 367.

Este capítulo contiene las secciones siguientes:

Acceso al proceso de configuración de NHRP

Para acceder a la configuración de NHRP.

1. En el indicador de supervisión del operador (*), escriba **talk 6** y pulse Intro.
2. En el indicador `config>`, escriba **protocol nhrp** y pulse Intro.
3. Aparecerá el indicador `NHRP config>`.

Mandatos de configuración de NHRP

Esta sección explica todos los mandatos de configuración de NHRP, tal como se muestra en la Tabla 63. Entre los mandatos en el indicador `NHRP config>`.

Tabla 63. Resumen de mandatos de configuración de NHRP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxv.
Enable NHRP	Activa NHRP para todas las interfaces que no estén definidas explícitamente.
Disable NHRP	Desactiva NHRP para todas las interfaces que no estén definidas explícitamente.
List	Muestra la configuración de NHRP.
Advanced config	Le lleva al indicador `NHRP Advanced config>`, en el que podrá entrar otros mandatos como los descritos en “Mandatos de configuración avanzada de NHRP” en la página 385.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxvi.

Enable NHRP

Use el mandato `enable` para habilitar NHRP en todas las interfaces que no estén definidas explícitamente usando un mandato de configuración avanzada de NHRP. Se trata de una forma simple de activar y ejecutar NHRP con parámetros por omisión.

Sintaxis:

enable nhrp

Disable NHRP

Use el mandato `disable` para inhabilitar NHRP en todas las interfaces que no estén explícitamente definidas con un mandato de configuración avanzada de NHRP.

Sintaxis:

disable nhrp

Ejemplo:

```
NHRP config> disable
  Disable NHRP for the router [No]:
```

Advanced Config

Use el mandato **advanced** para ir al indicador de configuración avanzada de NHRP, `NHRP Advanced config>`. Desde este indicador, podrá entrar los mandatos descritos en “Mandatos de configuración avanzada de NHRP” en la página 385.

Sintaxis:

advanced nhrp

Ejemplo:

```
NHRP config> advanced
  NHRP Advanced config>
```

Nota: La mayoría de las instalaciones no necesitarán usar el mandato “advanced”. El mandato **enable NHRP** es suficiente para habilitar NHRP con opciones por omisión recomendadas.

List

Use el mandato **list** para hacer una lista de la configuración de NHRP.

Sintaxis:

list

Ejemplo:

```
NHRP config> list
  Box level NHRP enabled
    Explicit interface definitions override box level setting

  Interfaces explicitly defined for NHRP
  --------------------------------------
   Interface 0: ATM
     NHRP enabled

  NHRP LANE Shortcut Interface:
  -----------------------------------------------------
   Interface: 1  ESI: burned-in          Sel: auto
   Use Best Effort: no   (Data)
   Cell Rate(kbps):  Peak: 155000    Sustained: 155000
   ATM adapter's burned-in MAC address is used as source address

  General Parameters
  ------------------
   Holding time:                          20 minutes
   Protocol Access Controls:              Use source and destination   address
   When should NHC attempt shortcuts?:    Based on datarate
      Data-rate threshold:                10 packets/second
   NHS allows shortcuts to ATMARP clients?: Yes

  Cache Sizes
  -----------
   Resolution cache:           10000 entries
   Server purge cache:         10000 entries
   Server registrations cache: 10000 entries

  Extension Usage
  ---------------
   Use NHRP Forward transit NHS record client extension: No
   Use NHRP Reverse transit NHS record client extension: No
   Use Responder Address client extension:               No
   Use LANE shortcuts extension:                         Yes



  List of NHRP IP exclude records
  -------------------------------
    # Address         Mask
    1 6.6.6.6         255.255.255.255
    2 5.5.5.0         255.255.255.0

  Disallowed router-to-router shortcuts for IP
  --------------------------------------------
     None
```

Mandatos de configuración avanzada de NHRP

Esta sección explica todos los mandatos de configuración avanzada de NHRP, tal como se muestra en la Tabla 64 en la página 386. Entre los mandatos desde el indicador `NHRP Advanced config>`.

Tabla 64. 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 xxv.
Add	Añade una interfaz de NHRP, una lista de exclusiones o métodos abreviados R2R no permitidos.
Change	Cambia una interfaz de NHRP o cambia una definición de la interfaz de atajo LANE.
Delete	Suprime una interfaz de NHRP, una lista de exclusiones o métodos abreviados R2R no permitidos.
List	Muestra la configuración de NHRP.
Set	Establece parámetros de NHRP.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxvi.

Add

Use el mandato **add** para añadir una definición de interfaz explícita, una entrada de la lista de exclusiones o métodos abreviados de direccionador a direccionador no permitidos.

Sintaxis:

add interface definition
exclude list
disallowed router-to-router shortcuts

interface definition

Añade una definición de interfaz explícita para habilitar o inhabilitar una interfaz de NHRP. Si NHRP está inhabilitado en una interfaz de red determinada, los paquetes de NHRP no se reenviarán a ningún direccionador al que se acceda a través de dicha interfaz. Además, las tramas de NHRP de entrada se descartarán.

Nota: Cualquier definición de interfaz explícita altera temporalmente el valor de nivel de entrega “NHRP enabled/disabled” (NHRP habilitado/inhabilitado).

Ejemplo: `add int`

```
Interface Number [0]?
Enable NHRP [Yes]:
```

exclude list

Añade una entrada en la lista de exclusiones. Especifica una dirección de protocolo que deberá excluirse de la red NHRP. Esta opción añade una entrada a la lista de exclusiones y le solicita que añada esta entrada a los métodos abreviados de direccionador a direccionador no permitidos. Consulte “Controles de acceso NHRP” en la página 380 para obtener más información.

Valores válidos: Máscara y dirección IP.

Valor por omisión: Empty (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 para la que no están permitidos los métodos abreviados.

Consulte “atajos de direccionador a direccionador no permitidos” en la página 379 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: Dirección IP y máscara.

Valor por omisión: Empty (Vacío).

Delete

Use el mandato **delete** para suprimir una definición de interfaz para NHRP, una entrada de la lista de exclusiones o métodos abreviados de direccionador a direccionador no permitidos.

Sintaxis:

de**lete**	interface definition for NHRP exclude list disallowed router-to-router shortcuts

interface definition for NHRP

Suprime una definición de interfaz de NHRP explícita.

Ejemplo: **`del int`**

```
Interface Number [0]?
```

exclude list

Suprime una entrada de la lista de exclusiones. Esta opción suprime una entrada de la lista de exclusiones y le solicita que suprima esta entrada de los métodos abreviados de direccionador a direccionador no permitidos. Consulte “Controles de acceso NHRP” en la página 380 para obtener más información.

Debe especificar un índice que debe suprimirse. Use el mandato **list exclude** para determinar el índice correcto.

Ejemplo: **`del exc`**

```
Enter index of access control to be deleted [1]?
# Address          Mask
1 6.6.6.6          255.255.255.255
Are you sure this the record you want to delete  [Yes]?
Record deleted from Exclude List
Delete from Disallowed Router-to-Router Shortcuts [Yes]?
Record deleted from Disallowed Router-to-Router Shortcuts
```

disallowed router-to-router shortcuts

Suprime una entrada de métodos abreviados de direccionador a direccionador no permitidos. Debe especificar un índice que debe supri-

mirse. Use el mandato **list disallowed** para determinar el índice correcto.

Ejemplo: **`del dis`**

```
Disallowed shortcuts index [1]?
```

Change

Use el mandato **change** para modificar definiciones de interfaz de NHRP.

Sintaxis:

change interface definition
nhrp lane shortcut interface

interface definition for NHRP

Cambia una definición de interfaz explícita para habilitar o inhabilitar una interfaz de NHRP.

Ejemplo: **`ch int`**

```
Interface Number [0]?
Enable NHRP [Yes]:
```

NHRP LANE shortcut Interface

Cambia una definición de una interfaz de atajo LANE.

Ejemplo: **`ch nhrp`**

```
Interface Number of NHRP LANE Shortcut Interface [0]?
(  1) Use burned in ESI
Select ESI [1]?
Use internally assigned selector? [Yes]:
Use Best Effort Service for Data VCCs? [Yes]:
Peak Cell Rate of outbound Data VCCs (Kbps) [0]?
Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?
Use ATM adapter's burned-in MAC address for source?
```

Interface Number of NHRP LANE Shortcut Interface

Use el número de interfaz asignado al LSI. El número de interfaz puede determinarse usando el mandato **list interface**.

(1) Use burned in ESI

Use el ESI administrado universalmente como parte de la dirección ATM. Es posible que, según la configuración, se le ofrezcan otras opciones.

Select ESI

Especifique el ESI.

Use internally assigned selector

Use el selector asignado internamente o asigne un selector que esté dentro del rango incluido entre 00 y FF.

Use Best Effort Service for Data VCCs

Especifica el tipo de características de tráfico que se asociarán con los VCC de datos. La anchura de banda no se reserva al tráfico de mejor esfuerzo.

Peak Cell Rate of outbound Data VCCs (kbps)

Especifica el tráfico de velocidad mayor de célula (PCR) para los VCC de datos.

Sustained Cell Rate of outbound Data VCCs (Kbps)
Especifica el parámetro de la velocidad sostenida de célula (SCR) para los VCC de datos.

Use ATM adapter's burned-in MAC address for source?
Puede usar como dirección del MAC de origen para métodos abreviados LANE:

1. La dirección del MAC administrada universalmente del adaptador
2. La dirección del MAC suministrada en la respuesta de resolución de NHRP
3. La dirección del MAC que configuró especificando una dirección del MAC con el mandato **change nhrp**.

Consulte "ATM and LAN Emulation" en el manual *Software User's Guide* para obtener mayor información.

Nota: Se recomienda que use los valores por omisión hasta que haya determinado las opciones de proceso específicas del entorno.

List

Use el mandato **list** para visualizar información de configuración de NHRP.

Sintaxis:

list all
exclude list
disallowed router-to-router shortcuts
interface definitions
cache size

all Muestra toda la configuración de NHRP.

Ejemplo: `li all`

La salida es la misma que la que se obtiene con el mandato **list**. Consulte "List" en la página 384.

exclude list
Muestra las entradas de la lista de exclusiones.

Ejemplo: `li exc`

```
List of NHRP IP exclude records
-------------------------------
  # Address         Mask
  1 7.7.7.7         255.255.255.255
```

disallowed router-to-router shortcuts
Muestra los métodos abreviados de direccionador a direccionador no permitidos.

Ejemplo: `li dis`

```
Disallowed router-to-router shortcuts for IP
--------------------------------------------
  1 8.8.8.1         255.255.255.255
  2 6.6.6.1         255.255.255.255
```

interface definitions
Muestra las definiciones de interfaces de NHRP.

Ejemplo: `li int`

```
Interfaces explicitly defined for NHRP
--------------------------------------
   None

NHRP LANE Shortcut Interface:
-----------------------------------------------------
Interface: 3  ESI: burned-in          Sel: auto
Use Best Effort: yes  (Data)
Cell Rate(kbps):  Peak:      0/     0    Sustained:   1000/538764944
MAC address supplied by NHS is used as source address
```

cache size

Muestra los tamaños de las antememorias.

Ejemplo: `li ca`

```
                  Cache
Sizes
                  ----- -----
   Resolution cache:           10000 entries
   Server purge cache:         10000 entries
   Server registrations cache: 10000 entries
```

Set

Use el mandato **set** para:

Sintaxis:

set
- protocol access control usage
- attempt shortcuts
- holding time
- data-rate threshold
- extensions ...
- cache size ...
- shortcuts to atmarp clients

protocol access control usage

Determina si los controles de acceso de IP se comprobarán y, si es así, cómo se aplicarán a los paquetes NHRP. Consulte “Uso del control de acceso de protocolos” en la página 380 para obtener más información.

Ejemplo: `set prot`

```
Use (Destination, Source & Destination, None) [None]?
```

Valores válidos: None (Ninguno), Source and Destination (Origen y destino), Destination (Destino)

Valor por omisión: None

attempt shortcuts

Determina cómo el cliente de NHRP decide cuándo originar solicitudes de resolución.

Valores válidos: Y, N, Data-rate (Velocidad de datos).

Y Sí. Intenta siempre establecer un VC de atajo creando una Next Hop Resolution Request y enviándola a la estación del salto siguiente.

N No. Nunca intenta establecer un atajo. Esta opción inhabilita básicamente la función de cliente en el direccionador. Este valor puede usarse en un direccionador intermedio (un direccionador

que no sea un punto de entrada a la red NBMA para el tráfico direccionado) para eliminar el “efecto dominó”, donde el tráfico que sigue la vía de acceso direccionada presenta NHRP Resolution Requests en cada direccionador de NHRP situado a lo largo de la vía de acceso.

Data-rate
Intenta establecer un atajo únicamente después de que se haya alcanzado el umbral de velocidad de datos.

Nota: Este valor puede evitar la creación de VCC para tráfico de “una ocasión” como, por ejemplo, indicadores de detección de condición de excepción de SNMP que se envían a un gestor de SNMP.

Valor por omisión: Data-rate.

Ejemplo: **`set attempt`**

```
Try shortcut VCs? (Yes, No, Data-rate) [Data-rate]?
```

holding time
Establece el tiempo de retención en minutos.

El parámetro del tiempo de retención se usa para estas funciones:

- Cuando el direccionador responde a una Next Hop Resolution Request con información acerca de sí mismo (es decir, el direccionador se va a convertir en el atajo del salto siguiente), el tiempo de retención se envía al peticionario como el período de tiempo en que se considerará válida la información.
- Cuando el direccionador responde a una Next Hop Resolution Request con información acerca de otra estación NBMA de la que no se supo usando NHRP (por ejemplo, la estación de destino es un dispositivo ATM con una dirección IP en una de las subredes de dispositivo), el tiempo de retención se envía al peticionario como el período de tiempo en que se considerará válida la información.

Valores válidos: De 1 a 60 minutos.

Valor por omisión: 20 minutos.

Ejemplo: **`set hold`**

```
Holding time (in minutes)  [20]?
```

data-rate threshold
Establece el umbral de velocidad de datos en paquetes/segundo.

Este umbral se usa cuando el parámetro **attempt shortcuts** se establece en **Data-rate**.

Cuando el tráfico esté destinado a una estación en concreto, pero la velocidad es inferior a este umbral, el direccionador no intentará establecer métodos abreviados. (Dicho de otra forma, no generará Next Hop Resolution Requests y los enviará al salto siguiente de la vía de acceso direccionada). Cuando la velocidad del tráfico supere el umbral, el direccionador intentará establecer un atajo. Si puede crear satisfactoriamente un atajo, éste se usará incluso si el tráfico cae por debajo del umbral. El recorrido seguirá utilizándose hasta que el tráfico se detenga por un período de tiempo. Esto se hace para evitar ir adelante

y atrás, de la vía de acceso direccionada al atajo y viceversa si el tráfico es esporádico.

Valores válidos: Mínimo 1 paquete/segundo. Máximo 5120 paquetes/segundo.

Valor por omisión: 10 paquetes/segundo.

Ejemplo: **`set data`**

```
Data-rate threshold in packets/second [10]?
```

extensions

Establece el uso de la extensión NHRP seleccionada en *yes* (sí) o *no*.

Forward transmit NHS (valor por omisión: no)
Reverse transmit NHS (valor por omisión: no)
Responder Address (valor por omisión: no)
Lane Shortcuts (valor por omisión: yes)

Valores válidos: yes o no

Ejemplo: **`set ext lane`**

```
Use LANE shortcuts extension [Yes]?
```

cache size *resolución* **O** *registro* **O** *depuración servidor*

Establece el número máximo de entradas de la antememoria seleccionada.

Los tamaños de la antememoria pueden seleccionarse entre los siguientes:

resolution cache

Este parámetro le permite determinar el número de entradas en la antememoria para las funciones cliente. Cada entrada de la antememoria contiene la correlación de la dirección de protocolo con la dirección NBMA que puede usarse para crear VC de atajo. Las entradas están en la antememoria cuando el direccionador:

- Ha resuelto satisfactoriamente una dirección de protocolo a una dirección NBMA enviando Next Hop Resolution Requests.
- Ha intentado resolver una solicitud de protocolo a una dirección NBMA pero no ha recibido respuesta o ha recibido una respuesta negativa y el tiempo del temporizador asociado no se ha excedido. Estas entradas se mantienen en la antememoria para evitar que el dispositivo genere Next Hop Resolution Requests adicionales durante un período de tiempo.
- Ha recibido una solicitud de registro de un cliente y el tiempo de retención indicado en la solicitud no ha expirado.

Cuando se supera el tamaño de la antememoria, ya no se efectuarán intentos nuevos de resolver direcciones de protocolo con direcciones NBMA (dicho de otra manera, no se envían Next Hop Resolution Requests nuevas) hasta que se depuren las entradas existentes, ya sea porque el tiempo de retención se ha agotado o porque se ha recibido una solicitud de depuración específica del originador de la información. Además, cuando se supera el tamaño de la antememoria, se rechazan las Registration Requests de los clientes nuevos.

Valores válidos: De 256 a 65535 entradas.

Valor por omisión: 10000 entradas.

Ejemplo: **set cache res**

```
Number of cache entries [10000]?
```

registration cache

Establece un límite en el número de entradas de registro de la antememoria de resolución. Cuando el servidor recibe una solicitud de registro, comprueba si el número de registros de clientes de NHRP está por debajo de este límite antes de añadir una entrada de registro en la antememoria de resolución.

Valores válidos: De 256 a 16384 entradas.

Valor por omisión: 10000 entradas.

Ejemplo: **set cache reg**

```
Number of cache entries [10000]?
```

server purge cache

Este parámetro le permite determinar el número de entradas en la antememoria de depuración del servidor. Una entrada de esta antememoria representa una dirección de protocolo de destino y un cliente al que el servidor ha proporcionado información Authoritative NBMA (NBMA de autorización) para dicho destino.

La dirección de destino puede representar al mismo servidor, a dispositivos de subredes con los que el servidor esté conectado, clientes de NHRP que se han registrado en el servidor o direccionadores a los que se ha anunciado un atajo R2R. El direccionador usa la información de estas entradas de antememoria para notificar a los clientes que depuren la información de dirección que se ha vuelto no válida antes de que se agote el temporizador de retención.

Cuando el tamaño de la antememoria de depuración del servidor se supere, el servidor rechazará las Authoritative Next Hop Resolution Requests.

Valores válidos: De 256 a 65535 entradas.

Valor por omisión: 10000 entradas.

Ejemplo: **set cache serv**

```
Number of cache entries
[10000]?
```

shortcuts to ATMARP clients

Permite o no permite métodos abreviados a clientes de ATMARP.

Puede usarse este parámetro para permitir o no permitir que el servidor ponga los métodos abreviados en manos de clientes de ATMARP nativos que no dan soporte a NHRP. Este parámetro puede ser necesario si estos clientes no son capaces de dar soporte a un gran número de VC. Use la opción “Exclude List” si es necesario no dar permiso a los métodos abreviados de forma selectiva a algunos clientes o subredes.

Ejemplo: **set shortcut**

```
Allow shortcuts to Classical IP clients?  [Yes]:
```

Acceso al proceso de supervisión de NHRP

Para acceder al indicador de supervisión de NHRP:

1. En el indicador de supervisión del operador (*), escriba **talk 5** y pulse Intro.
2. En el indicador +>, escriba **protocol nhrp** y pulse Intro.
3. Aparecerá el indicador NHRP>.

Mandatos de supervisión de NHRP

Esta sección explica todos los mandatos de supervisión de NHRP tal como se muestran en la Tabla 65. Entre los mandatos en el indicador NHRP>.

Tabla 65. 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 xxv.
Box Status	Muestra el estado de habilitación/inhabilitación de NHRP.
Interface Status	Muestra el estado de la interfaz de NHRP.
Statistics	Muestra las estadísticas de la interfaz de NHRP.
Cache	Muestra las entradas de antememoria de la resolución de NHRP.
Server_purge_cache	Muestra las entradas de server_purge_cache.
MIB	Muestra información del MIB.
LANE Shortcuts	Muestra las entradas de atajo LANE.
CONFIG Parameters	Muestra, cambia o restablece información de configuración de NHRP.
Reset	Vuelve a configurar dinámicamente protocolo o interfaces de HRPP.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxvi.

Box Status

Use el mandato **box status** para visualizar el estado de NHRP tal como se ha configurado para su entrega (por ejemplo, no se ha definido explícitamente ninguna interfaz).

Sintaxis:

b**ox-status**

Ejemplo:

```
box status
 Box level NHRP is ON by config
```

Interface Status

Use el mandato **interface status** para visualizar el estado de NHRP en las interfaces.

Sintaxis:

in**terface-status**

Ejemplo:

```
interface status
  Interface 0: UP  (NHRP enabled)
  Interface 1: UP  (NHRP disabled)
  Interface 2: DOWN
  Interface 3: UP  (NHRP LANE Shortcut Interface)
```

Statistics

Use el mandato **statistics** para visualizar estadísticas NHRP para todas las interfaces o para una interfaz específica.

Sintaxis:

statistics all
interface

all Establece una lista de estadísticas NHRP en todas las interfaces.

Ejemplo: statistics all

Se produce lo mismo que en el caso del mandato **statistics interface** tal como aparece en el ejemplo siguiente.

interface Establece una lista de las estadísticas de NHRP de una interfaz especificada.

Ejemplo: `statistics interface`

```
  Interface number [0]? 0

  Statistics for Interface 0
  --------------------------
  Field Description                          Value
  -----------------                          -----
  Inbound Requests                            5
  Outbound Requests                           3
  Inbound Replies                             3
  Outbound Replies                            5
  Inbound Registers                           0
  Outbound Registers                          0
  Inbound Error Packets                       0
  Inbound Error Indication Packets            0
  Outbound Error Indication Packets           0
  Reply Forwards                              0
  Unrecognized Options                        0
  Registration Overflows                      0
  ProtocolErrors                              0
  Negative Outbound Replies                   0
  Inbound Packets on NHRP disabled interface  0
  'Send_to_me' Outbound Replies               0
  Inbound Purges                              0
  Outbound Purges                             2
```

Cache

Use el mandato **cache** para visualizar todas las entradas de antememoria de resolución NHRP o una entrada de antememoria específica identificada por una dirección de destino.

Sintaxis:

cache	list
	entry

list Lista las entradas de antememoria de NHRP.

entry Lista una entrada de antememoria de NHRP específica.

Ejemplos:

```
cache list
          Total Client Cache Entries = 3

          NHRP Client Cache Entries
          =========================

          Dest Address    NextHop Address State Htime MTU  Net
          ------------    --------------- ----- ----- ---  ---
          5.5.5.1         5.5.5.1         Act   1121  4490  1
          5.5.5.2         5.5.5.2         Inact 1185  4490  1
          6.6.6.1         6.6.6.1         Act   602   9180  0


cache entry
          Enter destination address  [0.0.0.0]? 6.6.6.1
          Destination: 6.6.6.1
          NextHop:     6.6.6.1
          ATM Address: 39840F000000000000000000000410005A00DEADCA
          State:       Act
          Net:         0
          HoldingTime: 433 seconds
          MTU size:    9180
          Flags:       0x00420000
```

Server_purge_cache

Use el mandato **server_purge_cache** para listar todas las entradas de antememoria de depuración del servidor NHRP.

Sintaxis:

server_purge_cache

MIB

Use el mandato **MIB** para visualizar información relacionado con el MIB de NHRP.

Sintaxis:

mib	list ...
	entry ...

list Lista las entradas mib de NHRP para:

- Tabla de servidores
- Tabla de clientes
- Tabla de estadísticas del servidor del salto siguiente (NHS)

- Tabla de estadísticas del cliente del salto siguiente (NHC)
- Tabla de la antememoria de resolución

Ejemplo. `mib list server table`

```
MIB Server Table List
=====================

Index Server Address  State ATM Addr
----- --------------  ----- --------
0     6.6.6.2         UP    39840F00000000000000000000210005A00DEADC8
```

entry Lista una entrada mib de NHRP en:

- Tabla de servidores
- Tabla de clientes
- Tabla de estadísticas del servidor del salto siguiente (NHS)
- Tabla de estadísticas del cliente del salto siguiente (NHC)
- Tabla de la antememoria de resolución

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
```

Métodos abreviados LANE

Use el mandato **lane shortcuts** para visualizar todas las entradas o entradas específicas usando métodos abreviados LANE. También puede visualizar cualquier dirección ATM para la que no están habilitados métodos abreviados LANE debido a problemas operativos.

Sintaxis:

l**ane-shortcuts** all

entry

disallowed

all Muestra todos los métodos abreviados 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 Muestra una entrada de atajo LANE.

Ejemplo: `lane entry`

```
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:    39840F000000000000000000000310005A00DEAD02
Media type:     Token Ring
VPI/VCI:          0/34
Holding Time:   20 minutes
MTU size:       4490
RI Field:064001020203
```

disallowed

Muestra todas las entradas de atajo de LANE no permitidas.

Cualquier dirección ATM que aparezca listada indicará que la NHRP LANE Shortcut Interface recibió datos de la dirección ATM. Esto no está permitido ya que todos los VCC de NHRP LANE Shortcut Interface se usarán únicamente para transmitir datos a un LEC del otro extremo. Si el LEC intenta enviar datos sobre un VCC mediante una NHRP LANE Shortcut Interface, se desactivará el VCC y no se volverán a establecer más métodos abreviados LANE a dicho LEC.

Una vez corregida la condición que produjo que la NHRP LANE Shortcut Interface recibiera datos, el dispositivo deberá reiniciarse para que los métodos abreviados NHRP LANE vuelvan a utilizar la dirección ATM.

Ejemplo: `lan dis`

```
LAN Shortcut Interface #: 2, ATM Network Interface #: 0
=======================================================
Atm Address
-------------------------------------------
39840F000000000000000000000310005A00DEAD02
```

CONFIG Parameters

Use el mandato **config parameters** para acceder a los menús de mandatos de los parámetros de configuración de NHRP **display**, **change** o **reset**.

Tabla 66. 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 xxv.
Display	Muestra los parámetros de configuración de conmutación de rutas y NHRP.
Change	Permite cambiar dinámicamente los parámetros de configuración de NHRP sin influir en la configuración estática.
Reset	Lee el parámetro de configuración de la configuración estática y lo usa durante el tiempo de ejecución del direccionador.

Display

Use el mandato **display** para visualizar los parámetros de configuración de conmutación de rutas y NHRP.

Sintaxis:

display nhrp

nhrp Muestra los parámetros de configuración de NHRP, incluyendo los parámetros generales, los tamaños de antememorias, el uso de extensiones, la lista de exclusión y los métodos abreviados de direccionador a direccionador no permitidos.

Change

Use el mandato **change** para cambiar los parámetros de configuración de NHRP actuales. Consulte “Set” en la página 390 para obtener una descripción de los parámetros de configuración.

Sintaxis:

change protocol_access_control_usage
attempt_shortcuts
holding_time
data-rate_threshold
cache_size
extensions
shortcuts_to_atmarp_clients

Reset

Use el mandato **reset** para restablecer el valor del parámetro de configuración dinámica en el valor de la configuración estática. Consulte “Set” en la página 390 para obtener una descripción de los parámetros de configuración.

Sintaxis:

reset protocol_access_control_usage
attempt_shortcuts
holding_time
data-rate_threshold
cache_size
extensions
shortcuts_to_atmarp_clients
exclude_list
disallowed_router-to-router

Reset

Use el mandato **reset** para volver a configurar dinámicamente el protocolo NHRP o una interfaz. Un mandato reset hace que los valores de configuración estáticos aplicables se usen.

Sintaxis:

reset interface
nhrp

nhrp Restablece estadísticas, interfaces y parámetros de configuración de NHRP en los valores de configuración estáticos. Esto equivale a un inicio en frío de NHRP.

interface Desactiva la interfaz de NHRP y activa la interfaz con nuevos valores de configuración estática de la interfaz.

Rastreo de paquetes de NHRP

El rastreo de paquetes de NHRP puede activarse desde el sistema de anotación cronológica de sucesos (ELS), que es una parte integral del sistema operativo del direccionador. Consulte “Using and Configuring the Event Logging System” y “Monitoring the Event Logging System” en el manual *Software User’s Guide*.

El mecanismo de rastreo de paquetes NHRP da soporte a la opción “set trace decode on”. Esta opción permite que la producción de rastreo de paquetes NHRP pueda interpretarse para verla. También pueden rastrearse las tramas de control sobre LSI aparte de los paquetes del protocolo NHRP. Para obtener detalles sobre el uso de la función de rastreo, consulte la descripción del mandato **trace** en “Monitoring the Event Logging System” en el manual *Software User’s Guide*

Los paquetes del protocolo NHRP se identifican mediante el suceso 19 y los paquetes de control de LSI mediante el suceso 113.

Ejemplo de producción de rastreo núm. 1:

```
Dir:OUTGOING  Time:0.0.48.88  Trap:6035
Comp:NHRP  Type:UNKNOWN  Port:1  Circuit:0x000000  Size:160
----------------------------------------------------------------
** NHRP/MPOA Frame **
AddressFamily:ATM_NSAP  ProtocolType:IPv4  HopCount:64  PacketSize:160
Checksum:0x03F4  ExtensionOffset:0x0038  Version:1  PktType:ResolutionRequest
SrcAddrTL:20  SrcSubAddrTL:0  SrcProtoLen:4  DstProtoLen:4
Flags:requester is a router  Flags:want authoritative only  Flags:want unique
only  ReqID:1
Src NBMA:39840F000000000000000000610005A019600C9
Src Protocol Addr: 6.6.6.1  Dest Protocol Addr: 3.3.3.2
0038: 00 08 00 1C 08 00 5A 00  00 01 00 0A 00 00 00 00    | ......Z......... |
0048: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    | ................ |
0058: 00 08 00 34 08 00 5A 00  00 01 00 0C 00 00 00 00    | ...4..Z......... |
0068: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    | ................ |
0078: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    | ................ |
0088: 00 00 00 00 00 00 00 00  00 08 00 08 08 00 5A 00    | ..............Z. |
0098: 00 01 00 06 80 00 00 00                             | ................ |
```

Ejemplo de producción de rastreo núm. 2:

```
Dir:INCOMING  Time:0.0.50.69  Trap:6035
Comp:NHRP  Type:UNKNOWN  Port:1  Circuit:0x000000  Size:202
----------------------------------------------------------------
** NHRP/MPOA Frame **
AddressFamily:ATM_NSAP  ProtocolType:IPv4  HopCount:63  PacketSize:202
Checksum:0xEC88  ExtensionOffset:0x005C  Version:1  PktType:ResolutionReply
SrcAddrTL:20  SrcSubAddrTL:0  SrcProtoLen:4  DstProtoLen:4
Flags:requester is a router  Flags:authoritative info  Flags:requested info
unique  ReqID:1
Src NBMA:39840F000000000000000000000610005A019600C9
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:39840F000000000000000000000310005A01950103
  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    | ................ |
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          | .............. |
```

Uso de IP Versión 6 (IPv6)

Este capítulo describe cómo usar IPv6.

Visión general de IPv6

IP Versión 6 (IPv6) es una versión nueva de Internet Protocol. Se ha diseñado para que suceda a IP Versión 4 (IPv4). La lista siguiente indica algunas de las ventajas que IPv6 proporciona:

- Un espacio de dirección grande

  IPv6 usa una dirección de 128 bits.

- Direccionamiento

  Mediante el tamaño de dirección grande, IPv6 proporciona un esquema de dirección jerárquica que le permite crear una jerarquía de direccionamiento flexible.

- Configuración fácil

  NDP proporciona configuración automática del sistema principal.

- Seguridad

  IPv6 convierte en obligatoria la seguridad de IP.

- Soporte para tráfico multimedia

  La cabecera de IPv6 tiene campos de etiqueta de flujo y de prioridad para acomodar una calidad de servicio integrada.

- Simplificación

  La cabecera de IPv6 es fija y simplificada. Ya no es necesario el direccionador para efectuar una fragmentación que simplifique el proceso de paquetes. Además, los datos de tipos de opciones se implementan en cabeceras de extensión que sólo reciben proceso del nodo de destino.

Comparación de IPv6 con IPv4

IPv6 incluye varios cambios comparado con IPv4. Los cambios más significativos son:

- Dirección
- Formato de cabecera
- MTU mínima
- Mandatory Path MTU discovery
- Seguridad de IP obligatoria
- Neighbor Discovery Protocol (NDP)

Direccionamiento de IPv6

El direccionamiento de IPv6 aumenta la dirección, que pasa de 32 bits a 128 bits. Este aumento permite que hayan más grados de jerarquía que capas básicas de la red, subred y sistema principal.

Las direcciones de IPv6 pertenecen a una de las tres categorías siguientes:

- Difusión invidual. Se entrega un paquete a la interfaz identificada por la dirección.
- Difusión múltiple. Se envía un paquete a todos los miembros del grupo de difusión múltiple identificado por la dirección.
- Única difusión. Se envía un paquete únicamente al miembro más cercano del grupo identificado por la dirección.

En IPv6, se ha sustituido el direccionamiento de difusión por el direccionamiento de difusión múltiple.

Formato de dirección de IPv6

La dirección de IPv6 está compuesta por 128 bits. Estos bits se escriben como ocho números enteros de 16 bits separados por el signo de dos puntos.

Ejemplo:

ABCD:1234:0000:1234:5555:FFEE:7777:0123

Puede usar las reglas de simplificación siguientes:

- Saltar los ceros iniciales.

  Ejemplo:

  ABCD:1234:0:1234:0:FFEE:7777:123

- Dentro de una dirección, un conjunto de números consecutivos y nulos de 16 bits puede sustituirse por dos signos de dos puntos.

  Ejemplo:

  ABCD:1234::1234:5555:FFEE:7777:123

  1234::7899

  Los signos de dos puntos dobles sólo se pueden usar una vez dentro de la dirección.

- Cuando trate con un entorno mixto de nodos IPv4 e IPv6, puede usar la forma **x:x:x:x:x:x:d.d.d.d**

  , donde las x son valores hexadecimales de las seis partes de 16 bits más significativas de la dirección y las d son valores decimales de las cuatro partes de 8 bits menos significativas de la dirección en la representación de IPv4 estándar.

  Ejemplo:

  ABCD:1234::1234:5555:FFEE:1.2.3.4

  ::1.2.3.4

Representación textual de prefijos de direcciones

Un prefijo de dirección de IPv6 se representa mediante la notación:

Dirección-IPv6/longitud-prefijo

La dirección de IPv6 puede usar cualquiera de las notaciones listadas en “Formato de dirección de IPv6” en la página 404 y la longitud de prefijo es un valor decimal que especifica cuántos de los bits contiguos situados más a la izquierda de la dirección forman el prefijo.

Ejemplo:

ABCD:1234::1234:5555:FFEE:1.2.3.4/64

Formato de cabecera de IPv6

La cabecera de IPv6 tiene un total de 8 campos, en la que se eliminan algunos campos IPv4 como el de suma de comprobación y el de fragmentación.

MTU mínima de IPv6

La MTU mínima para IPv6 tiene 1280 bytes. No se puede habilitar IPv6 en una interfaz con una MTU con menos de 1280 bytes.

Path MTU Discovery obligatorio en IPv6

Path MTU Discovery es un protocolo que permite a un sistema principal determinar el paquete de tamaño máximo que atravesará satisfactoriamente una vía de acceso a un destino sin fragmentarse. A medida que se generen y envíen paquetes desde el sistema principal, la MTU de la interfaz de salida en particular a la que se envía el paquete, estará disponible.

Si el paquete se adapta a la interfaz de salida, ya sea en su totalidad o en fragmentos, se transmitirá. Si un direccionador de la vía de acceso necesita reenviar este paquete a una red con una MTU más pequeña que el tamaño del paquete, éste se eliminará y se enviará un mensaje ICMP al originador del paquete en el que se indica el tamaño necesario del paquete para que quepa en la red de salida del direccionador intermedio. El sistema principal que reciba este mensaje ajustará el tamaño de los paquetes posteriores reenviados en la vía de acceso. Este proceso puede producirse varias veces antes de que el paquete alcance el destino final. Una vez el paquete haya alcanzado su destino, los paquetes posteriores no deberán eliminarse porque el tamaño del paquete sea demasiado grande.

Dado que la ruta puede cambiar dinámicamente, la MTU de la vía de acceso puede aumentar y necesitar, por lo tanto, un ajuste en el nodo del sistema principal. Se asigna una edad a las MTU de la vía de acceso de las que se tiene conocimiento y el proceso de Path MTU Discovery vuelve a producirse. Esto permite que el tamaño del paquete transmitido reaccione a la naturaleza dinámica de las rutas de la red.

Path MTU Discovery es obligatorio ya que la fragmentación no está permitida en los direccionadores de tránsito.

Si el dispositivo actúa como direccionador de tránsito, no reenviará paquetes de tamaño superior a la MTU de la red de salida. Generará un mensaje ICMP Packet Too Big (Paquete ICMP demasiado grande) y lo enviará al origen del paquete.

El mandato **enable path-mtu-discovery** en el indicador`IPv6 Config>` puede usarse para habilitar o inhabilitar path MTU discovery. Por omisión, path MTU discovery se habilita.

Use el mandato **set path-mtu-aging-timer** en el indicador `IPv6 Config>` para especificar el tiempo de envejecimiento de las MTU de la vía de acceso que se han determinado.

Seguridad obligatoria de IPv6

Un nodo IPv6 debe dar soporte a la seguridad IP. Esta seguridad puede habilitarse o inhabilitarse. Consulte “Using IP Security” (Uso de la seguridad IP) y “Configuring and Monitoring IP Security” (Configuración y supervisión de la seguridad IP) en el manual *Using and Configuring Features* para obtener información adicional sobre la seguridad IP.

1. Use el mandato **add packet** en el indicador `IPv6 Config>` para añadir un filtro de paquetes.
2. Use el mandato **update packet** en el indicador `IPv6 Config>` para actualizar el filtro de paquetes.
3. Use el mandato **add access** en el indicador `Packet-filter 'nombre_filtro' Config>` para añadir controles de acceso.
4. Use el mandato **set acc on** en el indicador `IPv6 Config>` para habilitar el control de accesos.

IPv6 Neighbor Discovery Protocol (NDP)

IPv6 usa NDP para realizar la configuración automática. NDP permite que los nodos de IPv6 que estén en el mismo enlace descubran la presencia respectiva, a fin de determinar las direcciones de la capa de enlace de cada uno, encontrar direccionadores y mantener información de accesibilidad sobre las vías de acceso a los vecinos activos.

NDP tiene soporte de los tipos de soporte siguientes:

- Ethernet
- Red en anillo
- FDDI
- PPP
- IP64 Tunnel
- LCS

Router y Prefix Discovery

Los sistemas principales usan Router Discovery (descubrimiento de direccionadores) para descubrir direccionadores que residen en un enlace conectado. Cada direccionador ejecuta, periódicamente, una difusión múltiple de un paquete Router Advertisement (anuncio de direccionador), si está configurado, en el que anuncia su disponibilidad. Los anuncios de direccionador contienen una lista de prefijos usados para la determinación de enlaces activos y la configuración de direcciones autónoma. Los sistemas principales pueden usar los prefijos de enlace activo anunciados para determinar cuándo, el destino de un paquete, está en el enlace o más allá de un direccionador.

Configuración automática de direcciones

Los anuncios de direccionadores permiten a estos informar a los sistemas principales sobre cómo ejecutar la configuración automática de direcciones. Los direccionadores pueden especificar si los sistemas principales usan la configuración de direcciones autónoma (sin estado) o estatal.

Resolución de direcciones

Los direccionadores efectúan la resolución de direcciones ejecutando una difusión múltiple de un mensaje de solicitud de vecino que pide al nodo de destino que devuelva su dirección de capa de enlace. La dirección de la capa de enlace se devuelve en un anuncio de vecino de una difusión individual. Al incluir la dirección de la capa de enlace en el mensaje de solicitud de vecino, un par único de mensajes de solicitud y respuesta, el iniciador del mensaje y el destinatario pueden determinar las direcciones de la capa de enlace de ambos.

Detección de inaccesibilidad de vecinos

NDP puede detectar el fallo de un vecino o el de la vía de reenvío al vecino. Cuando no se ha recibido una confirmación positiva de un vecino para un intervalo de tiempo, el nodo ejecuta una prueba activamente en el vecino con mensajes de solicitud de vecino de una difusión invidual para verificar que la vía de acceso de reenvío sigue funcionando.

Redirección

Si la dirección de origen del paquete y del salto siguiente están en la misma red, un direccionador puede enviar un mensaje de redirección informando al remitente que el salto siguiente es un vecino.

Use el mandato **p ndp** en el indicador `Config>` para configurar parámetros de NDP.

Función de túnel de IPv6 sobre IPv4

La función de túnel de IPv6 sobre IPv4 le permite migrar de redes IPv4 a redes IPv6 sin tener que actualizar, simultáneamente, todo el equipo para dar soporte a IPv6. Esta función permite que las tramas de IPv6 crucen una red IPv4 y lleguen a un destino IPv6. La trama de IPv6 se encapsula en una trama de IPv4 y se reenvía a través de la red IPv4 a un destino IPv4 específico llamado punto final del túnel. En este punto final, se extrae el paquete de la cápsula y se reenvía al destino IPv6 final.

Añadir un túnel configurado hace que se añada una interfaz virtual. Esta interfaz se trata por IPv6 como si fuera una interfaz normal y el RIP puede usarla para el establecimiento de rutas.

Use el mandato **add tunnel** en el indicador `IPv6 Config>` para añadir un IPv6 sobre túnel IPv4.

Protocol Independent Multicast (PIM)

Protocol Independent Multicast (PIM) es un protocolo de difusión múltiple de poda y de difusión usado por IPv6. Funciona bien en redes de campus, donde la anchura de banda es abundante y los usuarios están fuertemente agrupados y no dispersos en una amplia área de redes. PIM usa un enfoque de poda y reenvío para la difusión en difusión múltiple de datagramas y se usa cuando grupos de difusión múltiple están distribuidos densamente por internet. Asume que todos los sistemas de comunicación de sentido directo desean recibir datagramas de difusión múltiple y poda hacia atrás las ramas de aquellos que no lo deseen.

PIM está basado en la modalidad de poca densidad de PIM (PIM-SM), que emplea los mismos formatos de paquete. A diferencia de DVMRP, PIM reenvía en todas las interfaces de salida hasta que se produce una poda o un truncamiento. Esto significa que PIM no mantiene sus propias tablas de direccionamientos, como hace DVMRP que usa información de padre-hijo para reducir el número de interfaces usadas antes de la poda. Una vez se ha producido ésta, el estado de poda se mantiene y los datagramas sólo se reenvían a los miembros de comunicación de sentido directo.

PIM-DM es un protocolo de estado suave. Esto significa que los estados de poda, si no se han eliminado mediante otra actividad (como, por ejemplo, injerto o empalme), se eliminan al cabo de un período de tiempo (configurable) y los datos de difusión múltiple se vuelven a difundir a todos los sistemas de comunicación de sentido directo donde se vuelve a producir la poda.

PIM-DM establece una adyacencia con direccionadores de PIM vecinos intercambiando mensajes Hello con todos los vecinos. Mantiene activa la adyacencia hasta que se agota. Mientras los direccionadores vecinos estén activos y ejecutándose, se enviarán mensajes Hello nuevos para renovar el estado Hello y evitar que la adyacencia se agote. La frecuencia de envío de los mensajes Hello se puede configurar. Mediante este mecanismo, se elige también un direccionador designado. En el caso de PIM-DM, dado que se trata de un protocolo de poda y difusión, el direccionador designado no tiene una función real. Este direccionador se usa, principalmente, para el funcionamiento de PIM-SM.

PIM-DM es totalmente independiente del protocolo de una difusión individual subyacente. Usa la tabla de direccionamientos de una difusión individual, sin tener en cuenta qué protocolo de difusión individual es propietario de una entrada, para llevar a cabo el cálculo de reenvío de vía de acceso inversa en un datagrama de difusión múltiple recibido. El reenvío de vía de acceso inversa (rpf) se usa para validar si el datagrama de difusión múltiple recibido llegó a una interfaz válida para la difusión a la dirección de origen contenida en el datagrama de difusión múltiple. Si se trata de una interfaz incorrecta, se descartará el datagrama o se creará una entrada de difusión múltiple nueva y se difundirá el datagrama de difusión múltiple al resto de las interfaces (aquellas que tengan PIM-DM activo, miembros del sistema principal local y cualquier interfaz que otros protocolos de difusión múltiple

hayan añadido). El uso de rpf para validar las interfaces de entrada requiere que el direccionamiento de difusión individual sea simétrico.

El injerto también tiene soporte para permitir que los sistemas principales se unan dinámicamente a un grupo. Esto injertará una rama a un árbol de difusión múltiple ya existente y eliminará todos los estados de poda donde sea necesario, para asegurarse de que los sistemas principales que se hayan unido reciban los datagramas de difusión múltiple de grupo solicitados.

Debido a la naturaleza independiente de PIM en relación con los protocolos de direccionamiento de difusión individual y la naturaleza de difusión de PIM-DM, pueden producirse vías de acceso paralelas de origen y reenviarse datos de difusión múltiple duplicados. PIM-DM usa un procedimiento de afirmación para elegir el direccionador de reenvío adecuado cuando esto se produce. Pueden configurarse preferencias en direccionadores que ejecutan diferentes protocolos de direccionamiento de una difusión para resolver qué direccionador se desea que tenga preferencia. Cuando el direccionamiento de una difusión individual sea el mismo, los costos métricos de una difusión individual al origen se usarán para determinar la mejor ruta. Y cuando el resto sea igual, se elegirá el direccionador que tenga la dirección de interfaz IP más grande como reenviador adecuado.

Use el mandato **p pim** en el indicador `Config>` para configurar parámetros de PIM.

Configuración y supervisión de IPv6

Este capítulo describe cómo usar los mandatos de funcionamiento y configuración de IPv6 e incluye las secciones siguientes:

Acceso al entorno de configuración de IPv6

Siga el procedimiento siguiente para acceder al proceso de configuración de IPv6.

1. En el indicador OPCON, entre **talk 6**. (Para obtener información detallada sobre este mandato, consulte *The OPCON Process and Commands* (Proceso y mandatos de OPCON) en la Software User's Guide.) Por ejemplo:

   ```
   * talk 6
   Config>
   ```

   Después de entrar el mandato **talk 6**, el indicador CONFIG (`Config>`) aparecerá en el terminal. Si el indicador no aparece cuando entre por primera vez la configuración, pulse de nuevo **Retorno**.

2. En el indicador CONFIG, entre el mandato **p ipv6** para obtener el indicador `IPv6 Config>`.

Mandatos de configuración de IPv6

Para configurar IPv6, entre los mandatos en el indicador `IPv6 Config>`.

Tabla 67. 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 xxv.
add	Añade una dirección, rutas filtradas, filtros de paquetes, ruta o túnel.
change	Cambia una dirección, rutas filtradas, filtros de paquetes, ruta o túnel.
delete	Suprime una dirección, rutas filtradas, filtros de paquetes, ruta o túnel.
disable	Inhabilita las redirecciones icmp, el filtro de paquetes o el descubrimiento de la MTU de la vía de acceso.
enable	Habilita las redirecciones ICMP, los filtros de paquetes o el descubrimiento de MTU de la vía de acceso.
list	Lista la configuración.
move	Mueve el control de acceso.
set	Establece los valores de configuración asociados a túneles automáticos, tamaños de almacenamiento intermedio de antememorias de vías de acceso de reenvío rápido, pasarelas por omisión, MLD, temporizadores de tiempo de la MTU de la vía de acceso, el tamaño del almacenamiento intermedio de ensamblaje de paquetes, el tamaño de las tablas de direccionamiento, el id de direccionadores y el tiempo de vida del direccionador.
update	Actualiza el filtro de paquetes.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxvi.

Add

Use el mandato **add** para añadir una dirección de IPv6, rutas filtradas, filtros de paquetes, rutas o túneles de IPv6 sobre IPv4.

add acess-control
address *prefijo dirección red*
leaked-routes *destino*
packet-filter *nombre interfaz*
route *coste de pasarela de la máscara de destino...*
tunnel *prefijo destino direcciónr direcciónlocal coste ttl fragmentación*

Ejemplo:

```
IPv6 config>add address
Which net is this address for [0]? 5
New address []? 1::2
Prefix length must between 8 and 128 [128]?

IPv6 config>add leaked
IPV4 destination []? 1.2.3.4
Address mask [255.0.0.0]? 255.255.255.255

IPv6 config>add packet-filter
Packet-filter name []?  pktf01
Filter incoming or outgoing traffic [IN]
Which interface is this filter for [0]? 3

IPv6 config>add route
IPv6 destination []? 8::9
Prefix length must between 8 and 128 [8]? 128
Via gateway 1 at []? 1::2
Cost [1]?
Via gateway 2 at []? 2::3
Cost [1]? 1000
Via gateway 3 at []? 3::4
Cost [1]? 10000
Via gateway 4 at []? 4::5
Cost [1]? 10
IPv6 config>add tunnel
Add a static route through this tunnel? [Yes[:
IPv6 destination network []? 3::4
Prefix length must between 0 and 128 [64]? 128
IPV4 tunnel remote address []?1.2.3.4
IPV4 tunnel local address []? 2.3.40.0
Cost [1]?
TTL value [64]?
Allow fragmentation in tunnel?(Yes or [No]):
```

access-control

Añade control de acceso

access control type

Indica lo que se hace con los paquetes que coinciden con los parámetros de la norma de control de acceso.

E — Excluyente; los paquetes que coincidan se descartarán.

I — Incluyente; los paquetes que coincidan recibirán proceso adicional del direccionador.

Internet source

Dirección Internet de origen.

Valores válidos: Cualquier dirección de internet válida

Valores por omisión: Ninguno

Source Prefix length

Especifica la longitud del prefijo de la dirección de origen de Internet.

Valores válidos: De 0 a 128

Valores por omisión: 128

Internet destination

Dirección Internet de destino.

Valores válidos: Cualquier dirección de internet válida

Valor por omisión: Ninguno

Destination Prefix length

Especifica la longitud del prefijo de la dirección de destino de Internet.

Valores válidos: De 0 a 128

Valores por omisión: 128

Starting protocol number

Especifica el número de protocolo de inicio de un rango de números de protocolo. Entre un *0* para seleccionar todos los protocolos.

Algunos números de protocolo comunes son:

1 para ICMP
6 para TCP
17 para UDP
89 para OSPF
50 para ESP-Encryption
51 para AH-Encryption

Valores válidos: de 0 a 255

Valores por omisión: 0

Ending protocol number

Especifica el número de protocolo final de un rango de números de protocolo. Entre un *0* para seleccionar todos los protocolos.

Algunos números de protocolo comunes son:

1 para ICMP
6 para TCP
17 para UDP
89 para OSPF
50 para ESP-Encryption
51 para AH-Encryption

Valores válidos: de 0 a 255

Valores por omisión: El valor especificado en el parámetro **starting protocol number**

Starting destination port number

Especifica el número del puerto de inicio de un rango de números de puerto de destino TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye 6 (para TCP) o 17 (para UDP). No se tendrán en cuenta estos parámetros para los paquetes en los cuales el número de protocolo no sea 6 ó 17.

Algunos números de puerto usados normalmente son:

21 para FTP
23 para Telnet

25 para SMTP
513 para rlogin
520 para RIP

Valores válidos: De 0 a 65535

Valor por omisión: 0

Ending destination port number
Especifica el número del puerto final de un rango de números de puerto de destino TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye 6 (para TCP) o 17 (para UDP). No se tendrán en cuenta estos parámetros para los paquetes en los cuales el número de protocolo no sea 6 ó 17.

Algunos números de puerto usados normalmente son:

21 para FTP
23 para Telnet
25 para SMTP
513 para rlogin
520 para RIP

Valores válidos: De 0 a 65535

Valores por omisión: El valor especificado como **starting destination port number**

Starting source port number
Especifica el número del puerto de inicio de un rango de números de puerto de origen TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye 6 (para TCP) o 17 (para UDP). No se tendrán en cuenta estos parámetros para los paquetes en los cuales el número de protocolo no sea 6 ó 17. Consulte la descripción de **starting destination port number** para obtener una lista de los números de puerto TCP/UDP más usados.

Valores válidos: De 0 a 65535

Valor por omisión: 0

Ending source port number
Especifica el número del puerto final de un rango de números de puerto de origen TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye 6 (para TCP) o 17 (para UDP). No se tendrán en cuenta estos parámetros para los paquetes en los cuales el número de protocolo no sea 6 ó 17. Consulte la descripción de **starting destination port number** para obtener una lista de los números de puerto TCP/UDP más usados.

Valores válidos: De 0 a 65535

Valor por omisión: El valor especificado como **starting source port number**

address Añade una dirección de IPv6.

Which net is this address for

Especifica la red a la que se añadirá la dirección IPv6.

Valores válidos: Un valor numérico que identifique una interfaz de red

Valor por omisión: 0

New address

Especifica la dirección de IPv6 nueva que se añadirá.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Prefix length

Valor decimal que especifica cuántos de los bits contiguos situados en el extremo izquierdo de la dirección forman el prefijo.

Valores válidos: De 8 a 128

Valor por omisión: 128

leaked-routes

Añade una ruta filtrada.

IPV4 destination

Especifica la dirección de IPv6 del destino de la ruta filtrada.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

packet-filter

Añade un filtro de paquetes

packet-filter name

Especifica un nombre alfanumérico usado para identificar el filtro de paquetes.

Valores válidos: Cualquier serie de caracteres alfanumérica que tenga un máximo de 16 caracteres

Valor por omisión: Ninguno

Filter incoming or outgoing traffic?

Especifica si desea filtrar el tráfico de entrada o de salida.

Valores válidos: OUT (salida) o IN (entrada)

Valor por omisión: IN

which interface is this filter for

Especifica el número de la interfaz de red a la que se añadirá el filtro de paquetes.

Valores válidos: Un valor numérico que identifique las interfaces para las que IPv6 sea un protocolo válido o “a”, que especifica que este filtro es para el túnel automático.

Valor por omisión: 0

route Añade una ruta.

IPv6 destination
Especifica la dirección de IPv6 del destino de la ruta.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Prefix length
Especifica la máscara que se aplicará a la dirección de destino.

Valores válidos: De 8 a 128 (0 está permitido si el destino IPv6 es 0::0)

Valor por omisión: 8

Via gateway 1
Especifica la dirección de IPv6 de la pasarela 1.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Cost Especifica el coste de esta ruta.

Valores válidos: Un valor numérico

Valor por omisión: 1

Via gateway 2
Especifica la dirección de IPv6 de la pasarela 2.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Cost Especifica el coste de esta ruta.

Valores válidos: Un valor numérico

Valor por omisión: 1

Via gateway 3
Especifica la dirección de IPv6 de la pasarela 3.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Cost Especifica el coste de esta ruta.

Valores válidos: Un valor numérico

Valor por omisión: 1

Via gateway 4
Especifica la dirección de IPv6 de la pasarela 4.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Cost Especifica el coste de esta ruta.

Valores válidos: Un valor numérico

Valor por omisión: 1

tunnel Añade un túnel.

Add a static route through this tunnel?
Especifica si el túnel tendrá o no una ruta estática definida.

Valores válidos: Yes (Sí) o No

Valor por omisión: Yes

IPv6 destination network
Especifica la dirección de IPv6 de la red de destino a la que se accederá mediante el túnel.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Prefix length
Valor decimal que especifica cuántos bits contiguos situados más a la izquierda de la dirección de IPv6 forman el prefijo.

Valores válidos: De 8 a 128

Valor por omisión: 64

IPv4 tunnel remote address
Especifica la dirección de IPv4 de las tramas IPv6 que han pasado por el túnel.

Valores válidos: Cualquier dirección IP válida (32 bits)

Valor por omisión: Ninguno

IPv4 tunnel local address
Especifica la dirección de origen de IPv4 para las tramas de IPv6 que han atravesado el túnel.

Valores válidos: Cualquier dirección IP válida (32 bits)

Valor por omisión: Ninguno

Cost Especifica el coste asociado con el túnel que se usará durante las búsquedas de ruta para encontrar la mejor ruta al destino.

Valores válidos: De 1 a 255

Valor por omisión: 1

TTL value
Especifica el valor de tiempo de vida usado en las tramas encapsuladas para este túnel

Valores válidos: Cualquier valor numérico del rango situado entre 1 y 255

Valor por omisión: 64

Allow fragmentation in the tunnel?
Especifica si estará permitida la fragmentación en el túnel. Si especifica *yes* estará permitida la fragmentación en el túnel, en el caso de que la red IPv4 que esté usando éste no proporcione la información suficiente para que el dispositivo devuelva un mensaje “Packet Too Big” (Paquete demasiado grande) al sistema principal de IPv6.

Valores válidos: yes o no

Valor por omisión: no

Change

Use el mandato **change** para añadir un registro de control de acceso, una dirección de IPv6, rutas filtradas, filtros de paquetes, rutas o túneles.

Sintaxis:

change
access-control *índice*
address *prefijo dirección red*
leaked-routes *destino*
packet-filter *nombre interfaz*
route *coste de pasarela de la máscara de destino...*
tunnel *prefijo destino direcciónr direcciónlocal coste ttl fragmentación*

access-control
Cambia la configuración del control de acceso.

address Cambia una dirección.

leaked-routes
Cambia la configuración de una ruta filtrada.

packet-filter
Cambia la configuración de un filtro de paquetes.

route Cambia la configuración de una ruta.

tunnel Cambia la configuración de un túnel.

Consulte “Add” en la página 412 para obtener una descripción de los parámetros asociados al mandato **change**.

Delete

Use el mandato **delete** para eliminar un registro de control de acceso, una dirección, rutas filtradas, filtros de paquetes, rutas o túneles.

Sintaxis:

delete
access-control *índice*
address *dirección*
leaked-routes *destino*
packet-filter *nombre*
route *pasarela máscara destino*
tunnel *núm.túnel*

Disable

Use el mandato **disable** para inhabilitar la redirección ICMP, filtros de paquetes y path MTU discovery.

Sintaxis:

disable
icmp-redirect *dirección*
packet-filter *nombre-filtro-paquetes*
path-mtu-discovery

icmp-redirect
Inhabilita las redirecciones de ICMP.

packet-filter
Inhabilita un filtro de paquetes.

packet-filter name
Especifica el nombre del filtro de paquetes que se inhabilitará.

Valores válidos: Cualquier filtro de paquete configurado

Valor por omisión: Ninguno

path-mtu-discovery
Inhabilita Path MTU Discovery.

Enable

Use el mandato **enable** para habilitar redirecciones de ICMP, filtros de paquetes o path MTU discovery.

Sintaxis:

enable icmp-redirect *dirección*
packet-filter *nombre-filtro-paquetes*
path-mtu-discovery

icmp-redirect
Habilita las redirecciones de ICMP.

interface address
Especifica la dirección de la interfaz.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Null (nulo) (especifica todas las direcciones)

packet-filter
Habilita un filtro de paquetes.

packet-filter name
Especifica el nombre del filtro de paquetes que se habilitará. Este nombre se configura usando el mandato **add packet-filter**.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

path-mtu-discovery
Habilita Path MTU Discovery, un protocolo que permite a un nodo de sistema principal determinar el paquete de tamaño máximo que seguirá un recorrido a un destino sin que sea necesario fragmentarlo.

List

Use el mandato **list** para visualizar la configuración de IPv6.

Sintaxis:

list all
access-control
addresses
icmp-redirect
leaked-routes
mld
packet-filter
routes
sizes
tunnels

Ejemplo:

```
IPv6 config>list all
Interface addresses
IPv6 addresses for each interface:
   intf  0                                    IP disabled on this interface
   intf  1                                    IP disabled on this
interface
   intf  2                                    IP disabled on this
interface
   intf  3                                    IP disabled on this interface
   intf  4                                    IP disabled on this interface
   intf  5   1234:1234:1234:1234:5234:6234:7234:8234/128
             1223::7:1234/8
Router-ID: 1::9
Internal IP address: 1::8

Routing

route to: 1234::1223/128
     via: 1234:0:9::8                          cost: 100
     via: 1234:0:9:8:8:7:6:8                   cost: 232
     via: 1:2:3:4:5:6:7:8                      cost: 1
     via: 8:7:6:5:4:3:2:1                      cost: 1
route to: ::/0
     via: 1::8                                 cost: 100
route to: 2::8:9/8
     via: 1::8                                 cost: 1



Path MTU Discovery:  disabled
Path MTU Aging Timer:  10 minutes


Access Control is:   enabled
```

```
IPv6 config>list addresses
IPv6 addresses for each interface:
   intf  0                                      IP disabled on this interface
   intf  1                                      IP disabled on this
interface
   intf  2                                      IP disabled on this
interface
   intf  3                                      IP disabled on this interface
   intf  4                                      IP disabled on this interface
   intf  5   1234:1234:1234:1234:5234:6234:7234:8234/128
             1223::7:1234/8
Router-ID: 1::9
Internal IP address: 1::8
IPv6 config>list icmp-redirect
ICMP Redirect generation for IP interface:
   intf  0                                      IP disabled on this interface
   intf  1                                      IP disabled on this
interface
   intf  2                                      IP disabled on this
interface
   intf  3                                      IP disabled on this interface
   intf  4                                      IP disabled on this interface
   intf  5   1234:1234:1234:1234:5234:6234:7234:8234/128 ICMP Redirect enabled
                                      1223::7:1234/8 ICMP Redirect enabled
   intf  6                                      IP disabled on this interface
   intf  7                                      IP disabled on this interface
```

```
IPv6 config>list leaked-routes
#  IPv4 Address     Mask
IPv6 config>list mld
Net      Query Interval      Response Interval      Leave Query Interval
             (secs)                (secs)                 (secs)
---      --------------      -----------------      --------------------

 5            125                    10                     1

IPv6 config>list packet-filter

List of packet-filter records:

Name               Interface   State
packet01           0           On
pack01             5           On
Access Control is: enabled
IPv6 config>list routes

route to: 1234::1223/128
     via: 1234:0:9::8                          cost: 100
     via: 1234:0:9:8:8:7:6:8                   cost: 232
     via: 1:2:3:4:5:6:7:8                      cost: 1
     via: 8:7:6:5:4:3:2:1                      cost: 1
route to: ::/0
     via: 1::8                                 cost: 100
route to: 2::8:9/8
     via: 1::8                                 cost: 1

IPv6 config>list sizes

Routing table size: 768 nets (79872 bytes)
Reassembly buffer size: 12000 bytes
Routing cache size: 64 entries
Time to live: 64
Path MTU aging timer: 10

IPv6 config>list tunnel
Tun#  Remote Endpoint  Local Endpoint   Frag Allowed   TTL  Cost Net#  IPv6 Address/Prefix
 1    1.2.3.4          2.3.4.5               No        100    100  7   1:2:3:4:5:6:7:8/128
IPv6 config>
```

Move

Use el mandato **move** para cambiar el orden de los registros de control de acceso configurados.

Sintaxis:

move access-control

Index of control to move
Seleccione el número de índice del registro de control de acceso que desea mover.

Move record AFTER record number
Seleccione el número de índice del registro de control de acceso que desea que este registro siga.

Are you sure that this is what you want to do
Le permite confirmar que la instrucción de movimiento es correcta.

Set

Use el mandato **set** para establecer parámetros de configuración.

Sintaxis:

set access-control
automatic-tunnel-parameters *ttl/fragmentación/cuenta saltos*
cache-size *núm.entradas*
default *...*
internal-ip-address
mld *...*
path-mtu-aging-timer
reassembly-size
router-id
routing *núm.redes*
ttl

Ejemplo:

```
IPv6 config>set au
TTL value [64]?
Allow fragmentation in tunnel?(Yes or [No]):

IPv6 config>set ca
number of cache entries [64]?

IPv6 config>set mld query-interval
Network interface [0]? 5
New Query Interval (in secs) [125]?

IPv6 config>set mld response-interval
Network interface [0]? 5
New Response Interval (in secs) [10]?

IPv6 config>set mld robust
Network interface [0]? 5
New Robustness Variable [2]?
IPv6 config>set mld leave
Network interface [0]?
New Leave Interval (in secs) [1]?
IPv6 config>?
```

access-control

Especifica si el control de acceso está habilitado o inhabilitado.

Valores válidos: on (activo) u off (inactivo)

Valor por omisión: off

automatic-tunnel-parameters

Especifica los valores del parámetro de túnel para los túneles automáticos que fluyen a través del direccionador.

ttl value Especifica el valor del tiempo de vida de las tramas encapsuladas para el túnel.

Valores válidos:

Valor por omisión: 64

allow fragmentation in tunnel?
Especifica si estará permitida la fragmentación en el túnel. Si especifica *yes* estará permitida la fragmentación en el túnel, en el caso de que la red IPv4 que esté usando éste no proporcione la información suficiente para que el dispositivo devuelva un mensaje “Packet Too Big” (Paquete demasiado grande) al sistema principal de IPv6.

Valores válidos: yes o no

Valor por omisión: no

hop count
Especifica la cuenta de saltos que se usará en los paquetes que se ponen en túnel automáticamente.

Valores válidos: De 1 a 255

Valor por omisión: 64

cache-size
Especifica el tamaño de almacenamiento intermedio para la antememoria de la vía de acceso de reenvío rápido.

number of cache entries
Especifica el número de entradas de la antememoria de la vía de acceso de reenvío rápido.

Valores válidos De 64 a 10 000

Valor por omisión: 64

default network-gateway

default gateway

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

gateway's cost
Especifica el coste asociado a esta pasarela.

Valores válidos: De 1 a 255

Valor por omisión: 1

default subnet-gateway

for which subnetted network

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: ninguno

default gateway

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: ninguno

gateway's cost

Especifica el coste asociado a esta pasarela.

Valores válidos: De 1 a 255

Valor por omisión: 1

internal-ip-address

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

mld

query-interval

network interface

Valores válidos: Cualquier número de interfaz de red válido

Valor por omisión: 0

new query interval (in secs)

Valores válidos: De 1 a 3600

Valor por omisión: 125

response-interval

network interface

Valores válidos: Cualquier número de interfaz de red válido

Valor por omisión: 0

new response interval (in secs)

Valores válidos: De 1 a 60

Valor por omisión: 10

robustness-variable

network interface

Valores válidos: Cualquier número de interfaz de red válido

Valor por omisión: 0

new robustness variable

Valores válidos: De 2 a 10

Valor por omisión: 2

leave-interval

network interface

Valores válidos: Cualquier número de interfaz de red válido

Valor por omisión: 0

new leave interval (in secs)

Valores válidos: De 1 a 60

Valor por omisión: 1

path-mtu-aging-timer
Especifica la antigüedad, en minutos, de las MTU de las vías de acceso determinadas usando path MTU discovery.

Valores válidos: De 10 a 60 minutos, donde 0 = inhabilitar

Valor por omisión: 10

reassembly-size
Especifica el tamaño del ensamblaje de almacenamientos intermedios usados para procesar la cabecera del fragmento.

Valores válidos: De 2048 a 65536

Valor por omisión: 12000

router-id Especifica la dirección de IPv6 del direccionador.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

routing table-size

number of nets

Valores válidos: De 64 a 65 535

Valor por omisión: 768

ttl Especifica el valor del tiempo de vida de IPv6.

Valores válidos:

Valor por omisión: 64

Update

Use el mandato **update** para actualizar el filtro de paquetes

Sintaxis:

u**pdate** p**acket-filter**

packet-filter

Use este mandato para acceder al indicador del mandato `Packet-filter 'xx' Config>` desde el que puede configurar filtros de paquetes.

Mandatos de actualización del filtro de paquetes

Tabla 68. Resumen de los mandatos de configuración del filtro de paquetes

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxv.
Add	Añade control de acceso.
Change	Cambia el control de acceso.
Delete	Suprime un control de acceso.
Move	Reordena la lista de control de acceso aplicada al filtro de paquetes.
List	
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxvi.

Add

Use el mandato **update packet-filter add** para añadir una lista de control de accesos.

Sintaxis:

add access-control *tipo dirorigen prefijorigen dirdest prefijodest*

access-control

Añade un elemento de control de acceso a la lista de control de acceso.

Type Especifica si el control de acceso es incluyente o excluyente.

Valores válidos: I o E

Valor por omisión: I

Internet source

Especifica la dirección de IPv6 del origen del paquete.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Prefix length

Valor decimal que especifica cuántos bits contiguos situados más a la izquierda de la dirección de IPv6 forman el prefijo.

Valores válidos: De 0 a 128

Valor por omisión: 128

Internet destination

Especifica la dirección de IPv6 del destino del paquete.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Prefix length

Valor decimal que especifica cuántos bits contiguos situados más a la izquierda de la dirección de IPv6 forman el prefijo.

Valores válidos: De 0 a 128

Valor por omisión: 128

Starting protocol number

Especifica el número de protocolo de inicio de un rango de números de protocolo. Entre un *0* para seleccionar todos los protocolos.

Algunos números de protocolo comunes son:

1 para ICMP
6 para TCP
17 para UDP
89 para OSPF
50 para ESP-Encryption
51 para AH-Encryption

Valores válidos: de 0 a 255

Valores por omisión: 0

Ending protocol number

Especifica el número de protocolo final de un rango de números de protocolo. Entre un *0* para seleccionar todos los protocolos.

Algunos números de protocolo comunes son:

1 para ICMP
6 para TCP
17 para UDP
89 para OSPF
50 para ESP-Encryption
51 para AH-Encryption

Valores válidos: de 0 a 255

Valores por omisión: el valor especificado en el parámetro **starting protocol number**

Starting destination port number

Especifica el número del puerto de inicio de un rango de números de puerto de destino TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye 6 (para TCP) o 17 (para UDP). No se tendrán en cuenta estos parámetros para los paquetes en los cuales el número de protocolo no sea 6 ó 17.

Algunos números de puerto usados normalmente son:

21 para FTP
23 para Telnet
25 para SMTP
513 para rlogin
520 para RIP

Valores válidos: De 0 a 65535

Valor por omisión: 0

Ending destination port number

Especifica el número del puerto final de un rango de números de puerto de destino TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye 6 (para TCP) o 17 (para UDP). No se tendrán en cuenta estos parámetros para los paquetes en los cuales el número de protocolo no sea 6 ó 17.

Algunos números de puerto usados normalmente son:

21 para FTP
23 para Telnet
25 para SMTP
513 para rlogin
520 para RIP

Valores válidos: De 0 a 65535

Valores por omisión: el valor especificado como **starting destination port number**

Starting source port number

Especifica el número del puerto de inicio de un rango de números de puerto de origen TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye 6 (para TCP) o 17 (para UDP). No se tendrán en cuenta estos parámetros para los paquetes en los cuales el número de protocolo no sea 6 ó 17. Consulte la descripción de **starting destination port number** para obtener una lista de los números de puerto TCP/UDP más usados.

Valores válidos: De 0 a 65535

Valor por omisión: 0

Ending source port number

Especifica el número del puerto final de un rango de números de puerto de origen TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye 6 (para TCP) o 17 (para UDP). No se tendrán en cuenta estos parámetros para los paquetes en los cuales el número de protocolo no sea 6 ó 17. Consulte la descripción de **starting destination port number** para obtener una lista de los números de puerto TCP/UDP más usados.

Valores válidos: De 0 a 65535

Valor por omisión: el valor especificado como **starting source port number**

Change

Use el mandato **update packet-filter change** para cambiar el control de acceso.

Sintaxis:

change access-control *tipo dirorigen prefijorigen dirdest prefijodest*

access-control

Cambia un elemento del control de acceso.

Type Especifica si el elemento del control de acceso es incluyente o se usa para identificar paquetes a asegurar.

Valores válidos: I o S

Valor por omisión: I

Internet source

Especifica la dirección de IPv6 del origen del paquete.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Prefix length

Valor decimal que especifica cuántos bits contiguos situados más a la izquierda de la dirección de IPv6 forman el prefijo.

Valores válidos: De 0 a 128

Valor por omisión: 128

Internet destination

Especifica la dirección de IPv6 del destino del paquete.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Prefix length

Valor decimal que especifica cuántos bits contiguos situados más a la izquierda de la dirección de IPv6 forman el prefijo.

Valores válidos: De 0 a 128

Valor por omisión: 128

Delete

Use el mandato **update packet-filter delete** para eliminar un elemento de control de acceso de la lista de control de acceso.

Sintaxis:

delete access-control *núm.índice*

access-control

Suprime un control de acceso.

index of access control to be deleted

Especifica el índice de la configuración del control de acceso a eliminar.

Valores válidos: 1 para el número de registros de control de acceso definidos para este filtro de paquetes

Valor por omisión: 1

Move

Use el mandato **update packet-filter move** para volver a ordenar la lista de control de acceso aplicada al filtro de paquetes.

Sintaxis:

move access-control *núm.índice despuésnúm.*

access-control

index of control to move

Valores válidos: 1 para el número de registros de control de acceso definidos para este filtro de paquetes

Valor por omisión: 1

Move record after record number

Especifica la ubicación de destino en la lista de control de acceso. Se le solicitará que verifique que se trata de la acción que desea configurar.

Valores válidos: 1 para el número de registros de control de acceso definidos para este filtro de paquetes

Valor por omisión: 0

List

Use el mandato **update packet-filter list** para visualizar la configuración de la lista de control de acceso.

Sintaxis:

list access-controls

Ejemplo:

```
Packet-filter 'x' Config> li acc
Access control is : enabled
List of access control records:

1   Type=IS   Source=2001:1::6101/128
              Dest=  2001:1::86/128
              Tid=3

2   Type=I    Source=::/0
              Dest=::/0

Packet-filter 'x' Config>
```

Acceso al entorno de supervisión de IPv6

Siga el procedimiento siguiente para acceder a los mandatos de configuración de IPv6. Este proceso le dará acceso al proceso de supervisión de IPv6.

1. En el indicador OPCON, entre **talk 5**. (Para obtener información más detallada sobre este mandato, consulte el capítulo titulado “The OPCON Process and

Commands" (Los mandatos y el proceso OPCON) en el manual *Software User's Guide*.) Por ejemplo:

```
* talk 5
+
```

Después de entrar el mandato **talk 5**, el indicador de GWCON (+) aparecerá en el terminal. Si el indicador no aparece cuando entre por primera vez la configuración, pulse de nuevo **Retorno**.

2. En el indicador +, entre el mandato **p ipv6** para obtener el indicador `ipv6>`.

   Ejemplo:

```
+ p ipv6
ipv6>
```

Mandatos de supervisión de IPv6

Esta sección describe los mandatos de supervisión de IPv6.

Tabla 69 (Página 1 de 2). Resumen de los mandatos de supervisión de IPv6

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxv.
access-control	Muestra los registros de control de acceso.
cache	Muestra las entradas de la antememoria.
counters	Visualiza los contadores
dump routing tables	Vuelca las tablas de direccionamientos configuradas.
interface addresses	Muestra las direcciones definidas en la interfaz.
internal address	Muestra la dirección interna especificada.
mcast	Muestra una lista de las direcciones de difusión múltiple registradas.
mld	Muestra los parámetros o contadores de MLD.
reset	Restablece la interfaz de IPv6.
route	
sizes	Muestra los tamaños de los almacenamientos intermedios.
sniffer	Establece diversas opciones de rastreo.
static routes	Muestra rutas estáticas.
packet-filter	Muestra filtros de paquetes configurados.
path-mtu	
ping6	Activa el Ping.
traceroute6	Rastrea dinámicamente una ruta.
tunnels	Muestra los túneles configurados.

Tabla 69 (Página 2 de 2). Resumen de los mandatos de supervisión de IPv6	
Mandato	Función
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxvi.

Access-control

Use el mandato **access-control** para supervisar los registros de control de acceso configurados.

Sintaxis:

a**ccess-control**

Cache

Use el mandato **cache** para visualizar.

Sintaxis:

ca**che**

Ejemplo:

```
IPv6>cache
Destination                                Usage        Next hop
```

Counters

Use el mandato **counters** para visualizar el estado de los contadores.

Sintaxis:

co**unters**

Ejemplo:

```
IPv6>counters
Routing errors
Count  Type
   0   Routing table overflow
   0   Net unreachable
   0   Bad subnet number
   0   Bad net number
   0   Unhandled broadcast
   0   Unhandled anycast
   0   Unhandled directed broadcast
   0   Attempted forward of LL broadcast
0
   0   None

Packets discarded through filter  0
IP multicasts accepted:           0

IP input packet overflows
    Net   Count
   ATM/0  0
 NHRPL/0  0
    TKR/0  0
   TKR/1  0
    FR/0  0
   PPP/0  0
  IP64/0  0
```

Vuelco de tablas de direccionamiento

Use el mandato **dump** para visualizar las tablas de direccionamientos configuradas.

Sintaxis:

d**ump**

Ejemplo:

```
IPv6>dump
Type   Dest net/Prefix            Cost     Age       Next hop(s)

Stat*  1:2:3:4:5:6:7:8/128               100 30        IP64/0

IPv6 Routing table size: 768 nets (79872 bytes), 1 nets known
                      0 nets hidden, 0 nets deleted, 0 nets inactive
                      0 routes used internally, 767 routes free
```

Direcciones de interfaz

Use el mandato **interface** para visualizar las direcciones configuradas en la interfaz.

Sintaxis:

interf**ace**

Ejemplo:

```
IPv6>interface

                         IPV6  IPV6    ICMP    IPV6
Interface    Net:Status  State MTU     redir   Address/Prefixlen
   Eth/0      0 : DWN    DWN   1500    Enabled 2003:6:14:1::610/64
   Eth/1      1 : DWN    DWN   1500    Enabled 2003:7:6:1::610/64
  IP64/0      3 : UP     UP    2048    Enabled FE80::14FF:FE80:3/64
```

Dirección interna

Use el mandato **internal** para visualizar la dirección interna especificada.

Sintaxis:

intern**al**

Mcast

Use el mandato **mcast** para visualizar las direcciones de difusión múltiple configuradas.

Sintaxis:

mc**ast**

Ejemplo:

```
IPv6>mcast
List of IPV6 registered multicast addresses



 Interface: Eth/0:

      Address/Ref_Cnt
      FF02::1/1
      FF02::2/1
      FF02::1:FF00:610/1
      FF02::1:FF02:6200/1
      FF02::9/1
```

Mld

Use el mandato **mld** para visualizar lo configurado.

Sintaxis:

ml**d** 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

Use el mandato **reset** para restablecer dinámicamente la interfaz IPv6.

Sintaxis:

re**set** ipv6

Ejemplo:

```
IPv6>reset ipv6
```

Route

Use el mandato **route** para mostrar la ruta a la dirección de IPv6.

Sintaxis:

r**oute** *dirección*

Ejemplo:

```
IPv6>route 6::9
IPv6>
```

Sizes

Use el mandato **sizes** para visualizar los tamaños de los almacenamientos intermedios configurados.

Sintaxis:

si**zes**

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

Use el mandato **sniffer** para establecer las diferentes opciones de rastreo.

Sintaxis:

s**niffer** mandato de rastreo

Elija el **mandato de rastreo** en la lista siguiente:

1 List current traces (Lista los rastreos actuales)

2 Trace source address (Rastreo de la dirección de origen)

3 Trace destination address (Rastreo de la dirección de destino)

4 Trace protocol (Rastreo de protocolo)

5 Trace TCP source port (Rastreo del puerto de origen del TCP)

6 Trace TCP destination port (Rastreo del puerto de destino del TCP)

7 Trace UDP source port (Rastreo del puerto de origen del UDP)

8 Trace UDP destination port (Rastreo del puerto de destino del UDP)

9 Clear trace (Borrar el rastreo)

10 Exit (Salida)

Rutas estáticas

Use el mandato **static** para visualizar las rutas estáticas configuradas.

Sintaxis:

st**atic**

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

Use el mandato **packet-filter** para visualizar un resumen de los filtros de paquetes configurados.

Sintaxis:

pac**ket-filter**

Ejemplo:

```
IPv6>pac
Name               Dir  Intf  State  #Access-Controls
packet01           Out  0     On     0
pack01             Out  5     On     2
IPv6>
```

Path-mtu

Use el mandato **path-mtu** para mostrar las vías de acceso identificadas como poseedoras de una MTU inferior al tamaño de un paquete enviado por la vía de acceso.

Sintaxis:

pa**th-mtu**

Ejemplo:

Ping6

Use el mandato **ping6** para ejecutar un ping a una dirección de IPv6.

Sintaxis:

ping**6**

Ejemplo:

```
IPv6>ping
Destination IPv6 address [::]? 8::9
Source IPv6 Address [1::8]?
Ping data size in bytes [56]?
Ping TTL [64]?
Ping rate in seconds [1]?
PING6 1::8 -> 8::9: 56 data bytes, ttl=64, every 1 sec.

----8::9 PING6 Statistics----
36 packets transmitted, 36 packets received
```

Destination IPv6 address

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Source IPv6 address

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Ping data size in bytes

Valores válidos: De 0 al tamaño del almacenamiento intermedio global

Valor por omisión: 56

Ping ttl Especifica el tiempo de vida restante del ping.

Valores válidos: De 1 a 255

Valor por omisión: 64

Ping rate in seconds

Especifica la frecuencia del ping.

Valores válidos: De 1 a 60

Valor por omisión: 1

Traceroute6

Use el mandato **traceroute6** para rastrear dinámicamente una ruta.

Sintaxis:

t**raceroute6 ...**

Ejemplo:

```
IPv6>traceroute6
Destination IPv6 address []? 7::8
Source IPv6 address []? 6::9
Data size in bytes [56]?
Number of probes per hop [3]?
Wait time between retries in seconds [3]?
Maximum TTL [32]?
TRACEROUTE6 7::8: 56 data bytes
 1 * * * *
IPv6>
```

Destination IPv6 address

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Source IPv6 address

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Data size in bytes

Valores válidos: De 0 al tamaño del almacenamiento intermedio global

Valor por omisión: 56

Number of probes per hop

Valores válidos: De 1 a 10

Valor por omisión: 3

Wait time between retries in seconds

Valores válidos: De 1 a 60

Valor por omisión: 3

Maximum ttl

Valores válidos: De 1 a 255

Valor por omisión: 32

Tunnels

Use el mandato **tunnels** para visualizar los túneles configurados.

Sintaxis:

tu**nnels**

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>
```

Configuración y supervisión de Neighbor Discovery Protocol (NDP)

En cada interfaz se configura NDP. Este capítulo describe cómo usar los mandatos de funcionamiento y de configuración de NDP e incluye las secciones siguientes:

- "Acceso al entorno de configuración de NDP"
- "Mandatos de configuración de NDP"
- "Acceso al entorno de supervisión de NDP" en la página 449
- "Mandatos de supervisión de NDP" en la página 450

Acceso al entorno de configuración de NDP

Siga el procedimiento siguiente para acceder al proceso de configuración de NDP.

1. En el indicador OPCON, entre **talk 6**. (Para obtener información detallada sobre este mandato, consulte *The OPCON Process and Commands* en el manual Software User's Guide.) Por ejemplo:

   ```
   * talk 6
   Config>
   ```

   Después de entrar el mandato **talk 6**, el indicador CONFIG (`Config>`) aparecerá en el terminal. Si el indicador no aparece cuando entre por primera vez en la configuración, pulse de nuevo **Retorno**.

2. En el indicador CONFIG, entre el mandato **p ndp** para obtener el indicador `NDP6 Config>`.

Mandatos de configuración de NDP

Para configurar NDP, entre los mandatos en el indicador `NDP6 Config>`.

Tabla 70. Resumen de mandatos de configuración de NDP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxv.
add	Añade un anuncio de direccionador o parámetros.
change	Cambia un anuncio de direccionador o parámetros.
delete	Suprime un anuncio de direccionador o parámetros.
disable	Inhabilita el anuncio del direccionador.
enable	Habilita el anuncio del direccionador.
list	Lista la configuración.
set	Establece la cuenta de saltos de DHCP.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxvi.

Add

Use el mandato **add** para añadir un anuncio de direccionador.

add ra ...
dhcp-server

ra Añade un anuncio de direccionador.

add router advertisement on which interface
Especifica la interfaz a la que se añadirá el anuncio del direccionador.

Valores válidos: Un valor numérico que identifique una interfaz de red

Valor por omisión: 0

Managed address configuration (stateful)
Especifica si los sistemas principales usan el protocolo administrado para la configuración automática de direcciones además de las direcciones configuradas automáticamente con la configuración automática sin estado.

Valores válidos: yes (sí) o no

Valor por omisión: no

Si especifica *yes*, el agente de retardo de DHCPv6 permitirá que los sistemas principales usen direcciones de enlace locales en el momento de la configuración de direcciones, incluso aunque el servidor DHCPv6 no esté en el mismo enlace.

Other stateful configuration
Especifica si los sistemas principales usan el protocolo administrado para la configuración automática de otra información (no de direcciones).

Valores válidos: yes (sí) o no

Valor por omisión: no

Include link layer address with router advertisement
Especifica si se ha de incluir la dirección de la capa de enlace en el anuncio del direccionador. Un direccionador puede omitir la dirección de la capa del enlace en el anuncio del direccionador para habilitar la compartición de carga de entrada por varias direcciones de capas de enlace.

Valores válidos: yes (sí) o no

Valor por omisión: yes

Hop limit Especifica el valor por omisión que se pondrá en el campo de límite de saltos de los mensajes de anuncio que el direccionador envía. Este valor se usa en el campo de cuenta de saltos de la cabecera IP para los paquetes IP de salida.

Valores válidos: De 0 a 255, donde 0 significa que este direccionador no especifica

Valor por omisión: 0

Maximum router advertisement interval
Especifica el tiempo máximo, en segundos, permitido entre el envío de anuncios del direccionador en difusión múltiple y sin solicitar, desde la interfaz.

Valores válidos: De 4 a 1800 segundos

Valor por omisión: 600

Minimum router advertisement interval
Especifica el tiempo mínimo, en segundos, permitido entre el envío de anuncios del direccionador en difusión múltiple y sin solicitar, desde la interfaz.

Valores válidos: De 3 a (.75 * *Maximum router advertisement interval*)

Valor por omisión: *Maximum router advertisement interval*/3

Router lifetime
Especifica el tiempo, en segundos, durante el cual se usará el direccionador como direccionador por omisión.

Valores válidos: De 0 ó 4 a 9000 segundos, donde 0 indica que el direccionador no se usa como direccionador por omisión

Valor por omisión: (3 * *Maximum router advertisement interval*)

Reachable Time
Especifica el tiempo, en segundos, en que un nodo asume que un vecino es accesible, después de haber recibido confirmación de accesibilidad.

Valores válidos: De 0 a 3600 segundos, donde el 0 indica sin especificar por este direccionador

Valor por omisión: 0

Retransmit timer
Especifica el tiempo, en segundos, entre los mensajes de solicitud de vecino retransmitidos.

Valores válidos: De 0 a 3600 segundos, donde el 0 indica sin especificar por este direccionador

Valor por omisión: 0

link-mtu Especifica el valor que se pondrá en las opciones de MTU enviadas por el direccionador. Este valor debe enviarse a enlaces que tienen una MTU variable y puede enviarse a otros enlaces.

Valores válidos: Un entero de 32 bits sin signo, donde el 0 indica que no se envía ninguna opción de MTU

Valor por omisión: 0

dhcp-server
Añade un servidor DHCP.

server addresses

Especifica una lista de direcciones de difusión individual del servidor de IPv6 que se usarán para reenviar el mensaje de solicitud DHCPv6 inicial. Si no se especifica ninguna dirección, el agente de relé DCHPv6 envía el paquete a las direcciones de difusión múltiple de los servidores de DHCP.

Nota: Si usa la dirección de servidores de difusión múltiple, deberá habilitar el direccionamiento de difusión múltiple en la caja habilitando y configurando Protocol Independent Multicast (PIM). Consulte “Configuración y supervisión de Protocol Independent Multicast Routing Protocol (PIM)” en la página 453 para obtener más información.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Change

Use el mandato **change** para cambiar un anuncio de ruta o un prefijo.

Sintaxis:

change ra ...
prefix ...

ra Cambia un anuncio de una ruta configurada. Consulte “Add” en la página 444 para obtener una descripción de los parámetros asociados al mandato **change ra**.

prefix Cambia un prefijo configurado. Los prefijos se añaden y se suprimen a medida que modifica la configuración de la dirección de IPv6. Consulte “Add” en la página 412 para obtener más información sobre cómo añadir direcciones de IPv6.

Para añadir un prefijo:

```
Config> p IPv6
IPv6 user configuration
IPv6 config> add addr
Which net is this address for [0]? 5
New address []? 2002:9::6204
Prefix length must be between 8 and 128 [128]? 64
IPv6 config> exit
```

Para cambiar un prefijo:

```
Config> p ndp6
Neighbor Discovery for IPv6 user configuration
NDP6 Config> change prefix
Change Prefix Information option for which Prefix address []? 2002:2::
Use this prefix for on-link determination? [Yes]:
Use this prefix for autonomous address configuration? [Yes]: n
Valid lifetime for Prefix [2592000]? 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 la dirección de IPv6 que se pondrá en la opción de información del prefijo, en los anuncios del direccionador enviados desde la interfaz.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Use this prefix for on-link determination?
Especifica el valor que se pondrá en el indicador de dentro del enlace en la opción de información del prefijo. Cuando se establece en *yes* (sí), puede usarse el prefijo para la determinación de dentro del enlace. Cuando se establece en *no*, el anuncio no indicará nada sobre las propiedades de dentro del enlace y de fuera del enlace, del prefijo.

Valores válidos: yes (sí) o no

Valor por omisión: yes

Use this prefix for autonomous address configuration?
Especifica el valor que se pondrá en el indicador de configuración de la dirección autónoma, dentro de la opción de información del prefijo. Cuando se establece en *yes* (sí), puede usarse el prefijo para la configuración autónoma de la dirección.

Valores válidos: yes (sí) o no

Valor por omisión: yes

Valid Lifetime for Prefix?
Especifica la cantidad de tiempo, en segundos, que se pondrá en el tiempo de vida válido, dentro de la opción de información del prefijo. Este valor representa el período de tiempo, relativo a la hora de envío del paquete, durante el cual el prefijo será válido para la determinación dentro del enlace.

Valores válidos: Un entero sin signo de 32 bits, donde `X'FFFFFFFF'` representa un tiempo de vida sin límite

Valor por omisión: 259200 (que corresponde a 30 días)

Decrement the Valid Lifetime in real time?
Especifica si el Valid Lifetime (tiempo de vida válido) disminuye en tiempo real, con lo que en un futuro, el tiempo de vida llegará a cero en el momento especificado O bien si es fijo (sigue siendo el mismo en los anuncios del direccionador consecutivos).

Valores válidos: yes (sí) o no

Valor por omisión: no

Preferred lifetime for prefix
Especifica la cantidad de tiempo, en segundos, que se pondrá en el tiempo de vida preferido, dentro de la opción de información del prefijo. Este valor representa el período de tiempo, relativo a la hora de envío del paquete, durante el cual las direcciones generadas a partir del prefijo a través de

la configuración automática de las direcciones sin estado, siguen siendo preferidas.

Valores válidos: Un entero sin signo de 32 bits, donde X'FFFFFFFF' representa un tiempo de vida sin límite

Valor por omisión: 604800

Decrement the Preferred Lifetime in real time?
Especifica si el Preferred Lifetime (tiempo de vida preferido) disminuye en tiempo real, con lo que en un futuro, el tiempo de vida llegará a cero en el momento especificado o bien si es fijo (sigue siendo el mismo en los anuncios del direccionador consecutivos).

Valores válidos: yes (sí) o no

Valor por omisión: no

Delete

Use el mandato **delete** para eliminar un anuncio de ruta configurado.

Sintaxis:

delete ra
dhcp-server

Disable

Use el mandato **disable** para inhabilitar el anuncio de rutas.

Sintaxis:

disable ra
dhcp-relay

ra Inhabilita el anuncio de ruta.

dhcp-relay
Inhabilita el agente de relé de DHCPv6.

Enable

Use el mandato **enable** para habilitar el anuncio de ruta.

Sintaxis:

enable ra
dhcp-relay

ra Habilita el anuncio de ruta.

dhcp-relay
Habilita el agente de relé de DHCPv6.

List

Use el mandato **list** para visualizar la configuración de NDP.

Sintaxis:

list dhcp
ndp6 configuration
prefix
ra

Ejemplo:

```
 NDP>list dhcp

DHCPv6 Relay Agent
------------------
State           Hopcount
DISABLED            4
NDP>

NDP config>list ndp6


NDP config>list ra


NDP config>list prefix
NDP config>
```

Set

Use el mandato **set** para establecer la cuenta de saltos de DHCP.

Sintaxis:

set dhcp-hopcount

dhcp-hopcount

Especifica el número de saltos que se usarán al pasar en relé paquetes de DHCPv6.

Valores válidos:

Valor por omisión: 4

Ejemplo:

```
 NDP6 Config>set dhcp-hopcount
 Hop Count [4]?
 NDP6 Config>
```

Acceso al entorno de supervisión de NDP

Siga el procedimiento siguiente para acceder a los mandatos de supervisión de NDP. Este proceso le dará acceso al proceso de supervisión de NDP.

1. En el indicador OPCON, entre **talk 5**. (Para obtener información más detallada sobre este mandato, consulte “The OPCON Process and Commands” (Los mandatos y el proceso de OPCON) en *Software User’s Guide*.) Por ejemplo:

```
* talk 5
    +
```

Después de entrar el mandato **talk 5**, el indicador de GWCON (+) aparecerá en el terminal. Si el indicador no aparece cuando entre por primera vez la configuración, pulse de nuevo **Retorno**.

2. En el indicador +, entre el mandato **p ndp** para obtener el indicador NDP>.

   Ejemplo:

```
+ p ndp
NDP>
```

Mandatos de supervisión de NDP

Esta sección describe los mandatos de supervisión de NDP.

Tabla 71. 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 xxv.
dhcpv6-relay	Establece los contadores y parámetros de relé de DHCPv6.
dump	Muestra las tablas de direccionamientos.
list	Muestra la configuración.
ping6	Ejecuta ping dinámicos en una dirección de IPv6.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxvi.

DHCPv6-Relay

Use el mandato **dhcpv6-relay** para establecer los parámetros y los contadores de relé de DHCPv6.

Sintaxis:

dh**cpv6-relay** counters
parameters

counters

parameters

Ejemplo:

Dump

Consulte “Vuelco de tablas de direccionamiento” en la página 459 para obtener información sobre el mandato **dump**.

List

Use el mandato **list** para visualizar la configuración. Sólo se mostrarán las interfaces que tengan configurado RA, incluso aunque pueda existir un prefijo en la lista de prefijos de otras interfaces, como consecuencia de la configuración de dirección de IPv6.

Sintaxis:

list	dhcpv6-relay dump routing tables ndp6 parameters ping6

Ejemplo:

```
NDP>list dhcp

DHCPv6 Relay Agent
------------------
State           Hopcount
DISABLED            4
NDP>
NDP>list ndp6

Router Advertisement for Interface 0 (PPP/0):
                      Hop    RA Interval  Rtr       Reach    Retrans
  State      M  O LLA Limit   Min - Max   Lifetime  Time     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 “Ping6” en la página 439 para obtener detalles sobre el mandato **ping6**.

Configuración y supervisión de Protocol Independent Multicast Routing Protocol (PIM)

La configuración de PIM se efectúa en cada interfaz. Este capítulo describe cómo usar los mandatos de funcionamiento y de configuración de PIM e incluye las secciones siguientes:

Acceso al entorno de configuración de PIM

Siga el procedimiento siguiente para acceder al proceso de configuración de PIM.

1. En el indicador OPCON, entre **talk 6**. (Para obtener información más detallada sobre este mandato, consulte "The OPCON Process and Commands" (Los mandatos y el proceso de OPCON) en *Software User's Guide*.) Por ejemplo:

   ```
   * talk 6
       Config>
   ```

   Después de entrar el mandato **talk 6**, el indicador CONFIG (`Config>`) aparecerá en el terminal. Si el indicador no aparece cuando entre por primera vez la configuración, pulse de nuevo **Retorno**.

2. En el indicador CONFIG, entre el mandato **p pim** para obtener el indicador `PIM6 Config>`.

Mandatos de configuración de PIM

Para configurar PIM, entre los mandatos en el indicador `PIM6 Config>`.

Tabla 72. 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 xxv.
delete	Suprime una interfaz de PIM.
disable	Inhabilita PIM en el dispositivo.
enable	Habilita PIM en el dispositivo y establece los valores de configuración por omisión de PIM globales.
list	Lista la configuración.
set	Establece los valores de los parámetros de configuración de PIM.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxvi.

Delete

Use el mandato **delete** para eliminar una interfaz de PIM configurada.

Sintaxis:

de**lete** *dirinterfaz*

Interface address

Ejemplo:

```
PIM6 Config> delete
 Interface address []?
```

Disable

Use el mandato **disable** para inhabilitar PIM en el dispositivo.

Sintaxis:

di**sable**

Enable

Use el mandato **enable** para habilitar PIM en el dispositivo y establecer los valores de configuración por omisión de PIM globales.

Sintaxis:

e**nable**

List

Use el mandato **list** para visualizar la configuración de PIM.

Sintaxis:

list all
interface
preference
variables

all Muestra toda la información de configuración de PIM.

interface Muestra la información de configuración de PIM de las interfaces configuradas actualmente.

Ejemplo:

```
PIM config>list i

                                              Hello         State
    Type             IP Address              Interval      Holdtime
    Physical         1:2:3:4:5::101             30           210
```

Type Identifica el tipo de interfaz configurada.

IP address
Identifica la dirección de IPv6 asignada a esta interfaz.

Hello Interval
Identifica el intervalo transcurrido entre los mensajes hello, en segundos, enviados en esta interfaz.

State holdtime

Identifica el número de segundos necesarios para indicar a otros dispositivos de comunicación de comunicación inversa que mantengan el estado PIM de este dispositivo. Para PIM, se trata de la cantidad de tiempo necesario para que los dispositivos de comunicación de sentido directo mantengan vivas las podas.

variables Muestra información de configuración de las variables de PIM globales.

Ejemplo:

```
PIM config>list v

          PIM Global Configuration Values

               PIM:  on

                 Graft Timeout:       3 seconds
                 Assert Timeout:    210 seconds
PIM config>
```

PIM: on/off

Identifica si PIM está habilitado o no actualmente.

Graft timeout

Identifica el número de segundos durante el cual se vuelven a transmitir injertos si no se ha recibido ningún acuse de recibo de injerto.

Assert timeout

Identifica el número de segundos durante el cual la información de validación, obtenida a partir de dispositivos de comunicaciones en sentido inverso, se retiene antes de volver a la información de direccionamiento local.

preference

Muestra las preferencias métricas del tipo de direccionamiento configurado actualmente.

Ejemplo:

```
PIM config>list p

     RIP        FFFF         Default     FFFF
     Direct     FFFF         Fixed       FFFF
     Filter     FFFF
PIM config>
```

Route type

Identifica el tipo de ruta con soporte y lista un valor hexadecimal mostrando la preferencia métrica configurada actualmente.

Set

Use el mandato **set** para cambiar los valores del parámetro de configuración de PIM. Puede usar este mandato para añadir una interfaz física nueva.

Sintaxis:

set interface *dirección interfaz períodohello tiemporetenciónpodaunida*
preference *tiporuta valorpreferencia*

variables

interface

Ejemplo:

```
PIM config>set interface
Interface address []?
Hello period [30]?
Join Prune Hold Time [210]?
```

Interface address (Dirección de interfaz)

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Hello period

Especifica el número de segundos transcurridos entre mensajes hello. En las interfaces de punto a punto, no se tiene en cuenta este valor. Una vez 2210 establece una adyacencia, los mensajes hello quedan silenciados.

Valores válidos: De 1 a 65535

Valor por omisión: 30

Join prune hold time

Controla mensajes para informar al dispositivo de recepción cuánto tiempo (en segundos) deberá mantener el estado activado por el mensaje. Las podas enviadas al dispositivo permanecen activas durante este período de segundos.

Valores válidos: De 1 a 65535

Valor por omisión: 210

preference routetype

Se trata de una preferencia métrica configurada para usarla en el proceso de validación. Permite al usuario seleccionar selectivamente qué tipos de rutas de difusión individual de las tablas de reenvío de una difusión individual tienen precedencia sobre otros tipos de ruta. Sólo es de significado local, lo que quiere decir que se usa para este dispositivo y todas sus interfaces activadas PIM conectadas. Puede utilizarse si este direccionador usa varios protocolos de direccionamiento de una difusión individual, los direccionadores adyacentes ejecutan diferentes protocolos de direccionamiento o si se prefieren tipos de ruta como, rutas por omisión, sobre las rutas ya sabidas.

Routetype puede especificar los tipos de rutas siguientes:

- rip
- direct (directo)
- fixed (fijo)
- default (por omisión)
- filter (filtro)

Ejemplo:

```
PIM Config> set preference rip
RIP Metric Preference (hex) [FFFF]?
```

Metric Preference

Este valor se envía a otros direccionadores en el proceso de validación, durante la detección de difusiones múltiples duplicadas y se usa con los costos de métrica de rutas para determinar qué direccionador debe ser el direccionador de reenvío. Todas las preferencias métricas se establecen inicialmente en X'FFFF'.

Valores válidos: Un valor hexadecimal de 4 dígitos

Valor por omisión: X'FFFF'

variables cache_life

Ejemplo:

```
PIM config>set v cache_life
Mcfwd cache Holdtime [60]
```

Mcfwd cache holdtime

Especifica el tiempo, en segundos, que se le permitirá existir a una entrada de difusión múltiple que no se ha usado para reenviar datagramas de difusión múltiple en la antememoria de reenvío antes de eliminarla.

Valores válidos: Un valor numérico superior a 0

Valor por omisión: 60

variables assert_tout

Ejemplo:

```
PIM config>set v assert_tout
PIM Assert Time Out [210]
```

Assert timeout

Cantidad de tiempo, en segundos, durante el cual los direccionadores de comunicaciones directas guardarán información de validación recibida de dos o varios direccionadores de comunicaciones en sentido inverso de validación. La información de validación se usa para asegurarse de que los direccionadores de comunicaciones en sentido directo comprendan cuál es el direccionador correcto de comunicaciones en sentido inverso, o direccionador de reenvío, a fin de que los mensajes de PIM se envíen al direccionador correcto. Si no se reciben más validaciones antes de que el tiempo de validación se agote, la información de validación se descartará y el direccionador usará información local de las tablas de direccionamientos de una difusión individual, para determinar el direccionador de reenvío de comunicaciones en sentido inverso correcto.

Valores válidos: De 1 a 65535

Valor por omisión: 210

variables graft_tout

Ejemplo:

```
PIM config>set v graft_tout
PIM Graft Time Out [3]
```

Graft time out

Especifica el número de segundos durante el cual, el dispositivo que ha enviado el mensaje de injerto, pero no ha recibido ningún acuse de recibo, esperará antes de enviar otro mensaje.

Valores válidos: De 1 a 65535

Valor por omisión: 3

Acceso al entorno de supervisión de PIM

Siga el procedimiento siguiente para acceder a los mandatos de supervisión de PIM. Este proceso le dará acceso al proceso de supervisión de PIM.

1. En el indicador OPCON, entre **talk 5**. (Para obtener información detallada sobre este mandato, consulte *The OPCON Process and Commands* en la Software User's Guide.) Por ejemplo:

   ```
   *
talk 5
   +
   ```

   Después de entrar el mandato **talk 5**, el indicador de GWCON (+) aparecerá en el terminal. Si el indicador no aparece cuando entre por primera vez la configuración, pulse de nuevo **Retorno**.

2. En el indicador +, entre el mandato **p pim** para ir al indicador PIM6>.

   Ejemplo:

   ```
   + p pim
   PIM>
   ```

Mandatos de supervisión de PIM

Esta sección describe los mandatos de supervisión de PIM.

Tabla 73. Resumen de mandatos de supervisión de PIM

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxv.
dump	Muestra las tablas de direccionamientos.
clear	Borra la tabla de difusiones múltiples.
interface	Muestra el estado de la interfaz.
join	Une un grupo de difusiones múltiples.
leave	Deja un grupo de difusiones múltiples.
mcache	Muestra las entradas de antememoria de la tabla de difusiones múltiples activa actualmente.
mgroups	Muestra la pertenencia de grupo de las interfaces conectadas al dispositivo.
mstats	Muestra diversas estadísticas de direccionamiento de difusión múltiple.
neighbor	Muestra información sobre las adyacencias actuales.
pim	Muestra la base de datos de estados de PIM.
summary pim	Muestra un resumen de la base de datos de estados de PIM.
ping	Ejecuta ping dinámicos en una dirección de IPv6.
reset	Restablece dinámicamente el PIM.
traceroute	Rastrea dinámicamente una ruta.
variables	Muestra los valores de configuración de las variables de PIM.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxvi.

Vuelco de tablas de direccionamiento

Use el mandato **dump** para visualizar las tablas de direccionamientos configuradas.

Sintaxis:

d**ump**

Ejemplo:

```
PIM6>dump
Type   Dest net/Prefix            Cost     Age       Next hop(s)

Fltr   ::102:304/128                0     576       filter
Stat*  1:2:3:4:5:6:7:8/128        100     576       IP64/0
Stat*  3::4/128                     1     576       IP64/1

IPv6 Routing table size: 768 nets (79872 bytes), 3 nets known
                         0 nets hidden, 0 nets deleted, 0 nets inactive
                         0 routes used internally, 765 routes free
PIM6>
```

Clear

Use el mandato **clear** para restablecer la antememoria.

Sintaxis:

clear

Ejemplo:

```
PIM6>clear

Mfwd Cache has been cleared!

PIM6>
```

Interface

Use el mandato **interface** para mostrar un resumen de las estadísticas y parámetros relacionados con la interfaz.

Sintaxis:

interface

Ejemplo:

```
PIM6>interface
PIM Interface Table
                                                  Hello          State
IP Address                                     Interval  Holdtime  Status   Type
1:2:3:4:5:6::101                                  30        210    up       TKR/0
1:2:5:6:7::102                                    30        210    up       TKR/1
PIM6>
```

IP address
Especifica la dirección IP de la interfaz.

Hello interval
Especifica la cantidad de segundos transcurridos entre los mensajes hello de esta interfaz.

State holdtime
Especifica el número de segundos durante el cual los dispositivos de comunicaciones en sentido inverso mantendrán la información de estado antes de descartarla. En el caso de PIM, se trata del número de segundos durante el cual una poda estará activa en las comunicaciones en sentido inverso.

Status Especifica el estado actual de la interfaz.

- **up** La interfaz está activada y plenamente operativa, pero no genera las consultas mld.
- **disabled** La interfaz es operativa pero está inhabilitada y el PIM no está activo.
- **down** La interfaz no es operativa.

Join

Use el mandato **join** para unir un grupo de difusión múltiple.

Sintaxis:

j**oin**

Ejemplo:

```
PIM6>join ff05:42::101
```

Leave

Use el mandato **leave** para dejar un grupo de difusión múltiple. Esto evita que el dispositivo responda a pings y consultas de SNMP enviadas a la dirección de grupo.

Sintaxis:

l**eave**

Ejemplo:

```
PIM6>leave ff05:42::101
```

Mcache

Use el mandato **mcache** para visualizar la lista de entradas de antememoria de difusión múltiple activas actualmente. Estas entradas se crean a petición, siempre que se recibe el primer datagrama de difusión múltiple coincidente. Existe una entrada de antememoria separada (y, por consiguiente una ruta separada) por cada combinación de red de origen de datagramas y grupo de destino.

Sintaxis:

mc**ache**

Ejemplo:

```
PIM6>mcache

        0: TKR/0           1: TKR/1           2: TKR/2
        3: IPPN/0          4: BDG/0           5: Internal


                                        Prot   Count   Upstr   Downstream
0:1:2::
 FF05:42::101                           PIM6   8       0       1,2
3:4:22::
 FF05:42::102                           PIM6   8       1       0
3:12:2::
 FF05:33:4::120                         PIM6   25      0       2
PIM6>
```

Prot Especifica el protocolo propietario de la entrada de la tabla de difusiones múltiples.

Count Muestra el número de paquetes de difusión múltiple recibidos para esta entrada de tabla de difusiones múltiples.

Upstr Muestra la red o el direccionador vecinos de los que debe recibirse el datagrama a fin de reenviarlo.

Downstream
Muestra el número total de interfaces de comunicaciones directas o vecinos a los que se reenviará el datagrama.

Mgroup

Use el mandato **mgroup** para visualizar la pertenencia al grupo de las interfaces conectadas al dispositivo. Sólo se visualizará la pertenencia al grupo de aquellas interfaces en las que el direccionador sea el direccionador designado o el direccionador designado de seguridad.

Sintaxis:

mg**roup**

Ejemplo:

```
PIM6>mgroup

           Local Group Database
Group                                  Interface              Lifetime (secs)

FF05:42::101                          1:2:3:4::25 (TRK/0)     176
FF05:4:23::122                        23:2:113::45:23 (Eth/1) 170
FF05:4:23::122                        Internal                1
PIM6>
```

Group Muestra la dirección del grupo tal como se ha informado (a través de MLD) en una interfaz en particular.

Interface Muestra la dirección de la interfaz a la que se ha indicado la dirección de grupo (a través de MLD). La pertenencia al grupo interno del direccionador se indica mediante un valor *internal* (interno). Para estas entradas, el campo lifetime (tiempo de vida - ver abajo) indica el número de aplicaciones que han solicitado pertenece a este grupo determinado.

Lifetime Muestra los segundos que persistirá la entrada si dejan de oírse los Membership Reports (Informes de pertenencia) en la interfaz del grupo determinado.

Mstats

Use el mandato **mstats** para visualizar diversas estadísticas de direccionamiento de difusión múltiple. El mandato indica si el direccionamiento de difusión múltiple está habilitado y si el direccionador es un reenviador entre áreas o de difusión múltiple entre AS.

Sintaxis:

ms**tats**

Ejemplo:

```
PIM6>mstats

Datagrams received:           2496
Datagrams fwd (multicast):       0  Datagrams fwd (unicast):   0
Locally delivered:               0
Unreachable source:              3  Unallocated cache entries: 0
Off multicast tree:              0  Unexpected DL multicast:   0
Buffer alloc failure:            0  TTL scoping:               0

# fwd cache alloc:               1  # fwd cache freed:         0
#fwd cache GC:                   0  # local group DB alloc:    0
#local group DB free:            1

PIM6>
```

Datagrams received
Muestra el número de datagramas de difusión múltiple recibidos por el direccionador.

Datagrams fwd (multicast)
Muestra el número de datagramas que se han reenviado como difusiones múltiples de enlaces de datos (esto incluye las réplicas de paquetes, cuando es necesario, por lo que esta cuenta puede ser superior al número recibido).

Datagrams fwd (unicast)
Muestra el número de datagramas que se han reenviado como difusiones individuales de enlace de datos.

Locally delivered
Muestra el número de datagramas que se han reenviado a aplicaciones internas.

Unreachable source
Muestra una cuenta de los datagramas cuya dirección de origen era inaccesible.

Unallocated cache entries
Muestra una cuenta de los datagramas cuyas entradas de antememoria no se pudieron crear debido a falta de recursos.

Off multicast tree
Muestra una cuenta de los datagramas que no se reenviaron porque no había vecino en las comunicaciones en sentido inverso o no había interfaces/vecinos en las comunicaciones directas, en la entrada de antememoria coincidente.

Unexpected DL multicast
Muestra una cuenta de los datagramas que se recibieron como difusiones individuales de enlaces de datos en las interfaces configuradas para difusión individual de enlace de datos.

Buffer alloc failure
Muestra una cuenta de los datagramas a los que no se pudo replicar debido a falta de almacenamientos intermedios.

TTL scoping
Indica los datagramas que no se reenviaron porque su TTL indicaba que no pudieron acceder nunca a un miembro de grupo.

#fwd cache alloc
Indica el número de las entradas de antememoria asignadas. El tamaño de antememoria de reenvío actual equivale al número de entradas asignadas (**# fwd cache alloc**) menos el número de entradas de antememoria liberadas (**# fwd cache freed**).

#fwd cache freed
Indica el número de entradas de antememoria liberadas. El tamaño de antememoria de reenvío actual equivale al número de entradas asignadas (**# fwd cache alloc**) menos el número de entradas de antememoria liberadas (**# fwd cache freed**).

#fwd cache GC
Indica el número de entradas de antememoria borradas debido a que no se usaron recientemente y la antememoria se desbordó.

#local group DB alloc
Indica el número de entradas de la base de datos de grupos local asignadas. El número asignado (**# asig BD grupos local**) menos el número liberado (**# DB grupo local libre**) es igual al tamaño actual de la base de datos de grupos local.

#local group DB free
Indica el número de entradas de la base de datos de grupos local liberadas. El número asignado (**# asig BD grupos local**) menos el número liberado (**# DB grupo local libre**) es igual al tamaño actual de la base de datos de grupos local.

Neighbor

Use el mandato **neighbor** para visualizar información sobre dispositivos PIM vecinos y el estado de adyacencia.

Sintaxis:

n**eighbors**

Ejemplo:

```
PIM6>neighbor
PIM Neighbor Listing

                                                  Last     First
Neighbor Addr                              DR     Heard    Heard    Ifc
9:4:3:101:2::123                           NO     21       6139     Tkr/0
23:2:45:2::12:3:111                        YES    29       6204     Tkr/1
PIM6>
```

Neighbor Addr
Identifica si este direccionador ha identificado el vecino como el direccionador designado.

DR Identifica si este direccionador ha identificado el vecino como el direccionador designado.

Last Heard
El número de segundos desde que se oyó por última vez al vecino.

First Heard
El número total de segundos desde que se estableció por primera vez la adyacencia con este vecino.

Ifc La interfaz en la que se descubrió al vecino.

PIM

Use el mandato **pim** para visualizar la base de datos de estados del PIM.

Sintaxis:

pim

Ejemplo:

```
PIM6>pim
                PIM State Database
                 ------------------
  1)     Group:  FF05:2:3::121
  1)    Source:  9:1:2:3::12:101
  1) Interface:  1 - PRUNE  Lifetime (sec): 210

  2)     Group:  FF05:2:3::121
  2)    Source:  9:1:2:3::12:101
  2) Interface:  1 - PRUNE  Lifetime (sec): 210
PIM6>
```

Group La dirección del grupo de destino asociada a la entrada.

Source La dirección de origen del originador del datagrama de difusión múltiple.

Interface El número de la interfaz del PIM y el tipo de estado de éste en la base de datos.

Lifetime El tiempo de vida total, en segundos, del estado recibido, obtenido a partir del mensaje de control de PIM que estableció el estado.

Summary PIM

Use el mandato **summary pim** para visualizar información resumida sobre la base de datos de estados del PIM.

Sintaxis:

s**ummary pim**

Ejemplo:

```
PIM6>s

            Summary PIM State Database
             -------------------------
0)     Group:  FF05:2:3::121
0)    Source:  9:1:2:3::12:101
0)    States:  1-P  2-P

PIM6>
```

Group La dirección del grupo de destino asociada a la entrada.

Source La dirección de origen del originador del datagrama de difusión múltiple.

States Muestra las interfaces y los estados asociados al par de grupos de origen. P identifica un estado de poda.

Ping

Use el mandato **ping** para ejecutar ping dinámicamente a otra dirección de IPv6 de destino.

Sintaxis:

ping

Ejemplo:

```
PIM6>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
```

Consulte “Ping6” en la página 439 para obtener una descripción de los parámetros.

Reset

Use el mandato **reset** para restablecer PIM y volver a cargar la configuración.

Sintaxis:

reset

Ejemplo:

```
PIM6>reset
```

Traceroute

Use el mandato **traceroute** para rastrear dinámicamente una ruta.

Sintaxis:

traceroute

Ejemplo:

```
IPv6>traceroute
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>
```

Consulte “Traceroute6” en la página 440 para obtener una descripción de los parámetros.

Variables

Use el mandato **variables** para visualizar información sobre las variables de configuración de PIM.

Sintaxis:

v**ariables**

Ejemplo:

```
PIM6>v

               PIM:  on

                 Graft Timeout:       3 seconds
                 Assert Timeout:    210 seconds

PIM Unicast Metric Preferences (hex)
     RIP        FFFF         Default     FFFF
     Direct     FFFF         Fixed       FFFF
     Filter     FFFF

PIM6>
```

PIM: on/off
Indica si PIM-DM está actualmente habilitado o inhabilitado.

Graft Timeout
Número de segundos durante los cuales se vuelven a transmitir injertos si no se ha recibido acuse de recibo de injerto.

Assert Timeout
Número de segundos durante el cual la información de validación, obtenida por direccionadores de comunicaciones en sentido inverso, se retiene antes de volver a la información de direccionamiento local.

PIM Unicast Metric Preferences
Muestra las preferencias métricas del tipo de direccionamiento configurado actualmente. Cada tipo de ruta con soporte está en una lista con un valor hex que muestra la preferencia métrica configurada actualmente.

Configuración y supervisión de Routing Information Protocol (RIP6)

RIP6 es un protocolo de direccionamiento del vector de distancia. La configuración de RIP6 se efectúa en cada interfaz. Este capítulo describe cómo usar los mandatos de funcionamiento y de configuración de RIP6 e incluye las secciones siguientes:

Acceso al entorno de configuración de RIP6

Siga el procedimiento siguiente para acceder al proceso de configuración de RIP6.

1. En el indicador OPCON, entre **talk 6**. (Para obtener información más detallada sobre este mandato, consulte "The OPCON Process and Commands" (Los mandatos y el proceso de OPCON) en *Software User's Guide*.) Por ejemplo:

   ```
   * talk 6
   Config>
   ```

   Después de entrar el mandato **talk 6**, el indicador CONFIG (`Config>`) aparecerá en el terminal. Si el indicador no aparece cuando entre por primera vez en la configuración, pulse de nuevo **Retorno**.

2. En el indicador CONFIG, entre el mandato **p rip6** para obtener el indicador `RIP66 Config>`.

Mandatos de configuración de RIP6

Para configurar RIP6, entre los mandatos en el indicador `RIP66 Config>`.

Tabla 74. Resumen de los mandatos de configuración de RIP6

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxv.
add	Añade RIP6 en una interfaz.
change	Cambia los valores de configuración métrica de RIP6.
delete	Elimina RIP6 de una interfaz.
disable	Inhabilita RIP6 en una interfaz.
enable	Habilita RIP6 en una interfaz.
list	Lista la configuración.
set	Establece los valores métricos de RIP6.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxvi.

Add

Use el mandato **add** para añadir RIP6 a una interfaz.

Sintaxis:

a**dd** *núm.interfaz*

núm.interfaz
Especifica la interfaz a la que se añadirá el protocolo RIP6.

Nota: Esta interfaz debe tener configurada una dirección de IPv6 o ser la interfaz virtual de un túnel de IPv6 sobre IPV4.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: Ninguno

Change

Use el mandato **change** para cambiar un valor métrico de RIP6.

Sintaxis:

c**hange** rip6-in-metric
rip6-out-metric

rip6-in-metric
Cambia el valor de la métrica de RIP6 por las actualizaciones de llegada de RIP6.

Change RIPng metric on which interface? Especifica el número de la interfaz donde se va a cambiar la métrica de entrada de RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

RIP6 input Metric Cambia el valor de la métrica de RIP6 en las actualizaciones de RIP6 de entrada.

Valores válidos: De 1 a 15

Valor por omisión: 1

rip6-out-metric
Cambia la métrica de RIP6 en las actualizaciones de RIP6 de salida.

Change RIPng metric on which interface? Especifica el número de la interfaz donde se va a cambiar la métrica de salida de RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

RIP6 output Metric Especifica el valor de la métrica de RIP6 en las actualizaciones de RIP6 de salida.

Valores válidos: De 0 a 15

Valor por omisión: 0

Delete

Use el mandato **delete** para sacar RIP6 de la interfaz especificada.

Sintaxis:

de**lete** *núm.interfaz*

núm.interfaz
Especifica la interfaz de la que se sacará el protocolo RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: Ninguno

Disable

Use el mandato **disable** para inhabilitar RIP6.

Sintaxis:

di**sable** rip6
override ...
sending ...

rip6 Inhabilita RIP6 en la interfaz especificada.

Valores válidos: Yes o No

Valor por omisión: Sí

Modify RIP6 flags on which interface? Especifica el número de la interfaz donde se va a inhabilitar RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

override ...

static-routes Altera temporalmente las rutas estáticas de RIP6 en una interfaz.

Modify RIP6 flags on which interface? Especifica el número de la interfaz donde se va a inhabilitar RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

default Altera temporalmente las rutas por omisión de RIP6 en una interfaz.

Modify RIP6 flags on which interface? Especifica el número de la interfaz donde se va a inhabilitar RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

sending ...

Modify RIP6 flags on which interface?
Especifica el número de la interfaz donde se va a inhabilitar RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

all-routes
Inhabilita el anuncio de todas las rutas de RIP6 en una interfaz.

Valores válidos: Yes (Sí) o No

Valor por omisión: Sí

default-routes
Inhabilita el anuncio de las rutas por omisión de RIP6 en una interfaz.

Valores válidos: Yes (Sí) o No

Valor por omisión: Sí

static-routes
Inhabilita el anuncio de las rutas estáticas de RIP6 en una interfaz.

Valores válidos: Yes (Sí) o No

Valor por omisión: Sí

poisoned-reverse-routes
Inhabilita la inversión de veneno al enviar actualizaciones de RIP6 a una interfaz.

Valores válidos: Yes (Sí) o No

Valor por omisión: Sí

Enable

Use el mandato **enable** para habilitar RIP6.

Sintaxis:

enable rip6
override ...
sending ...

rip6 Habilita RIP6 en la interfaz especificada.

Valores válidos: Yes (Sí) o No

Valor por omisión: Sí

Modify RIP6 flags on which interface? Especifica el número de la interfaz donde se va a habilitar RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

override ...

static-routes Altera temporalmente las rutas estáticas de RIP6 en una interfaz.

Modify RIP6 flags on which interface? Especifica el número de la interfaz donde se va a habilitar RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

default Altera temporalmente las rutas por omisión de RIP6 en una interfaz.

Modify RIP6 flags on which interface? Especifica el número de la interfaz donde se va a habilitar RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

sending ...

Modify RIP6 flags on which interface?
Especifica el número de la interfaz donde se va a habilitar RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

all-routes
Habilita el anuncio de todas las rutas de RIP6 en una interfaz.

Valores válidos: Yes (Sí) o No

Valor por omisión: Sí

default-routes
Habilita el anuncio de las rutas por omisión de RIP6 en una interfaz.

Valores válidos: Yes (Sí) o No

Valor por omisión: Sí

static-routes
Habilita el anuncio de las rutas estáticas de RIP6 en una interfaz.

Valores válidos: Yes (Sí) o No

Valor por omisión: Sí

poisoned-reverse-routes
Habilita la inversión de veneno al enviar actualizaciones de RIP6 a una interfaz.

Valores válidos: Yes o No

Valor por omisión: Sí

List

Use el mandato **list** para visualizar la configuración de RIP6.

Sintaxis:

list all

Ejemplo:

```
RIP6 config>list all
```

Set

Use el mandato **set** para establecer los parámetros de configuración de RIP6.

Sintaxis:

set rip6-in-metric
rip6-out-metric

rip6-in-metric
Establece la métrica de RIP6 en las actualizaciones de RIP6 de entrada.

Change RIPng metric on which interface? Especifica el número de la interfaz donde se va a establecer la métrica de entrada de RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

RIP6 input Metric Especifica el valor de la métrica de RIP6 usada en las actualizaciones de RIP6 de entrada.

Valores válidos: De 1 a 15

Valor por omisión: 1

rip6-out-metric
Establece la métrica de RIP6 usada en las actualizaciones de RIP6 de salida.

Change RIPng metric on which interface? Especifica el número de la interfaz en que se establecerá la métrica de salida de RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

RIP6 output Metric Especifica el valor de la métrica usada en actualizaciones RIP6 de salida.

Valores válidos: De 0 a 15

Valor por omisión: 0

Acceso al entorno de supervisión de RIP6

Siga el procedimiento siguiente para acceder a los mandatos de supervisión de RIP6. Este proceso le dará acceso al proceso de supervisión de RIP6.

1. En el indicador OPCON, entre **talk 5**. (Para obtener información más detallada sobre este mandato, consulte “The OPCON Process” (El proceso OPCON) en el manual *Software User's Guide*.) Por ejemplo:

   ```
   * talk 5
   +
   ```

   Después de entrar el mandato **talk 5**, el indicador de GWCON (+) aparecerá en el terminal. Si el indicador no aparece cuando entre por primera vez en la configuración, pulse de nuevo **Retorno**.

2. En el indicador +, entre el mandato **p rip6** para ir al indicador `RIP6>`.

   Ejemplo:

   ```
   + p rip6
   RIP6>
   ```

Mandatos de supervisión de RIP6

Esta sección describe los mandatos de supervisión de RIP6.

Tabla 75. 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 xxv.
list	Muestra la configuración.
dump	Muestra las tablas de direccionamientos.
ping6	Ejecuta ping dinámicos en una dirección de IPv6.
reset	Restablece dinámicamente RIP6.
traceroute6	Rastrea dinámicamente una ruta.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxvi.

List

Use el mandato **list** para visualizar la configuración.

Sintaxis:

list

Ejemplo:

```
RIP6>list
```

Dump

Consulte “Vuelco de tablas de direccionamiento” en la página 459 para obtener información sobre el mandato **dump**.

Ping6

Consulte “Ping6” en la página 439 para obtener detalles sobre el mandato **ping6**.

Reset

Sintaxis:

reset

Ejemplo:

```
RIP6>reset
```

Traceroute6

Consulte “Traceroute6” en la página 440 para obtener información detallada sobre el mandato **traceroute6**.

Apéndice A. Comparación de protocolos

Este apéndice compara algunos de los protocolos más conocidos a los que da soporte el direccionador. Se proporciona como guía de ayuda y su objetivo no es servir de consulta.

Tabla de comparación de los protocolos

La tabla siguiente compara los protocolos.

Tabla 76. Comparación de protocolos

Modelo OSI de ISO	TCP/IP	IPX	Otros
7 Aplicación 6 Presentación 5 Sesión	Telnet, FTP, TFTP, SGMP		
4 Transporte	TCP, UDP	PXP, SPX	
3 Red	IP, RIP, BGP, ICMP	RIP, SAP	
2 Enlace de datos	Red local		HDLC
1 Física			

Clave para los protocolos

La Tabla 77 es una clave para los protocolos.

Tabla 77 (Página 1 de 2). Clave para los protocolos

Protocolo	Descripción
BGP	Border Gateway Protocol. Protocolo de direccionamiento externo IP.
FTP, TFTP	File Transfer Protocol; Trivial File Transfer Protocol.
ICMP	Internet Control Message Protocol. Se usa para enviar mensajes de control y de error de nivel de red entre direccionadores y sistemas principales.
IP	Internet protocol. IP es un protocolo de transporte estándar de uso muy extendido. IP es el protocolo básico de los direccionadores 2210. IP deja una parte de la comprobación de errores a los protocolos de nivel superior (de extremo a extremo).
IPX	Internet Packet Exchange Protocol.
RIP	Routing Information Protocol (Los protocolos de direccionamiento se usan para determinar los recorridos de los datos y la topología de la red). RIP es el protocolo de direccionamiento de IP más difundido.
SGMP	Simple Gateway Monitoring Protocol. Se usa para obtener estadísticas en forma legible por máquina de los direccionadores 2210.
SNMP	Simple Network Management Protocol. Se usa para obtener estadísticas en forma legible por la máquina de direccionadores 2210.

Tabla 77 (Página 2 de 2). Clave para los protocolos

Protocolo	Descripción
TCP	Transport Control Protocol. Protocolo de extremo a extremo (sistema principal a sistema principal) utilizado con frecuencia con IP. Es útil para enviar flujos de datos. Usa sumas de comprobación, reconocimientos y tiempos de espera para asegurarse de la entrega correcta de todas las secuencias de datos.

Apéndice B. Tamaños de los paquetes

Este apéndice trata los tamaños de los paquetes para los diferentes protocolos y redes con soporte. Está formado por las secciones siguientes:

- Cuestiones generales
- Límites de tamaño específicos de la red
- Límites de tamaño específicos del protocolo
- Cambio de los tamaños máximos de paquete

Cuestiones generales

Como información general para el objetivo de la presente discusión, los paquetes que manejan los direccionadores están formados por datos del usuario e información de cabecera.

La cantidad de datos del usuario contenidos en el paquete está limitada por la cantidad de información de cabecera de dicho paquete. Esta cantidad de información depende (como mínimo):

- De los tipos de red sobre los que debe viajar el paquete.
- De los protocolos que usan las redes.

Los factores siguientes influyen en el tamaño del contenido del paquete:

- Longitud de la información de la cabecera de enlace de datos que el tipo de red y la interfaz actuales necesitan que tenga el paquete.
- Longitud de la información final (si la hay) que el tipo de red y la interfaz actuales necesitan que tenga el paquete.

En cualquier red, la suma del tamaño máximo de los datos junto con el tamaño de la cabecera y el de la información final es igual al tamaño máximo del paquete de la red. Cuando se direcciona entre redes cuyo tamaño máximo de paquete sea diferente, se producirá una fragmentación de éste.

Límites de tamaño específicos de la red

Teniendo en cuenta la información proporcionada en la sección anterior, es posible determinar la cantidad máxima de datos de la capa de la red que tiene soporte de cada capa de enlace de datos (interfaz de la red). La Tabla 78 en la página 480 lista los tamaños máximos de los paquetes por omisión para los tipos de interfaz comunes.

Tabla 78. Tamaño máximo por omisión del paquete específico de red

Tipo de red (enlace de datos)	Tamaño máximo del paquete de la capa de red (bytes)	Longitud de la cabecera de red	Parte final de la información
Red en anillo 4 Mbps	2052	22	0
Red en anillo 16 Mbps	2052	22	0
Ethernet	1500	18	4
PPP	2046	2	0
Frame Relay	2048*	variable	2

***:** Para las interfaces de Frame Relay se configura el tamaño de trama máximo y no el tamaño máximo del paquete de la capa de red. Para determinar el tamaño máximo del paquete de la capa de la red para un protocolo, consulte la descripción del mandato **set frame-size** en el capítulo titulado Configuring and Monitoring Frame Relay Interfaces (Configuración y supervisión de interfaces de Frame Relay) en el manual *Software User's Guide*.

Nota: Puede cambiar el tamaño máximo del paquete para las interfaces que no sean Ethernet. Use el mandato **network** en el indicador `Config>` para acceder a los mandatos de configuración de la interfaz.

El tamaño máximo del paquete es la cantidad máxima de datos que el reenviador de protocolos puede pasar al dispositivo.

Nota: Estos números corresponden a las MTU de 4.2 BSD UNIX.

Para un paquete IP, esto incluye la cabecera de IP, la cabecera de UDP o TCP y todos los datos.

El tamaño del paquete que se está usando se muestra cuando se usa el mandato de memoria GWCON del direccionador. El tamaño "Pkt" es el tamaño del paquete de la capa de red. Los tamaños de Hdr (cabecera) y Tlr (parte final) dependen de las redes y de sus respectivas interfaces de red.

Límites de tamaño específicos del protocolo

Esta sección explica los límites de tamaño específicos de los protocolos.

Longitudes de paquete IP

Las especificaciones del protocolo IP no necesitan una implementación de IP en el sistema principal para aceptar paquetes IP de más de 576 octetos; no obstante, las implementaciones de IP del direccionador deben acomodar paquetes IP de cualquier longitud hasta los límites impuestos por los paquetes específicos de la red en uso.

Además, el IP del direccionador efectúa una fragmentación y ensambla de nuevo los paquetes de forma transparente y, de no ser así, superarían las restricciones de longitud específicas de la red, tal como están indicadas en la especificación de IP.

La falta de coincidencia del tamaño del paquete no produce problemas de conectividad. No obstante, el ensamblamiento de fragmentos perjudica el rendimiento, por lo que debe evitarse en la medida de lo posible la fragmentación.

Cambio de los tamaños máximos de paquete

Por lo general, el direccionador establece automáticamente el tamaño máximo del paquete de la capa de red en el tamaño de paquete más grande posible en todas las redes conectadas. A continuación, añade las cabeceras e información final necesarias para que las redes determinen el tamaño del almacenamiento intermedio interno, que es superior al tamaño de la capa de red.

Algunas redes (Red en anillo 4 Mbps y Red en anillo 16 Mbps) le permiten configurar tamaños de paquete máximos. La configuración de tamaños máximos de paquete influye en el tamaño de los almacenamientos intermedios usados en el direccionador y esto, a su vez, influye en el número de almacenamientos intermedios disponibles para un tamaño de memoria determinado. Los direccionadores determinan automáticamente qué tamaño va a necesitar el almacenamiento intermedio. Puede cambiar el tamaño de paquete máximo de la capa de red que el direccionador maneja usando el mandato set packet-size; no obstante, no use este mandato a menos que el servicio de atención al cliente se lo indique específicamente.

Apéndice C. Lista de Abreviaturas

AARP	AppleTalk Address Resolution Protocol
ABR	direccionador de marco de área
ack	acuse de recibo
AIX	Advanced Interactive Executive
AMA	direccionamiento del MAC arbitrario
AMP	supervisor presente activo
ANSI	American National Standards Institute
AP2	AppleTalk Phase 2
APPN	Advanced Peer-to-Peer Networking
ARE	explorador de todas las rutas
ARI	interfaz ATM real
ARI/FCI	indicador de dirección reconocida/indicador de trama copiada
ARP	Address Resolution Protocol
AS	sistema autónomo
ASBR	direccionador de límite de sistema autónomo
ASCII	American National Standard Code for Information Interchange
ASN.1	notación de sintaxis de abstracción 1
ASRT	direccionamiento transparente de origen adaptable
ASYNC	asíncrono
ATCP	AppleTalk Control Protocol
ATP	AppleTalk Transaction Protocol
AUI	interfaz de unidad de conexión
AVI	interfaz ATM virtual
ayt	¿hay alguien ahí?
BAN	Boundary Access Node
BBCM	Bridging Broadcast Manager
BECN	notificación de congestión explícita hacia atrás
BGP	Border Gateway Protocol
BNC	bayonet Niell-Concelman
BNCP	Bridging Network Control Protocol
BOOTP	protocolo BOOT
BPDU	unidad de datos de protocolo de puente
bps	bits por segundo
BR	función de puente/direccionamiento

BRS reserva de ancho de banda

BSD distribución de software de Berkeley

BTP agente de relay de BOOTP

BTU unidad básica de transmisión

CAM memoria dirigible a través del contenido

CCITT Comisión Consultiva de la Telefonía y Telegrafía Internacionales

CD detección de colisión

CGWCON Consola de pasarela

CIDR Direccionamiento entre dominios sin clase

CIP Classical IP

CIR velocidad de información comprometida

CLNP Connectionless-Mode Network Protocol

CPU unidad central de proceso

CRC comprobación de redundancia cíclica

CRS servidor de informes de configuración

CTS preparado para transmitir

CUD datos de usuario de llamada

DAF filtración de direcciones de destino

DB base de datos

DBsum resumen de la base de datos

DCD detector de señal de línea recibida de canal de datos

DCE equipo de terminación de circuito de datos

DCS servidor conectado directamente

DDLC controlador de enlace de datos dual

DDN Defense Data Network

DDP Datagram Delivery Protocol

DDT Dynamic Debugging Tool

DHCP Dynamic Host Configuration Protocol

dir conectado directamente

DL enlace de datos

DLC control de enlace de datos

DLCI identificador de conexión de enlace de datos

DLS conmutación del enlace de datos

DLSw conmutación del enlace de datos

DMA acceso de memoria directo

DNA Digital Network Architecture

DNCP DECnet Protocol Control Protocol

DNIC Código de identificador de red de datos

DdD Departamento de Defensa

DOS Disk Operating System

DR direccionador designado

DRAM Memoria de acceso aleatorio dinámica

DSAP punto de acceso a servicios de destino

DSE equipo de conmutación de datos

DSE intercambio de conmutaciones de datos

DSR aparato de datos preparado

DSU unidad de servicio de datos

DTE equipo terminal de datos

DTR terminal de datos preparado

Dtype tipo de destino

DVMRP Distance Vector Multicast Routing Protocol

E1 velocidad de transmisión de 2,048 Mbps

EDEL delimitador de final

EDI indicador de errores detectados

EGP Exterior Gateway Protocol

EIA Electronics Industries Association

ELAN LAN emulada

ELAP EtherTalk Link Access Protocol

ELS Sistema de anotación cronológica de sucesos

ESI identificador de sistema final

EST Horario Estándar del Este de los EE.UU

Eth Ethernet

fa-ga dirección funcional-dirección de grupo

FCS secuencia de comprobación de trama

FECN notificación de congestión explícita hacia adelante

FIFO primero en entrar, primero en salir

FLT biblioteca de filtros

FR Frame Relay

FRL Frame Relay

FTP File Transfer Protocol

GMT Hora Media de Greenwich

GOSIP Perfil de Interconexión de Sistemas Abiertos del Gobierno

GTE Compañía Telefónica General

GWCON Consola de pasarela

HDLC control de enlace de datos de alto nivel

HEX hexadecimal

HPR direccionamiento de alto rendimiento

HST servicios de sistema principal de TCP/IP

HTF formato de tabla de sistema principal

IBD Dispositivo de arranque integrado

ICMP Internet Control Message Protocol

ICP Internet Control Protocol

ID identificación

IDP Parte de dominio inicial

IDP Internet Datagram Protocol

IEEE Institute of Electrical and Electronics Engineers

Ifc# número de interfaz

IGP Interior Gateway Protocol

InARP Inverse Address Resolution Protocol

IP Internet Protocol

IPCP IP Control Protocol

IPPN IP Protocol Network

IPX Internetwork Packet Exchange

IPXCP IPX Control Protocol

RDSI red digital de servicios integrados

ISO Organización Internacional para la Normalización

Kbps kilobits por segundo

LAC Concentrador del acceso a la red L2TP

LAN red de área local

LAPB protocolo de acceso a enlace equilibrado

LAT transporte de área local

LCP Link Control Protocol

LED diodo emisor de luz

LF trama mayor; salto de línea

LIS subred IP lógica

LLC control de enlace lógico

LLC2 control de enlace lógico 2

LMI interfaz de gestión local

LNS Servidor de red L2TP

LRM mecanismo de información de LAN

LS estado de los enlaces

LSA notificación del estado de los enlaces

LSB bit menos significativo

LSI interfaz de métodos abreviados de LAN

LSreq petición del estado de los enlaces

LSrxl lista de retransmisiones del estado de los enlaces

LU unidad lógica

MAC control del acceso al medio

Mb megabit

MB megabyte

Mbps megabits por segundo

MBps megabytes por segundo

MC vertimiento múltiple

MCF filtración del MAC

MIB Base de la información de gestión

MIB II Base de la información de gestión II

MILNET red militar

MOS Micro Operating System

MOSDBG Micro Operating System Debugging Tool

MOSPF Open Shortest Path First con extensiones de vertimiento múltiple

MSB bit más significativo

MSDU unidad de datos de servicio del MAC

MRU unidad máxima de recepción

MTU unidad máxima de transmisión

nak sin acuse de recibo

NBMA Acceso múltiple sin difusión

NBP Name Binding Protocol

NBR direccionador contiguo

NCP Network Control Protocol

NCP Network Core Protocol

NetBIOS Network Basic Input/Output System

NHRP Next Hop Resolution Protocol

NIST National Institute of Standards and Technology

NPDU Unidad de datos de protocolo de red

NRZ sin vuelta a cero

NRZI sin vuelta a cero invertido

NSAP Punto de acceso a servicios de red

NSF National Science Foundation

NSFNET National Science Foundation NETwork

NVCNFG configuración permanente

OPCON Consola del operador

OSI interconexión de sistemas abiertos

OSICP OSI Control Protocol

OSPF Open Shortest Path First

OUI identificador exclusivo de organización

PC Personal Computer

PCR velocidad mayor de célula

PDN red de datos pública

PING sonda de paquetes InterNet

PDU unidad de datos de protocolo

PID identificación de proceso

P-P Punto a punto

PPP Point-to-Point Protocol

PROM memoria de sólo lectura programable

PU unidad física

PVC circuito virtual permanente

RAM memoria de acceso aleatorio

RD descriptor de ruta

REM supervisor de errores de anillo

REV recepción

RFC Request for Comments

RI indicador de llamada; información de direccionamiento

RIF campo de información de direccionamiento

RII indicador de información de direccionamiento

RIP Routing Information Protocol

RISC sistema de juego reducido de instrucciones

RNR recepción no preparada

ROM memoria de sólo lectura

ROpcon Consola del operador remota

RPS servidor de parámetros de anillo

RTMP Routing Table Maintenance Protocol

RTP RouTing update Protocol

RTS petición de emisión

Rtype tipo de ruta

rxmits retransmisiones

rxmt retransmisión

SAF filtración de direcciones de origen

SAP punto de acceso a servicios

SAP Service Advertising Protocol

SCR velocidad sostenida de célula

SCSP Server Cache Synchronization Protocol

sdel delimitador de inicio

SDLC relay de SDLC, control síncrono de enlace de datos

seqno número de secuencia

SGID identificación de grupo de servidores

SGMP Simple Gateway Monitoring Protocol

SL línea serie

SMP supervisor presente en espera

SMTP Simple Mail Transfer Protocol

SNA Systems Network Architecture

SNAP Subnetwork Access Protocol

SNMP Simple Network Management Protocol

SNPA punto de conexión de subred

SPF ruta intraárea OSPF

SPE1 tipo 1 de ruta externa OSPF

SPE2 tipo 2 de ruta externa OSPF

SPIA tipo de ruta interárea OSPF

SPID identificación de perfil de servicio

SPX Sequenced Packet Exchange

SQE error en calidad de señal

SRAM memoria de acceso aleatorio estática

SRB puente de direccionamiento de origen

SRF trama específicamente direccionada

SRLY relay de SDLC

SRT direccionamiento transparente de origen

SR-TB puente de direccionamiento transparente de origen

STA estático

STB puente de árbol de expansión

STE explorador de árbol de expansión

STP par trenzado y apantallado; protocolo de árbol de expansión

SVC circuito virtual conmutado

TB puente transparente

TCN notificación de cambio de topología

TCP Transmission Control Protocol

TCP/IP Transmission Control Protocol/Internet Protocol

TEI identificador de punto de terminal

TFTP Trivial File Transfer Protocol

TKR Red en Anillo

TMO tiempo de espera excedido

TOS tipo de servicio

TSF tramas de expansión transparentes

TTL período de duración

TTY teletipo

TX transmisión

UA acuse de recibo sin número

UDP User Datagram Protocol

UI información sin número

UTP par trenzado y no apantallado

VCC Conexión de canal virtual

VINES VIrtual NEtworking System

VIR velocidad de información variable

VL enlace virtual

VNI Virtual Network Interface

VR ruta virtual

WAN red de área amplia

WRS redireccionamiento/restauración de WAN

X.25 redes de paquetes conmutados

X.251 capa física de X.25

X.252 capa de trama de X.25

X.253 capa de paquetes de X.25

XID identificación de intercambio

XNS Xerox Network Systems

XSUM suma de comprobación

ZIP AppleTalk Zone Information Protocol

ZIP2 AppleTalk Zone Information Protocol 2

ZIT Tabla de información de zonas

Glosario

Este glosario incluye términos y definiciones de la documentación siguiente:

- El *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 del American National Standards Institute (ANSI). Los ejemplares pueden adquirirse en el American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Las definiciones se identifican mediante el símbolo (A) que aparece después de la definición.
- La *Fiber Optic Terminology*, ANSI/EIA norma—440-A. Los ejemplares pueden adquirirse en la Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006. Las definiciones se identifican mediante el símbolo (E) que aparece después de la definición.
- El *Information Technology Vocabulary* desarrollado por la Subcomisión 1, Comisión Técnica Mixta 1, de la Organización Internacional para la Normalización y la Comisión Electrotécnica Internacional (JTC1/SC1 de la ISO/IEC). Las definiciones de las secciones publicadas de este vocabulario se identifican mediante el símbolo (I) que aparece después de la definición; las definiciones de los borradores de normas internacionales, borradores de comisiones y documentos de trabajo que está desarrollando la JTC1/SC1 de la ISO/IEC se identifican mediante el símbolo (T) que aparece después de la definición, símbolo que indica que las Corporaciones Nacionales de la SC1 participantes todavía no han llegado a un acuerdo definitivo.
- El *IBM Dictionary of Computing*, New York: McGraw-Hill, 1994.
- Internet Request for Comments: 1208, *Glossary of Networking Terms*
- Internet Request for Comments: 1392, *Internet Users' Glossary*
- El *Object-Oriented Interface Design: IBM Common User Access Guidelines*, Carmel, Indiana: Que, 1992.

En este glosario, se utilizan las siguientes referencias cruzadas:

Compárese con: Se refiere a un término que tiene un significado opuesto o esencialmente distinto.

Sinónimo de: Indica que el término tiene el mismo significado que un término preferente, el cual está definido en el lugar que le corresponde dentro del glosario.

Sinónimo con: Es una referencia 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. Capa de adaptación de ATM, que es la que adapta los datos de usuario a/de la red ATM añadiendo/eliminando cabeceras y segmentando/volviendo a ensamblar los datos en/a partir de células.

AAL-5. Capa de adaptación de ATM 5, una de las diversas AAL estándares. AAL-5 se ha diseñado para las comunicaciones de datos y la utilizan la Emulación de LAN y el IP clásico.

acceso de memoria directo (DMA). Recurso del sistema que permite que un dispositivo del bus Micro Channel obtenga acceso directo a la memoria del sistema o a la memoria del bus sin la intervención del procesador del sistema.

acceso múltiple con detección de portadora y detección de colisión (CSMA/CD). Protocolo que necesita detección de portadora y en el que una estación de datos transmisora que detecta otra señal mientras transmite detiene la emisión, envía una señal de atasco y luego espera durante un período variable antes de volver a intentar la acción. (T) (A)

ACCESS. En el protocolo Simple Network Management Protocol (SNMP), cláusula de un módulo de la Base de la información de gestión (MIB) que define el nivel mínimo de soporte que proporciona un nodo gestionado para un objeto.

activo. (1) Operativo. (2) Perteneciente a un nodo o dispositivo que está conectado o está disponible para la conexión con otro nodo o dispositivo.

actualización de base de datos de topología (TDU). Mensaje sobre un nodo o enlace nuevo o modificado que se difunde entre los nodos de red APPN para mantener la base de datos de topología de red, que está reproducida en su totalidad en cada nodo de red. Una TDU contiene información para identificar lo siguiente:

- El nodo emisor
- Las características de nodo y enlace de diversos recursos de la red
- El número de secuencia de la actualización más reciente para cada uno de los recursos descritos.

acuse de recibo. (1) Transmisión, por parte de un receptor, de caracteres de acuse de recibo como respuesta afirmativa a un remitente. (T) (2) Indicación de que se ha recibido un elemento enviado.

Address Resolution Protocol (ARP). (1) En el conjunto de protocolos de Internet, protocolo que correlaciona dinámicamente una dirección IP con una dirección utilizada por una red de área metropolitana o local de soporte, como, por ejemplo, Ethernet o Red en Anillo. (2) Véase también *Reverse Address Resolution Protocol (RARP)*.

Advanced Peer-to-Peer Networking (APPN). Extensión de SNA que ofrece (a) un control superior de las redes distribuidas que evita las dependencias jerárquicas críticas y, por lo tanto, aisla los efectos de puntos anómalos individuales; (b) intercambio dinámico de información de topología de red para facilitar la conexión, reconfiguración y selección de rutas adaptables; (c) definición dinámica de recursos de red; y (d) automatización en el registro de recursos y la búsqueda en directorios. APPN hace extensiva la orientación de igual de la LU 6.2 para los servicios de usuario final al control de redes y da soporte a diversos tipos de LU, incluidas la LU 2, la LU 3 y la LU 6.2.

Agencia Operativa Privada Reconocida (RPOA). Cualquier individuo, empresa o corporación (que no sea un departamento o servicio del gobierno) que realiza operaciones en un servicio de telecomunicaciones y está sujeta a las obligaciones definidas en el Convenio de la Unión de Telecomunicaciones Internacionales y en la legislación; por ejemplo, una empresa de telecomunicación.

agente. Sistema que asume un papel de agente.

alerta. Mensaje enviado a un punto focal de servicios de gestión de una red para identificar un problema o un problema inminente.

American National Standards Institute (ANSI). Organización compuesta por productores, clientes y grupos con intereses generales que establece los procedimientos mediante los cuales organizaciones acreditadas crean y mantienen normas voluntarias de la industria en los Estados Unidos. (A)

analógico. (1) Perteneciente a datos compuestos por cantidades físicas continuamente variables. (A) (2) Compárese con *digital*.

Ancho de banda. El ancho de banda de un enlace óptico designa la capacidad de contener información del enlace y está relacionado con la máxima velocidad en bits a la que puede dar soporte un enlace de fibra.

anillo. Véase *red de tipo anillo*.

anomalía en la autenticación. En el protocolo Simple Network Management Protocol (SNMP), detección (de condición de excepción) que una entidad de autenticación puede haber generado cuando un cliente peticionario no es miembro de la comunidad de SNMP.

antememoria. (1) Almacenamiento intermedio de fines especiales más pequeño y rápido que el almacenamiento principal; se utiliza para que contenga una copia de instrucciones y datos obtenidos del almacenamiento principal y que probablemente necesitará a continuación el procesador. (T) (2) Almacenamiento intermedio que contiene instrucciones y datos a los que se accede frecuentemente; se utiliza para reducir el tiempo del acceso. (3) Parte opcional de la base de datos de directorios existente en los nodos de red donde puede almacenarse información de directorios de uso frecuente para acelerar las búsquedas en directorios. (4) Colocar, ocultar o almacenar en antememoria.

aparato de datos preparado (DSR). Sinónimo de *DCE preparado*.

AppleTalk. Protocolo de red desarrollado por Apple Computer, Inc. Este protocolo se utiliza para la interconexión de dispositivos de red, que pueden ser una mezcla de productos Apple y productos que no son Apple.

AppleTalk Address Resolution Protocol (AARP). En redes AppleTalk, protocolo que (a) convierte las direcciones de nodo AppleTalk en direcciones de hardware y (b) soluciona las discrepancias de direccionamiento en las redes que dan soporte a más de un conjunto de protocolos.

AppleTalk Transaction Protocol (ATP). En redes AppleTalk, protocolo que proporciona funciones de petición y respuesta de cliente/servidor a los sistemas principales que acceden al protocolo Zone Information Protocol (ZIP) para la información de zonas.

árbol de expansión. En contextos de LAN, método mediante el cual los puentes desarrollan automáticamente una tabla de direccionamiento y actualizan esta tabla en respuesta a un cambio de la topología para asegurarse de la existencia de una sola ruta entre dos LAN cualesquiera en la red con puentes. Este método evita bucles de paquetes, donde un paquete vuelve en una ruta de circuito al direccionador emisor.

archivo de configuración. Archivo que especifica las características de un dispositivo del sistema o una red.

área. En los protocolos de direccionamiento de Internet y DECnet, subconjunto de una red o pasarela que se ha agrupado por definición del administrador de red. Cada área es independiente; la información sobre la topología de un área permanece oculta respecto a las otras áreas.

arquitectura de red. Estructura lógica y principios operativos de una red de sistema. (T)

Nota: Los principios operativos de una red incluyen los principios de los servicios, funciones y protocolos.

arquitectura Interconexión de Sistemas Abiertos (OSI). Arquitectura de red que se ajusta al conjunto particular de normas ISO relacionado con Interconexión de Sistemas Abiertos. (T)

arreglo temporal del programa (PTF). Solución o ajuste temporal de un problema diagnosticado por IBM del release actual no modificado del programa.

asequibilidad. Capacidad de un nodo o recurso para comunicarse con otro nodo o recurso.

asíncrono (ASYNC). Perteneciente a dos o más procesos que no dependen de la aparición de sucesos específicos, como, por ejemplo, señales comunes de temporización. (T)

ATM. Asynchronous Transfer Mode, tecnología de red de gran velocidad orientada a las conexiones que se basa en la conmutación de células.

ATMARP. ARP en Classical IP.

B

base de datos de configuración (CDB). Base de datos que almacena los parámetros de configuración de uno o diversos dispositivos. Se prepara y actualiza utilizando el programa de configuración.

Base de la información de gestión (MIB). (1) Conjunto de objetos a los que se puede acceder por medio de un protocolo de gestión de red. (2) Definición de información de gestión que especifica la información disponible de un sistema principal o una pasarela y las operaciones permitidas. (3) En OSI, depósito conceptual de información de gestión dentro de un sistema abierto.

baudio. En la transmisión asíncrona, unidad de velocidad de modulación correspondiente al intervalo de una unidad por segundo; es decir, si la duración del intervalo de la unidad es de 20 milisegundos, la velocidad de modulación es de 50 baudios. (A)

bit D. Bit de confirmación de entrega. En comunicaciones X.25, bit de un paquete de datos o paquete de petición de llamada que se establece en 1 si el destinatario necesita acuse de recibo (confirmación de entrega) de extremo a extremo.

Border Gateway Protocol (BGP). Protocolo de direccionamiento Internet Protocol (IP) utilizado entre dominios y sistemas autónomos.

bucle de direccionamiento. Situación que ocurre cuando los direccionadores hacen circular información entre ellos hasta que se produce la convergencia o hasta que se consideran inasequibles las redes implicadas.

C

cabecera. (1) Información de control definida por el sistema que precede a los datos de usuario. (2) Parte de un mensaje que contiene información de control para el mismo, como, por ejemplo, uno o más campos de destino, el nombre de la estación de origen, el número de secuencia de entrada, una serie de caracteres que indica el tipo de mensaje y el nivel de prioridad del mensaje.

cabecera de transmisión (TH). Información de control, seguida opcionalmente de una unidad básica de información (BIU) o de un segmento de BIU, que crea y utiliza el control de la vía de acceso para direccionar unidades de mensajes y controlar su flujo dentro de la red. Véase también *unidad de información de vía de acceso*.

canal. (1) Vía de acceso por la que pueden enviarse señales, como, por ejemplo, canal de datos, canal de salida. (A) (2) Unidad funcional, controlada por el procesador, que maneja la transferencia de datos entre el almacenamiento del procesador y el equipo de periféricos local.

canal de entrada/salida. En un sistema de proceso de datos, unidad funcional que maneja la transferencia de datos entre el equipo interno y el equipo de periféricos. (I) (A)

canal lógico. En el funcionamiento en modalidad de paquete, canal de emisión y canal de recepción que se utilizan conjuntamente para enviar y recibir datos sobre un enlace de datos al mismo tiempo. Pueden establecerse varios canales lógicos en el mismo enlace de datos si se interpone la transmisión de paquetes.

capa. (1) En una arquitectura de red, grupo de servicios que está completo desde un punto de vista conceptual, que es uno de los grupos de un conjunto de grupos ordenados jerárquicamente y que se extiende por todos los sistemas que se ajustan a la arquitectura de red. (T) (2) En el modelo de referencia Interconexión de Sistemas Abiertos, uno de los siete grupos de servicios, funciones y protocolos ordenados jerárquicamente y completos conceptualmente que se extienden por todos los sistemas abiertos. (T) (3) En SNA, agrupación de funciones relacionadas que están separadas lógicamente de las funciones de otros grupos. La implementación de las funciones de una

capa puede cambiar sin que ello afecte a las funciones de otras capas.

capa de control de enlace de datos (DLC). En SNA, capa que está compuesta por las estaciones de enlace que planifican la transferencia de datos sobre un enlace entre dos nodos y realizan un control de errores para el enlace. Ejemplos de control de enlace de datos son: el SDLC para la conexión de enlaces serie por bit y el control de enlace de datos para el canal de System/370.

Nota: Normalmente, la capa de DLC es independiente del mecanismo de transporte físico y asegura la integridad de los datos que alcanzan las capas superiores.

capa de enlace de datos. En el modelo de referencia 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 relay en la vía de acceso. (T) Véase también *modelo de referencia Interconexión de Sistemas Abiertos*.

capa física. En el modelo de referencia Interconexión de Sistemas Abiertos, capa que proporciona los medios mecánicos, eléctricos, funcionales y de procedimiento para establecer, mantener y liberar conexiones físicas sobre el medio de transmisión. (T)

carácter comodín. Sinónimo de *carácter de coincidencia con el patrón*.

carácter de coincidencia con el patrón. Carácter especial, como, por ejemplo, un asterisco (*) o un signo de interrogación (?), que puede utilizarse para representar uno o más caracteres. Cualquier carácter o conjunto de caracteres puede sustituir a un carácter de coincidencia con el patrón. Sinónimo con *carácter global* y *carácter comodín*.

CCITT. Comisión Consultiva de la Telefonía y Telegrafía Internacionales. Era una organización de la Unión de Telecomunicaciones Internacionales (ITU). El 1 de marzo de 1993 se reorganizó la ITU y las responsabilidades de la normalización recayeron en una organización subordinada que se denomina Sector de Normalización de Telecomunicaciones de la Unión de Telecomunicaciones (ITU-TS). La “CCITT” sigue funcionando para las recomendaciones que se aprobaron antes de la reorganización.

central privada (PBX). Central telefónica privada para la transmisión de llamadas a y de la red telefónica pública.

Centro de información de la red (NIC). En comunicaciones de Internet, grupos locales, regionales y nacionales de todo el mundo que proporcionan ayuda, documentación, formación y otros servicios a los usuarios.

circuito de datos. (1) Par de canales de transmisión y recepción asociados que proporcionan un medio de comunicación de datos de dos direcciones. (I) (2) En SNA, sinónimo de *conexión de enlace*. (3) Véase también *circuito físico* y *circuito virtual*.

Notas:

1. Entre los intercambios de conmutaciones de datos, el circuito de datos puede incluir un equipo de terminación de circuito de datos (DCE) de acuerdo con el tipo de interfaz que se utilice en el intercambio de conmutaciones de datos.
2. Entre una estación de datos y un intercambio de conmmutaciones 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 (inteligente). Concentrador de cableado, como, por ejemplo, el IBM 8260, que proporciona funciones de puente y direccionamiento a las LAN con diferentes cables y protocolos.

Concentrador del acceso a L2TP (LAC). Dispositivo conectado a una o más líneas RDSI o de red telefónica de servicios públicos (PSTN) con posibilidades de manejar el funcionamiento de PPP y el del protocolo L2TP. El LAC implementa el medio sobre el que funciona L2TP. L2TP pasa el tráfico a uno o más Servidores de red L2TP (LNS). L2TP puede proporcionar la función de túnel para cualquier protocolo que conlleve la red PPP.

conectado mediante enlace. (1) Perteneciente a dispositivos que están conectados a una unidad de control por medio de un enlace de datos. (2) Compárese con *conectado mediante canal*. (3) Sinónimo con *remoto*.

conexión. En la comunicación de datos, asociación establecida entre unidades funcionales para comunicar información. (I) (A)

conexión de enlace. (1) Equipo físico que proporciona comunicación en dos direcciones entre una estación de enlace y otra u otras estaciones de enlace; por ejemplo, un equipo de terminación de circuito de datos (DCE) y una línea de telecomunicaciones. (2) En SNA, sinonimia con *circuito de datos*.

conexión Rapid Transport Protocol (RTP). En el direccionamiento de alto rendimiento (HPR), conexión establecida entre los puntos finales de la ruta para transportar tráfico de sesión.

conexión virtual. En frame relay, vía de acceso de vuelta de una conexión potencial.

configuración. (1) Manera en que están organizados e interconectados el hardware y el software de un sistema de proceso de información. (T) (2) Dispositivos y programas que componen un sistema, un subsistema o una red.

configuración del sistema. Proceso que especifica los dispositivos y programas que componen un sistema de proceso de datos determinado.

congestión. Véase *congestión de la red*.

congestión de la red. Condición no deseada de carga excesiva causada por la presencia de más tráfico del que puede manejar una red.

conmutación de la línea. Sinónimo de *conmutación del circuito*.

conmutación de paquetes. (1) Proceso consistente en direccionar y transferir datos por medio de paquetes dirigidos de manera que un canal esté ocupado durante la transmisión de un paquete solamente. Cuando se completa la transmisión, el canal queda disponible para la transferencia de otros paquetes. (I) (2) Sinónimo con *funcionamiento en modalidad de paquete*. Véase también *conmutación del circuito*.

conmutación del circuito. (1) Proceso que, a petición, conecta dos o más equipos terminales de datos (DTE) y permite el uso exclusivo de un circuito de datos entre ellos hasta que se libera la conexión. (I) (A) (2) Sinónimo con *conmutación de la línea*.

conmutación del enlace de datos (DLSw). Método para transportar protocolos de red que utilizan el tipo 2 de control de enlace lógico (LLC) de IEEE 802.2. SNA y NetBIOS son ejemplos de protocolos que utilizan el

tipo 2 de LLC. Véase también *encapsulación* y *simulación*.

contigua activa de donde proceden los datos (NAUN). En la Red en Anillo de IBM, estación que envía datos directamente a una estación determinada del anillo.

control de enlace de datos (DLC). Conjunto de normas utilizado por los nodos de un enlace de datos (como, por ejemplo, un enlace de SDLC o una Red en Anillo) para efectuar un intercambio de información ordenado.

control de enlace de datos de alto nivel (HDLC). En la comunicación de datos, utilización de una serie de bits especificada para controlar enlaces de datos de acuerdo con las normas internacionales respecto al HDLC: la estructura de trama de ISO 3309 y los elementos de procedimientos de ISO 4335.

control de enlace lógico (LLC). Subcapa de LAN de control de enlace de datos (DLC) que proporciona dos tipos de operaciones de DLC para el intercambio ordenado de información. El primer tipo es el servicio sin conexiones, que permite enviar y recibir información sin establecer un enlace. La subcapa de LLC no efectúa recuperación de errores ni control del flujo para el servicio sin conexiones. El segundo tipo es el servicio orientado a las conexiones, que requiere el establecimiento de un enlace antes del intercambio de información. El servicio orientado a las conexiones proporciona transferencia de información en secuencia, control del flujo y recuperación de errores.

control de la vía de acceso (PC). Función que direcciona unidades de mensajes entre las unidades de red accesibles de la red y proporciona las vías de acceso entre éstas. Convierte las unidades básicas de información (BIU) del control de transmisión (posiblemente segmentándolas) en unidades de información de vía de acceso (PIU) e intercambia unidades básicas de transmisión que contienen una o más PIU con el control de enlace de datos. El control de la vía de acceso difiere según el tipo de nodo: algunos nodos (los nodos APPN, por ejemplo) utilizan identificadores de sesión generados localmente para el direccionamiento y otros (los nodos de subárea) utilizan direcciones de red para el direccionamiento.

control del acceso al medio (MAC). En las LAN, subcapa de la capa de control de enlace de datos que da soporte a funciones dependientes del medio y utiliza los servicios de la capa física para proporcionar servicios a la subcapa de control de enlace lógico (LLC). La subcapa del MAC incluye el método para determinar cuándo un dispositivo tiene acceso al medio de transmisión.

control del flujo. (1) En SNA, proceso consistente en gestionar la velocidad a la que pasa el tráfico de datos entre los componentes de la red. La finalidad del control del flujo es optimizar la velocidad del flujo de unidades de mensajes con la congestión mínima de la red; es decir, ni desbordar los almacenamientos intermedios del receptor o de nodos de direccionamiento intermedio ni dejar al receptor esperando más unidades de mensajes. (2) Véase también *ritmo*.

Control síncrono de enlace de datos (SDLC). (1) Disciplina que se ajusta a los subconjuntos de los Advanced Data Communication Control Procedures (ADCCP) del American National Standards Institute (ANSI) y del High-level Data Link Control (HDLC) de la Organización Internacional para la Normalización, y está destinada a la gestión de la transferencia síncrona de información serie por bit de código transparente sobre una conexión de enlace. Los intercambios de transmisiones pueden ser dúplex o semi-dúplex sobre enlaces conmutados o no conmutados. La configuración de la conexión de enlace puede ser de punto a punto, de multipunto o de bucle. (I) (2) Compárese con *comunicación síncrona en binario (BSC)*.

correlación. Proceso consistente en convertir datos que el emisor transmite con un formato en el formato de datos que puede aceptar el receptor.

corriente de datos general (GDS). Corriente de datos utilizada para las conversaciones en sesiones de LU 6.2.

coste de la vía de acceso. En los protocolos de direccionamiento de estado de los enlaces, suma de los costes de enlace a lo largo de la vía de acceso entre dos nodos o redes.

cronometraje. (1) En la comunicación síncrona en binario, utilización de pulsaciones de reloj para controlar la sincronización de los datos y caracteres de control. (2) Método para controlar el número de bits de datos enviados en una línea de telecomunicaciones en un momento determinado.

cuenta de saltos. (1) Métrica o medida de distancia entre dos puntos. (2) En comunicaciones de Internet, número de direccionadores por los que pasa un datagrama cuando se dirige a su destino. (3) En SNA, medida consistente en el número de enlaces por los que pasar en la vía de acceso a un destino.

D

daemon. Programa que se ejecuta desatendido para realizar un servicio estándar. Algunos daemons se desencadenan de manera automática para realizar su tarea; otros realizan las operaciones periódicamente.

Datagram Delivery Protocol (DDP). En redes

AppleTalk, protocolo que proporciona conectividad de red por medio de un servicio de entrega de socket a socket sin conexiones de la capa de internet.

datagrama. (1) En la conmutación de paquetes, paquete individual e independiente de otros paquetes que contiene información suficiente para el direccionamiento desde el equipo terminal de datos (DTE) de origen al DTE de destino sin apoyarse en intercambios anteriores entre los DTE y la red. (I) (2) En TCP/IP, unidad básica de información que pasa a través del entorno de Internet. Un datagrama contiene direcciones de origen y de destino junto con los datos. Un datagrama de Internet Protocol (IP) está compuesto por una cabecera de IP seguida de los datos de capa de transporte. (3) Véase también *paquete* y *segmento*.

datagrama de IP. En el conjunto de protocolos de Internet, unidad básica de información transmitida a través de una internet. Contiene direcciones de origen y de destino, datos de usuario e información de control, como, por ejemplo, la longitud del datagrama, la suma de comprobación de cabecera y distintivos que indican si el datagrama puede fragmentarse o si se ha fragmentado.

DCE preparado. En la norma EIA 232, señal que indica al equipo terminal de datos (DTE) que el equipo de terminación de circuito de datos (DCE) local está conectado al canal de comunicaciones y se encuentra preparado para enviar datos. Sinónimo con *aparato de datos preparado (DSR)*.

DECnet. Arquitectura de red que define el funcionamiento de una familia de módulos de software, bases de datos y componentes de hardware que se utilizan normalmente con el fin de conectar entre sí sistemas Digital Equipment Corporation para el compartimiento de recursos, cálculo distribuido o configuración de sistemas remotos. Las implementaciones de la red DECnet siguen el modelo Digital Network Architecture (DNA).

detección (de condición de excepción). En Simple Network Management Protocol (SNMP), mensaje enviado por un nodo gestionado (la función de agente) a una estación de gestión para informarle de una condición de excepción.

detección de colisión. En el acceso múltiple con detección de portadora y detección de colisión (CSMA/CD), señal que indica que dos o más estaciones están transmitiendo simultáneamente.

detección de portadora. En una red de área local, actividad continua de una estación de datos para detectar si otra estación está transmitiendo. (T)

detector de portadora. Sinónimo de *detector de señal de línea recibida (RLSD)*.

detector de portadora de datos (DCD). Sinónimo de *detector de señal de línea recibida (RLSD)*.

detector de señal de línea recibida (RLSD). En la norma EIA 232, señal que indica al equipo terminal de datos (DTE) que está recibiendo una señal del equipo de terminación de circuito de datos (DCE) remoto. Sinónimo con *detector de portadora* y *detector de portadora de datos (DCD)*.

determinación de problemas. Proceso consistente en determinar el origen de un problema; por ejemplo, un componente de un programa, una anomalía en una máquina, recursos de telecomunicaciones, programas o equipos instalados por el contratista o por el usuario, una anomalía del entorno, como, por ejemplo, pérdida de alimentación, o un error del usuario.

difusión. (1) Transmisión de los mismos datos a todos los destinos. (T) (2) Transmisión simultánea de datos a más de un destino. (3) Compárese con *multidifusión*.

digital. (1) Perteneciente a datos compuestos por dígitos. (T) (2) Perteneciente a datos con formato de dígitos. (A) (3) Compárese con *analógico*.

Digital Network Architecture (DNA). Modelo para todas las implementaciones de hardware y software DECnet.

dirección. En la comunicación de datos, código exclusivo asignado a cada dispositivo, estación de trabajo o usuario conectado a una red.

dirección administrada localmente. En una red de área local, dirección de adaptador que el usuario puede asignar para alterar temporalmente la dirección administrada universalmente. Compárese con *dirección administrada universalmente*.

dirección administrada universalmente. En una red de área local, dirección codificada de forma permanente en un adaptador en el momento de la fabricación. Todas las direcciones administradas universalmente son exclusivas. Compárese con *dirección administrada localmente*.

dirección canónica. En las LAN, formato de IEEE 802.1 de la transmisión de direcciones del control del acceso al medio (MAC) para adaptadores de Red en Anillo y Ethernet. En el formato canónico, el bit menos significativo (situado más a la derecha) de cada byte de dirección se transmite en primer lugar. Compárese con *dirección no canónica*.

dirección de difusión. En comunicaciones, dirección de estación (ocho números 1) reservada como dirección común a todas las estaciones de un enlace. Sinónimo con *dirección de todas las estaciones*.

dirección de red. Según ISO 7498-3, nombre que no es ambiguo en el entorno de OSI y que identifica a un conjunto de puntos de acceso a servicios de red.

dirección de subred. En comunicaciones de Internet, extensión del esquema básico de direccionamiento de IP donde una parte de la dirección de sistema principal se interpreta como dirección de red local.

dirección de todas las estaciones. En comunicaciones, sinónimo de *dirección de difusión*.

dirección de usuario de red (NUA). En comunicaciones de X.25, dirección X.121 que contiene hasta 15 dígitos en código binario.

dirección Internet. Véase *dirección IP*.

dirección IP. Dirección de 32 bits definida por Internet Protocol, norma 5, Request for Comments (RFC) 791. Normalmente, se representa mediante notación decimal con puntos.

dirección no canónica. En las LAN, formato de la transmisión de direcciones del control del acceso al medio (MAC) para adaptadores de Red en Anillo. En el formato no canónico, el bit más significativo (situado más a la izquierda) de cada byte de dirección se transmite en primer lugar. Compárese con *dirección canónica*.

direccionador. (1) Sistema que determina la vía de acceso del flujo de tráfico de red. La selección de vía de acceso se realiza entre diversas vías de acceso sobre la base de la información obtenida a partir de protocolos específicos, algoritmos que intentan identificar la vía de acceso mejor o la más corta, y otros criterios, como, por ejemplo, direcciones de destino específicas de los protocolos o la métrica. (2) Dispositivo de conexión que conecta dos segmentos de LAN, los cuales utilizan arquitecturas similares o diferentes, en la capa de red del modelo de referencia. (3) En terminología de OSI, función que determina una vía de acceso mediante la cual puede accederse a una entidad. (4) En TCP/IP, sinonimia con *pasarela*. (5) Compárese con *puente*.

direccionador contiguo. Direccionador de una subred común designado por un administrador de red para recibir información de direccionamiento.

direccionador de frontera. En comunicaciones de Internet, direccionador que está posicionado al borde de un sistema autónomo y se comunica con un direccionador que está posicionado al borde de un sistema autónomo diferente.

direccionador de germinación. En redes AppleTalk, direccionador que mantiene datos de configuración (números de red de rango y listas de zonas, por ejemplo) para la red. Cada red debe tener, como mínimo, un direccionador de germinación. El direccionador de germinación debe configurarse 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. (1) Asignación de la vía de acceso mediante la cual un mensaje va a alcanzar su destino. (2) En SNA, reenvío de una unidad de mensaje por una vía de acceso determinada a través de una red tal como lo determinan los parámetros contenidos en la unidad de mensaje, como, por ejemplo, la dirección de red de destino de una cabecera de transmisión.

direccionamiento. En la comunicación de datos, manera que tiene una estación de seleccionar la estación a la que va a enviar datos.

direccionamiento de alto rendimiento (HPR). Adición para la arquitectura Advanced Peer-to-Peer Networking (APPN) que mejora el rendimiento y la fiabilidad del direccionamiento de datos, especialmente en la utilización de enlaces de gran velocidad.

direccionamiento de origen. En las LAN, método mediante el cual la estación emisora determina la ruta que la trama seguirá e incluye la información de direccionamiento en la trama. A continuación, los puentes leen la información de direccionamiento para determinar si deben reenviar la trama.

direccionamiento de sesiones intermedias (ISR). Tipo de función de direccionamiento de un nodo de red

APPN que proporciona información de indisponibilidad y control del flujo de nivel de sesión para todas las sesiones que pasan por el nodo pero cuyos puntos finales están en otra parte.

direccionamiento 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 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.

directorio. Tabla de identificadores y referencias para los elementos de datos correspondientes. (I) (A)

dispositivo. Aparato mecánico, eléctrico o electrónico con un fin específico.

dominio. (1) Parte de una red de sistema en la que los recursos de proceso de datos están bajo un control común. (T) (2) En Interconexión de Sistemas Abiertos (OSI), parte de un sistema distribuido o conjunto de objetos gestionados a los que se aplica una política común. (3) Véase *Dominio administrativo* y *nombre de dominio*.

Dominio administrativo. Conjunto de sistemas principales y direccionadores, y las redes de interconexión, que gestiona una sola autoridad administrativa.

dominio de direccionamiento. En comunicaciones de Internet, grupo de sistemas intermedios que utilizan un protocolo de direccionamiento para que la representación de la red en un conjunto sea la misma en cada sistema intermedio. Los dominios de direccionamiento se conectan entre sí mediante enlaces exteriores.

E

eco. En la comunicación de datos, señal de un canal de comunicaciones reflejada. Por ejemplo, en un terminal de comunicaciones, cada señal se visualiza dos veces, una cuando entra en el terminal local y otra cuando vuelve sobre el enlace de comunicaciones. Esto permite comprobar la exactitud de las señales.

EIA 232. En la comunicación de datos, especificación de la Electronic Industries Association (EIA) que define la interfaz entre el equipo terminal de datos (DTE) y el equipo de terminación de circuito de datos (DCE), que utiliza el intercambio de datos binarios serie.

Electronic Industries Association (EIA). Organización de fabricantes del campo de la electrónica que anticipa el crecimiento tecnológico de la industria, representa los puntos de vista de sus miembros y desarrolla normas para la industria.

Emulación de LAN (LE). Norma del ATM Forum que da soporte a aplicaciones de legado de LAN sobre redes ATM.

encapsulación. (1) En comunicaciones, técnica utilizada por protocolos de capa mediante la cual una capa añade a la unidad de datos de protocolo (PDU) información de control de la capa a la que da soporte. A este respecto, la capa encapsula los datos de la capa soportada. En el conjunto de protocolos de Internet, por ejemplo, un paquete contendrá información de control de la capa física, a continuación información de control de la capa de red y a continuación los datos de protocolo de la aplicación. (2) Véase también *conmutación del enlace de datos*.

enlace. Combinación de la conexión de enlace (el medio de transmisión) y dos estaciones de enlace, una a cada extremo de la conexión de enlace. Una conexión de enlace puede estar compartida entre diversos enlaces en una configuración de multipunto o Red en Anillo.

enlace lógico. Par de estaciones de enlace, una en cada uno de dos nodos adyacentes, y su conexión de enlace subyacente que proporcionan una sola conexión de capa de enlace entre los dos nodos. Pueden distinguirse diversos enlaces lógicos mientras comparten el uso del mismo medio físico de conexión de dos nodos. Ejemplos son los enlaces lógicos de 802.2 utilizados en recursos de red de área local (LAN) y los enlaces lógicos de LAP E del mismo enlace físico punto a punto entre dos nodos. El término enlace lógico también incluye los diversos canales lógicos de X.25 que comparten el uso del enlace de acceso de un DTE con una red X.25.

enlace virtual. En Open Shortest Path First (OSPF), interfaz punto a punto que conecta direccionadores de frontera separados por un área de tránsito no troncal. Puesto que los direccionadores de área forman parte del troncal OSPF, el enlace virtual conecta el troncal. Los enlaces virtuales aseguran que el troncal OSPF no se vuelva discontinuo.

equipo de terminación de circuito de datos (DCE). En una estación de datos, equipo que proporciona la conversión de señal y la codificación entre el equipo terminal de datos (DTE) y la línea. (I)

Notas:

1. El DCE puede ser un equipo independiente o parte integral del DTE o del equipo intermedio.
2. Un DCE puede realizar otras funciones que normalmente se llevan a cabo al final de red de la línea.

equipo terminal de datos (DTE). Parte de una estación de datos que funciona como origen y/o destino de datos. (I) (A)

esfera de control (SOC). Conjunto de dominios de punto de control servidos por un solo punto focal de servicios de gestión.

estación. Punto de entrada o salida de un sistema que utiliza recursos de telecomunicaciones; por ejemplo, uno o más sistemas, terminales, dispositivos y programas asociados de una ubicación determinada que pueden enviar o recibir datos sobre una línea de telecomunicaciones.

estación de enlace. (1) Componentes de hardware y software de un nodo que representan una conexión con un nodo adyacente sobre un enlace específico. Por ejemplo, si el nodo A es el extremo primario de una línea multipunto que se conecta con tres nodos adyacentes, el nodo A tendrá tres estaciones de enlace que representarán las conexiones con los nodos adyacentes. (2) Véase también *estación de enlace adyacente (ALS)*.

estación de gestión. En comunicaciones de Internet, sistema responsable de la gestión de toda una red o de parte de la misma. La estación de gestión se comunica con agentes de gestión de red que residen en el nodo gestionado por medio de un protocolo de gestión de red, como, por ejemplo, Simple Network Management Protocol (SNMP).

estación de gestión de red. En el protocolo Simple Network Management Protocol (SNMP), estación que ejecuta programas de aplicación de gestión que supervisan y controlan elementos de red.

estado de los enlaces. En los protocolos de direccionamiento, información anunciada sobre las interfaces utilizables y los direccionadores contiguos a un direccionador o una red asequibles. La base de datos topológica del protocolo se forma a partir de los anuncios reunidos sobre el estado de los enlaces.

Estructura de la información de gestión (SMI). (1) En el protocolo Simple Network Management Protocol (SNMP), normas utilizadas para definir los objetos a los que puede accederse por medio de un protocolo de gestión de red. (2) En OSI, conjunto de normas relativas a la información de gestión. El conjunto incluye el *Management Information Model* y las *Guidelines for the Definition of Managed Objects.*

Ethernet. Red de área local de banda base de 10 Mbps que permite que diversas estaciones accedan al medio de transmisión a voluntad sin coordinación previa, evita la 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.

fragmentación. (1) Proceso consistente en dividir un datagrama en partes más pequeñas, o fragmentos, para que se ajuste a las posibilidades del medio físico por el que se va a transmitir. (2) Véase también *segmentación*.

fragmento. Véase *fragmentación*.

frame relay. (1) Norma de interfaz que describe el límite entre el equipo de un usuario y una red de paquetes rápidos. En los sistemas frame-relay, se eliminan las tramas defectuosas; la recuperación tiene lugar de 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.

función de puente. En las LAN, el reenvío de una trama de un segmento de LAN a otro. El destino está especificado mediante la dirección de subcapa del control del acceso al medio (MAC) codificada en el campo de dirección de destino de la cabecera de la trama.

función de puente de ruta de origen. En las LAN, método de función de puente que utiliza el campo de información de direccionamiento de la cabecera del control del acceso al medio (MAC) de IEEE 802.5 de una trama para determinar los anillos o segmentos de Red en Anillo que debe recorrer la trama. El nodo de origen inserta el campo de información de direccionamiento en la cabecera del MAC. La información del campo de información de direccionamiento deriva de los paquetes exploradores generados por el sistema principal de origen.

función de puente local. Función de un programa de puente que permite que un solo puente conecte diversos segmentos de LAN sin la utilización de un enlace de telecomunicaciones. Compárese con *función de puente remota*.

función de puente remota. Función de un puente que permite que dos puentes conecten diversas LAN utilizando un enlace de telecomunicaciones. Compárese con *función de puente local*.

función de puente transparente. En las LAN, método para relacionar redes de área local individuales entre sí en el nivel del control del acceso al medio (MAC). Un puente transparente almacena las tablas que contienen direcciones del MAC para que las tramas que ve el puente puedan reenviarse a otra LAN si las tablas lo indican así.

función de túnel. Trata a una red de transporte como si fuera una sola LAN o un solo enlace de comunicaciones. Véase también *encapsulación*.

funcionamiento en modalidad de paquete. Sinónimo de *conmutación de paquetes*.

G

gestión de red. Proceso consistente en planificar, organizar y controlar un proceso de datos o sistema de información orientado a las comunicaciones.

gestor de red. Programa o grupo de programas que se utiliza para supervisar y gestionar una red así como para diagnosticar los problemas de la misma.

grupo de transmisión (TG). (1) Conexión entre nodos adyacentes que se identifica mediante un número de grupo de transmisión. (2) En una red de subárea, enlace o grupo de enlaces entre nodos adyacentes. Cuando un grupo de transmisión está compuesto por un grupo de enlaces, los enlaces se ven como un solo enlace lógico y el grupo de transmisión se denomina *grupo de transmisión multienlace (MLTG)*. Un *grupo de transmisión multienlace de mezcla de medios (MMMLTG)* contiene enlaces de diferentes tipos de medios (por ejemplo, Red en Anillo, SDLC conmutado, SDLC no conmutado y enlaces frame-relay). (3) En una red APPN, enlace entre nodos adyacentes. (4) Véase también *grupos de transmisión paralelo*.

grupos de transmisión paralelo. Diversos grupos de transmisión entre nodos adyacentes, teniendo cada grupo un número de grupo de transmisión distinto.

H

Hello. Protocolo utilizado por un grupo de direccionadores que cooperan y se apoyan entre sí para poder descubrir rutas de retardo mínimo.

heurístico. Perteneciente a métodos exploratorios para la resolución de problemas en los que se descubren soluciones mediante una evaluación del progreso realizada respecto al resultado final.

histéresis. Cantidad que indica cuánto debe cambiar la temperatura una vez pasado el umbral del establecimiento de alerta y antes de que se elimine la condición de alerta.

horizonte dividido. Técnica destinada a minimizar el tiempo para conseguir la convergencia en la red. Un direccionador registra la interfaz sobre la que ha recibido una ruta en particular y no propaga su información sobre la ruta otra vez sobre la misma interfaz.

I

identificación de intercambio (XID). Tipo específico de unidad básica de enlace que se utiliza para la comunicación de características de nodo y enlace entre nodos adyacentes. Los XID se intercambian entre estaciones de enlace antes de la activación del enlace y durante la misma para establecer y negociar las características de enlace y nodo, y después de la activación del enlace para comunicar los cambios de estas características.

identificador de conexión de enlace de datos (DLCI). Identificador numérico de un subpuerto frame-relay o segmento de PVC en una red frame-relay. Cada subpuerto de un puerto frame-relay individual tiene un DLCI exclusivo. La tabla siguiente, extraída de la norma T1.618 del American National Standards Institute (ANSI) y la norma Q.922 de la Comisión Consultiva de la Telefonía y Telegrafía Internacionales (ITU-T/CCITT),

indica las funciones asociadas con determinados valores de DLCI:

Valores de DLCI	Función
0	señalización de canal de entrada
1–15	se reserva
16–991	se asigna utilizando procedimientos de conexión de frame-relay
992–1007	gestión de capa 2 de servicio portador de frame-relay
1008–1022	se reserva
1023	gestión de capa de canal de entrada

identificador de puente. Campo de 8 bytes que se utiliza en un protocolo de árbol de expansión y está compuesto por la dirección MAC del puerto con el identificador de puerto más 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 ID de red depende del tipo de la clase de red (A, B o C).
(2) Nombre de 1 a 8 bytes seleccionado por el cliente o nombre de 8 bytes registrado por IBM que identifica de manera exclusiva a una subred específica.

inhabilitado. (1) Perteneciente a un estado de una unidad de proceso que evita la aparición de determinados tipos de interrupciones. (2) Perteneciente al estado en el cual una unidad de control de transmisión o unidad de respuestas audibles no puede aceptar llamadas de entrada de una línea.

inhabilitar. Convertir en no funcional.

Integrated Digital Network Exchange (IDNX). Procesador que integra aplicaciones a base de voz, datos e imágenes. También gestiona los recursos de transmisión y se conecta a multiplexores y sistemas de soporte de gestión de redes. Permite la integración de equipos de diferentes proveedores.

intercambio de conmutaciones de datos (DSE). Equipo instalado en una ubicación individual para proporcionar funciones de conmutación, como, por ejemplo, conmutación del circuito, conmutación de mensajes y conmutación de paquetes. (I)

Interconexión de Sistemas Abiertos (OSI).
(1) Interconexión de sistemas abiertos que sigue las normas de la Organización Internacional para la Normalización (ISO) para el intercambio de información. (T) (A) (2) Utilización de procedimientos normalizados para permitir la interconexión de sistemas de proceso de datos.

Nota: La arquitectura OSI establece una infraestructura para coordinar el desarrollo de normas actuales y futuras de cara a la interconexión de sistemas. Las funciones de red se dividen en siete capas. Cada capa representa un grupo de funciones relacionadas de proceso de datos y comunicación que pueden llevarse a cabo de una manera estándar para dar soporte a diferentes aplicaciones.

interfaz. (1) Límite compartido entre dos unidades funcionales en cuya definición entran características funcionales, características de señalización u otras características según lo que corresponda. El concepto incluye la especificación de la conexión de dos dispositivos que tienen funciones diferentes. (T)
(2) Hardware y/o software para el enlace de sistemas, programas o dispositivos.

interfaz de gestión local (LMI). Véase *protocolo de interfaz de gestión local (LMI)*.

interfaz de unidad de conexión (AUI). En una red de área local, interfaz entre la unidad de conexión al medio y el equipo terminal de datos de una estación de datos. (I) (A)

Interior Gateway Protocol (IGP). En el conjunto de protocolos de Internet, protocolo utilizado para propagar información sobre la asequibilidad y direccionamiento de la red dentro de un sistema autónomo. Ejemplos de IGP son Routing Information Protocol (RIP) y Open Shortest Path First (OSPF).

Internet. Red internet administrada por la Internet Architecture Board (IAB) y compuesta por grandes redes troncales nacionales así como por muchas redes regionales y de campus en todo el mundo. Internet utiliza el conjunto de protocolos de Internet.

internet. Conjunto de redes interconectadas por una serie de direccionadores que les permiten funcionar como una sola red grande. Véase también *Internet*.

Internet Architecture Board (IAB). Corporación técnica que supervisa el desarrollo del conjunto de protocolos de Internet conocidos como TCP/IP.

Internet Control Message Protocol (ICMP). Protocolo utilizado para manejar mensajes de control y errores en la capa de Internet Protocol (IP). Los informes sobre problemas y destinos incorrectos de datagramas se devuelven al origen del datagrama. ICMP forma parte de Internet Protocol.

Internet Control Protocol (ICP). Protocolo de VIrtual NEtworking System (VINES) que proporciona notificaciones de excepciones, notificaciones sobre métrica y el soporte del programa PING. Véase también *RouTing update Protocol (RTP)*.

Internet Engineering Task Force (IETF). Grupo de operaciones de la Internet Architecture Board (IAB) que

es responsable de la resolución de las necesidades técnicas de la Internet a corto plazo.

Internet Protocol (IP). Protocolo sin conexiones que direcciona datos a través de una red o redes interconectadas. IP actúa como intermediario entre las capas de protocolos superiores y la red física. No obstante, este protocolo no proporciona recuperación de errores ni control del flujo ni garantiza la fiabilidad de la red física.

Internetwork Packet Exchange (IPX). (1) Protocolo de red utilizado para conectar servidores Novell, o cualquier estación de trabajo o direccionador que implemente IPX, con otras estaciones de trabajo. Aunque es similar a Internet Protocol (IP), IPX utiliza unos formatos de paquete y una terminología diferentes. (2) Véase también *Xerox Network Systems (XNS)*.

interoperatividad. Posibilidad de comunicarse, ejecutar programas o transferir datos entre diversas unidades funcionales de tal forma que el usuario necesite tener poco conocimiento, o ninguno, de las características exclusivas de estas unidades. (T)

Inverse Address Resolution Protocol (InARP). En el conjunto de protocolos de Internet, protocolo utilizado para ubicar una dirección de protocolo mediante la dirección de hardware conocida. En un contexto de frame-relay, identificador de conexión de enlace de datos (DLCI) es sinónimo de dirección de hardware conocida.

IPPN. Interfaz que otros protocolos pueden utilizar para transportar datos sobre IP.

IPXWAN. Protocolo de Novell que se utiliza para intercambiar información de direccionador a direccionador antes de intercambiar información de direccionamiento de Internetwork Packet Exchange (IPX) estándar y tráfico sobre redes de área amplia (WAN).

L

LAN Network Manager (LNM). Programa bajo licencia de IBM que permite que un usuario gestione y supervise recursos de LAN desde una estación de trabajo central.

LE. Emulación de LAN. Norma del ATM Forum que da soporte a aplicaciones de legado de LAN sobre redes ATM.

LEC. Cliente de emulación de LAN. Componente de la Emulación de LAN que representa a los usuarios de la LAN emulada.

LECS. Servidor de configuración de emulación de LAN. Componente de LAN Emulation Service que centraliza y difunde datos de configuración.

LES. Servidor de emulación de LAN. Componente de LAN Emulation Service que resuelve destinos de LAN en direcciones ATM.

local. (1) Perteneciente a un dispositivo al que se accede directamente sin utilizar una línea de telecomunicaciones. (2) Compárese con *remoto*. (3) Sinónimo de *conectado mediante canal*.

M

mandato ping. Mandato que envía un paquete de 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.

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.

módulo. (1) Perteneciente a un módulo matemático; por ejemplo, 9 equivale a 4 módulo 5. (2) Véase también *módulo (diferencia)*.

módulo (diferencia). Número, como, por ejemplo, un entero positivo, de una relación que divide la diferencia entre dos números relacionados sin dejar un resto; por ejemplo, 9 y 4 tienen un módulo de 5 (9 - 4 = 5; 4 - 9 = -5; y 5 divide tanto 5 como -5 sin dejar un resto).

N

Name Binding Protocol (NBP). En redes AppleTalk, protocolo que proporciona la función de conversión de nombre del nombre (serie de caracteres) de entidad (recurso) AppleTalk en una dirección IP AppleTalk (número de 16 bits) en la capa de transporte.

NetBIOS. Network Basic Input/Output System. Interfaz estándar para redes, IBM PC (Personal Computer) y PC compatibles que se utiliza en las LAN para proporcionar funciones de mensajes, de servidor de impresión y de servidor de archivos. Los programas de aplicación que utilizan NetBIOS no necesitan manejar los detalles de protocolos de control de enlace de datos (DLC) de LAN.

nivel de enlace. (1) Parte de la recomendación X.25 que define el protocolo de enlace utilizado para entrar datos en la red y sacarlos de la misma a través del enlace dúplex que conecta la máquina del abonado con el nodo de red. LAP y LAPB son los protocolos de acceso de enlace recomendados por la CCITT. (2) Véase *nivel de enlace de datos*.

nivel de enlace de datos. (1) En la estructura jerárquica de una estación de datos, nivel conceptual de control o lógica de proceso entre la lógica de alto nivel y el enlace de datos que mantiene el control del enlace de datos. El nivel de enlace de datos realiza funciones tales como la inserción de bits de transmisión y supresión de bits de recepción; interpretación de campos de dirección y control; generación, transmisión e interpretación de mandatos y respuestas; y cálculo e interpretación de secuencias de comprobación de trama. Véase también *nivel de paquete* y *nivel físico*. (2) En comunicaciones de X.25, sinónimo de *nivel de trama*.

nivel de trama. Sinónimo con *nivel de enlace de datos*. Véase *nivel de enlace*.

nodo. (1) En una red, punto donde una o más unidades funcionales conectan canales o circuitos de datos. (I) (2) Cualquier dispositivo conectado a una red que transmite y recibe datos.

nodo Advanced Peer-to-Peer Networking (APPN). Nodo de red APPN o nodo final APPN.

nodo de destino. Nodo al que se envían datos o una petición.

nodo de esfera de control (SOC). Nodo que está incluido directamente en la esfera de control de un punto focal. Un nodo de SOC ha intercambiado elementos de habilitación de los servicios de gestión con su punto focal. Un nodo final APPN puede ser un nodo de SOC si da soporte a la función de intercambio de elementos de habilitación de los servicios de gestión.

nodo de red (NN). Véase *nodo de red Advanced Peer-to-Peer Networking (APPN)*.

nodo de red Advanced Peer-to-Peer Networking (APPN). Nodo que ofrece un amplio rango de servicios de usuario final y que puede proporcionar lo siguiente:

- Servicios de directorios distribuidos, incluido el registro de los recursos del dominio con un servidor de directorios central
- Intercambios de bases de datos de topología con otros nodos de red APPN, lo que permite que los nodos de red de la red seleccionen las rutas

óptimas para sesiones de LU-LU basándose en las clases de servicio solicitadas

- Servicios de sesiones para los nodos finales clientes y las LU locales
- Servicios de direccionamiento intermedio de una red APPN

nodo de red APPN. Véase *nodo de red Advanced Peer-to-Peer Networking (APPN)*.

nodo de red de entrada baja (LEN). Nodo que proporciona un rango de servicios de usuario final, se conecta directamente con otros nodos utilizando protocolos de igual a igual y hace derivar servicios de red de un nodo de red APPN adyacente implícitamente, es decir, sin el uso directo de sesiones de CP-CP.

nodo final (EN). (1) Véase *nodo final Advanced Peer-to-Peer Networking (APPN)* y *nodo final de red de entrada baja (LEN)*. (2) En comunicaciones, nodo que se conecta frecuentemente a un solo enlace de datos y no puede realizar funciones de direccionamiento intermedio.

nodo final Advanced Peer-to-Peer Networking (APPN). Nodo que proporciona un amplio rango de servicios de usuario final y da soporte a las sesiones entre su punto de control (CP) local y el CP de un nodo de red adyacente. Utiliza estas sesiones con el fin de registrar dinámicamente sus recursos con el CP adyacente (su servidor de nodos de red) para enviar y recibir peticiones de búsqueda en directorios y obtener servicios de gestión. Un nodo final APPN también puede conectarse a una red de subárea como nodo periférico o a otros nodos finales.

nodo final de red de entrada baja (LEN). Nodo LEN que recibe servicios de red de un nodo de red APPN adyacente.

nodo intermedio. Nodo que está al final de más de una rama. (T)

nodos adyacentes. Dos nodos conectados conjuntamente por una vía de acceso, como mínimo, que no conecta ningún otro nodo. (T)

nombre de comunidad. En el protocolo Simple Network Management Protocol (SNMP), serie de octetos que identifica a una comunidad.

nombre de dominio. En el conjunto de protocolos de Internet, nombre de un sistema principal. Un nombre de dominio está compuesto por una secuencia de subnombres separados por un carácter delimitador. Por ejemplo, si el nombre de dominio calificado al completo (FQDN) de un sistema principal es `ralvm7.vnet.ibm.com`, cada uno de los siguientes es un nombre de dominio:

- `ralvm7.vnet.ibm.com`
- `vnet.ibm.com`
- `ibm.com`

notación de sintaxis de abstracción 1 (ASN.1). Método de Interconexión de Sistemas Abiertos (OSI) para la sintaxis de abstracción que se especifica en las normas siguientes:

- ITU-T recomendación X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T recomendación X.680 (1994) | ISO/IEC 8824-1: 1994

Véase también *normas básicas de codificación (BER)*.

notación decimal con puntos. Representación sintáctica de un entero de 32 bits que consta de cuatro números de 8 bits escritos en base 10 con puntos que los separan. Se utiliza para representar direcciones IP.

número de puerto. En comunicaciones de Internet, identificación de una entidad de aplicación para el servicio de transporte.

número de secuencia. En comunicaciones, número asignado a una trama o paquete determinados para controlar el flujo de la transmisión y la recepción de datos.

número de sistema autónomo. En TCP/IP, número asignado a un sistema autónomo por la misma autorización central que también asigna direcciones IP. El número de sistema autónomo hace posible que los algoritmos de direccionamiento automatizado distingan los sistemas autónomos.

O

objeto de la MIB. Sinónimo de *variable de la MIB*.

Open Shortest Path First (OSPF). En el conjunto de protocolos de Internet, función que proporciona transferencia de información intradominio. Como alternativa al protocolo Routing Information Protocol (RIP), OSPF permite el direccionamiento de menor coste y lo maneja en grandes redes regionales o corporativas.

Organización Internacional para la Normalización (ISO). Organización de corporaciones nacionales de normas de varios países establecida para promocionar el desarrollo de normas con el fin de facilitar el intercambio internacional de artículos y servicios además de desarrollar la cooperación en la actividad intelectual, científica, tecnológica y económica.

origen. Unidad lógica (LU) externa o programa de aplicación de donde parten un mensaje u otros datos. Véase también *destino*.

P

paquete. En la comunicación de datos, secuencia de dígitos binarios, con inclusión de señales de control y datos, que se transmite y se conmuta como un todo compuesto. Los datos, las señales de control y, posiblemente, la información de control de errores se ordenan siguiendo un formato específico. (I)

paquete de datos. En comunicaciones de X.25, paquete utilizado para la transmisión de datos de usuario dentro de un circuito virtual en la interfaz DTE/DCE.

paquete de petición de llamada. (1) Paquete de supervisión de llamada que un equipo terminal de datos (DTE) transmite con el fin de solicitar que se establezca una conexión para una llamada en la red. (2) En comunicaciones de X.25, paquete de supervisión de llamada transmitido por un DTE para solicitar el establecimiento de una llamada en la red.

paquete de petición de restablecimiento. En comunicaciones X.25, paquete transmitido por el equipo terminal de datos (DTE) al equipo de terminación de circuito de datos (DCE) para solicitar que se restablezca una llamada virtual o un circuito virtual permanente. En el paquete también puede especificarse la razón de la petición.

paquete de recepción no preparada (RNR). Véase *paquete de RNR*.

paquete de RNR. Paquete utilizado por un equipo terminal de datos (DTE) o por un equipo de terminación de circuito de datos (DCE) con el fin de indicar una incapacidad temporal para aceptar paquetes adicionales de petición de llamada virtual o circuito virtual permanente.

paquete explorador. En las LAN, paquete que está generado por el sistema principal de origen y que atraviesa toda la parte de direccionamiento de origen de una LAN con el fin de recoger información sobre las posibles vías de acceso que se encuentran disponibles para el sistema principal.

Par de valores de atributo (AVP). Método uniforme de codificación de tipos y cuerpos de mensajes. Este método maximiza la extensibilidad mientras permite la interoperatividad de L2TP.

parámetro de configuración. Variable de una definición de configuración cuyos valores pueden caracterizar la relación de un producto con otros productos de la misma red o pueden definir características del producto en sí.

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.

peticionario 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 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 (SAP). (1) En la arquitectura Interconexión de Sistemas Abiertos (OSI), punto en el que una entidad de una capa proporciona los servicios de esta capa a una entidad de la capa superior más próxima. (T) (2) Punto lógico que queda disponible mediante un adaptador y donde puede recibirse y transmitirse información. Muchos enlaces pueden terminar en un solo punto de acceso a servicios.

punto de acceso a servicios de destino (DSAP). En SNA y TCP/IP, dirección lógica que permite que un sistema direccione datos desde un dispositivo remoto al soporte de comunicaciones correspondiente. Compárese con *punto de acceso a servicios de origen (SSAP)*.

punto de acceso a servicios de origen (SSAP). En SNA y TCP/IP, dirección lógica que permite que un sistema envíe datos a un dispositivo remoto desde el

soporte de comunicaciones correspondiente. Compárese con *punto de acceso a servicios de destino (DSAP)*.

punto de control (CP). (1) Componente de un nodo APPN o LEN que gestiona los recursos de dicho nodo. En un nodo APPN, el CP puede dedicarse a establecer sesiones de CP-CP con otros nodos APPN. En un nodo de red APPN, el CP también proporciona servicios a nodos finales adyacentes de la red APPN. (2) Componente de un nodo que gestiona los recursos de dicho nodo y, opcionalmente, proporciona servicios a otros nodos de la red. Pueden citarse como ejemplos el punto de control de servicios del sistema (SSCP) de un nodo de subárea de tipo 5, el punto de control de nodo de red (NNCP) de un nodo de red APPN y el punto de control de nodo final (ENCP) de un nodo final APPN o LEN. Un SSCP y un NNCP pueden proporcionar servicios a otros nodos.

punto de control de servicios del sistema (SSCP). Componente de una red de subárea destinado a gestionar la configuración, coordinar las peticiones del operador de red y las de determinación de problemas y proporcionar servicios de directorios además de otros servicios de sesiones para los usuarios de la red. Diversos SSCP, cooperando como iguales entre sí, pueden dividir la red en dominios de control y tener, cada uno de los SSCP, una relación de control jerárquica con las unidades físicas y las unidades lógicas de su propio dominio.

punto de entrada (EP). En SNA, nodo de tipo 2.0, tipo 2.1, tipo 4 ó tipo 5 que proporciona soporte de gestión de redes distribuidas. Envía datos de gestión de redes sobre sí mismo y los recursos que controla a un punto focal para el proceso centralizado, y recibe y ejecuta los mandatos iniciados por el punto focal para gestionar y controlar sus recursos.

R

rastreo. (1) Registro de la ejecución de un programa de sistema. Muestra las secuencias en que se han ejecutado las instrucciones. (A) (2) Para los enlaces de datos, registro de las tramas y bytes transmitidos o recibidos.

recepción no preparada (RNR). En comunicaciones, mandato o respuesta de enlace de datos que indica una condición temporal de incapacidad para aceptar tramas de entrada.

reconfiguración dinámica (DR). Proceso consistente en cambiar la configuración de una red (las PU y LU periféricas) sin regenerar las tablas de configuración al completo ni desactivar el nodo principal afectado.

red. (1) Configuración de software y dispositivos de proceso de datos conectados para el intercambio de información. (2) Grupo de nodos y los enlaces que los interconectan.

red Advanced Peer-to-Peer Networking (APPN). Conjunto de nodos de red interconectados y sus nodos finales clientes.

red APPN. Véase *red Advanced Peer-to-Peer Networking (APPN)*.

red de área amplia (WAN). (1) Red que proporciona servicios de comunicación a un área geográfica mayor que la servida por una red de área local o una red de área metropolitana, y que puede utilizar o proporcionar recursos públicos de comunicación. (T) (2) Red de comunicación de datos diseñada para servir a un área de cientos o miles de kilómetros; por ejemplo, las redes públicas y privadas de conmutación de paquetes y las redes telefónicas nacionales. (3) Compárese con *red de área local (LAN)* y *red de área metropolitana (MAN)*.

red de área local (LAN). (1) Red de sistema ubicada en el lugar de un usuario dentro de un área geográfica limitada. La comunicación dentro de una red de área local no está sujeta a reglamentos externos; no obstante, la comunicación más allá del límite de una LAN puede estar sujeta a alguna forma de reglamento. (T) (2) Red en la que un conjunto de dispositivos están conectados entre sí para la comunicación y que puede conectarse a una red mayor. (3) Véase también *Ethernet* y *Red en Anillo*. (4) Compárese con *red de área metropolitana (MAN)* y *red de área amplia (WAN)*.

red de área metropolitana (MAN). Red formada por la interconexión de dos o más redes que puede funcionar a una velocidad mayor que éstas, puede atravesar límites administrativos y puede utilizar diversos métodos de acceso. (T) Compárese con *red de área local (LAN)* y *red de área amplia (WAN)*.

red de clase A. En comunicaciones de Internet, red en la que el bit situado más a la izquierda (más significativo) de la dirección IP está establecido en 0 y el ID de sistema principal ocupa los tres octetos situados más a la derecha.

red de clase B. En comunicaciones de Internet, red en la que los dos bits situados más a la izquierda (más significativo y próximo al más significativo) de la dirección IP están establecidos en 1 y 0, respectivamente, y el ID de sistema principal ocupa los dos octetos situados más a la derecha.

red de entrada baja (LEN). Posibilidad de los nodos de conectarse directamente entre sí utilizando protocolos básicos de igual a igual para dar soporte a sesiones múltiples y en paralelo entre unidades lógicas.

red de tipo anillo. (1) Red en la que cada nodo tiene exactamente dos ramas conectadas y en la que hay

exactamente dos vías de acceso entre dos nodos cualesquiera. (T) (2) Configuración de red en la que los dispositivos están conectados mediante enlaces de transmisión unidireccional para formar una vía de acceso cerrada.

red digital de servicios integrados (RDSI). Red digital de telecomunicaciones de 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 IEEE 802.5, tecnología de red que controla el acceso al medio pasando una señal (paquete o trama especial) entre las estaciones conectadas al medio. (2) IEEE 802.5 con una topología de anillo que pasa señales de una estación de anillo de conexión (nodo) a otra. (3) Véase también *red de área local (LAN)*.

red según Red en Anillo. (1) Red de tipo anillo que permite la transmisión de datos unidireccional entre estaciones de datos, mediante un procedimiento consistente en pasar señales, de tal manera que los datos transmitidos vuelven a la estación transmisora. (T) (2) Red que utiliza una topología de anillo, según la cual pasan señales en un circuito de nodo a nodo. Un nodo que está preparado para emitir puede capturar la señal e insertar datos para la transmisión.

red troncal. Red central a la que se conectan redes más pequeñas, casi siempre de menor velocidad. Normalmente, la red troncal tiene una capacidad muy superior a las redes a las que ayuda a interconectarse o es una red de área amplia (WAN), como, por ejemplo, una red pública de datagramas de paquetes conmutados.

reensamblaje. En comunicaciones, proceso consistente en volver a juntar paquetes segmentados después de haberlos recibido.

Registro sin vuelta a cero y con cambios en los unos (NRZ-1). Método de registro donde los unos están representados mediante un cambio en la condición de magnetización y los ceros están representados mediante la ausencia de cambio. Sólo se registran explícitamente las señales de los unos. (Denominado anteriormente registro ***sin vuelta a cero invertido***, NRZI.)

Remote Execution Protocol (REXEC). Protocolo que permite la ejecución de un mandato o programa en cualquier sistema principal de la red. El sistema principal local recibe los resultados de la ejecución del mandato.

remoto. (1) Perteneciente a un sistema, programa o dispositivo al que se accede mediante una línea de telecomunicaciones. (2) Sinónimo de *conectado mediante enlace*. (3) Compárese con *local*.

Request for Comments (RFC). En comunicaciones de Internet, serie de documentos que describe una parte del conjunto de protocolos de Internet y experimentos relacionados. Todas las normas de Internet están documentadas como RFC.

resolución de direcciones. (1) Método para correlacionar direcciones de capa de red con direcciones específicas de los medios. (2) Véase también *Address Resolution Protocol (ARP)* y *AppleTalk Address Resolution Protocol (AARP)*.

resolución de nombres. En comunicaciones de Internet, proceso consistente en correlacionar un nombre de máquina con la dirección Internet Protocol (IP) correspondiente. Véase también *Sistema de nombres de dominio (DNS)*.

respuesta a excepción (ER). En SNA, protocolo solicitado en el campo de formato de respuesta solicitado de la cabecera de una petición que indica al receptor que devuelva una respuesta sólo si la petición no es aceptable tal como se recibe o si no puede procesarse; es decir, puede devolverse una respuesta negativa, pero no una respuesta positiva. Compárese con *respuesta definida* y *sin respuesta*.

restablecimiento. En un circuito virtual, reinicialización del control del flujo de datos. En el restablecimiento, se eliminan todos los datos en tránsito.

ritmo. (1) Técnica mediante la cual un componente de recepción controla la velocidad de transmisión de un componente de emisión para evitar un desbordamiento o una congestión. (2) Véase también *control del flujo*, *ritmo de recepción*, *ritmo de emisión*, *ritmo de nivel de sesión* y *ritmo de ruta virtual (VR)*.

rlogin (inicio de sesión remoto). Servicio ofrecido por los sistemas de Berkeley basados en UNIX que permite que los usuarios autorizados de una máquina se conecten con otros sistemas UNIX en una internet e interactúen como si sus terminales estuvieran conectados directamente. El software rlogin pasa información sobre el entorno del usuario (por ejemplo, el tipo de terminal) a la máquina remota.

Routing Information Protocol (RIP). En el conjunto de protocolos de Internet, protocolo de pasarela interior utilizado para intercambiar información de direccionamiento intradominio y para determinar las rutas óptimas entre los sistemas principales de internet. RIP determina las rutas óptimas sobre la base de la métrica de ruta y no sobre la base de la velocidad de transmisión de un enlace.

Routing Table Maintenance Protocol (RTMP). En redes AppleTalk, protocolo que proporciona generación y mantenimiento de información de direccionamiento en la capa de transporte por medio de la tabla de direccionamiento AppleTalk. La tabla de direccionamiento AppleTalk dirige la transmisión de paquetes por la internet de socket de origen a socket de destino.

RouTing update Protocol (RTP). Protocolo de VIrtual NEtworking System (VINES) que mantiene la base de datos de direccionamiento y permite el intercambio de información de direccionamiento entre nodos VINES. Véase también *Internet Control Protocol (ICP)*.

rsh. Variante del mandato rlogin que invoca un interpretador de mandatos en una máquina remota UNIX y pasa los argumentos de línea de mandatos al interpretador de mandatos saltándose completamente el paso de inicio de sesión.

ruta. (1) Secuencia ordenada de nodos y grupos de transmisión (TG) que representan una vía de acceso de un nodo de origen a un nodo de destino por la que pasa el tráfico intercambiado entre éstos. (2) Vía de acceso que el tráfico de red utiliza para ir del origen al destino.

ruta estática. Ruta entre sistemas principales y/o redes que se entra manualmente en una tabla de direccionamiento.

ruta explícita (ER). En SNA, serie de uno o más grupos de transmisión que conectan dos nodos de subárea. Una ruta explícita se identifica mediante una dirección de subárea de origen, una dirección de subárea de destino, un número de ruta explícita y un número de ruta explícita inversa. Compárese con *ruta virtual (VR)*.

ruta virtual (VR). (1) En SNA, (a) conexión lógica entre dos nodos de subárea que se realiza físicamente como una ruta explícita en particular o (b) conexión lógica contenida en su totalidad dentro de un nodo de subárea para las sesiones intranodo. Una ruta virtual entre nodos de subárea distintos impone una prioridad de transmisión sobre la ruta explícita subyacente, proporciona control del flujo mediante el ritmo de ruta virtual y proporciona la integridad de los datos mediante la numeración en secuencia de las unidades de información de vía de acceso (PIU). (2) Compárese con *ruta explícita (ER)*. Véase también *vía de acceso* y *extensión de ruta (REX)*.

rutina de carga. (1) Secuencia de instrucciones cuya ejecución hace que se carguen y se ejecuten unas instrucciones adicionales hasta que se haya almacenado todo el programa de sistema. (T) (2) Técnica o dispositivo diseñado para que entre en un estado determinado por medio de su propia acción, por ejemplo, una rutina de máquina cuyas primeras instrucciones sean suficientes para que el resto de la misma entre en el sistema desde un dispositivo de entrada. (A)

S

salto. (1) En APPN, parte de una ruta que no tiene nodos intermedios. Está compuesto por un solo grupo de transmisión que conecta nodos adyacentes. (2) Para la capa de direccionamiento, distancia lógica entre dos nodos en una red.

SAP. Véase punto de acceso a servicios.

segmentación. En OSI, función realizada por una capa para correlacionar una unidad de datos de protocolo (PDU) de la capa a la que da soporte con diversas PDU.

segmento. (1) Sección de cable entre componentes o dispositivos. Un segmento puede estar compuesto por un solo cable provisional, diversos cables provisionales conectados o una combinación de cables provisionales y de construcción conectados. (2) En comunicaciones de Internet, unidad de transferencia entre funciones de TCP en diferentes máquinas. Cada segmento contiene campos de control y de datos; la posición de corriente de bytes actual y los bytes de datos reales se identifican conjuntamente con una suma de comprobación para validar los datos recibidos.

segmento de anillo. Parte de un anillo que puede aislarse (desenchufando conectores) del resto del anillo. Véase *segmento de LAN*.

segmento de LAN. (1) Cualquier parte de una LAN (por ejemplo, un bus o un anillo) que puede funcionar independientemente pero está conectada a otras partes de la red por medio de puentes. (2) Red de tipo bus o anillo sin puentes.

señal. (1) En una red de área local, símbolo de autorización pasado sucesivamente de una estación de datos a otra para indicar la estación que tiene temporalmente el control del medio de transmisión. Cada estación de datos tiene una oportunidad de obtener y utilizar la señal para controlar el medio. Una señal es un mensaje o patrón de bits determinado que significa el permiso para transmitir. (T) (2) En las LAN, secuencia de bits pasada de un dispositivo a otro por el medio de transmisión. Cuando la señal tiene datos añadidos, se convierte en una trama.

Serial Line Internet Protocol (SLIP). Protocolo utilizado sobre una conexión punto a punto entre dos sistemas principales de IP de una línea serie, como, por ejemplo, un cable serie o una conexión RS232 con un módem, de una línea telefónica.

Service Advertising Protocol (SAP). En Internetwork Packet Exchange (IPX), protocolo que proporciona lo siguiente:

- Un mecanismo que permite que los servidores IPX de una internet anuncien sus servicios por el nombre y el tipo. Los servidores que utilizan este protocolo tienen registrados su nombre, tipo de servicios y dirección en todos los servidores de archivos que ejecutan NetWare.
- Un mecanismo que permite que una estación de trabajo difunda una consulta para descubrir las identidades de todos los servidores de todos los tipos, todos los servidores de un tipo específico o el servidor más cercano de un tipo específico.
- Un mecanismo que permite que una estación de trabajo consulte cualquier servidor de archivos que ejecute NetWare para descubrir nombre y dirección de todos los servidores de un tipo específico.

servicio de directorios (DS). Elemento de servicio de aplicaciones que convierte los nombres simbólicos utilizados por procesos de aplicaciones en direcciones de red completas utilizadas en un entorno de OSI. (T)

servicios de directorios (DS). Componente del punto de control de un nodo APPN que mantiene la información sobre la ubicación de los recursos de red.

servicios de gestión de punto de control (CPMS). Componente de un punto de control que consta de conjuntos de funciones de servicios de gestión y proporciona recursos de ayuda para realizar la gestión de problemas, gestión del rendimiento y de la contabilidad, gestión de los cambios y gestión de la configuración. Las posibilidades proporcionadas por los CPMS incluyen el envío de peticiones a los servicios de gestión de unidad física (PUMS) para probar recursos del sistema, la reunión de información estadística (por ejemplo, datos de errores y del rendimiento) de los PUMS sobre los recursos del sistema y el análisis y presentación de los resultados de las pruebas y la información estadística reunida sobre los recursos del sistema. Las responsabilidades del análisis y de la presentación para la determinación de problemas y la supervisión del rendimiento pueden distribuirse entre los diversos CPMS.

servicios de gestión de SNA (SNA/MS). Servicios proporcionados como ayuda para la gestión de las redes SNA.

servidor. Unidad funcional que proporciona servicios compartidos a estaciones de trabajo sobre una red; por ejemplo, un servidor de archivos, un servidor de impresión, un servidor de correo. (T)

Servidor de acceso a red (NAS). Dispositivo que proporciona a los usuarios acceso a red temporal a petición. Este acceso es punto a punto por medio de líneas PSTN o RDSI.

Servidor de configuración de Emulación de LAN (LECS). Componente de LAN Emulation Service que centraliza y difunde datos de configuración.

Servidor de emulación de LAN (LES). Componente de LAN Emulation Service que resuelve destinos de LAN en direcciones ATM.

servidor de informes de configuración (CRS). En el programa Bridge 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 suministra la conversión de nombres en direcciones correlacionando nombres de dominio con direcciones IP. Sinónimo con *servidor de nombres*.

servidor de puentes de LAN (LBS). En el programa Bridge para la Red en Anillo de IBM, servidor que mantiene información estadística sobre las tramas reenviadas entre dos o más anillos (mediante un puente). El LBS envía estas estadísticas a los gestores de LAN correspondientes mediante el mecanismo de información de LAN (LRM).

Servidor de red L2TP (LNS). Un LNS funciona en cualquier plataforma capacitada que pueda ser una estación final de PPP. El LNS maneja la parte del servidor del protocolo L2TP. Puesto que L2TP sólo se apoya en el único medio por el que llegan los túneles de L2TP, el LNS sólo tiene una interfaz LAN o WAN, aunque puede terminar las llamadas que lleguen de cualquier interfaz del rango completo de interfaces PPP soportadas por un LAC. Entre éstas se incluyen la RDSI asíncrona, RDSI síncrona, V.120 y otros tipos de conexiones.

sesión. (1) En la arquitectura de red, con el fin de la comunicación de datos entre unidades funcionales, todas las actividades que tienen lugar durante el establecimiento, mantenimiento y liberación de la conexión. (T) (2) Conexión lógica entre dos unidades de red accesibles (NAUs) que puede activarse, adaptarse para proporcionar varios protocolos y desactivarse

de la manera solicitada. Cada sesión está identificada de manera exclusiva en la cabecera de transmisión (TH) que acompaña a cualquier transmisión intercambiada durante la sesión. (3) En L2TP, L2TP crea una sesión cuando se intenta una conexión PPP de 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 mensaje de soporte de diversos dominios (MDS-MU)*.

StreetTalk. En VIrtual NEtworking System (VINES), sistema exclusivo de denominación y direccionamiento de red amplia que permite que los usuarios ubiquen cualquier recurso de la red y accedan al mismo sin conocer la topología de la red. Véase también *Internet Control Protocol (ICP)* y *RouTing update Protocol (RTP)*.

subárea. Parte de la red SNA compuesta por un nodo de subárea, nodos periféricos conectados y recursos asociados. En un nodo de subárea, todas las unidades de red accesibles (NAU), enlaces y estaciones de enlace adyacentes (de nodos de subárea o nodos periféricos conectados) que son dirigibles dentro de la subárea comparten una dirección de subárea común y tienen direcciones de elementos distintas.

subcapa del control del acceso al medio (MAC). En una red de área local, parte de la capa de enlace de datos que aplica un método de acceso al medio. La subcapa del MAC da soporte a funciones dependientes de la topología y utiliza los servicios de la capa física para proporcionar servicios a la subcapa de control de enlace lógico. (T)

Subnetwork Access Protocol (SNAP). En las LAN, protocolo encargado de establecer diferencias entre protocolos de 5 bytes que identifica la familia de protocolos estándares distintos de IEEE a la que pertenece un paquete. El valor de SNAP se utiliza para diferenciar los protocolos que utilizan $AA como valor de punto de acceso a servicios (SAP).

subred. (1) En TCP/IP, parte de una red que se identifica mediante una parte de la dirección IP. (2) Sinónimo de *subred (grupo de nodos)*.

subred (grupo de nodos). (1) Cualquier grupo de nodos que tienen un conjunto de características comunes, como, por ejemplo, el mismo ID de red. (2) Sinónimo con *subred*.

subsistema. Sistema secundario o subordinado que a menudo puede funcionar de manera independiente o asíncrona respecto a un sistema de control. (T)

suma de comprobación. (1) Suma de un grupo de datos que se asocia con el grupo y se utiliza con fines de comprobación. (T) (2) En la detección de errores, función de todos los bits de un bloque. Si las sumas grabadas y las calculadas no coinciden, se indica que hay un error. (3) En un disquete, datos grabados en un sector con fines de detección de errores; una suma de comprobación calculada que no coincide con la suma de comprobación de los datos grabados en el sector indica que hay un sector anómalo. Los datos son numéricos u otras series de caracteres consideradas numéricas con el fin de calcular la suma de comprobación.

supervisor. (1) Dispositivo que observa y registra actividades seleccionadas en un sistema de proceso de datos para el análisis. Sus usos posibles son para indicar cualquier desviación significativa de la norma o para determinar los niveles de utilización de unidades funcionales en particular. (T) (2) Software o hardware que observa, supervisa, controla o verifica operaciones de un sistema. (A) (3) Función necesaria para iniciar la transmisión de una señal del anillo y para proporcionar recuperación de errores de software en el caso de que se pierdan señales, tramas en circulación u otras dificultades. La posibilidad está presente en todas las estaciones de anillo.

supervisor activo. En una Red en Anillo, función realizada en cualquier momento por una estación de anillo que inicia la transmisión de señales y proporciona recursos de recuperación de errores de señales. Cualquier adaptador activo del anillo tiene la posibilidad de proporcionar la función de supervisor activo si falla el supervisor activo actual.

SYNTAX. En el protocolo Simple Network Management Protocol (SNMP), cláusula del módulo de la MIB que define la estructura de datos abstracta correspondiente a un objeto gestionado.

Systems Network Architecture (SNA). Descripción de la estructura lógica, formatos, protocolos y secuencias operativas para la transmisión de unidades de información a través de las redes y para el control de la configuración y del funcionamiento de las mismas. La estructura de capas de SNA permite que los orígenes y destinos finales de la información, es decir, los usuarios, sean independientes de los servicios y recursos de red SNA específicos utilizados para el intercambio de información y que no se vean afectados por dichos servicios y recursos.

T

T1. En los Estados Unidos, línea de acceso público de 1,544 Mbps. Está disponible en veinticuatro canales de 64 Kbps. La versión europea (E1) transmite a 2,048 Mbps.

tabla de correlación de direcciones (AMT). Tabla mantenida en el direccionador AppleTalk que proporciona la correlación actual de las direcciones de nodo con las direcciones de hardware.

tabla de direccionamiento. Conjunto de rutas utilizadas para dirigir el reenvío de datagramas o para establecer una conexión. La información pasa entre direccionadores para identificar la topología de red y la factibilidad de los destinos.

tabla de información de zonas (ZIT). Listado de números de red y sus correlaciones con los nombres de zonas asociadas de internet. Cada direccionador de internet mantiene este listado en una internet AppleTalk.

TCP/IP. (1) Transmission Control Protocol/Internet Protocol. (2) Protocolo de interconexión de sistemas basado en Ethernet/de tipo UNIX que desarrolló originalmente el Departamento de Defensa de los EE.UU. TCP/IP facilitó ARPANET (Advanced Research Projects Agency Network), una red de paquetes conmutados para la investigación en que la capa 4 era TCP y la capa 3, IP.

Telnet. En el conjunto de protocolos de Internet, protocolo que proporciona un servicio de conexión de terminales remotos. Permite que los usuarios de un sistema principal se conecten con un sistema principal remoto e

interactúen como usuarios de terminal conectado directamente de este sistema principal.

terminal de datos preparado (DTR). Señal para el módem que se utiliza con el protocolo EIA 232.

tiempo de espera excedido. (1) Suceso que se produce al final de un período predeterminado de tiempo que ha empezado al aparecer otro suceso especificado. (I) (2) Intervalo de tiempo asignado para que tengan lugar determinadas operaciones; por ejemplo, la respuesta a un sondeo o direccionamiento antes de que se interrumpa el funcionamiento del sistema y deba reiniciarse.

topología. En comunicaciones, ordenación física o lógica de los nodos de una red, especialmente las relaciones de un nodo con otro nodo y los enlaces entre los mismos.

trama. (1) En la arquitectura Interconexión de Sistemas Abiertos, estructura de datos perteneciente a un área particular de información y compuesta por ranuras que pueden aceptar los valores de atributos específicos y de las que pueden deducirse inferencias mediante conexiones apropiadas de procedimiento. (T) (2) Unidad de transmisión en algunas redes de área local, incluida la Red en Anillo de IBM. Incluye delimitadores, caracteres de control, información y caracteres de comprobación. (3) En SDLC, vehículo para cada mandato, cada respuesta y toda información transmitida con procedimientos de SDLC.

trama de información (I). Trama de formato I que se utiliza para la transferencia de información numerada.

trama exploradora. Véase *paquete explorador*.

trama I. Trama de información.

transceptor (transmisor-receptor). En las LAN, dispositivo físico que conecta una interfaz de sistema principal a una red de área local, como, por ejemplo, Ethernet. Los transceptores de Ethernet contienen elementos electrónicos que aplican señales al cable y que detectan colisiones.

Transmission Control Protocol (TCP). Protocolo de comunicaciones utilizado en Internet y en cualquier red que siga las normas del Departamento de Defensa de los EE.UU. para el protocolo interredes. TCP proporciona un protocolo fiable de sistema principal a sistema principal entre sistemas principales en redes de comunicaciones de paquetes conmutados y en los sistemas interconectados de dichas redes. Utiliza Internet Protocol (IP) como protocolo subyacente.

Transmission Control Protocol/Internet Protocol (TCP/IP). Conjunto de protocolos de comunicaciones que dan soporte a funciones de conectividad de igual a igual para redes de área local y amplia.

transporte de vector de gestión de red (NMVT). Unidad de petición/respuesta (RU) de servicios de gestión que fluye sobre una sesión activa entre servicios de gestión de unidad física y servicios de gestión de punto de control (sesión de SSCP-PU).

troncal. (1) En una configuración de anillo de diversos puentes de una red de área local, enlace de gran velocidad al que se conectan los anillos por medio de puentes o direccionadores. Un troncal puede configurarse como bus o como anillo. (2) En una red de área amplia, enlace de gran velocidad al que se conectan nodos o intercambios de conmutaciones de datos (DSE).

Túnel. Un túnel está definido mediante un par LNS-LAC. El túnel lleva datagramas de PPP entre el LAC y el LNS. Un solo túnel puede multiplexar muchas sesiones. Una conexión de control que funciona sobre el mismo túnel controla el establecimiento, liberación y mantenimiento de todas las sesiones y del túnel en sí.

U

umbral. (1) En programas de puente de IBM, valor asignado al número máximo de tramas que no se reenvían por un puente debido a errores antes de que se cuente una aparición de “umbral sobrepasado” y se indique en los programas de gestión de red. (2) Valor inicial a partir del cual un contador disminuye hasta 0 o valor hasta el que aumenta o disminuye un contador a partir de un valor inicial.

unidad básica de transmisión (BTU). En SNA, unidad de datos e información de control que pasa entre los componentes del control de la vía de acceso. Una BTU puede constar de una o más unidades de información de vía de acceso (PIU).

unidad de datos de protocolo (PDU). Unidad de datos especificada en un protocolo de una capa determinada y compuesta por información de control de protocolo de esta capa además de, posiblemente, datos de usuario de esta capa. (T)

unidad de datos de protocolo de control de enlace lógico (LLC). Unidad de información intercambiada entre estaciones de enlace de diferentes nodos. La unidad de datos de protocolo de LLC contiene un punto de acceso a servicios de destino (DSAP), un punto de acceso a servicios de origen (SSAP), un campo de control y datos de usuario.

unidad de información de vía de acceso (PIU). Unidad de mensaje compuesta por una sola cabecera de transmisión (TH) o por una TH seguida de una unidad básica de información (BIU) o un segmento de BIU.

unidad de mensaje de soporte de diversos dominios (MDS-MU). Unidad de mensaje utilizada en el soporte de diversos dominios que contiene datos de servicios de gestión y fluye entre conjuntos de funciones de servicios de gestión sobre las sesiones de LU-LU y CP-CP. Esta unidad de mensaje, así como los datos reales de servicios de gestión que contiene, tiene el formato de corriente de datos general (GDS). Véase también *unidad de servicios de gestión de punto de control (CP-MSU)*, *unidad de servicios de gestión (MSU)* y *transporte de vector de gestión de red (NMVT)*.

unidad de red accesible (NAU). Unidad lógica (LU), unidad física (PU), punto de control (CP) o punto de control de servicios del sistema (SSCP). Es el origen o el destino de la información transmitida por la red de control de la vía de acceso. Sinónimo con *unidad de red direccionable*.

unidad de red direccionable (NAU). Sinónimo de *unidad de red accesible*.

unidad de servicio de canal (CSU). Unidad que proporciona la interfaz a una red digital. La CSU proporciona funciones de acondicionamiento (o igualación) de línea, que mantienen la uniformidad del rendimiento de la señal a lo largo del ancho de banda de canal; remodelación de señal, que constituye la corriente de pulsaciones binarias; y prueba de bucle de retorno, que incluye la transmisión de señales de prueba entre la CSU y la unidad de canal de oficina de la portadora de red. Véase también *unidad de servicio de datos (DSU)*.

unidad de servicio de datos (DSU). Dispositivo que proporciona una interfaz de servicio de datos digital al equipo terminal de datos de manera directa. La DSU proporciona igualación de bucle y posibilidades de pruebas locales y remotas, así como una interfaz EIA/CCITT estándar.

unidad de servicios de gestión de punto de control (CP-MSU). Unidad de mensaje que contiene datos de servicios de gestión y fluye entre los conjuntos de funciones de servicios de gestión. Esta unidad de mensaje tiene el formato de corriente de datos general (GDS). Véase también *unidad de servicios de gestión (MSU)* y *transporte de vector de gestión de red (NMVT)*.

unidad EIA. Unidad de medida que ha establecido la Electronic Industries Association y es igual a 44,45 milímetros (1,75 pulgadas).

unidad física (PU). (1) Componente que gestiona y supervisa los recursos (como, por ejemplo, enlaces conectados y estaciones de enlace adyacentes) asociados con un nodo tal como lo solicita un SSCP mediante una sesión de SSCP-PU. Un SSCP activa una sesión con la unidad física con el fin de gestionar indirectamente, a través de la PU, recursos del nodo, como, por ejemplo, enlaces conectados. Este término sólo se aplica los nodos de tipo 2.0, tipo 4 y tipo 5. (2) Véase también *PU periférica* y *PU de subárea*.

unidad lógica (LU). Tipo de unidad de red accesible que permite que los usuarios obtengan acceso a recursos de red y se comuniquen entre sí.

unidad máxima de transmisión (MTU). En las LAN, mayor unidad de datos posible que puede enviarse por un medio físico determinado en una sola trama. Por ejemplo, la MTU para Ethernet tiene 1500 bytes.

Unión de Telecomunicaciones Internacionales (ITU). Agencia de telecomunicaciones especializada de las Naciones Unidas que se ha establecido con el fin de proporcionar procedimientos y prácticas para la normalización de las comunicaciones, lo cual incluye asignación de frecuencia y regulaciones de la radio universales.

User Datagram Protocol (UDP). En el conjunto de protocolos de Internet, protocolo que proporciona un servicio no fiable de datagramas sin conexiones. Permite que un programa de aplicación de una máquina o proceso envíe un datagrama a un programa de aplicación de otra máquina o proceso. UDP utiliza Internet Protocol (IP) para entregar datagramas.

V

V.24. En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito de datos (DCE).

V.25. En la comunicación de datos, especificación de la CCITT que define el equipo de respuesta automática y el equipo de llamada automática paralelo de la Red Telefónica General Conmutada, incluidos los procedimientos de inhabilitación de dispositivos controlados con eco para las llamadas establecidas de manera manual y automática.

V.34. Recomendación del ITU-T para la comunicación por módem sobre canales estándares de transmisión de voz de 33,6 Kbps (y más lentos) disponibles comercialmente.

V.35. En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito de datos (DCE) con varias velocidades de datos.

V.36. En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito

de datos (DCE) con las velocidades de 48, 56, 64 ó 72 kilobits por segundo.

valor por omisión. Perteneciente a un atributo, condición, valor u opción que se supone cuando no se especifica nada de forma explícita. (I)

variable de corriente de datos general (GDS). Tipo de subestructura de RU que va precedida de un identificador y un campo de longitud e incluye datos de aplicación, datos de control de usuario o datos de control definidos según SNA.

variable de la MIB. En el protocolo Simple Network Management Protocol (SNMP), instancia específica de datos definida en un módulo de la MIB. Sinónimo con *objeto de la MIB*.

vector de control de selección de ruta (RSCV). Vector de control que describe una ruta de una red APPN. El RSCV consta de una secuencia ordenada de vectores de control que identifican los TG y nodos que componen la vía de acceso de un nodo de origen a un nodo de destino.

Velocidad de información comprometida. Cantidad máxima de datos en bits que la red acepta entregar.

velocidad de transferencia de datos. Promedio de los bits, caracteres o bloques por unidad de tiempo que pasan entre los miembros del equipo correspondiente en un sistema de transmisión de datos. (I)

Notas:

1. La velocidad se expresa en bits, caracteres o bloques por segundo, minuto u hora.
2. Debe indicarse el equipo correspondiente; por ejemplo, módems, equipo intermedio u origen y destino.

versión. Programa bajo licencia independiente que a menudo tiene un nuevo código o una nueva función significativos.

vertimiento múltiple. (1) Transmisión de los mismos datos a un grupo seleccionado de destinos. (T) (2) Forma especial de difusión en que se entregan copias de un paquete a un subconjunto de todos los destinos posibles solamente.

vía de acceso. (1) En una red, cualquier ruta entre dos nodos cualesquiera. Una vía de acceso puede incluir más de una rama. (T) (2) Serie de componentes de red de transporte (control de la vía de acceso y control de enlace de datos) por los que pasa la información intercambiada entre dos unidades de red accesibles. Véase también *ruta explícita (ER)*, *extensión de ruta* y *ruta virtual (VR)*.

VINES. VIrtual NEtworking System.

VIrtual NEtworking System (VINES). Sistema operativo de red y software de red de Banyan Systems, Inc. En una red VINES, la función de enlace virtual permite que todos los dispositivos y servicios aparenten estar conectados directamente entre sí cuando en realidad pueden encontrarse a miles de kilómetros de distancia. Véase también *StreetTalk*.

vista de la MIB. En el protocolo Simple Network Management Protocol (SNMP), conjunto de objetos gestionados, conocidos por el agente, que es visible en una comunidad en particular.

vuelco. (1) Datos que se han volcado. (T) (2) Copiar el contenido de la totalidad o de parte del almacenamiento virtual con el fin de reunir información de errores.

X

X.21. Recomendación de la Comisión Consultiva de la Telefonía y Telegrafía Internacionales (CCITT) relativa a una interfaz de fines generales entre un equipo terminal de datos y un equipo de terminación de circuito de datos para las operaciones síncronas en una red pública de datos.

X.25. (1) Recomendación de la Comisión Consultiva de la Telefonía y Telegrafía Internacionales (CCITT) relativa a la interfaz entre un equipo terminal de datos y las redes de datos de paquetes conmutados. (2) Véase también *conmutación de paquetes*.

Xerox Network Systems (XNS). Conjunto de protocolos de internet desarrollados por Xerox Corporation. Aunque es similar a los protocolos TCP/IP, XNS utiliza unos formatos de paquete y una terminología diferentes. Véase también *Internetwork Packet Exchange (IPX)*.

Z

zona. En redes AppleTalk, subconjunto de nodos dentro de una internet.

Zone Information Protocol (ZIP). En redes AppleTalk, protocolo que proporciona un servicio de gestión de zonas manteniendo una correlación de los nombres de zonas y los números de red de la internet en la capa de sesión.

Índice

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

Hoja de Comentarios

Nways Multiprotocol Routing Services
Manual de consulta de supervisión
y configuración de protocolos
Volumen 2 Versión 3.3

Número de Publicación SC10-3428-00

En general, ¿está Ud. satisfecho con la información de este libro?

	Muy satisfecho	Satisfecho	Normal	Insatisfecho	Muy insatisfecho
Satisfacción general	□	□	□	□	□

¿Cómo valora los siguientes aspectos de este libro?

	Muy bien	Bien	Acep-table	Insatisfecho	Muy insatisfecho
Organización	□	□	□	□	□
Información completa y precisa	□	□	□	□	□
Información fácil de encontrar	□	□	□	□	□
Utilidad de las ilustraciones	□	□	□	□	□
Claridad de la redacción	□	□	□	□	□
Calidad de la edición	□	□	□	□	□
Adaptación a los formatos, unidades, etc. del país	□	□	□	□	□

Comentarios y sugerencias:

Nombre

Dirección

Compañía u Organización

Teléfono

Hoja de Comentarios
SC10-3428-00

Corte o Doble
Por la Línea

Dóblese por la línea de puntos **Por favor no lo grape** Dóblese por la línea de puntos

PONER
EL
SELLO
AQUÍ

IBM, S.A.
National Language Solutions Center
Av. Diagonal, 571
08029 Barcelona
España

Dóblese por la línea de puntos **Por favor no lo grape** Dóblese por la línea de puntos

SC10-3428-00

Corte o Doble
Por la Línea

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

SC10-3428-00