Nways Multiprotocol Routing Services

# Consulta de configuración y supervisión de protocolos, Volumen 1
# Versión 3.3

SC10-3426-00

Nways Multiprotocol Routing Services

# Consulta de configuración y supervisión de protocolos, Volumen 1
# Versión 3.3

SC10-3426-00

**Nota**

Antes de utilizar este documento, lea la información general del tema “Avisos” en la página xxi.

**Primera edición (Junio de 1999)**

Este manual es la traducción del original inglés *Nways Multiprotocol Routing Services Protocol Configuration and Monitoring Reference Volume 1, Version 3.3, SC30-3680-09*.

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

Puede solicitar las publicaciones a través del representante de IBM o la sucursal de IBM de su localidad. Las publicaciones no se almacenan en la dirección siguiente.

IBM agradece sus comentarios. Al final de esta publicación se incluye una hoja de comentarios. Si la hoja no está, puede dirigir sus comentarios a:

IBM S.A.
National Language Solutions Center
Avda. Diagonal 572, Edif. "L'Illa"
09029 Barcelona
España

También puede acceder a la siguiente dirección en la Web para enviar sus comentarios en línea:

http://www.networking.ibm.com/feedback/pubsurv.html

Cuando envía información a IBM, otorga a IBM un derecho no exclusivo de utilizar o distribuir la información del modo que considere más apropiado sin incurrir por ello en ninguna obligación hacia usted.

# 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 el tema “Publicaciones de IBM 2210 Nways Multiprotocol Router” en la página xxix y describe un grupo de protocolos que reciben soporte del 2210. Puede que un determinado 2210 no dé soporte a todas las características y funciones descritas en estos manuales. Si una característica o función es específica de un dispositivo, esta restricción se indica en el manual correspondiente.

Este manual hace referencia al 2210 como “el direccionador” o como “el dispositivo”. Los ejemplos de la biblioteca representan la configuración de un 2210, pero la salida real que vea el usuario puede variar. Utilice los ejemplo como guía de lo que puede ver al configurar el dispositivo.

**A quién va destinado este manual:** Este manual va destinado a las personas que instalen o gestionen redes. Aunque la experiencia en hardware y software de red resultará de ayuda, no necesita experiencia en programación para utilizar el software del 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 Programa de configuración para IBM Nways Multiprotocol Routing Services (denominado en este manual: *Programa de configuración*) es una interfaz gráfica de usuario que permite configurar el dispositivo desde una estación de trabajo autónoma. El Programa de configuración incluye la función de comprobación de errores e información de ayuda en línea.

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

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

## Convenios utilizados en este manual

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

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

   ```
   reload
   ```

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

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

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

   Elija una de las palabras clave como valor del parámetro.

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

   ```
   time host ...
   ```

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

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

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

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

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

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

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

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

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

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

## Publicaciones de IBM 2210 Nways Multiprotocol Router

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

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

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

SC10-3429 *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 para productos Nways Multiprotocol and Access Services*

Este manual describe cómo utilizar el Programa de configuración.

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

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

**Seguridad**

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

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

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

**Planificación e instalación**

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

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

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

**Diagnósticos y mantenimiento**

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

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

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

La lista siguiente 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).

# Configuración y supervisión de funciones de puente

# Conceptos básicos sobre la función de puente

Este capítulo contiene información básica sobre puentes y sobre las funciones de los puentes. Este capítulo incluye las siguientes secciones:



## Visión general de la función de puente

Un puente es un dispositivo que enlaza dos o más redes de área local. El puente acepta tramas de datos procedentes de cada una de las redes conectadas y decide si reenviar cada trama en función de la cabecera de control de acceso al medio (MAC) contenida en la trama. Los puentes originalmente enlazaban dos o más redes homogéneas. El término *homogéneas* significa que las redes conectadas utilizan el mismo método de conexión por puente y los mismos tipos de soporte. Serían ejemplos de este término las redes que ***sólo*** dan soporte al método de conexión por puente de direccionamiento de origen o que ***sólo*** dan soporte al algoritmo de puente transparente (ambos métodos se explican más adelante).

Los puentes existentes actualmente también permiten la comunicación entre redes que no son homogéneas. *No homogéneas* significa que las redes pueden combinar distintos métodos de puente y también pueden ofrecer más opciones de configuración. La Figura 1 en la página 4 ilustra ejemplos de configuraciones de puentes sencilla y compleja.

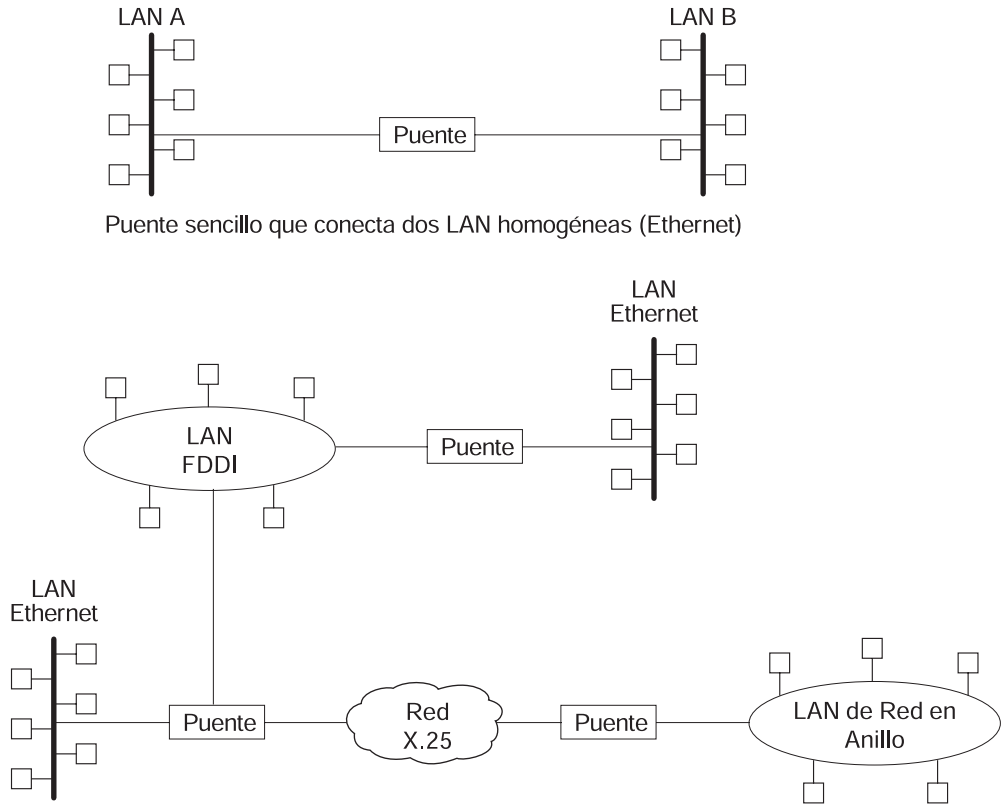



*Figura 1. Configuración de la función de puente simple y compleja*

## Función de puente y direccionamiento

El 2210 puede realizar funciones de puente y de direccionamiento. El filtrado de protocolos es el proceso que determina si los datos entrantes se deben direccionar o pasar por la función de puente.

## Filtrado de protocolos

Al procesar un paquete de datos entrante, se produce la siguiente acción:

- Los paquetes se direccionan si se ha activado globalmente un distribuidor específico de protocolo
- Los paquetes se filtran si el usuario ha configurado filtros específicos de protocolo
- Los paquetes que no se direccionan ni se filtran son candidatos a la función de puente, según la dirección de control de acceso al medio (MAC) de destino.

La Tabla 1 en la página 5 muestra cómo se responde a la pregunta “¿Pasar por puente o direccionar?” en función del contenido de la dirección de destino.

| *Tabla 1. Tabla de decisión sobre si direccionar/pasar por puente* | |
|---|---|
| **Si la Dirección MAC de destino de la trama recibida contiene:** | **El puente emprende esta acción:** |
| Dirección de puente | El puente pasa la trama al protocolo configurado, que direcciona la trama. |
| Dirección de difusión múltiple o difusión general | Si hay un protocolo configurado en la trama, esta se direcciona. Si no es así, la trama se pasa por el puente. |
| Difusión individual | La trama se pasa por el puente. |

### Direccionamiento o paso por puente según la interfaz

Para IP, IPX, y AppleTalk, se aplican las siguientes reglas para el direccionamiento o paso por puente sobre una determinada interfaz:

- Los paquetes se direccionan si hay un determinado protocolo configurado para la interfaz receptora
- Los paquetes se filtran si el usuario ha configurado filtros específicos de protocolo en la interfaz receptora
- Los paquetes que no se direccionan ni se filtran son candidatos a la función de puente, según la dirección de control de acceso al medio (MAC) de destino.

## Conexiones de direccionador

Establecer conexión en la capa 3 con un direccionador permite la conectividad y la selección de vía de acceso entre estaciones finales situadas en áreas geográficas distantes. Mediante protocolos de direccionamiento, puede seleccionar la mejor vía de acceso para conectar LAN distantes y diversas. Debido a la gran variedad de opciones de configuración de red y subred disponibles en las redes grandes, la conexión de varias LAN a través de una Capa de red suele ser el método preferido. Se ha comprobado que los protocolos de capa de red son muy eficaces para mover información en configuraciones de redes grandes y diversas.

## Conexiones de puente

La conexión en la capa 2 con un puente ofrece conectividad a través de un enlace físico. Esta conexión es esencialmente “transparente” para los sistemas principales conectados a la red.

**Nota:** Los puentes de direccionamiento de origen no se consideran completamente “transparentes.” Consulte el tema “Métodos de conexión por puente” en la página 13 para obtener más información sobre el direccionamiento de origen y los puentes transparentes.

La Capa de enlace mantiene los esquemas de direccionamiento físico (frente al lógico de la capa 3), la disciplina de línea, el sistema de notificación de la topología, la notificación de errores, el control del flujo y la distribución ordenada de las tramas de datos. El aislamiento de los protocolos de las capas superiores es una de las ventajas de la función de puente. Puesto que los puentes funcionan en la Capa de enlace, no deben preocuparse de buscar la información sobre protocolo que se produce en las capas superiores. Esto reduce la actividad general de proceso y aumenta la velocidad de comunicación del tráfico del protocolo de la

capa de red. Puesto que los puentes no se preocupan de la información de la Capa 3, también pueden reenviar distintos tipos de tráficos de protocolo (por ejemplo, IP o IPX) entre dos o más redes (como hacen los direccionadores).

Los puentes también pueden filtrar tramas en función de los campos de la Capa 2. Esto significa que el puente se puede configurar para que acepte y reenvíe sólo tramas de un determinado tipo o las que se originan en una determinada red. Esta posibilidad de configurar filtros resulta muy útil para mantener un flujo de tráfico eficiente.

Los puentes constituyen una ventaja cuando se dividen redes grandes en segmentos más fáciles de gestionar. Las ventajas de la conexión por puente en redes grandes son las siguientes:

- La función de puente le permite aislar determinadas áreas de la red, y exponerlas en menor medida a los principales problemas de la red.
- La función de filtro le permite regular la cantidad de tráfico que se reenvía a determinados segmentos.
- Los puentes permiten establecer comunicación entre un mayor número de dispositivos internos a la red de lo que no sería posible en una sola LAN conectada a un puente.
- La función de puente elimina la limitación de nodos (el número total de nodos de un segmento). El tráfico de la red local no se pasa a todas las demás redes conectadas.
- Los puentes aumentan la “longitud” conectada de una LAN permitiendo la conexión de segmentos de LAN distantes. Los puentes conectan segmentos de dos LAN en la capa 2, con lo que se pueden formar redes de mayor tamaño. Esto evita los problemas de congestión que se producen cuando hay demasiadas estaciones en una LAN Ethernet y el límite de 256 estaciones de la arquitectura de la red en anillo.

## Puentes frente a direccionadores

Los dispositivos internos de la red, como puentes y direccionadores, tienen funciones similares puesto que conectan segmentos de la red. Sin embargo, cada dispositivo utiliza un método diferente de establecer y mantener las conexiones de LAN a LAN. Los direccionadores conectan las LAN en la Capa 3 (Capa de red) del modelo OSI, mientras que los puentes conectan las LAN en la Capa 2 (Capa de enlace).

## Tipos de puentes

Las siguientes secciones describen distintos tipos de puentes y el modo en que se clasifican por su capacidad de hardware y de software.

## Puentes sencillos

Los puentes sencillos constan de dos o más interfaces de red enlazadas que conectan redes de área local (Figura 1 en la página 4). Los puentes interconectan redes de área local (LAN) separadas, transmitiendo tramas de datos entre las entidades MAC (control de acceso al medio) separadas de las LAN conectadas mediante puente.

Las principales funciones de un puente sencillo son las siguientes:

- El puente lee todas las tramas de datos transmitidas en la LAN A y recibe aquellas destinadas a la LAN B. Los puentes sencillos no efectúan cambios en el contenido ni en el formato de las tramas de datos que reciben. Tampoco encapsulan tramas con cabeceras adicionales.

  La mayoría de los puentes sencillos contienen inteligencia en cuanto a direccionamiento y destino de direccionamiento. Como mínimo, el puente debe saber qué direcciones hay en cada red conectada, para poder saber qué tramas debe pasar.
- El puente retransmite las tramas de datos destinadas a la LAN B a la LAN B mediante el protocolo MAC correspondiente a dicha LAN. Los puentes deben tener suficiente espacio de almacenamiento intermedio para dar soporte a las demandas del tráfico punta de datos, puesto que las tramas de datos pueden llegar más rápido de lo que el puente puede transmitir.
- El puente hace lo mismo para el tráfico de trama de datos de la LAN B a la LAN A.

## Puentes complejos

Los puentes complejos llevan a cabo funciones más sofisticadas que los puentes sencillos. Estas funciones pueden incluir que el puente mantenga información de estado sobre los demás puentes. Esta información incluye el coste de la vía de acceso de la comunicación, así como el número de saltos necesarios para llegar a cada red conectada. Los intercambios periódicos de información entre puentes actualizan toda la información sobre puentes. Estos tipos de intercambios permiten el direccionamiento dinámico entre puentes.

Los puentes complejos también pueden modificar tramas y reconocer y transmitir paquetes procedentes de distintas tecnologías de LAN (por ejemplo, Red en anillo, y Ethernet). En este caso, a veces se dice que el puente es un puente *de conversión*.

El puente transparente de direccionamiento de origen adaptable (ASRT) constituye la implantación de 2210 de la tecnología de puente. El puente ASRT es un grupo de componentes de software con capacidad para varias de las opciones de función de puente descritas anteriormente y más. Todas estas funciones se explican con mayor detalle en este capítulo.

## Puentes locales

Los puentes locales ofrecen conexiones entre segmentos de distintas LAN de la misma área geográfica. Un ejemplo sería un puente que se utilice para conectar diversas LAN situadas en las oficinas principales de su empresa.

## Puentes remotos

Los puentes remotos conectan segmentos de varias LAN de distintas áreas geográficas. Un ejemplo sería puentes que se utilizaran para conectar las LAN de la oficina principal de su empresa a las LAN de otras oficinas sucursales dispersas por el país. Debido a las diferencias geográficas, esta configuración pasa de una configuración de red de área local a una configuración de red de área amplia (WAN).

Los puentes remotos pueden diferir de los puentes locales en varios aspectos. Una de las principales diferencias es la velocidad a la que se transmiten los datos. Las conexiones de WAN pueden ser más lentas que las conexiones de LAN. Esta diferencia en la velocidad puede ser significativa cuando se ejecutan aplicaciones muy sensibles al tiempo. Otra diferencia es el método físico en que los puentes remotos y locales se conectan a las LAN. En los puentes locales, las conexiones se realizan mediante soporte de cableado local (por ejemplo, Ethernet, Thinet). Las conexiones de puentes remotos se realiza sobre líneas serie.

## Funcionamiento básico del puente

De acuerdo con el estándar de LAN IEEE 802, todas las direcciones de estaciones se especifican al nivel MAC. En el nivel de Control de enlace lógico (LLC), sólo se designan las direcciones SAP (Punto de acceso de servicio). Por lo tanto, el nivel MAC es el nivel al que funciona el puente. Los siguientes ejemplos explican cómo funciona la conexión por puente a este nivel.

## Ejemplo 1 de funcionamiento: puente local que conecta dos LAN

La Figura 2 muestra un modelo de puente de dos puertos que conecta estaciones finales de dos LAN separadas. En este ejemplo, el puente local conecta dos LAN con capas LLC y MAC idénticas (es decir, dos LAN de red en anillo). Conceptualmente, puede pensar en el puente como un método de transmisión de enlace de datos que reenvía tramas entre las subcapas de control de acceso al medio (MAC) y los canales físicos de las LAN conectadas, ofreciendo conectividad de enlace de datos entre ellas.

Para resumir el proceso de la función de puente, el puente captura tramas MAC cuyas direcciones de destino no se encuentran en la LAN local (es decir, la LAN conectada a la interfaz que recibe la trama transmitida). Luego las reenvía a la LAN de destino adecuada. A través de este proceso, se establece un diálogo entre las entidades LLC similares de las dos estaciones finales. A nivel de arquitectura, el puente no necesita contener una capa LLC, puesto que la función de la capa LLC consiste únicamente en retransmitir tramas MAC procedentes de niveles superiores del modelo OSI.

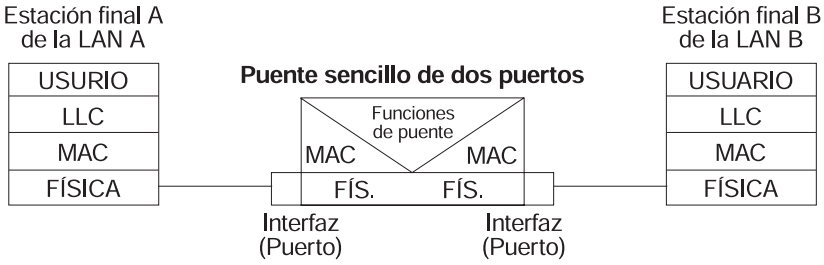



*Figura 2. Puente de dos puertos que conecta dos LAN*

## Ejemplo 2 de funcionamiento: Función de puente remoto sobre un enlace serie

La Figura 3 en la página 9 muestra un par de puentes conectados sobre un enlace serie. Estos puentes remotos conectan dos LAN con capas LLC y MAC idénticas (es decir, dos LAN de red en anillo).

Para resumir, el puente captura una trama MAC cuya dirección de destino no está en la LAN local y la envía a la LAN de destino adecuada mediante el puente de dicha LAN. A través de este proceso, se establece un diálogo entre las entidades LLC similares de las dos estaciones finales. A nivel de arquitectura, el puente no necesita contener una capa LLC, puesto que la función de la capa LLC consiste únicamente en retransmitir tramas MAC procedentes de niveles superiores del modelo OSI.

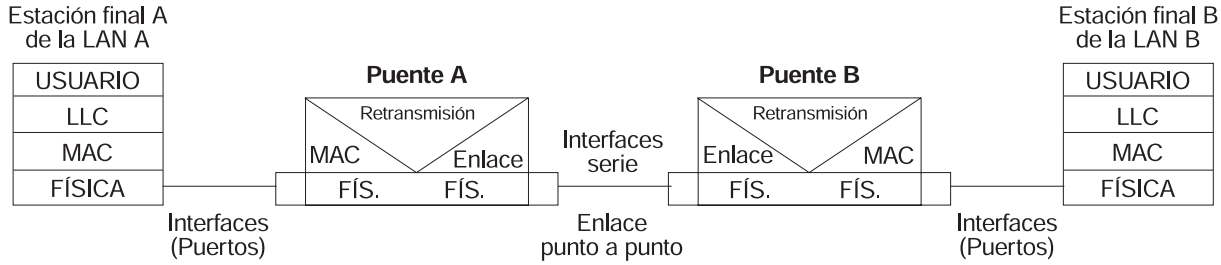



*Figura 3. Función de puente sobre un enlace punto a punto*

Los datos se encapsulan a medida que los puentes comunican datos sobre el enlace serie. La Figura 4 ilustra el proceso de encapsulación.

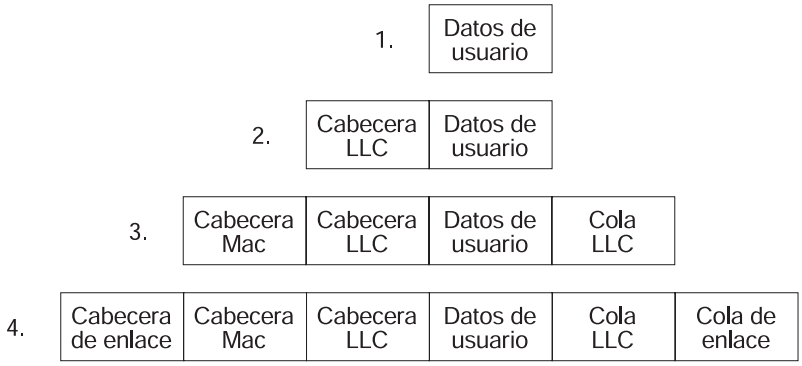



*Figura 4. Encapsulación de datos sobre un enlace punto a punto*

La encapsulación se produce del siguiente modo:

1. La estación final A proporciona datos a su LLC.
2. El LLC añade una cabecera y pasa la unidad de datos resultante al nivel MAC.
3. El MAC añade una cabecera (3) y una cola para formar una trama MAC. El Puente A captura la trama.
4. El Puente A no elimina los campos MAC porque su función consiste en retransmitir la trama MAC intacta a la LAN de destino. Sin embargo, en la configuración punto a punto el puente añade una cabecera y cola de capa de enlace (por ejemplo, HDLC) y transmite la trama MAC por el enlace.

Cuando la trama de datos alcanza el Puente B (el puente de destino), los campos de enlace se eliminan y el Puente B transmite la trama MAC *original, sin modificar* a su destino, la estación final B.

## Formatos de trama de puente MAC

Tal como se ha mencionado, los puentes interconectan LAN retransmitiendo tramas de datos, especialmente tramas MAC, entre entidades MAC separadas de las LAN conectadas por el puente. Las tramas MAC contienen la información sobre "¿Dónde?" necesaria para reenviar la trama en forma de direcciones de origen y de destino. Esta información resulta esencial para la transmisión y recepción satisfactorias de los datos.

IEEE 802 da soporte a tres tipos de tramas MAC: CSMA/CD (802.3), bus de señal (802.4) y red en anillo (802.5). La Figura 5 muestra los formatos de trama MAC a los que da soporte el puente. Las tramas específicas se detallan en la siguiente sección.

**Nota:** En el nivel LLC se utiliza otro formato de trama. Esta trama se incorpora a la trama MAC adecuada.

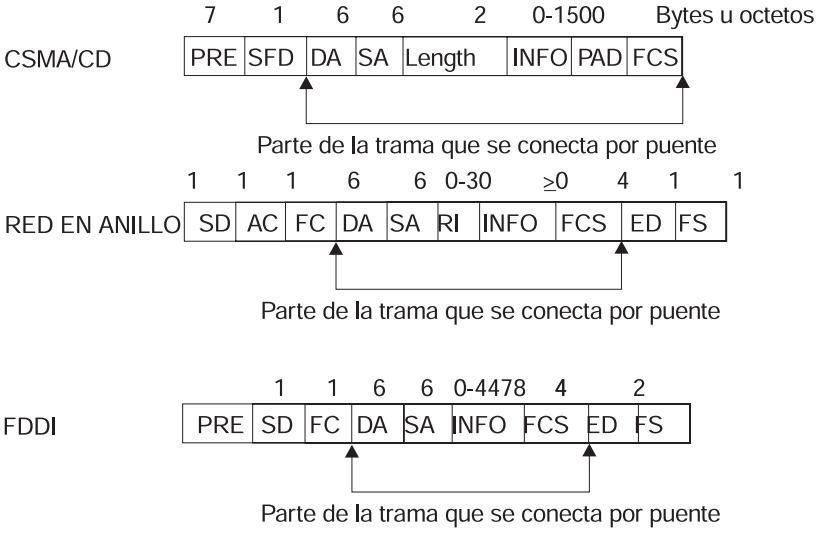



*Figura 5. Ejemplos de formatos de trama del MAC*

## Tramas MAC de CSMA/CD (Ethernet)

La información siguiente describe cada uno de los campos que se encuentran en las tramas MAC de CSMA/CD (Ethernet):

- *Preámbulo (PRE)*. Un patrón de 7 bytes que utiliza la estación final receptora para establecer la sincronización de bits y luego localizar el primer bit de la trama.
- *Delimitador de inicio de trama (SFD)*. Indica el inicio de la trama.

La parte de la trama que actualmente se conecta por puente consta de los siguientes campos:

- *Dirección de destino (DA)*. Especifica la estación final a la que va destinada la trama. Esta dirección puede ser una dirección física única (un destino), una dirección de difusión múltiple (un grupo de estaciones finales como destino) o una dirección global (todas las estaciones como destino). El formato es de 48 bits (6 octetos) y debe ser igual para todas las estaciones de una determinada LAN.

- *Dirección de origen (SA)*. Especifica la estación final que ha transmitido la trama. El formato debe ser igual que el formato de la dirección de destino.
- *Longitud*. Especifica el número de bytes LLC que siguen.
- *Info (INFO)*. Archivos incluidos creados al nivel LLC y que contienen información sobre el punto de acceso de servicio, información de control y datos de usuario.
- *Relleno*. Secuencia de bytes que aseguran que la trama es lo suficientemente larga para el funcionamiento correcto de la detección de colisiones (CD).
- *Secuencia de comprobación de trama (FCS)*. Un valor de comprobación de redundancia cíclica de 32 bits. Este valor se basa en todos los campos, comenzando por la dirección de destino.

## Tramas MAC de red en anillo

La siguiente información describe cada uno de los campos de las tramas MAC de red en anillo:

- *Delimitador de inicio (SD)*. Patrón exclusivo de 8 bits que indica el inicio de la trama.
- *Control de acceso (AC)*. Campo con el formato PPPTMRRR, donde PPP y RRR son variables de prioridad y de reserva de 3 bits, M es el bit de supervisión y T indica que se trata de una trama de señal o de datos. Si es una trama de señal, el único campo restante es el delimitador de fin (ED).
- *Control de trama (FC)*. Indica si es una trama de datos LLC. Si no lo es, los bits de este campo controlan el funcionamiento del protocolo MAC de red en anillo.

La parte de la trama que actualmente se conecta por puente consta de los siguientes campos:

- *Dirección de destino (DA)*. Igual que CSMA/CD y bus de señal.
- *Dirección de origen (SA)*. Identifica la estación que ha originado la trama. Este campo puede ser una dirección de 2 o de 6 octetos. Ambas longitudes de dirección llevan un bit de indicador de información de direccionamiento (RII) que indica si hay un campo de información de direccionamiento (RIF) en la trama tras la dirección de origen, del siguiente modo:

  RII=1 Hay un campo de información de direccionamiento.
  RII=0 No hay ningún campo de información de direccionamiento.

  Este campo se explica con más detalle en el tema “Conexión por puente de ruta de origen (SRB)” en la página 23.
- *Campo de información de direccionamiento (RIF)*. El RIF se necesita para el protocolo de direccionamiento de origen. Consta de un campo de control de direccionamiento de 2 octetos y una serie de campos de designación de ruta de 2 octetos. Este campo se explica con más detalle en el tema “Conexión por puente de ruta de origen (SRB)” en la página 23.
- *Info (INFO)*. Archivos incluidos creados al nivel LLC y que contienen información sobre el punto de acceso de servicio, información de control y datos de usuario.

- *Secuencia de comprobación de trama (FCS)*. Un valor de comprobación de redundancia cíclica de 32 bits. Este valor se basa en todos los campos, comenzando por la dirección de destino.

Finalmente, el *Delimitador de fin (ED)* contiene el bit de detección de errores (E) y el bit de trama intermedia (I). El bit I indica que no es la trama final de una transmisión de varias tramas. El *Estado de trama (FS)* contiene los bits de dirección reconocida (A) y trama copiada (C).

# Métodos de conexión por puente

Este capítulo describe los métodos de conexión por puente que reciben soporte del puente transparente de direccionamiento de origen adaptable (ASRT). Cada sección contiene una visión general de una determinada tecnología que va seguida de una descripción de las tramas de datos que reciben soporte de dicha tecnología. Este capítulo incluye las siguientes secciones:



## Conexión por puente transparente

El puente transparente se denomina también puente de árbol de expansión (STB). El término *transparente* hace referencia al hecho de que el puente reenvía de forma silenciosa tráfico que no es local a las LAN conectadas de un modo que resulta *transparente* al usuario (el usuario no lo ve). Las aplicaciones de estación final no tienen conocimiento de la presencia del puente. El puente conoce la presencia de las estaciones finales escuchando el tráfico que pasa. A partir de este proceso de escucha, crea una base de datos de direcciones de estaciones finales conectadas a sus LAN.

Para cada trama que recibe, el puente compara la dirección de destino de la trama con las que tiene en su base de datos. Si el destino de la trama es una estación final de la misma LAN, la trama no se reenvía. Si el destino se encuentra en otra LAN, la trama se reenvía. Si la dirección de destino no se encuentra en la base de datos, la trama se reenvía a todas las LAN conectadas al puente, excepto a la LAN de la que procede.

Todos los puentes transparentes utilizan el algoritmo y el protocolo de árbol de expansión. El algoritmo de árbol de expansión genera y mantiene una topología libre de bucles en una red conectada por puente que puede contener bucles en su diseño físico. En una topología de malla, en la que hay más de un puente conectado entre dos LAN, *se producen bucles*. En estos casos, los paquetes de datos van de un extremo al otro entre las dos LAN en los puentes paralelos. Esto crea una redundancia en el tráfico de datos y genera un fenómeno conocido como bucle.

Cuando se produce un bucle, debe configurar la LAN local y/o remota de modo que elimine el bucle físico. Con el árbol de expansión, un algoritmo de configuración automática permite añadir un puente en cualquier lugar de la de la LAN sin crear bucles. Cuando se añade el nuevo puente, el protocolo de árbol de expansión vuelve a configurar, de forma automática, todos los puentes de la LAN en un solo *árbol de expansión* libre de bucles.

Un árbol de expansión nunca tiene más de una ruta de datos activa entre dos estaciones finales, por lo que se eliminan los bucles de datos. Para cada puente, el algoritmo determina qué puertos de puente pueden reenviar datos y cuáles se

deben bloquear para formar una topología libre de bucles. Las características del árbol de expansión incluyen:

- *Detección de bucles*. Detecta y elimina los bucles de enlaces de datos físicos en configuraciones de LAN ampliadas.
- *Modalidad automática de reserva de vías de acceso a los datos*. Los puentes que se conectan a las vías de acceso redundantes entran de forma automática en la modalidad de reserva. Cuando un puente principal falla, el puente de reserva se activa.
- *Posibilidad de configuración por parte del usuario*. Le permite adaptar su topología de red. A veces, los valores por omisión no generan la topología de red deseada. Puede ajustar los parámetros de prioridad de puente, de prioridad de puerto y de coste de vía de acceso para ajustar el árbol de expansión a su topología de red.
- *Interoperatividad sin igual*. Permite la interoperatividad de LAN sin limitaciones en la configuración ocasionadas por distintos entornos de comunicaciones.
- *Conexión por puente de protocolos que no son de direccionamiento*. Ofrece una conexión por puente asequible de protocolos que no son de direccionamiento.

## Direccionadores y puentes transparentes

Mientras está funcionando un direccionador equipado con la opción de árbol de expansión, el software de direccionador y de puente se ejecutan simultáneamente. En esta modalidad, el direccionador es un puente y un direccionador.

Durante este tipo de operación, se producen las siguientes acciones:

- Los paquetes se direccionan si se ha activado globalmente un distribuidor específico de protocolo
- Los paquetes se filtran si el usuario ha configurado filtros específicos de protocolo
- Los paquetes que no se direccionan ni se filtran son candidatos a la función de puente, según la dirección de control de acceso al medio (MAC) de destino.

## Requisitos de la red

El puente transparente implanta un puente de árbol de expansión que cumple con el estándar IEEE 802.1D.Todos los puentes transparentes (como Ethernet y red en anillo) de la red deben ser puentes de árbol de expansión 802.1D. Este protocolo de árbol de expansión no es compatible con los puentes que implantan el protocolo de árbol de expansión de Digital Equipment Corporation, utilizado en algunos puentes antiguos.

## Funcionamiento del árbol transparente

En una topología de malla, en la que hay más de un puente conectado entre dos LAN, se puede producir el fenómeno denominado bucle, en el que dos LAN envían paquetes de un extremo a otro sobre los puentes paralelos. Un bucle es una condición en la que hay varias vías de acceso de datos entre dos LAN. El protocolo de árbol de expansión que funciona automáticamente elimina los bucles, bloqueando las vías de acceso redundantes.

Durante el arranque, todos los puentes que participan en la red intercambian unidades de datos de protocolo de puente (BPDU) tipo Hello, que proporcionan

información sobre la configuración de cada puente. Las BPDU incluyen información como el ID de puente, ID raíz y coste de vía de acceso raíz. Esta información ayuda a los puentes a determinar qué puente es el puente raíz y qué puentes son los puentes designados por las LAN a las que están conectados.

De toda la información que se intercambia en los mensajes HELLO, los siguientes parámetros son los más importantes para calcular el árbol de expansión:

- *ID del puente raíz*. El ID del puente raíz es el ID de puente del puente. El puente raíz es el puente designado para todas las LAN a las que está conectado.
- *Coste de vía de acceso raíz*. La suma total de los costes de vías de acceso designadas para el raíz mediante el puerto raíz de este puente. Esta información la transmite el puente raíz y los puentes designados, a fin de actualizar la información de vía de acceso de todos los puentes si la topología cambia.
- *ID de puente*. Un ID exclusivo utilizado por el algoritmo de árbol de expansión para determinar el árbol de expansión. A cada puente de la red se le asigna un identificador de puente exclusivo.
- *ID de puerto*. El ID del puerto desde el que se ha transmitido el mensaje BPDU HELLO actual.

Cuando dispone de esta información, el árbol de expansión empieza a determinar su forma y dirección y luego crea una configuración de vías de acceso lógicas. Este proceso se puede resumir del siguiente modo:

1. Se selecciona un puente raíz para la red, comparando los ID de puente de cada puente de la red. Gana el puente con el ID más bajo (es decir, con el valor más alto).
2. A continuación, el árbol de expansión selecciona un puente designado para cada LAN. Si hay más de un puente conectado a la misma LAN, el puente con el menor coste de vía de acceso al raíz se selecciona como puente designado. En el caso de que haya costes de vía de acceso coincidentes, se selecciona el puente con el ID de puente más bajo como puente designado.
3. Los puentes no designados de las LAN colocan cada puerto que no ha sido seleccionado como puerto raíz en estado BLOQUEADO. En el estado BLOQUEADO, un puente sigue escuchando las BPDU tipo Hello, de modo que puede actuar sobre cambios realizados en la red (por ejemplo, que falle el puente designado) y puede cambiar su estado de BLOQUEADO a REENVIANDO (es decir, reenviando datos).

Durante este proceso, el algoritmo de árbol de expansión reduce una red LAN conectada por puente de topología arbitraria a un solo árbol de expansión. Con el árbol de expansión, nunca hay más de una vía de acceso de datos activa entre dos estaciones finales, por lo que se eliminan los bucles de datos. Por cada puente de la red, el árbol de expansión determina qué puertos de puente bloquear para que no se formen bucles.

Esta nueva configuración está limitada por un factor de tiempo. Si un puente designado falla o se extrae (físicamente), los demás puentes de la LAN detectan la situación al no recibir BPDU tipo Hello dentro del periodo de tiempo definido por el tiempo máximo de puente. Este suceso activa un nuevo proceso de configuración, en el que se selecciona otro puente como puente designado. También se crea una nueva configuración si el puente raíz falla.

## Cómo formar el árbol de expansión

Cuando el árbol de expansión utiliza sus valores por omisión, el algoritmo de árbol de expansión suele ofrecer resultados aceptables. Sin embargo, en ocasiones el algoritmo puede generar un árbol de expansión de rendimiento pobre en la red. En este caso, puede ajustar la prioridad de puente, la prioridad de puerto y el coste de vía de acceso para formar un árbol de expansión que se ajuste al rendimiento de red que esperaba. A continuación se muestran ejemplos de cómo hacerlo.

La Figura 6 en la página 17 muestra tres LAN conectadas en red mediante tres puentes. Cada puente utiliza los valores de prioridad de puente por omisión para su configuración de árbol de expansión. En este caso, el puente con la dirección física más baja se elige como puente raíz, puesto que las prioridades de puente de cada puente coinciden. En este ejemplo, es el Puente 2.

El árbol de expansión recién configurado permanece intacto debido a las transmisiones repetidas de BPDU tipo Hello procedentes del puente raíz a intervalos predefinidos (tiempo de hello de puente). Durante este proceso, los puentes designados se actualizan con toda la información de configuración. A continuación, los puentes designados vuelven a generar la información procedente de las BPDU tipo Hello y la distribuyen a las LAN para las que son puentes designados.

*Tabla 2. Valores por omisión del árbol de expansión*

| **Puente 1** | **Puente 2** | **Puente 3** |
|---|---|---|
| Prioridad puente: 32768<br>Dirección:<br>00:00:90:00:00:10<br>**Puerto 1**<br>Prioridad: 128<br>Coste vía acceso: 100<br>**Puerto 2**<br>Prioridad: 128<br>Coste vía acceso: 17857<br>**Puerto 3**<br>Prioridad: 128<br>Coste vía acceso: 17857 | Prioridad puente: 32768<br>Dirección:<br>00:00:90:00:00:01<br>**Puerto 1**<br>Prioridad: 128<br>Coste vía acceso: 100<br>**Puerto 2**<br>Prioridad: 128<br>Coste vía acceso: 17857<br>**Puerto 3**<br>Prioridad: 128<br>Coste vía acceso: 17857 | Prioridad puente: 32768<br>Dirección:<br>00:00:90:00:00:05<br>**Puerto 1**<br>Prioridad: 128<br>Coste vía acceso: 100<br>**Puerto 2**<br>Prioridad: 128<br>Coste vía acceso: 17857<br>**Puerto 3**<br>Prioridad: 128<br>Coste vía acceso: 17857 |

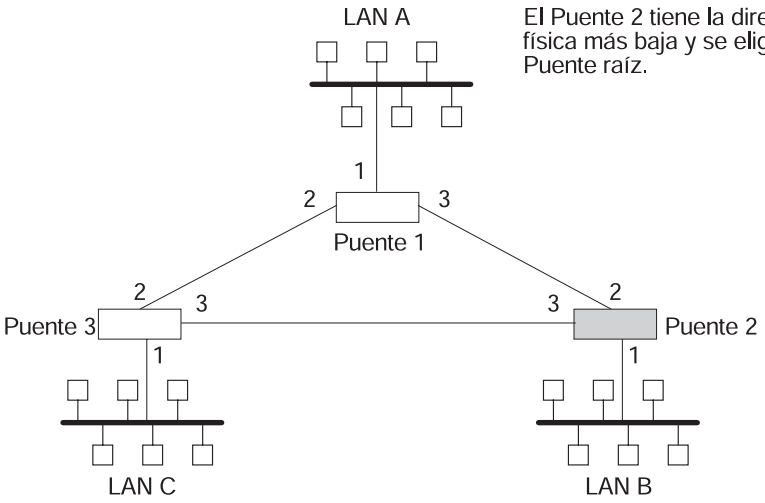



*Figura 6. LAN conectadas en red antes del árbol de expansión*

El algoritmo de árbol de expansión designa el puerto que conecta el Puente 1 al Puente 3 (puerto 2) como puerto de reserva y lo bloquea para que no reenvíe tramas que ocasionarían una condición de bucle. El árbol de expansión creado por el algoritmo utilizando los valores por omisión de la Tabla 2 en la página 16 se muestra en la Figura 7 como las líneas oscuras que conectan el Puente 1 al Puente 2, y luego el Puente 2 al Puente 3. El puente raíz el el Puente 2.

Este árbol de expansión da como resultado un rendimiento pobre de la red porque las estaciones de trabajo de la LAN C sólo pueden llegar al servidor de la LAN A de forma indirecta a través del Puente 2, en lugar de utilizar la conexión directa que hay entre el Puente 1 y el Puente 3.

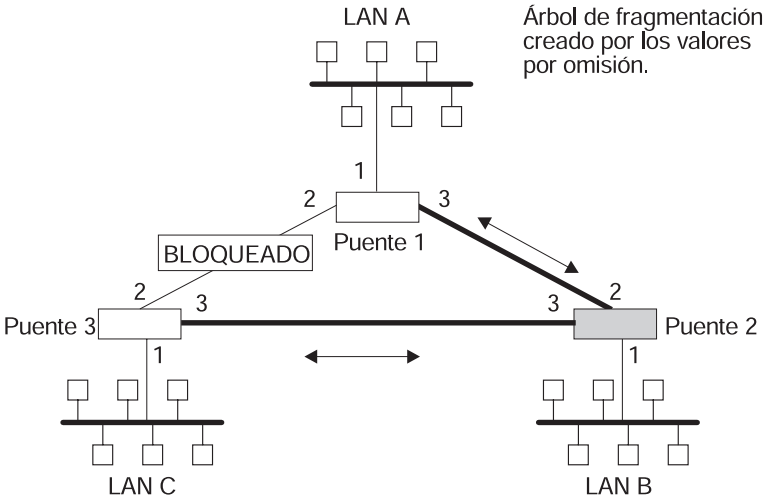



*Figura 7. Árbol de expansión creado con valores por omisión*

Normalmente, esta red utiliza el puerto entre el Puente 2 y el Puente 3 con poca frecuencia. Por lo tanto, puede mejorar el rendimiento de la red convirtiendo el Puente 1 en el puente raíz del árbol de expansión. Para ello, debe configurar el Puente 1 con la máxima prioridad, es decir, 1000. El árbol de expansión resultante de esta modificación se muestra en la Figura 8 en la página 18 como las líneas oscuras que conectan el Puente 1 al Puente 3 y el Puente 1 al Puente 2. El puente

raíz es ahora el Puente 1. Ahora la conexión entre el Puente 2 y el Puente 3 está bloqueada y sirve como vía de acceso de datos de reserva.

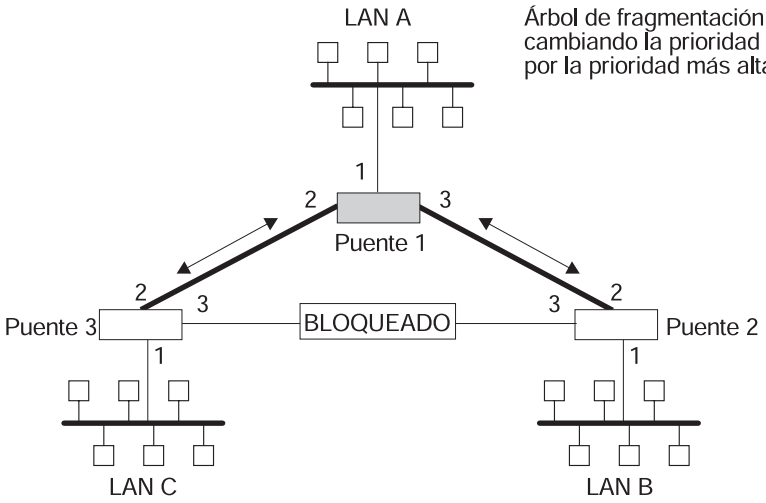



*Figura 8. Árbol de expansión ajustado por el usuario*

## Puentes de árbol de expansión y conversiones de formatos de paquetes Ethernet

El protocolo de puente de árbol de expansión 2210 ofrece dispositivos de conexión por puente y de reenvío de acuerdo con los puentes de control de acceso al medio (MAC) 802.1D-1990 del estándar IEEE. El protocolo también ofrece la conversión de cabecera adecuada para paquetes Ethernet.

Una red Ethernet/IEEE 802.3 puede dar soporte simultáneo a la capa de enlace de datos Ethernet y a la capa de enlace de datos IEEE, según el valor del campo de longitud/tipo de la cabecera MAC. El puente debe convertir del formato Ethernet y al formato Ethernet para ofrecer transparencia entre tipos mixtos de LAN. El algoritmo que se utiliza se basa en los estándares emergentes IEEE.

El enfoque básico consiste en convertir los paquetes Ethernet a paquetes de Información no numerada (UI) IEEE 802.2 mediante el SAP SNAP IEEE 802. El Identificador de protocolo SNAP tiene el identificador de organización exclusivo (OUI) de 00-00-00 (los dos últimos bytes corresponden al valor de *tipo* de Ethernet).

## Característica RT de IBM para el tráfico SNA

Algunos PC (IBM RT PC con AIX o cualquier PC con OS/2 EE) encapsulan SNA dentro de paquetes Ethernet de tipo 2 en lugar de utilizar el sistema de encapsulación de Ethernet IEEE 802.3. Para ello se necesita una cabecera Ethertype especial que contiene la longitud de los datos de usuario MAC seguida de la cabecera IEEE 802.2 (LLC).

El proceso de estas tramas se puede activar/desactivar por puertos. En la modalidad activada, el puente conoce el comportamiento de la estación de origen. Cuando las tramas se destinan a dichas estaciones, el puente genera el formato de trama correcto. Si no hay información sobre el comportamiento de la estación (como en difusiones generales o estaciones desconocidas), el puente genera

tramas duplicadas, una en formato IEEE 802.3 y IEEE 802.2 y otra con la cabecera IBM-RT.

## Encapsulado UB de tramas XNS

Las tramas XNS Ethernet utilizan Ethertype 0x0600. Cuando se convierten a formato de red en anillo, estas tramas obtienen SNAP según lo especificado en IEEE 802.1H. Puesto que algunas estaciones finales de red en anillo utilizan Ungermann-Bass OUI en SNAP para dichas tramas, hay un conmutador de configuración que sirve para activar este tipo de encapsulado. El conmutador que sirve para activar este encapsulado se define con el mandato **frame token_ring_SNAP**.

## Conexión por puente transparente y Frame Relay

La interfaz Frame Relay reenvía tramas transparentes procedentes de redes Ethernet y red en anillo, suponiendo que la conexión por puente esté activada en el circuito. No se tiene que utilizar la conexión por túnel IP.

Se generan y se transmiten BPDU tipo Hello por cada circuito configurado para la conexión por puente transparente. El protocolo de árbol de expansión hace que los circuitos Frame Relay que no han sido designados como parte de la vía de acceso de datos activa se BLOQUEEN, eliminando así la posibilidad de bucles.

## Conexión por puente transparente y ATM

La interfaz ATM reenvía tramas transparentes procedentes de redes Ethernet y red en anillo, suponiendo que la conexión por puente esté activada en la conexión de canal virtual (VCC). No se tiene que utilizar la conexión por túnel IP.

Se generan y se transmiten BPDU tipo Hello por cada VCC configurado para la conexión por puente transparente. El protocolo de árbol de expansión hace que los VCC ATM que no han sido designados como parte de la vía de acceso de datos activa se BLOQUEEN, eliminando así la posibilidad de bucles.

## Terminología y conceptos sobre el puente transparente

En esta sección se revisan los términos y conceptos que se suelen utilizar en la conexión por puente transparente.

### Periodo de antigüedad

Periodo de tiempo (antigüedad) que pasa antes de que se elimine una entrada dinámica de la base de datos de filtro, cuando el puerto con la entrada se encuentra en el estado de reenvío. Si el periodo de antigüedad no hace referencia a las entradas dinámicas, se suprimen.

### Puente

Dispositivo, independiente del protocolo, que conecta redes de área local (LAN). Estos dispositivos funcionan en la capa de enlace de datos, guardando y reenviando paquetes de datos entre las LAN.

### Dirección de puente

La parte de 6 octetos menos significativa del identificador de puente, que utiliza el algoritmo de árbol de expansión para identificar un puente en la red. La dirección de puente toma por omisión el valor de dirección MAC del puerto con el número más bajo. Puede alterar temporalmente la dirección por omisión mediante el mandato de configuración **set bridge**.

### Periodo Hello de puente

El periodo hello de puente especifica la frecuencia con que un puente envía BPDU tipo Hello (que contienen información de configuración del puente) cuando pasa a ser el puente raíz del árbol de expansión. Este valor sólo es útil para el puente raíz, puesto que controla el periodo hello de todos los puentes del árbol de expansión. Puede utilizar el mandato **set protocol bridge** para definir el periodo hello del puente.

### Retraso de reenvío de puente

La cantidad de tiempo que el puente está en estado de escucha y en estado de conocimiento. El retraso de reenvío es el periodo de tiempo en que el puerto del puente está escuchando, a fin de ajustar la topología del árbol de expansión. También es la cantidad de tiempo que emplea el puente en conocer la dirección de origen de cada paquete que recibe mientras se está configurando el árbol de expansión. Este valor sólo es útil para el puente raíz, puesto que controla el retraso de reenvío de todos los puentes del árbol de expansión.

El puente raíz transmite este valor a todos los puentes. Este periodo se define mediante el mandato **set protocol bridge**. El procedimiento para definir este parámetro se describe en el siguiente capítulo.

### Identificador de puente

Un identificador exclusivo que utiliza el algoritmo de árbol de expansión para determinar dicho árbol. Cada puente de la red debe tener un identificador de puente exclusivo.

El identificador de puente consta de dos partes: una dirección de puente de 6 octetos menos significativa y una prioridad de puente de 2 octetos más significativa. Por omisión, el valor de la dirección de puente es la dirección MAC del puerto con el número más bajo. Puede alterar temporalmente la dirección por omisión mediante el mandato de configuración **set bridge**,

### Antigüedad máxima de puente

La cantidad de tiempo en que la información del protocolo del árbol de expansión se considera válida antes de que el protocolo elimine la información y cambie una topología. Todos los puentes del árbol de expansión utilizan este valor para establecer el tiempo de espera de la información de configuración recibida en sus bases de datos. Esto puede hacer que se exceda de forma uniforme el tiempo de espera para cada puente del árbol de expansión. Utilice el mandato **set protocol bridge** para definir la antigüedad máxima de puente.

## Prioridad de puente

La parte de 2 octetos más significativa del identificador de puente definido por el mandato **set protocol bridge**. Este valor indica las oportunidades de cada puente de convertirse en el puente raíz de la red. Al definir la prioridad de puente, el algoritmo de árbol de expansión elige el puente con el valor de prioridad más alto como puente raíz del árbol de expansión. El puente con el valor numérico más bajo tiene el valor de prioridad más alto.

## Puente designado

El puente que se define como el más cercano al puente raíz de una determinada LAN. Esta cercanía se mide según el coste acumulado de vía de acceso al puente raíz.

## Puerto designado

El ID de puerto del puente designado conectado a la LAN.

## Bases de datos de filtro y permanente

Bases de datos que contienen información sobre las direcciones de estación que pertenecen a determinados números de puerto de puertos conectados a la LAN.

La base de datos de filtro se inicializa con entradas procedentes de la base de datos permanente. Estas entradas son permanentes y no se modifican porque se apague y encienda o se restaure el sistema. Puede añadir o suprimir estas entradas mediante los mandatos de configuración del árbol de expansión. Las entradas de la base de datos permanente se guardan como registros de memoria estática de acceso aleatorio (SRAM) y el número de entradas está limitado por el tamaño de la SRAM.

**Nota:** También puede añadir entradas (estáticas) mediante los mandatos de supervisión, pero estas ***no*** se conservan cuando se apaga y enciende o cuando se restaura el sistema.

La base de datos de filtro también acumula entradas que ha conocido el puente (entradas dinámicas), que tienen asociado un periodo de antigüedad. Cuando no se hace referencia a las entradas durante un determinado periodo de tiempo (periodo de antigüedad), se suprimen. Las entradas estáticas no tienen antigüedad, de modo que las entradas dinámicas no se pueden grabar sobre aquellas.

Las entradas de las bases de datos de filtro y permanente contienen la siguiente información:

- *Dirección*. La dirección MAC de 6 bytes de la entrada
- *Mapa de puertos*. Especifica todos los números de puertos asociados a la entrada
- *Tipo de entrada*. Especifica uno de los siguientes tipos:
  - Entradas reservadas. Reservadas por el comité IEEE 802.1d.
  - Entradas registradas. Constan de direcciones de difusión individual que pertenecen al hardware de comunicaciones conectado al recuadro o direcciones de difusión múltiple activadas por los distribuidores del protocolo.
  - Entradas permanentes. Las especifica el usuario en el proceso de configuración. Se conservan aunque se apague y encienda o se restaure el sistema.

  - Entradas estáticas. Las especifica el usuario en el proceso de supervisión. No se conservan cuando se apaga y enciende o se restaura el sistema y no tienen antigüedad.
  - Entradas dinámicas. Las conoce el puente de forma dinámica. No se conservan cuando se apaga y enciende o se restaura el sistema y tienen una antigüedad asociada.
  - Libres. Ubicaciones de la base de datos que están libres y se pueden rellenar con entradas de direcciones.
- *Antigüedad de dirección (sólo entradas dinámicas)*. Resolución del periodo de tiempo tras el que las entradas de dirección se marcan antes de ser eliminadas. El usuario puede definir este valor.

Puede realizar cambios en la base de datos permanente mediante los mandatos de configuración del árbol de expansión, y en la base de datos de filtro mediante el proceso de supervisión GWCON.

### Puentes paralelos
Dos o más puentes que conectan las mismas LAN.

### Coste de vía de acceso
Cada interfaz de puerto tiene un coste de vía de acceso asociado, que es el valor relativo de utilizar dicho puerto para alcanzar el puente raíz de una red conectada por puente. El algoritmo de árbol de expansión utiliza el coste de vía de acceso para calcular la vía de acceso que minimiza el coste desde el puente raíz a los demás puentes de la topología de red. La suma total de todos los costes designados y los costes de vía de acceso del puerto raíz recibe el nombre de coste de vía de acceso raíz.

### Puerto
La conexión del puente a cada LAN o WAN conectada. Un puente debe tener al menos dos puertos para que pueda funcionar como puente.

### ID de puerto
Un identificador de puerto de 2 octetos. El octeto más significativo representa la prioridad de puerto y el menos significativo representa el número de puerto. El usuario puede asignar tanto el número de puerto como la prioridad de puerto. El ID de puerto debe ser exclusivo dentro del puente.

### Número de puerto
Una parte de 1 octeto, asignada por el usuario, del ID de puerto, cuyo valor representa la conexión al medio físico. No se permite un valor de puerto de cero.

### Prioridad de puerto
La segunda parte de 1 octeto del ID de puerto. Este valor representa la prioridad del puerto que utiliza el algoritmo de árbol de expansión para realizar comparaciones para la selección de puerto y para las decisiones de bloqueo.

### Resolución
El factor de tiempo por el que las entradas dinámicas se marcan según su antigüedad en la base de datos. El rango permitido es de 1 a 60 segundos.

### Puente raíz
El puente seleccionado como el *raíz* del árbol de expansión porque posee el ID de puente con la prioridad más alta. Este puente es el responsable de mantener el árbol de expansión intacto, emitiendo con regularidad BPDU tipo Hello (que contienen información de configuración del puente). El puente raíz es el puente designado para todas las LAN a las que está conectado.

### Puerto raíz
El ID del puerto de un puente que ofrece la vía de acceso de coste más bajo al puente raíz.

### Árbol de expansión
Una topología de puentes en la que sólo hay una ruta de datos entre dos estaciones finales cualesquiera.

### Conexión por puente transparente
Este tipo de conexión por puente incluye un mecanismo que es *transparente* para las aplicaciones de las estaciones finales. La conexión por puente transparente interconecta segmentos de redes de área local mediante puentes designados para reenviar tramas de datos a través de un algoritmo de árbol de expansión.

## Conexión por puente de ruta de origen (SRB)

El direccionamiento de origen es un método de reenviar tramas a través de una red conectada por puente, según el que la estación de origen identifica la ruta que seguirá la trama. En un esquema de direccionamiento distribuido, las tablas de direccionamiento de cada puente determinan la vía de acceso que toman los datos a través de la red. Por el contrario, en un esquema de direccionamiento de origen, la estación de origen define la ruta completa en la trama transmitida.

El puente de direccionamiento de origen (SRB) ofrece conexión por puente local sobre redes en anillo de 4 y de 16 Mbps, tal como se muestra en la Figura 9. También puede conectar LAN remotas a través de un enlace de telecomunicaciones que funcione a velocidades de hasta E1.

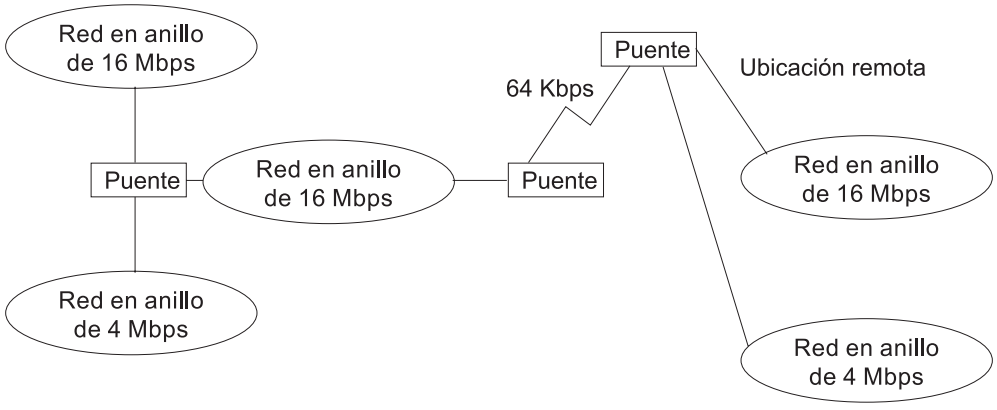



*Figura 9. Ejemplo de conectividad por puente de direccionamiento de origen*

Entre sus características, el puente de direccionamiento de origen ofrece:

- *Compatibilidad de puente*. Puede utilizar el puente para conectar LAN de PC que ejecutan sistemas como OS/2, PC LAN Manager y NetBIOS. El puente también puede transportar tráfico SNA entre LAN de PC y sistemas principales.
- *Rendimiento y velocidad*. Puesto que la conexión por puente se establece en la capa de enlace de datos en lugar de establecerse en la capa de red, no se necesitan funciones de conversión de paquetes ni de mantenimiento de tablas de direcciones. Esto genera una menor actividad generan y permite tomar decisiones de direccionamiento de mayor velocidad.
- *conexión por túnel de puente*. Al encapsular paquetes de direccionamiento de origen, el puente/direccionador dirige de forma dinámica estos paquetes a través de interredes a la estación final de destino deseada, sin degradación ni restricciones en el tamaño de la red.

  Las estaciones finales de direccionamiento de origen ven esta vía de acceso como un solo salto, independientemente de la complejidad de la red. Esto ayuda ayuda a evitar el límite habitual de distancia de siete saltos de las configuraciones de direccionamiento de origen. Esta característica también le permite conectar estaciones finales de direccionamiento de origen entre soportes de direccionamiento que no son de origen (por ejemplo, redes Ethernet).

## Funcionamiento del puente de direccionamiento de origen

Como ya se ha dicho, la estación de origen define la ruta completa en la trama transmitida en una configuración de direccionamiento de origen. El puente de direccionamiento de origen es dinámico. Ambas estaciones finales y los puentes participan en el proceso de descubrimiento de ruta y de reenvío. Los siguientes pasos describen este proceso:

1. Una estación de origen envía una trama y descubre que el destino de la trama no se encuentra en su mismo (local) segmento o anillo.
2. La estación de origen crea una trama de difusión general de *descubrimiento de ruta* y la transmite por el segmento local.
3. Todos los puentes del segmento local capturan la trama de descubrimiento de ruta y la envían sobre sus redes conectadas.

   A medida que la trama de descubrimiento de ruta continúa su búsqueda de la estación final de destino, cada puente que la reenvía añade su propio número de puente y número de segmento al campo de información de direccionamiento (RIF) de la trama. A medida que la trama sigue pasando por la red conectada por puente, el RIF acumula una lista de pares de número de puente y de segmento que describen la vía de acceso al destino.

   Cuando finalmente la trama de difusión general alcanza su destino, contiene la secuencia exacta de direcciones por las que ha pasado desde el origen hasta el destino.
4. Cuando la estación final de destino recibe la trama, genera una trama de respuesta que incluye la vía de acceso de origen para su comunicación. Las tramas que vagan por otras partes de la red conectada por puente (acumulando mientras información de direccionamiento irrelevante) nunca alcanzad la estación final de destino, y ninguna estación las recibe.

5. La estación originaria recibe la vía de acceso de ruta aprendida. Luego puede transmitir información por la vía de acceso establecida.

## Tramas de direccionamiento de origen

Tal como se ha mencionado, los puentes interconectan LAN transmitiendo tramas de datos, especialmente tramas MAC, entre entidades MAC separadas de las LAN conectadas por el puente. Las tramas MAC contienen la información sobre "¿Dónde?" necesaria en forma de direcciones de origen y de destino. Esta información resulta esencial para la transmisión y recepción satisfactorias de los datos.

En el direccionamiento de origen, la decisión sobre el reenvío de tramas de datos se basa en la información de direccionamiento que se encuentra en la trama. Antes de reenviar la trama, las estaciones finales han obtenido la ruta a la estación de destino mediante el proceso de *descubrimiento de ruta*. La estación de destino que origina la trama designa la ruta por la que viajará la trama, incluyendo una descripción de la ruta en el campo de información de direccionamiento (RIF) de la trama transmitida. Un examen más detallado de los diversos tipos de tramas de puente de direccionamiento de origen nos ayudará a explicar el modo en que el puente obtiene y transmite esta información de direccionamiento.

Puesto que las tramas MAC de direccionamiento de origen contienen la información de direccionamiento necesaria para la comunicación de datos sobre entornos de varios anillos, difieren ligeramente en formato de las típicas tramas MAC de red en anillo. La presencia de un "1" en el RII del campo de dirección de origen indica que hay un RIF que contiene información de direccionamiento después de la dirección de origen. La Figura 10 ofrece una visión más detallada del formato del campo de dirección de origen de una trama de direccionamiento de origen.

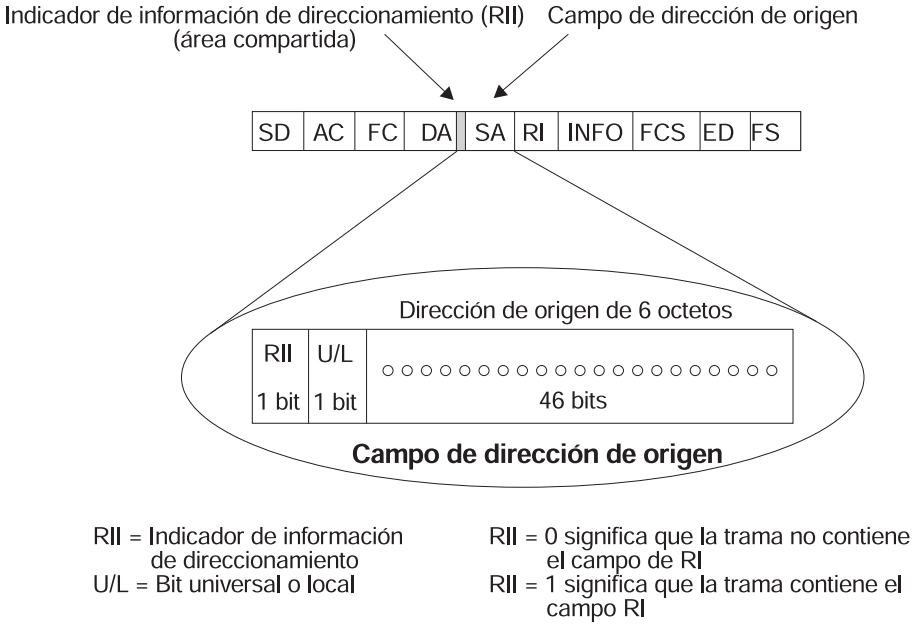



*Figura 10. Formato de dirección de origen 802.5*

Cuando el valor del RII del campo de dirección de origen es 1, significa que hay un RIF después de la dirección de origen. El RIF es necesario porque ofrece información de ruta durante el direccionamiento de origen. Consta de un campo de

control de direccionamiento (RC) de 2 octetos y una serie de campos de designador de ruta (RD) de 2 octetos. La Figura 11 en la página 26 ofrece una visión más detallada del formato de un campo de información de direccionamiento.

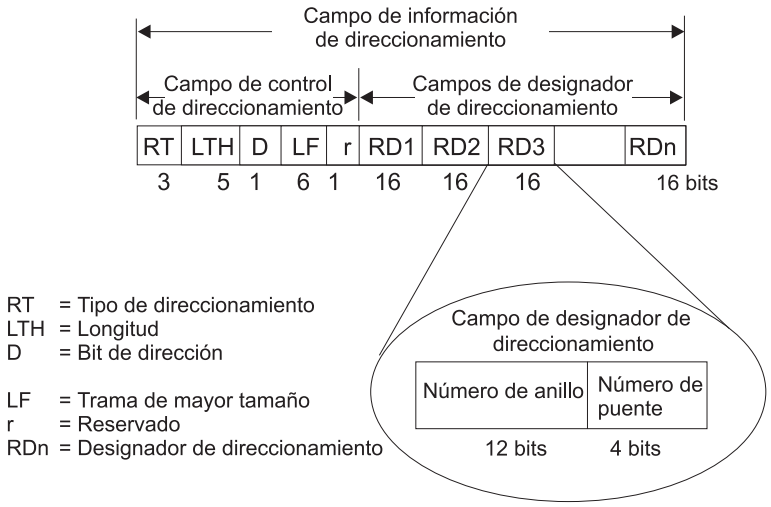



*Figura 11. Campo de información de direccionamiento 802.5*

La siguiente información describe cada campo del RIF:

- **Tipo de direccionamiento (RT)**.

  Indica, mediante valores de bits, si la trama se debe reenviar por la red a través de una ruta específica o a través de una ruta (o rutas) que llegue a todas las LAN interconectadas. En función de los valores de bits de este campo, la trama se puede identificar como de uno de los siguientes tipos:

  – Trama exploradora de todas las vías de acceso (trama exploradora)
  – Trama exploradora del árbol de expansión (trama exploradora)
  – Trama direccionada específicamente (trama de direccionamiento)
  – Trama direccionada por el árbol de expansión (trama de direccionamiento)

  Hay *tramas exploradoras de todas las vías de acceso* si el valor de los bits RT es 100. Estas tramas se generan y se direccionan por cada ruta no repetitiva de la red (del origen al destino). El resultado de este proceso es que muchas tramas llegan a la estación final de destino, puesto que hay distintas rutas que parten de la estación final de origen. Este tipo de direccionamiento es la respuesta a recibir una trama de descubrimiento de ruta enviada por el árbol de expansión a la estación original, utilizando todas las rutas disponibles. Los puentes que efectúan reenvíos añaden designadores de direccionamiento a la trama.

  Hay una *trama exploradora del árbol de expansión* si el valor de los bits RT es 110. Sólo los puentes del árbol de expansión transmiten la trama de una red a otra. Esto significa que que la trama aparece una sola vez en cada anillo de la red, y por lo tanto una sola vez en la estación final de destino. Una estación que inicia el proceso de descubrimiento de ruta utiliza este tipo de trama. El puente añade campos de designación de direccionamiento a la trama. También se puede utilizar para tramas enviadas a estaciones con direcciones de grupo, lo que se describe con más detalle en la siguiente sección.

  Hay *tramas direccionadas específicamente* si el valor del primer bit RT es 0. En este caso, los campos de Desginador de ruta (RD) que contienen infor-

mación de direccionamiento específico guían a la trama a través de la red hasta la dirección de destino. Cuando la trama alcanza su destino y descubre una vía de acceso de ruta, la estación de destino devuelve una trama direccionada específicamente (SRF) a la estación de origen. A continuación, la estación de origen transmite sus datos en una trama direccionada específicamente.

- **Bits de longitud (LTH)**. Indican la longitud (en octetos) del campo RI.
- **Bit de dirección (D)**. Indica la dirección que toma la trama para atravesar las redes conectadas. Si el valor de este bit es 0, la trama viaja por las redes conectadas en el orden en el que están especificadas en el campo de información de direccionamiento (por ejemplo, de RD1 a RD2 a... a RDn). Si el valor del bit de dirección es 1, la trama viaja por las redes en el orden inverso.
- **Bits de trama mayor (LF)**. Indica el tamaño mayor de trama del campo INFO que se puede transmitir entre dos estaciones finales comunicadas en una determinada ruta. Los bits LF sólo tienen significado para tramas STE y ARE. En tramas direccionadas específicamente (SRF), el puente pasa por alto los bits LF y no los puede modificar. Una estación que envía una trama exploradora, define para los bits LF el mayor tamaño de trama que puede manejar. Los puentes de reenvío definen para los bits LF el valor más alto posible que no supere el mínimo de:
  - El valor indicado de los bits LF recibidos
  - El mayor tamaño posible de la unidad máxima de datos de servicio (MSDU) que recibe soporte del puente
  - El mayor tamaño de MSDU posible que recibe soporte del puerto desde el que se ha recibido la trama
  - El mayor tamaño de MSDU posible que recibe soporte del puerto al que se va a transmitir la trama.

  Si es necesario, la estación de destino reduce el valor de LF para indicar su capacidad máxima de trama.

  La codificación de bits LF se compone de una codificación base de 3 bits y una codificación ampliada de 3 bits (6 bits en total). El puente SRT (que se explica en una sección posterior) contiene un indicador de modalidad LF que permite al puente seleccionar los bits LF base o ampliados. Cuando el valor del indicador de modalidad de LF es *base mode* (modalidad base), el puente define para los bits LF de tramas exploradoras los valores mayores de base de trama. Cuando el valor del indicador de modalidad LF es *extended mode* (modalidad ampliada), el puente define para los bits LF de tramas exploradoras los mayores valores ampliados de trama.
- Los **campos de designador de ruta (RDn)** indican la ruta específica de la red de acuerdo a la secuencia de los campos RD. Cada campo RD contiene un número de anillo exclusivo de red de 12 bits y un número de puente de 4 bits que establece una diferencia entre dos o más puentes que conectan los mismos anillos (puentes paralelos). El último número de puente del campo de información de direccionamiento contiene un valor nulo (todo ceros).

# La opción de exploración del árbol de expansión

La característica de exploración del árbol de expansión le permite seleccionar una sola ruta al destino cuando la red tiene dos o más puentes que conectan las mismas LAN. Con esta característica activada, sólo los puentes seleccionados reciben tramas exploradoras del árbol de expansión (STE). Para no confundirlo con el protocolo de árbol de expansión, esta opción le permite:

- Simular una red de árbol de expansión
- Equilibrar las cargas de tráfico

## Simulación de una red de árbol de expansión

Una red de árbol de expansión contiene una sola ruta entre dos estaciones finales cualesquiera. Si la red utiliza dos o más puentes paralelos, como los de la Figura 12, puede configurar de forma manual un árbol de expansión en la red, evitando la duplicación de tramas de descubrimiento en la red. Si la característica de exploración de árbol de expansión no está activada, si la Estación Q transmite una trama de descubrimiento a la Estación R, tanto el Puente A como el Puente B retransmiten dicha trama. El Segmento 2 recibe dos copias de la misma trama.

Con la opción de exploración de árbol de expansión activada, cada segmento de la LAN de la red recibe una sola copia de la trama transmitida. Sólo los puentes que seleccione pueden recibir tramas STE, reduciendo la creación de tramas redundantes y la actividad general de la red.

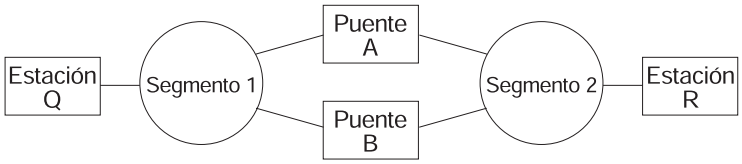



*Figura 12. Ejemplo de puentes paralelos*

## Equilibrio de cargas de tráfico

También puede utilizar la opción de exploración de árbol de expansión para equilibrar la carga. Por ejemplo, en la Figura 13 el Puente A está configurado para que acepte tramas STE sobre la interfaz que conecta el Segmento 2. El Puente B está configurado para que acepte tramas sobre la interfaz que conecta el Segmento 1. El tráfico viaja en la dirección de las flechas. Esta configuración permite a los puentes paralelos compartir la carga de tráfico.

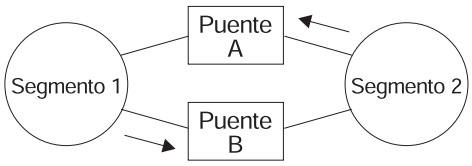



*Figura 13. Utilización de la opción de exploración de árbol de expansión para equilibrar cargas*

**Nota:** Para que funcione el direccionamiento de origen, algunas aplicaciones de nodo final, como los programas de la LAN de PC, necesitan que active la opción de exploración de árbol de expansión en las interfaces conectadas. En el caso de una configuración de puentes paralelos, la opción de exploración de árbol de expansión sólo debe estar activada en una de las

interfaces paralelas. Sin embargo, no se produce ningún error serio (que no sea un exceso de tráfico) si se tienen demasiadas interfaces activadas para el árbol de expansión.

Si utiliza la opción de exploración de árbol de expansión y algún puente de la única vía de acceso deja de funcionar, el tráfico de direccionamiento de origen no puede alcanzar su destino. Debe volver a configurar de forma manual una vía de acceso alternativa.

## Conexión por puente de direccionamiento de origen y Frame Relay

Si la conexión por puente de direccionamiento de origen está activada, las tramas direccionadas por el origen se reenvían entre la interfaz Frame Relay y el distribuidor de la conexión por puente. Puede configurar el puente para que trate cada circuito virtual Frame Relay como un puerto de puente con un número de anillo exclusivo. Además, los circuitos virtuales Frame Relay que no están configurados como puertos de puente, se pueden agrupar como un solo puerto de puente multiacceso con un número de anillo exclusivo. Para obtener más información, consulte el tema “Visión general de los puertos de puente multiacceso” en la página 58. Algunos circuitos virtuales que no forman parte de la vía de acceso de datos activa se BLOQUEAN, a fin de mantener una topología libre de bucles.

## Conexión por puente de direccionamiento de origen y ATM

Si la conexión por puente de direccionamiento de origen está activada en la conexión de canal virtual (VCC), las tramas direccionadas por el origen se reenvían entre la interfaz ATM y el distribuidor de la conexión por puente. Se configura un número de anillo de destino exclusivo para cada VCC. Algunas VCC que no forman parte de la vía de acceso de datos activa se BLOQUEAN, a fin de mantener una topología libre de bucles.

## Terminología y conceptos sobre el puente de direccionamiento de origen

En esta sección se revisan los términos y conceptos que se suelen utilizar en la conexión por puente de direccionamiento de origen.

### Instancia de puente

La instancia de puente identifica la secuencia de un puente definido en el software. Por ejemplo, en un puente con dos puentes configurados, las instancias de puentes serían 1 y 2.

Las instancias de puente dentro de un solo puente son independientes y no se comunican entre sí. Por ejemplo, en la Figura 14 en la página 30, la Estación A no puede pasar datos a ninguna estación de la Instancia de puente 2. Sólo puede pasar tramas a la Estación B. De hecho, la instancia de puente le permite crear dos redes separadas. Estas redes no se comunican entre sí a no ser que estén físicamente conectadas a otro punto.

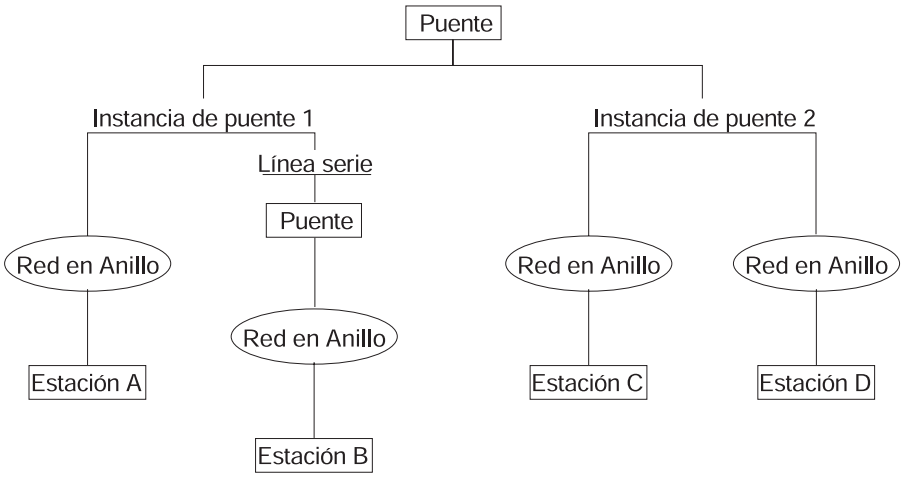



*Figura 14. Instancias de puente dentro de un puente*

## Número de puente

El número de puente es un valor hexadecimal de 4 bits que identifica un puente. Aunque los puentes que se conectan al mismo anillo pueden tener el mismo número de puente, los puentes paralelos (puentes que están conectados a los mismos anillo) deben tener números de puente exclusivos.

## Tramas exploradoras

El puente de direccionamiento de origen añade información de direccionamiento a una trama exploradora a medida que reenvía la trama a través de la red a la estación final de destino. La trama exploradora sirve para descubrir rutas. Hay dos tipos de tramas exploradoras: tramas exploradoras de todas las rutas (ARE) y tramas exploradoras del árbol de expansión (STE). Todos los puertos reenvían tramas ARE, mientras que únicamente los puertos asignados para ello por el protocolo de árbol de expansión reenvían tramas STE.

## Número de interfaz

El número de interfaz identifica una interfaz “física” dentro del producto/hardware y debe estar enlazada a una interfaz “lógica”, que el puente pueda comprender (es decir, un puerto). Al configurar el software del dispositivo, el direccionador/puente numera los puertos de forma secuencial. Para utilizar el puente de direccionamiento de origen, debe utilizar los números de puerto para identificar la interfaz que conecta cada segmento de la red.

## Ruta

La ruta es una vía de acceso a través de una serie de LAN y puentes, por ejemplo puentes SRB.

## Descubrimiento de ruta

El descubrimiento de ruta es el proceso por el cual se aprende una ruta a la estación final de destino.

### Número de segmento

El número de segmento identifica cada LAN, como una sola red en anillo o una línea serie. Un segmento se conecta al puente, pero también puede funcionar de forma independiente.

### Direccionamiento de origen

El direccionamiento de origen es un mecanismo de conexión por puente que direcciona tramas a través de una red de varias LAN, especificando en la trama la ruta por la cual viajará.

## Puente transparente de direccionamiento de origen (SRT)

Después de haber dedicado mucho esfuerzo a adoptar tecnologías estandarizadas (tanto Ethernet como red en anillo están definidas por IEEE), es posible que en realidad deba trabajar con sistemas no estandarizados al intentar conectarlas. Esto se debe a que los puentes funcionan de forma diferente en redes en anillo y Ethernet.

Aparte de las diferencias como la clasificación de bits, el tamaño de paquetes y los bits de acuse de recibo, las diferencias en los métodos de conexión por puente representan otro obstáculo. Los puentes Ethernet utilizan el método de conexión por puente transparente, en el que el puente determina la ruta del tráfico a través de la red. Las redes en anillo sólo utilizan la conexión por puente transparente en algunos casos, por lo que generalmente dependen del direccionamiento de origen como método principal de conexión por puente.

El direccionamiento de origen no funciona en un entorno transparente, puesto que los paquetes transparentes no contienen información de direccionamiento. En este caso, el puente no tiene modo de saber dónde reenviar el paquete. Aunque que la conexión por puente transparente puede funcionar en un entorno de direccionamiento de origen, lo hace sin que se pase información de direccionamiento a la estación final. Falta información significativa (por ejemplo, sobre tamaños de paquetes), lo que puede ocasionar problemas.

IEEE ha ratificado una extensión al estándar de conexión por puente transparente 802.1D denominado transparencia de direccionamiento de origen (SRT). SRT es una tecnología de conexión por puente que intenta resolver gran parte de la incompatibilidad inherente de conectar por puente redes en anillo y Ethernet. Le ahorra el coste de instalar varios puentes y diversos enlaces para dar soporte a los dos tipos de tráfico, añadiendo una arquitectura de conexión por puente paralelo (en lugar de una alternativa) al estándar de conexión por puente transparente.

## Descripción general

Un puente transparente de direccionamiento de origen (SRT) es un puente MAC que realiza funciones de direccionamiento de origen cuando recibe tramas de direccionamiento de origen con información de direccionamiento y realiza la conexión por puente transparente cuando recibe tramas sin información de direccionamiento. En SRT, todos los puentes entre redes Ethernet y redes en anillo son transparentes. Los puentes funcionan en la subcapa MAC de la capa de enlace de datos y resultan completamente invisibles ante las estaciones finales.

El puente SRT distingue entre los dos tipos de tramas comprobando el valor del campo RII de la trama (consulte el tema “Tramas de direccionamiento de origen”

en la página 25 para obtener más información). El valor 1 del campo RII indica que la trama lleva información de direccionamiento, mientras que el valor 0 del campo RII indica que no lleva información de direccionamiento. Con este método, el puente SRT reenvía tramas de conexión por puente transparente sin conversiones al soporte de salida (incluida la red en anillo). Las tramas de direccionamiento de origen están restringidas al dominio de conexión por puente de direccionamiento de origen.

El algoritmo y el protocolo de árbol de expansión forman un solo árbol que incluye todas las redes conectadas por puentes SRT. La red conectada por puente SRT ofrece un dominio de mayor tamaño de conexión por puente transparente con subdominio de direccionamiento de origen. De este modo, las tramas transparentes pueden alcanzar el extremo más alejado de la LAN conectada por puente SRT y TB, mientras que las tramas direccionadas por el origen están limitadas a la LAN conectada por puente SRT y SRB. En el modelo de conexión por puente SRT, las partes de direccionamiento de origen y de conexión por puente transparente utilizan el mismo árbol de expansión. En el dominio conectado por puente SRT, las estaciones finales son las responsables de responder a la pregunta "¿Direccionamiento de origen o conexión por puente transparente?".

## Arquitectura y funcionamiento del puente transparente de direccionamiento de origen

Con un puente SRT, cada puerto de puente recibe y transmite tramas destinadas y procedentes de las redes de área local conectadas mediante los servicios MAC suministrados por la entidad MAC individual asociada a cada puerto. La entidad de transmisión MAC es la encargada de las tareas, independientes de MAC, de transmitir tramas entre puertos de puente. Si la trama recibida no está direccionada por el origen (RII = 0), la trama de puente se reenvía o se elimina utilizando la lógica de conexión por puente transparente. Si la trama recibida está direccionada por el origen (RII = 1), la trama se maneja de acuerdo a la lógica de direccionamiento de origen. Este proceso se ilustra en la Figura 15. Las flechas representan la vía de acceso de datos.

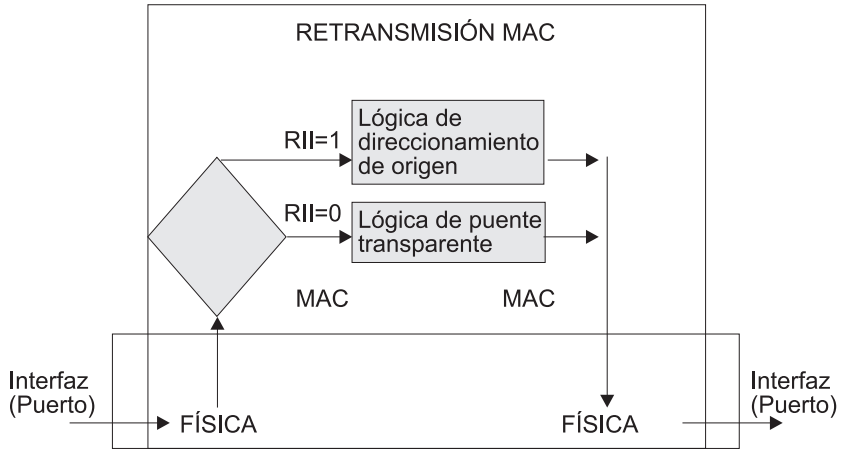



*Figura 15. Funcionamiento del puente SRT*

SRT distingue entre tráfico direccionado por el origen y tráfico no direccionado por el origen trama a trama. Si el paquete está direccionado por el origen, el puente lo reenvía como tal. Si se trata de un paquete de puente transparente, el puente determina la dirección de destino y reenvía el paquete.

## Conexión por puente transparente de direccionamiento de origen y Frame Relay

Si la conexión por puente SRT está activada en el circuito, se reenvían tramas direccionadas por origen y transparentes entre la interfaz Frame Relay y el distribuidor de la conexión por puente.

## Conexión por puente transparente de direccionamiento de origen y ATM

Si la conexión por puente SRT está activada en la conexión de canal virtual (VCC), se reenvían tramas direccionadas por origen y transparentes entre la interfaz ATM y el distribuidor de la conexión por puente.

## Terminología del puente transparente de direccionamiento de origen

En esta sección se revisan los términos y conceptos que se suelen utilizar en la conexión por puente SRT.

### Tramas exploradoras

El puente de direccionamiento de origen añade información de direccionamiento a una trama exploradora a medida que reenvía la trama a través de la red a la estación final de destino. La trama exploradora descubre la ruta. Hay dos tipos de tramas exploradoras:

- Tramas exploradoras de todas las rutas (ARE)
- Tramas exploradoras del árbol de expansión (STE)

Todos los puertos pueden reenviar tramas ARE, mientras que únicamente los puertos asignados para ello por el protocolo de árbol de expansión pueden reenviar tramas STE.

### Campo de información de direccionamiento (RIF)

En el direccionamiento de origen, la decisión sobre el reenvío de tramas de datos se basa en la información de direccionamiento que se encuentra en la trama. Antes de reenviar la trama, las estaciones finales obtienen la ruta a la estación de destino mediante el proceso de *descubrimiento de ruta*. La estación que origina la trama (es decir, la estación de *origen*) designa la ruta por la que viajará la trama incluyendo una descripción de la ruta en el Campo de información de direccionamiento (RIF) de la trama transmitida.

### Indicador de información de direccionamiento (RII)

Puesto que las tramas MAC de direccionamiento de origen contienen la información de direccionamiento necesaria para la comunicación de datos sobre entornos de varios anillos, sus formatos difieren ligeramente de los de las típicas tramas MAC de red en anillo. La presencia de un 1 en el campo de dirección de origen denominado Indicador de información de direccionamiento indica que hay un Campo de información de direccionamiento después de la dirección de origen. El puente SRT distingue entre tramas direccionadas por el origen y tramas no direccionadas por el origen comprobando si hay el valor 1 ó 0 en el campo RII.

### Direccionamiento de origen
Un mecanismo de conexión por puente que direcciona tramas a través de una red de varias LAN, especificando en la trama la ruta por la cual viajará.

### Árbol de expansión
Una topología de puentes en la que sólo hay una ruta de datos entre dos estaciones finales cualesquiera.

### Conexión por puente transparente
Un tipo de conexión por puente que incluye un mecanismo que resulta transparente para las estaciones finales. La conexión por puente transparente interconecta segmentos de redes de área local mediante puentes designados para reenviar tramas de datos a través de un algoritmo de árbol de expansión.

## Visión general del puente ASRT

El puente transparente de direccionamiento de origen adaptable (ASRT) es un grupo de software de varias opciones de conexión por puente. El software de puente ASRT combina la conexión por puente transparente y el direccionamiento por puente de modo que pueden funcionar por separado o se pueden combinar como un solo puente ASRT. Esta función ampliada permite la comunicación entre una estación final de direccionamiento de origen estricto y una estación final transparente mediante un puente ASRT. En función del grupo de mandatos de configuración que se utilice, el puente ASRT ofrece las siguientes opciones de conexión por puente:

- Puente transparente (STB)
- Puente de direccionamiento de origen (SRB)
- Puente transparente de direccionamiento de origen (ASRT)
- Direccionamiento de origen—puente transparente (SR-TB)

El diseño del puente ASRT se basa en el puente transparente de direccionamiento de origen descrito en IEEE 802.5M/Borrador 6 (1991) de SRT. Se han incorporado modificaciones en el puente ASRT que ofrecen a los usuarios la función ampliada que cumple con el estándar SRT. El puente ASRT permite la compatibilidad con la base instalada de puentes de direccionamiento de origen, mientras que les sigue permitiendo establecer enlace con LAN Ethernet y de red en anillo. ASRT también mejora la función SRT básica de algunos modos alternativos que se describen en las siguientes secciones.

## Puente transparente de direccionamiento de origen adaptable (ASRT) (Conversión SR-TB)

Aunque el direccionamiento de origen sigue estando disponible en el modelo SRT, sólo está disponible entre redes en anillo adyacentes de direccionamiento de origen. Los puentes que sólo sean de direccionamiento de origen no pueden coexistir con puentes SRT que enlazan LAN Ethernet y de red en anillo. Puesto que un nodo final de red en anillo se tiene que comunicar con un nodo Ethernet, se debe configurar para que omita los RIF. Además, si el nodo final se configura de modo que omita los RIF, no puede comunicarse a través de los puentes de direccionamiento de origen ordinarios que necesitan dicho RIF.

## Descripción general

La opción direccionamiento de origen - puente transparente (SR-TB) interconecta redes que utilizan la conexión por puente de direccionamiento de origen (dominio de direccionamiento de origen) y la conexión por puente transparente (dominio de conexión por puente transparente). Une de forma transparente ambos dominios. Durante su funcionamiento, las estaciones de ambos dominios no conocen su existencia entre sí ni la existencia del puente SR-TB. Desde el punto de vista de una estación, cualquier estación de la red combinada aparece como si estuviera en su propio dominio.

El puente consigue realizar esta función convirtiendo tramas procedentes del dominio de conexión por puente transparente a tramas de direccionamiento de origen antes de reenviarlas al dominio de direccionamiento de origen (y viceversa). El puente lleva a cabo esta tarea manteniendo una base de datos de direcciones de estaciones finales, cada una de ellas con su Campo de información de direccionamiento del dominio de direccionamiento de origen. El puente también lleva a cabo la tarea de descubrimiento de ruta en nombre de las estaciones finales del dominio de conexión por puente transparente. El proceso de descubrimiento de ruta sirve para buscar la ruta a la estación de destino del dominio de direccionamiento de origen. Las tramas que se envían a un destino desconocido se envían en el formato del explorador de árbol de expansión (STE).

El puente SR-TB anticipa tres tipos de árboles de expansión:

- Un árbol de expansión formado por el dominio de puente transparente
- Un árbol de expansión formado por el dominio de puente de direccionamiento
- Un árbol de expansión especial de todos los puentes SR-TB

En las siguientes secciones se describe con más detalle el funcionamiento del árbol SR-TB.

## Funcionamiento del direccionamiento de origen-puente transparente

Durante el funcionamiento SR-TB, una red se particiona en una serie de dos o más dominios. Cada dominio consta de una serie de segmentos de la LAN, interconectados por puentes que funcionan bajo un método común de conexión por puente. Esto permite crear redes que consten de dos tipos de dominios (en función del método de conexión por puente):

- Dominios de direccionamiento de origen
- Dominios de conexión por puente transparente

La Figura 16 en la página 36 muestra un ejemplo de estos dominios. Con dominios separados, cada dominio de direccionamiento de origen tiene una sola topología de difusión general de una sola ruta configurada por sus puentes. Sólo los puentes que pertenecen a dicho *árbol de expansión* de direccionamiento de origen quedan designados para reenviar tramas de difusión general de una sola ruta. En este caso, las tramas que llevan el indicador de difusión general de una sola ruta se direccionan a cada segmento del dominio de direccionamiento de origen. Sólo una copia de la trama llega a cada segmento, puesto que el árbol de expansión de direccionamiento de origen no permite más de una vía de acceso entre dos estaciones del dominio.

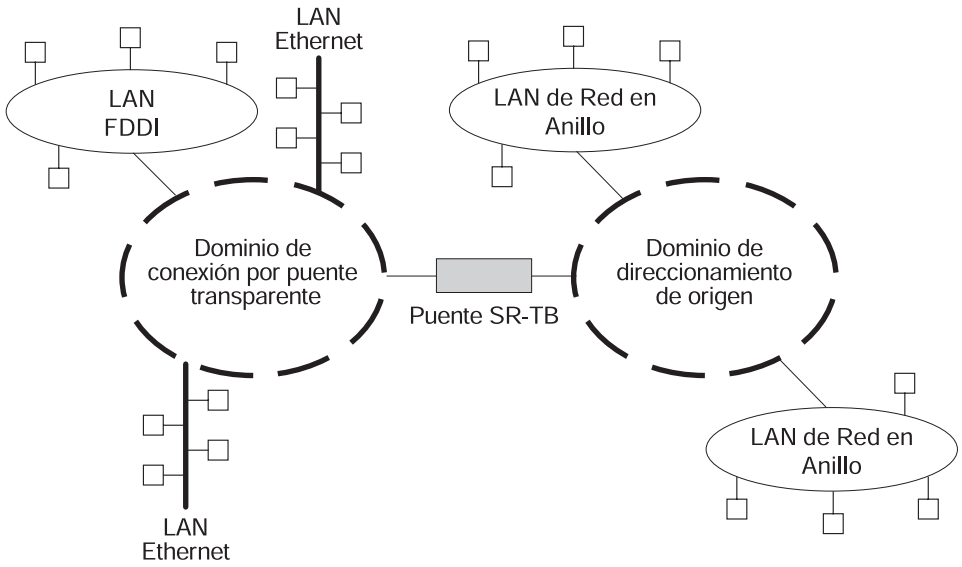



*Figura 16. Puente SR-TB de conexión de dos dominios*

## Operaciones específicas de direccionamiento de origen y conexión por puente transparente

El puente SR-TB es un *dispositivo de dos puertos* con una interfaz MAC asignada al segmento de la LAN del lado de direccionamiento de origen y otra asignada al segmento de la LAN del lado de conexión por puente transparente. Cada estación final lee la capa MAC adecuada a su segmento de la LAN. Esto significa que las funciones de conexión por puente se pueden dividir en dos tipos de operaciones:

- Operaciones de conexión por puente transparente
- Operaciones de conexión por puente de direccionamiento de origen

En el lado de la conexión por puente transparente, el puente SR-TB funciona igual que cualquier otro puente transparente. El puente mantiene una tabla de direcciones correspondientes a las estaciones que sabe que son estaciones de conexión por puente transparente. El puente SR-TB observa los protocolos *entre puentes* necesarios para crear y mantener el árbol de expansión de la red, puesto que más de un puente SR-TB une distintos dominios.

El puente SR-TB reenvía las tramas recibidas procedentes de su estación de conexión por puente transparente al lado de direccionamiento de origen del puente sólo en el caso de que la dirección de destino que lleva la trama no se encuentre en la tabla de direcciones del lado de la conexión por puente transparente del puente.

En el lado de conexión por puente de direccionamiento de origen, el puente SR-TB combina las funciones de un puente de direccionamiento de origen y de una estación final de direccionamiento de origen de un modo específico. Como estación final de direccionamiento de origen, el puente mantiene una asociación de direcciones de destino e información de direccionamiento en el lado de direccionamiento de origen. Se comunica como estación final para aplicaciones que se encuentran en el puente mismo (por ejemplo, gestión de red) o como intermediario para las estaciones que se encuentran en el lado de conexión por puente transparente.

El puente SR-TB reenvía las tramas recibidas procedentes de su estación de conexión por puente transparente al lado de direccionamiento de origen del puente sólo en el caso de que la dirección de destino que lleva la trama no se encuentre en la tabla de direcciones del lado de la conexión por puente transparente del puente. Las tramas que transmite la estación de direccionamiento de origen del puente llevan información de direccionamiento asociada al puente, en el caso de que el puente conozca y mantenga dicha información.

Como puente de direccionamiento de origen, el puente SR-TB participa en el proceso de descubrimiento de ruta y en el direccionamiento de tramas que ya llevan información de direccionamiento. El designador de ruta exclusivo del puente SR-TB consta del número de LAN de cada LAN de su lado de direccionamiento de origen y el número de puente individual del puente.

El puente también mantiene un solo número de LAN que representa todas las LAN del lado de conexión por puente transparente. El puente SR-TB trata cada caso de tramas recibidas y reenviadas de forma distinta, tal como se describe en la Tabla 3.

*Tabla 3 (Página 1 de 2). Tabla de decisiones del puente SR-TB*

| **Tipo de trama recibida** | **Acción emprendida por el puente SR-TB** |
|---|---|
| Tramas no direccionadas recibidas por la estación de direccionamiento de origen. | No copia ni reenvía tramas que lleven información de direccionamiento. |
| Trama de difusión general a todas las rutas recibida por la estación de direccionamiento de origen. | Copia la trama y define los bits A y C del indicador de difusión general en la trama repetida. Si la dirección de destino se encuentra en la tabla de conexión por puente transparente, el puente reenvía la trama sin información de direccionamiento a través de la red de conexión por puente transparente. Si no es así, no se reenvía la trama. |
| Trama de difusión general de una sola ruta recibida por la estación de direccionamiento de origen. El puente no está designado como puente de difusión general de una sola ruta. | No copia ni reenvía la trama. |
| Trama de difusión general de una sola ruta recibida por la estación de direccionamiento de origen. El puente está designado como puente de difusión general de una sola ruta. | Copia la trama, define los bits A y C del indicador de difusión general, elimina la información de direccionamiento de la trama y reenvía la trama modificada al lado de conexión por puente transparente. Añade su número de puente al campo guardado de información de direccionamiento y el número de LAN para el lado de conexión por puente transparente. Cambia el indicador de difusión general a no de difusión general, complementa el bit D y guarda esta información de direccionamiento para la dirección de origen de la trama. |

*Tabla 3 (Página 2 de 2). Tabla de decisiones del puente SR-TB*

| Tipo de trama recibida | Acción emprendida por el puente SR-TB |
|---|---|
| Trama no de difusión general recibida por la estación de direccionamiento de origen. | Si la trama lleva una ruta específica, el puente examina la información de direccionamiento. Si el puente SR-TB forma parte de la ruta y aparece entre el número de LAN correspondiente al lado de direccionamiento de origen y el número de LAN correspondiente a lado de puente transparente, el puente copia la trama y define los bits A y C en la trama repetida. Reenvía la trama al lado de conexión por puente transparente sin información de direccionamiento. Si el puente aún no tiene una ruta permanente para la dirección de origen, guarda una copia de la información de direccionamiento, complementa el bit D y guarda la información de direccionamiento correspondiente a la dirección de origen de la trama. |
| Trama recibida procedente del lado de conexión por puente transparente. | Para reenviar la trama al lado de direccionamiento de origen, el puente primero determina si tiene información de direccionamiento asociada a la dirección de destino que lleva la trama. Si es así, el puente añade información de direccionamiento a la trama, define el valor 1 para el RII y coloca la trama en cola para su transmisión al lado de direccionamiento de origen. Si no es así, el puente añade un campo de control de direccionamiento a la trama que contiene un indicador de difusión general de una sola ruta y dos designadores de ruta que contienen los dos primeros números de LAN de su propio número de puente individual. |

## Conexión por puente SR-TB: cuatro ejemplos

El puente SR-TB interconecta dominios de direccionamiento de origen con dominios de conexión por puente transparente, uniendo dichos dominios de forma transparente. Durante su funcionamiento, las estaciones de ambos dominios no conocen su existencia entre sí ni la existencia del puente SR-TB. Desde el punto de vista de la estación, cualquier estación de la red combinada aparece como si estuviera en su propio dominio.

Las siguientes secciones contienen ejemplos específicos de reenvío de tramas durante una conexión por puente SR-TB. En estos ejemplos se da por supuesto que el puente SR-TB está designado como un puente de difusión general de una sola ruta. La Figura 17 en la página 39 ofrece la siguiente información que acompaña a las situaciones descritas en cada sección:

- Q es el número de puente del puente
- X es el número de LAN correspondiente a la LAN del lado de direccionamiento de origen
- Y es el número de LAN correspondiente a la LAN del lado de conexión por puente transparente
- A, B, C y D representan estaciones finales

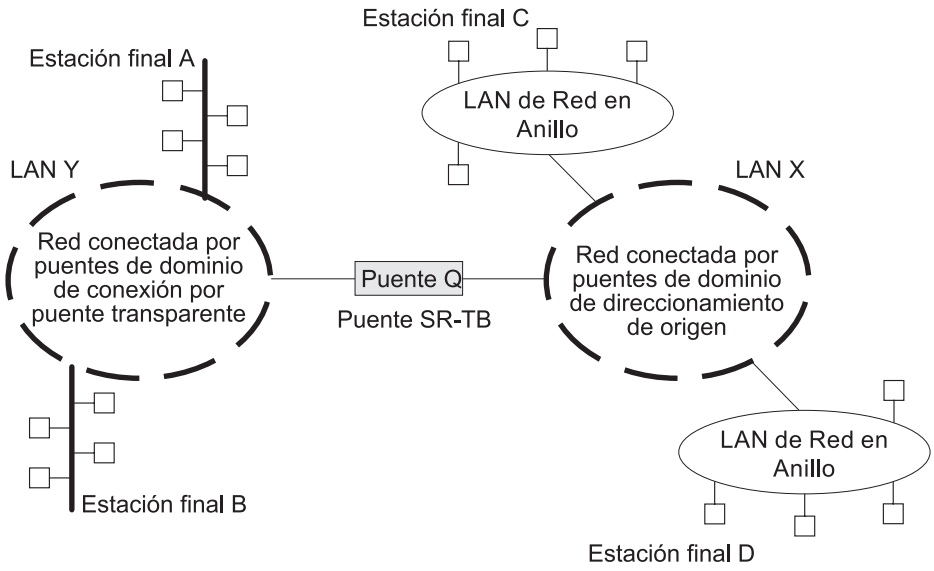



*Figura 17. Ejemplos de conexión por puente SR-TB*

## Ejemplo 1: Se envía una trama de la Estación final A a la Estación final B

Cuando el puente SR-TB recibe una trama con una dirección de origen de estación final A una dirección de destino de estación final B, entra la dirección de la estación final A en su tabla de direcciones del lado de conexión por puente transparente. Esta tabla contiene las direcciones de las estaciones que se sabe que están en el lado de conexión por puente transparente del puente, que es el proceso normal para la conexión por puente transparente.

Si la dirección de la estación final B está en la tabla de direcciones del lado de conexión por puente transparente, el puente SR-TB no reenvía la trama. Si la dirección de la estación final B no está en la tabla de direcciones del lado de conexión por puente transparente ni en la tabla de direcciones del lado de direccionamiento de origen, su ubicación es desconocida para el puente SR-TB. En este caso, la trama se reenvía al lado de direccionamiento de origen como una difusión general de una sola ruta sin solicitud de devolución del explorador de ruta. Cualquier trama que envíe la estación final B (independientemente de su destino) hace que su dirección se añada a la tabla de direcciones de conexión por puente transparente. Esto evita el futuro reenvío de tramas destinadas a la estación final B al lado de direccionamiento de origen.

## Ejemplo 2: Se envía una trama de la Estación final A a la Estación final C

En este ejemplo, la dirección de la estación final A se trata igual que en el ejemplo anterior. Puesto que la dirección de la estación final C seguro que no estará en la tabla de direcciones del puente transparente, el puente SR-TB reenviará la trama al lado de direccionamiento de origen.

Luego el puente busca la dirección final de la estación final C en su tabla de direcciones de direccionamiento de origen. Esta tabla contiene todas las direcciones conocidas con información de direccionamiento relacionada correspondientes a estaciones que se sabe que están en el lado de direccionamiento de origen del puente. Si la dirección de C se encuentra en la tabla de direccionamiento de

origen, el puente reenvía la trama utilizando la información de direccionamiento de la tabla de direcciones. Si la dirección de C no se encuentra en la tabla de direccionamiento de origen (o si aparece, pero contiene información de direccionamiento nula), el puente reenvía la trama al lado de direccionamiento de origen como una difusión general de una sola ruta sin solicitud de devolución del explorador de ruta.

Cuando la estación final C recibe esta trama, entra la dirección de la estación final A en su tabla de direccionamiento de origen, junto con la dirección invertida de la ruta creada a partir del puente SR-TB y la marca como una entrada temporal. Cuando posteriormente la estación final C intente enviar una trama a la estación final A, utilizará esta ruta específica, y, puesto que la ruta está marcada como temporal, la trama se enviará como una ruta no de difusión general *con* solicitud de devolución del explorador de ruta.

Cuando la trama de devolución llegue al puente SR-TB, se reenviará al lado del puente transparente sin información de ruta, pero hará que se entre la ruta a la estación final C en la tabla de direccionamiento de origen como una ruta temporal. Esto hará que la entidad de gestión de la red envíe una trama de explorador de ruta con un valor de difusión general de todas las rutas de nuevo a la estación final C. Esto permitirá a la estación C seleccionar el direccionamiento óptimo para las tramas destinadas a la estación final A y entrarlo como ruta permanente en la tabla de direccionamiento de origen del puente SR-TB.

### Ejemplo 3: Se envía una trama de la Estación final C a la Estación final D

Si la trama se envía como no de difusión general y cruza el segmento al que está conectado el puente SR-TB, el campo explora el campo RII en busca de la secuencia de direccionamiento (de LAN X a Puente Q a LAN Y). No encuentra la secuencia, por lo que no reenvía la trama.

Si la trama se envía como difusión general de una sola ruta, el puente eliminará la trama si se sabe que la estación final D está en el lado de direccionamiento de origen. Si no se sabe que la estación final D está en el lado de direccionamiento de origen, el puente reenvía la trama al lado de conexión por puente transparente (menos la información de direccionamiento), y añade “Q a Y” a la información de direccionamiento. Finalmente, guarda la información de direccionamiento correspondiente a la estación final C como una ruta temporal en la tabla de direccionamiento de origen con un indicador de no difusión general y el bit de dirección complementado.

Si la trama se envía como difusión general de todas las rutas, el puente SR-TB elimina la trama (porque la dirección de la estación final D no aparece en la tabla de direcciones de conexión por puente transparente) y se asegura de que la dirección de la estación final C se encuentra en la tabla de direccionamiento de origen.

### Ejemplo 4: Se envía una trama de la Estación final C a la Estación final A

Si la trama se envía como no de difusión general, el puente explora en campo RII en busca de la secuencia de direccionamiento (de X a Q a Y). Cuando la encuentra, reenvía la trama al lado de conexión por puente transparente. También guarda la información de direccionamiento correspondiente a la estación final C.

Si la trama se envía como una difusión general de una sola ruta, el puente reenvía la trama (menos la información de direccionamiento) al lado de conexión por puente transparente y añade “de Q a Y” a la información de direccionamiento. También define el indicador de no difusión general, complementa el bit de dirección y entra la información de direccionamiento correspondiente a la dirección de C en la tabla de direccionamiento de origen.

Si ya existe una entrada temporal correspondiente a la estación final C en la tabla de direccionamiento de origen, el puente SR-TB actualiza la información de direccionamiento. Si la trama se envía como una difusión general de todas las rutas, el puente elimina la trama pero se asegura de que la dirección de la estación final C se encuentra en la tabla de direccionamiento de origen.

## SR-TB y Frame Relay

La interfaz Frame Relay da soporte a la conexión por puente SR-TB reenviando todas las tramas conectadas por puente al distribuidor de conexión por puente adecuado, siempre y cuando la conexión por puente se haya activado en el circuito.

## SR-TB y ATM

La interfaz ATM da soporte a la conexión por puente SR-TB reenviando todas las tramas conectadas por puente al distribuidor de conexión por puente adecuado, siempre y cuando la conexión por puente se haya activado en el VCC.

## Terminología y conceptos sobre Direccionamiento de origen-Puente transparente (SR-TB)

Esta sección describe los términos y conceptos que se utilizan en la conexión por puente SR-TB.

### Difusión general a todas las rutas

El proceso de enviar una trama a través de cada ruta no repetitiva de la LAN conectada por puente.

### Difusión general a todas las estaciones

El proceso de enviar una trama (colocándolas todas en la dirección de destino) de modo que cada estación del anillo en la que aparece la trama copia dicha trama.

### Puente

Dispositivo, independiente del protocolo, que conecta redes de área local (LAN). Los puentes funcionan en la capa de enlace de datos, guardando y reenviando paquetes de datos entre las LAN.

### Número de puente

El número exclusivo que identifica un puente. Distingue entre varios puentes que conectan los mismos anillos.

### Tramas exploradoras

El puente de direccionamiento de origen añade información de direccionamiento a una trama exploradora a medida que reenvía la trama a través de la red a la estación final de destino. La trama exploradora descubre la ruta. Hay dos tipos de tramas exploradoras: tramas exploradoras de todas las rutas (ARE) y tramas exploradoras del árbol de expansión (STE). Todos los puertos reenvían tramas ARE,

mientras que únicamente los puertos asignados para ello por el protocolo de árbol de expansión reenvían tramas STE.

### Número de anillo
El número exclusivo que identifica un anillo en una red conectada por puente.

### Ruta
Una vía de acceso a través de una serie de LAN y puentes (por ejemplo, puentes de direccionamiento de origen).

### Designador de ruta
Un número de anillo y un número de puente del Campo de información de direccionamiento que sirven para crear una ruta a través de la red.

### Descubrimiento de ruta
El proceso de conocer una ruta a una estación final de destino.

### Número de segmento
Un número que identifica cada LAN, como una sola red en anillo o una línea serie. Un segmento se conecta al puente, pero también puede funcionar de forma independiente.

### Difusión general de una sola ruta
El proceso en enviar una trama a través de una red de modo que aparezca una sola copia de la trama en cada anillo de la red.

### Conexión por puente de direccionamiento de origen
Un mecanismo de conexión por puente que direcciona tramas a través de una red de varias LAN, especificando en la trama la ruta por la cual viajará.

### Árbol de expansión
Una topología de puentes en la que sólo hay una ruta de datos entre dos estaciones finales cualesquiera.

### Conexión por puente transparente
Un tipo de conexión por puente que incluye un mecanismo que resulta*transparente* para las aplicaciones de la estación final. La conexión por puente transparente interconecta segmentos de redes de área local mediante puentes designados para reenviar tramas de datos a través de un algoritmo de árbol de expansión.

## Compatibilidad entre el direccionamiento de origen-transparente - Problemas y soluciones

En primer lugar, el puente ASRT ofrece compatibilidad de puente transparente con los puentes de direccionamiento de origen ordinarios a través de la conversión de puente de direccionamiento de origen (SR-TB). SR-TB se propuso originalmente como parte de la especificación 802.5. Esta implantación es parecida a la del puente de conversión 8209 de IBM, y puede interoperar con esta.

SR-TB convierte tramas de conexión por puente transparente en tramas de direccionamiento de origen y viceversa. En otras palabras, en lugar de limitarse a comprobar si hay un RIF en un paquete y reenviarlo a un destino parecido, el campo ASRT puede convertir el paquete en cualquier formato; funciona como

puente transparente o como puente de direccionamiento de origen insertando o eliminando un RIF, según convenga. Con esta función, se pueden mover paquetes entre LAN Ethernet y de red en anillo SRT y siguen siendo compatibles con una base instalada de LAN de red en anillo de direccionamiento de origen.

## Eliminación de problemas de tamaño de paquetes

SR-TB elimina los problemas de tamaño de paquetes de las redes en anillo conectadas por puente a través de un dominio Ethernet. En esta configuración, las estaciones finales utilizan el protocolo de direccionamiento de origen, que les permite determinar de forma dinámica que hay una red con un tamaño de trama máximo de 1518 bytes entre ellas. La estación final final respeta automáticamente este límite sin reconfiguración manual. En la situación inversa, dos LAN Ethernet conectadas por puente a través de un dominio de red en anillo, el tamaño no representa un problema puesto que el tamaño máximo de paquete de red en anillo es mucho mayor.

## Filtro de direcciones de hardware

Otra característica clave que ofrece el puente ASRT es el filtro de direcciones de hardware. La función de filtro de direcciones de hardware soluciona el conflicto en métodos de acuse de recibo de paquetes que existe entre las tecnologías de LAN Ethernet y red en anillo. Se produce en la capa MAC y es la única técnica que define correctamente bits de acuse de recibo basados en la dirección MAC de destino. El puente ASRT utiliza memorias direccionables por contenido (CAM) para implantar la función de filtro de direcciones de hardware. Esta tecnología ofrece al puente un gran nivel efectivo de inteligencia, al ofrecerle capacidad de búsqueda instantánea de direcciones MAC sin que disminuya el rendimiento.

## Clasificación de bits en puentes STB y SRB

Puesto que constantemente se crean puentes para conectar LAN con distintos tipos de direcciones MAC, la clasificación de bits durante la transmisión de datos afecta a la interoperatividad de estas tecnologías.

Al administrar direcciones MAC, IEEE asigna direcciones conocidas como direcciones MAC exclusivas de 48 bits asignadas globalmente por IEEE. Estas direcciones reciben soporte de las LAN 802.3, 802.4 y 802.5. Debido a la falta de estándares en el momento en que se desarrolló este esquema de direcciones, se ha llegado a dos situaciones distintas:

- Las LAN 802.3 (Ethernet) y 802.4 transmiten direcciones de origen y de destino con el bit de grupo primero y campos de datos LLC con el bit menos significativo (LSB) primero.
- Las LAN 802.5 (red en anillo) transmiten direcciones de origen y de destino con el bit de grupo primero y campos de datos LLC con el bit más significativo (MSB) primero.

**Nota:** Para simplificar, a partir de ahora se denominará a las LAN y puentes 802.3 y 802.4 LAN y puentes LSB. 802.5 se les denominará LAN y puentes MSB.

la diferencia en el estándar de transmisión de bit significa que un puente de una LAN LSB a una MSB tiene que invertir el orden de los bits de las direcciones MAC de destino y de origen al principio de la trama MAC. Esto se debe a que distintos tipos de LAN utilizan el mismo orden de bits para direcciones MAC (es decir, el bit

de grupo primero) pero un orden de bits distinto para datos de usuario (LSB o MSB primero).

La interpretación incorrecta de direcciones debido al orden de bits inverso se agrava con el hecho de que algunos protocolos de comunicaciones de alto nivel interpretan incorrectamente las direcciones MAC. Algunos protocolos, como IP y Novell IPX, interpretan las direcciones de conexión por puente incorrectamente porque en el momento de su desarrollo inicial no había ninguna representación estándar de direcciones MAC.

La diferencia de orden de bits se resuelve combinando la tecnología de conexión por puente (tecnología de capa de enlace de datos) con la tecnología de direccionamiento (tecnología de capa de red). En lugar de solicitar al usuario que "invierta el diseño" de los protocolos de comunicaciones y configure cada puente para que "alterne" o invierta direcciones según cada caso, el problema se puede solucionar de forma más sencilla direccionando estos protocolos.

El direccionamiento elimina los problemas de orden de bits y direccionamiento de protocolos accediendo a las direcciones detalladas del paquete que se ejecuta en el nivel superior. El direccionamiento solo no constituye una solución completa, puesto que otros protocolos, como IBM Frames y NetBIOS, no se pueden direccionar, y el direccionamiento SNA está limitado. Por lo tanto, es importante implantar SRT en un dispositivo en el que la conexión por puente y el direccionamiento funcionen en combinación.

## Consideraciones sobre la configuración ASRT

El puente ASRT utiliza el protocolo de árbol de expansión y el algoritmo descrito en el estándar de puente 802.1D de IEEE sobre todas las interfaces. Es posible que más de un árbol de expansión formen un entorno en el que existan varios tipos de puentes. Por ejemplo, puede haber un árbol de expansión de todos los puentes que practiquen el protocolo IEEE 802.1d (por ejemplo STB y SRT) con con otro árbol de puentes IBM 8209. La formación de bucles derivada de esta configuración se debe corregir.

Servicios de sistema principal en TCP/IP da soporte a la retransmisión SDLC. Cuando funciona como puente puro, y no como direccionador IP, las funciones que suelen estar asociadas con el direccionador IP no están disponibles. Por ejemplo, no hay función de distribuidor BootP ni funciones de direccionamiento de subred ARP.

## Matriz de configuraciones ASRT

Con un puente ASRT, el grupo de parámetros de configuración correspondientes al puente y a todas las interfaces conectadas genera una *personalidad de puente* correspondiente a dicho puente. La siguiente matriz constituye una guía de los valores de configuración necesarios para cada tipo de interfaz para generar la personalidad de puente deseada para que maneje la red.

| Personalidad de puente | ¿ Conversión SR <-> TB activada? | Tipo de interfaz y valor de método de conexión por puente | | | |
|---|---|---|---|---|---|
| | | Red en anillo | Ethernet | Línea serie o túnel | ATM |
| STB | No | TB | TB | TB | TB |
| SRB | No | SR | -- | SR | SR |
| STB y SRB | No | SR | TB | TB o SR | TB o SR |
| SR-TB | Sí | SR | TB | TB | TB |
| SR-TB | Sí | SR | TB | SR | SR |
| SRT | No | SR y TB | TB | SR y TB | SR y TB |
| ASRT | Sí | SR y TB | TB | SR y TB | SR y TB |
| ASRT | Sí | SR | TB | SR y TB | SR y TB |
| ASRT | Sí | SR o TB | TB | SR y TB | SR y TB |

Clave de personalidad de puente:

STB = Puente transparente (árbol de expansión)
SRB = Puente de direccionamiento de origen
= Puente de conversión transparente de direccionamiento de origen
SRT = Puente transparente de direccionamiento de origen
ASRT = Puente transparente de direccionamiento de origen adaptable

Clave de método de conexión por puente:

SR = Direccionamiento de origen TB = Conexión por puente transparente

# Características de la conexión por puente

Este capítulo describe las características de conexión por puente disponibles en el puente transparente de direccionamiento de origen adaptable (ASRT). Este capítulo incluye las siguientes secciones:



## Túnel de conexión por puente

El túnel de conexión por puente (encapsulación) es otra característica del software del puente ASRT. Al encapsular paquetes en paquetes TCP/IP estándares de la industria, el dispositivo de conexión por puente puede direccionar de forma dinámica estos paquetes a través de grandes interredes IP a las estaciones finales de destino.

Las estaciones finales ven la vía de acceso IP (el túnel) como un solo salto, independientemente de la complejidad de la red. Esto ayuda a solucionar el límite habitual de distancia de 7 saltos de las configuraciones de direccionamiento de origen. También le permite conectar estaciones finales de direccionamiento de origen a través de un soporte de direccionamiento que no es de origen, como las redes Ethernet.

El túnel de conexión por puente también ayuda a evitar problemas derivados de limitaciones normales de direccionamiento de origen, como las siguientes:

- Limitaciones de distancia de siete saltos
- Gran cantidad de actividad general que causa el direccionamiento de origen en redes de área amplia (WAN)
- El gran impacto que causa en el direccionamiento de origen los errores de la WAN (por ejemplo, si falla una vía de acceso todos los sistemas deben reiniciar sus transmisiones)

Con la característica de túnel de conexión por puente activada, el software encapsula los paquetes en paquetes TCP/IP. Para el dispositivo, el paquete tiene el aspecto de un paquete TCP/IP. Una vez se ha encapsulado una trama en un sobre IP, el distribuidor IP es el responsable de seleccionar la interfaz de red adecuada según la dirección IP de destino. Este paquete se puede direccionar de forma dinámica a través de grandes interredes sin que se degrade y sin restricciones de tamaño de red. Las estaciones finales ven esta vía de acceso o túnel como un solo salto, independientemente de la complejidad de la interred. La

Figura 18 en la página 48 muestra un ejemplo de una interred IP que utiliza la característica de túnel en su configuración.

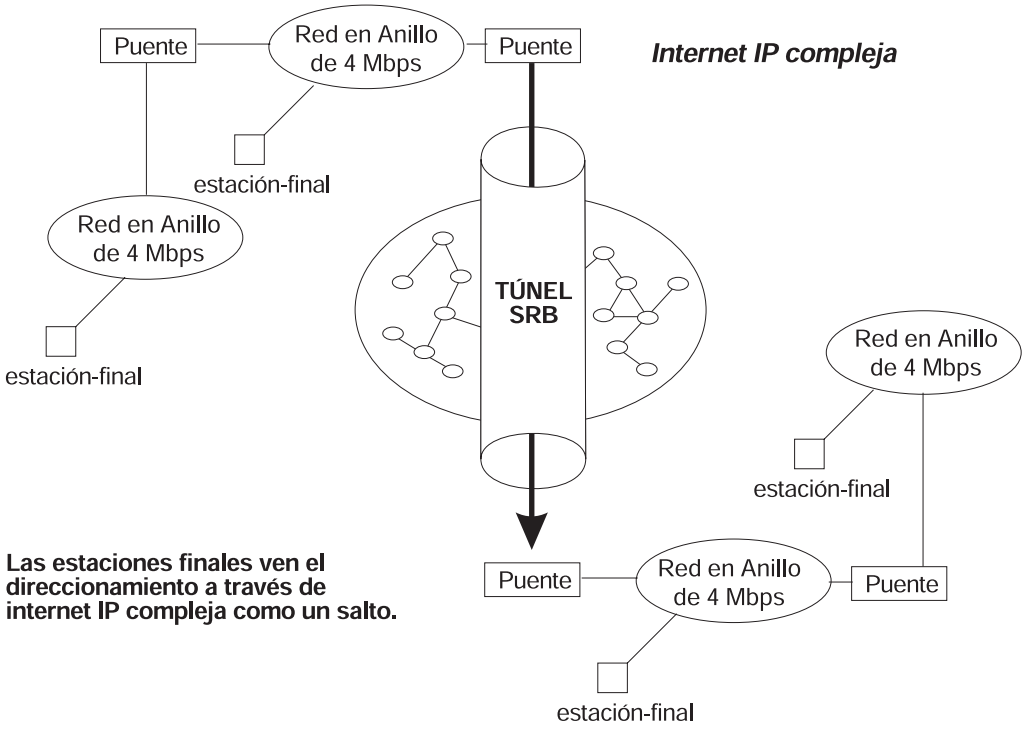



*Figura 18. Ejemplo de la característica de túnel de puente*

El túnel resulta transparente para las estaciones finales. Los dispositivos de la conexión por puente que participan en la conexión por túnel tratan la interred IP como uno de los segmentos del puente. Cuando el paquete alcanza la interfaz de destino, las cabeceras TCP/IP se eliminan de forma automática y el paquete interno continúa como un paquete de direccionamiento de origen estándar.

## Encapsulamiento y OSPF

Una de las principales ventajas de la característica de encapsulamiento es la adición del protocolo de direccionamiento dinámico OSPF al proceso de direccionamiento. OSPF ofrece las siguientes ventajas si se utiliza junto con encapsulamiento:

- *Direccionamiento de menor coste*. OSPF accede a la vía de acceso (túnel) más rápida con el menor número de retrasos, lo que permite a los administradores de la red distribuir el tráfico sobre la ruta menos costosa.
- *Direccionamiento dinámico*. OSPF busca la vía de acceso de menor coste y detecta anomalías y redirecciona el tráfico con una actividad general baja.
- *Dirccionamiento de varias vías de acceso*. La compartición de cargas utiliza de forma eficiente el ancho de banda disponible.

Con OSPF, los túneles gestionar, de forma automática, vías de acceso dentro de la interred. Si una línea o puente de la vía de acceso falla, el puente de túnel redirecciona automáticamente el tráfico por una nueva vía de acceso. Si se restaura una vía de acceso, el túnel actualiza automáticamente el direccionamiento por la mejor vía de acceso. Este redireccionamiento resulta completamente transparente para las estaciones finales. Para obtener más información sobre OSPF,

consulte los capítulos sobre configuración y supervisión que comienzan en el tema “Utilización de OSPF” en la página 359.

## Servicios de sistema principal en TCP/IP (gestión sólo de puentes)

El IBM 2210 también da soporte a Servicios de sistema principal en TCP/IP, que le permiten configurar y supervisar un puente cuando las funciones de direccionamiento están desactivadas. Esta opción le ofrece las siguientes funciones:

- Gestión a través de SNMP
- Función de servidor Telnet
- Posibilidad de bajar y subir configuraciones a través del protocolo TFTP
- Función TFTP Neighbor Boot
- Herramientas de diagnóstico de IP de ruta ping y de rastreo
- Control del dispositivo a través de valores SNMP y del cliente telnet

Si se mira desde la interfaz de supervisión del puente, Servicios de sistema principal en TCP/IP se maneja como un nuevo protocolo que tiene sus propios indicadores de configuración y supervisión. Se puede acceder a estos indicadores mediante el mandato **protocol** en `talk 6` y `talk 5`.

La función de gestión sólo de puentes se activa asignando una dirección IP al puente y activando Servicios de sistema principal en TCP/IP (consulte el tema “Configuración y supervisión de Servicios de sistema principal en TCP/IP” en la página 225). Esta dirección IP está asociada al puente como una unidad, en lugar de estar asociada a una sola interfaz. Cuando se arranca la red, se pueden conocer de forma automática la dirección IP del puente y una pasarela por omisión a través de la interfaz ROMCOMM con los PROM de arranque. El usuario puede configurar las asignaciones de pasarela por omisión.

Servicios de sistema principal en TCP/IP está disponible siempre que la conexión por puente sea una opción de la carga de software de dispositivos.

## Soporte Puente-MIB

Para la gestión de puentes mediante SNMP, IBM Nways Multiprotocol Routing Services da soporte a las bases de información de gestión (MIB) tal como se especifica en RFC 1493 y RFC 1525, ***excepto*** a las siguientes MIB:

- dot1dStaticTable
- dot1dTpFdbTable
- dot1dPortPairTable

## Colocación en antememoria de nombres de NetBIOS

La característica de colocación en antememoria de nombres de NetBIOS permite al dispositivo de conexión por puente reducir significativamente el número de tramas Name-Query que abandonan un anillo de origen y se reenvían a través de un puente. La configuración de la característica de colocación en antememoria de nombres de NetBIOS forma parte de la configuración de NetBIOS. Encontrará más información en el tema “Colocación en antememoria de nombres NetBIOS y colocación en antememoria de rutas” en la página 164.

## Función de filtro de tramas duplicadas NetBIOS

Tres tipos de tramas se suelen enviar en grupos de seis:

- Name-Query
- Add-Name
- Add-Group-Name

La función de filtro de tramas duplicadas utiliza un temporizador para permitir que se reenvíe una sola instancia de cada tipo de trama a través del puente durante el intervalo de tiempo definido por el usuario.

Este proceso utiliza una base de datos distinta a la utilizada en la función de colocación en antememoria de nombres. Las entradas de la base de datos de tramas duplicadas contienen la dirección MAC del cliente y tres indicaciones horarias, una para cada uno de los tipos de tramas mencionados. La función de filtro de tramas duplicadas se procesa antes que la colocación en antememoria de nombres. Encontrará más información en el tema “Función de filtro de tramas duplicadas” en la página 157.

## Filtros de bytes y nombres de NetBIOS

La función de filtro de NetBIOS es una característica que le permite mejorar el rendimiento de la conexión por puente ASRT. Esta característica le permite configurar filtros específicos mediante el proceso de configuración de dispositivos. Los filtros de NetBIOS son grupos de reglas que se aplican a los paquetes NetBIOS para determinar si los paquetes se deben conectar por puente (reenviar) o se deben filtrar (eliminar).

## Tipos de funciones de filtro de NetBIOS

Hay dos tipos de funciones de filtro de NetBIOS, *nombre de sistema principal* y *byte*:

**nombre de sistema principal**
Puede implantar una función de filtro de nombre de sistema principal mediante los campos de los paquetes NetBIOS que le permiten seleccionar paquetes con determinados nombres de sistema principal de NetBIOS para conectarlos por puente o filtrarlos. Los filtros de nombre de sistema principal sólo son para la conexión por puente. Puede utilizarlos en función de los nombres de origen o de destino de NetBIOS, dependiendo del tipo de trama.

Los filtros de nombre se aplican al tráfico de NetBIOS que se conecta por puente o se conmuta por enlace de datos.

**Byte** Puede implantar una función de filtro por byte mediante los bytes (campos arbitrarios) de los paquetes NetBIOS que le permiten especificar determinados paquetes NetBIOS para conectarlos por puente o filtrarlos.

No hay umbrales ni temporizadores asociados a estos filtros y permanecen activos hasta que los desactiva o los elimina. Un filtro de NetBIOS está formado por tres partes: el filtro real, listas de filtro y elementos de filtro (que se describen con más detalle en el tema “Creación de un filtro” en la página 52).

La configuración y supervisión de NetBIOS se describe en el tema “Configuración y supervisión de NetBIOS” en la página 175. El resto de esta sección describe la función de filtro de nombre de sistema principal de NetBIOS y la función de filtro de byte de NetBIOS.

## Función de filtro de nombre de sistema principal de NetBIOS

La función de filtro de NetBIOS mediante nombres de sistema principal le permite seleccionar paquetes con determinados nombres de sistema principal de NetBIOS para conectarlos por puente o filtrarlos. Cuando especifica que los paquetes con un determinado nombre de sistema principal de NetBIOS (o grupo de nombres de sistema principal de NetBIOS) se deben conectar por puente o filtrar, se examinan los campos de nombre de origen y nombre de destino de los siguientes tipos de paquetes NetBIOS:

- ADD_GROUP_NAME_QUERY (origen)
- ADD_NAME_QUERY (origen)
- DATAGRAM (destino)
- NAME_QUERY (destino)

Las listas de filtro de nombre de sistema principal especifican los nombres de NetBIOS que se deben comparar con los campos de nombre de origen y de destino de los cuatro tipos de paquetes NetBIOS. El resultado de aplicar una lista de filtro de nombre de sistema principal a un paquete NetBIOS que no es de uno de estos cuatro tipos es *Inclusive*.

Al configurar la función de filtro de NetBIOS mediante nombres de sistema principal, debe especificar a qué puertos se aplica el filtro y si se aplica a los paquetes de entrada o de salida de dichos puertos. Sólo los paquetes de Información no numerada (UI) de NetBIOS se tienen en cuenta para la función de filtro. La función de filtro se aplica a los paquetes NetBIOS que llegan al dispositivo para su conexión por puente de direccionamiento de origen (todos los tipos de RIF) o para su conexión por puente transparente.

Cuando especifique un nombre de sistema principal de NetBIOS en un filtro, puede indicar el carácter número 16 (último) del nombre, como un argumento separado, y su formato hexadecimal. Si lo hace, los 15 primeros bytes del nombre se toman tal como se hayan especificado y el byte número 16 (si se especifica) lo determina el argumento final. Si especifica menos de 16 caracteres (no hay byte número 16), el nombre se rellena con caracteres ASCII en blanco hasta el carácter número 15 y el carácter número 16 se trata como un comodín.

Cuando se evalúa un determinado nombre de sistema principal de NetBIOS, se compara dicho nombre con determinados campos de determinados paquetes NetBIOS. Los nombres de sistema principal de NetBIOS de los elementos de filtro pueden incluir un comodín (?) en cualquier posición del nombre de sistema principal de NetBIOS o bien un asterisco (*) como carácter final de un nombre de sistema principal de NetBIOS. El símbolo ? coincide con cualquier carácter (un solo carácter) de un nombre de sistema principal. El * coincide con uno o más caracteres al final de un nombre de sistema principal.

### Función de filtro de byte de NetBIOS

Otro mecanismo de filtro, la función de filtro de byte, le permite especificar qué paquetes NetBIOS se deben conectar por puente o filtrar en función de los campos de los paquetes NetBIOS que están relacionados con la dirección MAC. En este caso, se examinan todos los paquetes NetBIOS para determinar si coinciden con los criterios de filtro configurados.

Para crear un filtro de byte, debe especificar los siguientes elementos de filtro:

- Un desplazamiento a partir del principio de la cabecera NetBIOS
- Un patrón de bytes con el que deben coincidir
- Una máscara opcional a aplicar a los campos seleccionados de la cabecera NetBIOS

La longitud de la máscara, si la hay, debe ser de igual longitud que el patrón de bytes. La máscara especifica los bytes que se deben añadir (AND) de forma lógica a los bytes de la cabecera NetBIOS antes de que el dispositivo compare los bytes de cabecera con el patrón hexadecimal para ver si son iguales. Si no se especifica ninguna máscara, se da por supuesto que son todos. La longitud máxima del patrón hexadecimal (y, por lo tanto, de la máscara) es de 16 bytes (32 dígitos hexadecimales).

Al configurar la función de filtro de NetBIOS mediante determinados bytes, también debe especificar a qué puertos se aplica el filtro y si se aplica a los paquetes de entrada o de salida de dichos puertos.

## Creación de un filtro

Cada filtro consta de una o más listas de filtro. Cada lista de filtro consta de uno o más elementos de filtro. Cada elemento de filtro se compara con un paquete en el orden en el que se ha especificado el elemento de filtro.

Cuando se encuentra una coincidencia entre un elemento de filtro y un paquete, el dispositivo:

- Conecta por puente el paquete si la lista de filtro se ha especificado como *Inclusive*
- Elimina el paquete si la lista de filtro se ha especificado como *Exclusive*

Si no se encuentra ninguna coincidencia de elementos de filtro de la lista de filtro, el dispositivo:

- Reenvía el paquete si el filtro, como unidad, si se ha especificado como *Inclusive*
- Elimina el paquete si el filtro, como unidad, si se ha especificado como *Exclusive*

Un elemento de filtro es una sola regla que se aplica a un determinado campo de un paquete NetBIOS. El resultado de la aplicación de la regla es una indicación Inclusive (conectar por puente) o Exclusive (filtrar). Los siguientes elementos de filtro se pueden configurar con función de filtro de NetBIOS (los dos primeros elementos son filtros de nombre de sistema principal, los dos últimos elementos son filtros de byte):

- Incluir el carácter opcional número 16 del nombre de sistema principal de NetBIOS (hex)

- Excluir el carácter opcional número 16 del nombre de sistema principal de NetBIOS (hex)
- Incluir el desplazamiento de byte decimal en el patrón hexadecimal de la cabecera NetBIOS comenzando en dicha máscara hexadecimal de desplazamiento
- Excluir el desplazamiento de byte decimal en el patrón hexadecimal de la cabecera NetBIOS comenzando en dicha máscara hexadecimal de desplazamiento

Parte de la especificación de un filtro indica si los paquetes que no coinciden con ningún elemento de filtro de la lista de filtro se deben conectar por puente (incluir) o filtrar (excluir). Esta es la acción por omisión para la lista de filtro. La acción por omisión para una lista de filtro se define inicialmente en Include, pero el usuario puede modificar este valor.

## Filtros sencillos y complejos

Un filtro sencillo se crea combinando una lista de filtro con un número de puerto de dispositivo y una designación de entrada/salida. Esto indica que la lista de filtro se debe aplicar a todos los paquetes NetBIOS que se reciben o transmiten en un determinado puerto. Si la lista de filtro evalúa que se debe incluir, el paquete que se gestiona se conecta por puente. Si no es así, el paquete se filtra.

Un filtro complejo se puede crear especificando un número de puerto, una designación de entrada/salida y varias listas de filtro separadas por uno de los operadores lógicos AND u OR. Las listas de filtro de un filtro complejo se evalúan estrictamente de izquierda a derecha, y se evalúa cada lista de filtro del filtro complejo. Cada resultado "incluir" de la lista de filtro se trata como verdadero y cada resultado "excluir" de la lista de filtro se trata como falso. El resultado de aplicar todas las listas de filtro y sus operadores a un paquetes es verdadero o falso, que indican respectivamente que el paquete se debe conectar por puente o filtrar. Cada combinación de entrada/puerto o salida/puerto puede tener un filtro como máximo.

---

## Opciones de protocolo de varios árboles de expansión

El puente ASRT le permiten ampliar las opciones del protocolo de árbol de expansión para cubrir tantas opciones de configuración como sea posible. Las siguientes secciones contienen información sobre estas características:

## Fondo: Problemas con protocolos de varios árboles de expansión

La tecnología de conexión por puente emplea distintas versiones de algoritmos de árbol de expansión para dar soporte a distintos métodos de conexión por puente. El objetivo común de cada algoritmo consiste en generar una topología libre de bucles.

En el algoritmo de árbol de expansión que utilizan los puentes transparentes (TB), las BPDU tipo Hello y la BPDU de Notificación de cambio de topología (TCN) se envían en una trama transparente a las direcciones conocidas de todos los soportes participantes (red en anillo, Ethernet, etc.). A partir de esta información intercambiada se crean tablas y se calcula una topología libre de bucles.

Los puentes de direccionamiento de origen (SRB) transmiten tramas exploradoras del árbol de expansión (STE) a través de otros SRB para determinar una topología libre de bucles. El algoritmo envía BPDU tipo Hello en una trama transparente a las direcciones funcionales conocidas. Puesto que los SRB no utilizan BDPU TCN,

el valor de estado de puerto creado como resultado de este algoritmo de árbol de expansión no afecta a la trama exploradora de todas las rutas (ARE) ni al tráfico de trama direccionada específicamente (SRF).

En configuraciones de conexión por puente que utilizan puentes IBM 8209, se utiliza otro método de árbol de expansión para detectar los puentes IBM 8209 paralelos. Este algoritmo utiliza BPDU tipo Hello enviadas como tramas STE a direcciones del grupo IEEE 802.1d de la red en anillo. En Ethernet, se utilizan BPDU tipo Hello enviadas como tramas transparentes a la misma dirección de grupo. Este método permite a los 8209 crear árboles de expansión con puentes transparentes y otros puentes IBM 8209. Sin embargo, no participa en el protocolo de árbol de expansión SRB y las BPDU tipo Hello que envían los SRB se filtran. Por lo tanto, no hay modo de evitar que el 8209 se convierta en el puente raíz. Si el puente 8209 *se* selecciona como el raíz, puede que el tráfico entre dos dominios de puente transparente tenga que pasar a través de dominios de red en anillo/SRB.

Como puede observar, la ejecución de protocolos de varios árboles de expansión puede ocasionar problemas de compatibilidad con el modo en que el algoritmo crea su propia topología libre de bucles.

## STP/8209

La característica de conexión por puente STP/8209 le permite ampliar el protocolo de árbol de expansión. Anteriormente, los SRB sólo permitían la configuración manual de un árbol libre de bucles sobre la red en anillo. Este era el único mecanismo disponible para evitar bucles en el caso de puentes SR-TB paralelos. Con la adición de la característica STP/8209, son posibles las siguientes combinaciones de algoritmos de árbol de expansión:

- Puente transparente puro (TB) - se utiliza el protocolo de árbol de expansión IEEE 802.1d.
- Puente de direccionamiento de origen puro (SRB) - se utiliza el protocolo de árbol de expansión SRB.
- Puentes transparente y de direccionamiento de origen como entidades separadas - se utiliza el protocolo de árbol de expansión IEEE 802.1d para TB y configuración manual (sin protocolo de árbol de expansión para SRB.
- Puente SR-TB - se utiliza el protocolo de árbol de expansión IEEE 802.1d para puertos TB y BPDU IBM 8209 y puertos SRB para formar un solo árbol de TB y SR-TB. Las BPDU tipo Hello de SRB pueden pasar al dominio SR, pero no se procesan. Los puentes IBM 8209 filtran dichas tramas, lo cual se permite porque es un puente de dos puertos y el otro puerto es un puerto TB.
- Puente SRT puro - ***Sólo*** se utiliza el protocolo de árbol de expansión IEEE 802.1d. Las BPDU tipo Hello de SRB y las BPDU IBM 8209 BPDUs pueden pasar, pero no se procesan.
- Puente ASRT - se utiliza el protocolo de árbol de expansión IEEE 802.1d para formar un árbol con TB y puentes SRT. También se generan BPDU “tipo 8209” en todas las interfaces SR. Estas BPDU se procesan en cuanto se reciben. Esto hace que se generen y reciban dos BPDU en todas las interfaces SR. Puesto que las dos BPDU llevan la misma información, no habrá conflicto de información de puerto. Esto permite al puente ASRT crear un árbol de expansión con puentes IBM 8209 y SR-TB junto con otros TB y puentes SRT.

## Creación de hebras (descubrimiento de ruta)

La creación de hebras es un proceso utilizado por un protocolo de estación final de red en anillo (por ejemplo, IP, IPX o AppleTalk) para descubrir una ruta a otra estación final a través de una red conectada por puente de direccionamiento de origen.

Los detalles del proceso de creación de hebras varía según el protocolo de la estación final. Las siguientes secciones describen el proceso de creación de hebras para IP, IPX y AppleTalk.

## Creación de hebras IP con ARP

Las estaciones finales IP utilizan paquetes ARP REQUEST y REPLY para descubrir un RIF. Ambas estaciones finales IP y los puentes participan en el descubrimiento de ruta y en el proceso de reenvío. Los pasos siguientes describen el proceso de creación de hebras IP.

1. Una estación final IP mantiene una tabla ARP y una tabla RIF. La dirección MAC de la tabla ARP sirve como referencia cruzada para el RIF de destino de la tabla RIF. Si no existe ningún RIF para una determinada dirección MAC, la estación final transmite un paquete ARP REQUEST con un ARE (explorador de todas las rutas) o un STE (explorador del árbol de expansión) al segmento local.
2. Todos los puentes del segmento local capturan el paquete ARP REQUEST y lo envían sobre sus redes conectadas.

   A medida que el paquete ARP REQUEST continúa su búsqueda de la estación final de destino, cada puente que lo reenvía añade su propio número de puente y número de segmento al RIF del paquete. A medida que la trama sigue pasando por la red conectada por puente, el RIF acumula una lista de pares de número de puente y de segmento que describen la vía de acceso al destino.

   Cuando finalmente el paquete ARP REQUEST alcanza su destino, contiene la secuencia exacta de números de puente y de segmento desde el origen hasta el destino.
3. Cuando la estación final de destino recibe la trama, coloca la dirección MAC y su RIF en sus propias tablas ARP y RIF. Si la estación final de destino tiene que recibir algún otro paquete ARP REQUEST procedente del mismo origen, dicho paquete se elimina.
4. Luego la estación final de destino genera un paquete ARP REPLY que incluye el RIF y lo envía de nuevo a la estación final de origen.
5. La estación final de origen recibe la vía de acceso de ruta aprendida. La dirección MAC y su RIF se entran en las tablas ARP y RIF. El RIF se conecta al paquete de datos y se reenvía a su destino.
6. La antigüedad de las entradas RIF se gestiona mediante un temporizador de renovación ARP de IP.

## Creación de hebras IPX

Las estaciones finales IPX comprueban en cada paquete que reciben la existencia de un RIF. Si el RIF no existe en la tabla, añaden el RIF a la tabla y designan dicha ruta como *HAVE_ROUTE*. Si el RIF indica que el paquete procede de una estación final del anillo local, la ruta se designa como *ON_RING*.

Si la estación final tiene que enviar un paquete y no hay ninguna entrada en la tabla RIF correspondiente a la dirección MAC, la estación final transmite los datos como un STE.

Cuando caduca el temporizador del RIF, la entrada de la tabla se borra y no se vuelve a entrar hasta que llega otro paquete que contiene un RIF correspondiente a dicha entrada.

## Creación de hebras AppleTalk 2

Las estaciones finales AppleTalk utilizan paquetes ARP y XID para descubrir una ruta. Tanto las estacione finales AppleTalk como los puentes participan en el proceso de descubrimiento y reenvío. Los pasos siguientes describen el proceso de creación de hebras AppleTalk.

1. Si no existe ningún RIF para una determinada dirección MAC, la estación final transmite un paquete ARP REQUEST con un ARE (explorador de todas las rutas) al segmento local.
2. Todos los puentes del segmento local capturan el paquete ARP REQUEST y lo envían sobre sus redes conectadas. A medida que el paquete ARP REQUEST continúa su búsqueda de la estación final de destino, cada puente que lo reenvía añade su propio número de puente y número de segmento al RIF del paquete. A medida que la trama sigue pasando por la red conectada por puente, el RIF acumula una lista de pares de número de puente y de segmento que describen la vía de acceso al destino.
3. Cuando la estación final de destino recibe la trama, coloca la dirección MAC y su RIF en sus propias tablas ARP y RIF y el estado de la entrada se designa como *HAVE_ROUTE*. Si la estación final de destino tiene que recibir algún otro paquete ARP REQUEST procedente del mismo origen, dicho paquete se elimina.
4. Luego, la estación final de destino genera un paquete ARP REPLY y lo envía de nuevo a la estación final de origen con el bit de dirección del RIF modificado.
5. La estación final de origen recibe la vía de acceso de ruta aprendida. A continuación, la dirección MAC y su RIF se entran en las tablas ARP y RIF y el estado se designa como *HAVE_ROUTE*. Si el RIF indica que el paquete procede de una estación final del anillo local, la ruta se designa como *ON_RING*.
6. Si el temporizador del RIF caduca, se envía un XID con un ARE y el estado pasa a ser *DISCOVERING*. Si no se recibe ninguna respuesta XID, la entrada se elimina.

## Característica de dirección MAC duplicada de SR-TB

La característica de dirección MAC duplicada (DMAC) le permite conectar un puente SR-TB a una red conectada por puente SR que tiene configuradas direcciones MAC duplicadas. La característica de dirección MAC duplicada se puede activar con dos opciones:

- **Característica de MAC duplicada sin equilibrio de carga**

  Esta opción le permite duplicar direcciones MAC sin equilibrio de carga. En este caso, sólo se aprende un RIF correspondiente a la dirección MAC duplicada y el cálculo de la antigüedad se realiza en este RIF aprendido. Todas las estaciones del dominio TB utilizan este RIF para comunicarse con esta dirección MAC. Cuando la entrada correspondiente a este RIF caduca, la siguiente trama se envía desde el dominio TB como una trama exploradora del árbol de expansión (STE).

- **Característica de MAC duplicada con equilibrio de carga**

  Esta opción le permite duplicar direcciones MAC con equilibrio de carga y sólo se puede activar después de activar DMAC sin equilibrio de carga. En este caso, se aprenden y se mantienen dos RIF para cada dirección MAC duplicada. Cada uno de los dos RIF tiene su propio temporizador de antigüedad. Cuando el puente recibe una trama con un determinado RIF, el valor de antigüedad correspondiente a dicho RIF se renueva. La primera vez que una estación del dominio TB envía una trama a una dirección MAC duplicada, el software del puente decide qué RIF se utilizará para enviar dicha trama. Las siguientes tramas procedentes de la estación emisora se enviarán utilizando el mismo RIF. El puente mantendrá un RIF principal y uno secundario para un máximo de siete direcciones MAC duplicadas. Si especifica valores de antigüedad separados para las direcciones MAC duplicadas, se utilizará el valor adecuado para calcular la antigüedad de las entradas correspondientes a dicha dirección MAC duplicada, lo que le permite ajustar el valor de antigüedad correspondiente a las direcciones MAC duplicadas.

## Conexión por puente en ATM

El dispositivo da soporte a la conexión por puente sobre ATM nativo (RFC 1483). Cuando se establece una conexión por puente sobre ATM nativo, se pueden configurar varios puertos (virtuales) para una sola interfaz (física).

## Soporte RFC 1483 para la conexión por puente

RFC 1483 especifica el valor de LLC 0xAA-AA-03 y el valor de OUI 0x00-80-C2 para los protocolos conectados por puente. La parte del PID de 2 octetos de la cabecera SNAP, en el caso de protocolos conectados por puente, especifica el soporte conectado por puente y, adicionalmente, si la secuencia de comprobación de trama (FCS) original se mantiene dentro de la PDU conectada por puente original. Se especifican los valores PID correspondientes a distintos soportes. Consulte RFC 1483 para obtener más información.

La interfaz ATM reenviará las tramas MAC conectadas por puente procedentes de Red en anillo/802.5, Ethernet/802.3. Se utiliza un puerto de puente por VCC. Al configurar un puerto de puente en una interfaz ATM, debe especificar un VCC que esté permanentemente enlazado a dicho puerto. Las tramas conectadas por puente que ser reciben en un VCC/puerto se envían a uno o más VCC/puertos

según el protocolo de conexión por puente utilizado y la configuración de la conexión por puente. Una vez se ha configurado un puerto de puente en una interfaz ATM y tiene un VCC asociado, funciona como una puerta normal de conexión por puente de una LAN antigua. La asociación del puerto con la interfaz ATM resulta transparente para el usuario y para la función de conexión por puente.

Al configurar un puerto de puente en una interfaz ATM, el usuario debe especificar si se debe utilizar soporte PVC o SVC. Para el soporte PVC, debe suministrar el VPI y el VCI para el PVC. Para el soporte SVC, debe suministrar la dirección ATM remota, así como el selector a utilizar para la dirección local.

**Nota:** A diferencia del soporte PVC, la utilización de SVC no requiere ninguna configuración de los conmutadores intermedios.

Una vez se ha añadido un puerto a una interfaz ATM, los mandatos de configuración de conexión por puente que necesitan un número de puerto como parámetro se pueden utilizar con este número de puerto.

Consulte los temas “Utilización de ARP” en la página 627 y “Configuración y supervisión de la conexión por puente” en la página 79 para obtener información adicional sobre cómo configurar una conexión por puente sobre ATM.

## Visión general de los puertos de puente multiacceso

Un puerto de puente multiacceso es un puerto de puente que incluye todos los circuitos virtuales Frame Relay que no están configurados de forma individual como puertos de puente.El puerto de puente multiacceso tiene asignado un número de segmento de puente exclusivo, que sirve para la conexión por puente de direccionamiento de origen.

Un puerto de puente multiacceso tiene las siguientes características de conexión por puente:

- Sólo da soporte a la conexión por puente de direccionamiento de origen (SR).
- Las configuraciones de malla completa dan soporte a la conectividad "de cualquiera a cualquiera" y pueden utilizar el protocolo de árbol de expansión para evitar bucles de conexión por puente.
- Las configuraciones que no sean de malla completa sólo dan soporte a la conectividad subordinado-a/de-centro de datos, porque no se da soporte a la conexión por puente entre circuitos virtuales del mismo segmento multiacceso. Esta configuración no puede utilizar el protocolo de árbol de expansión, de modo que se debe activar el reenvío de tramas STE. Por omisión, el protocolo de árbol de expansión está desactivado y el reenvío de tramas STE está activado.

  **Nota:** Esta es la configuración más recomendable, puesto que el protocolo de árbol de expansión puede consumir un ancho de banda de la WAN considerable y la mayoría de las configuraciones no son de malla completa.
- Se necesita el segmento virtual de puente 1-a-N.
- Ofrece conectividad independiente del protocolo entre estaciones finales parecidas y conectividad limitada entre estaciones finales de distintos soporte.

- Puede ofrecer captadores de datos eficientes para varios dispositivos IBM 2218. (Consulte el tema “Interoperatividad con dispositivos IBM 2218” en la página 59.)

## La base de datos multiacceso

Cada puerto de puente multiacceso mantiene una base de datos multiacceso que correlaciona el número de segmento del siguiente salto con el circuito virtual Frame Relay en el que se ha recibido la trama. Las entradas de la base de datos se crean o actualizan a medida que el segmento recibe tramas ARE, STE o direccionadas específicamente procedentes de los circuitos. Las tramas STE y ARE que se tienen que reenviar al segmento multiacceso inundan todos los circuitos virtuales del segmento multiacceso. Las tramas direccionadas específicamente que se tienen que reenviar al segmento multiacceso sólo se reenvían si hay una entrada de la base de datos multiacceso que coincide con el número de segmento del siguiente salto a un circuito virtual.

El software “hace caducar” las entradas de la base multiacceso a la velocidad especificada en el mandato **multiaccess-age**.

## Configuración de puertos de puente multiacceso

El siguiente ejemplo ilustra el modo de configurar bases de puente multiacceso en las interfaces 1 y 4 de Frame Relay. El puerto 5 es el siguiente puerto de puente disponible y esta es la primera vez que se activa el direccionamiento de origen.

```
* talk 6
Config> prot asrt
ASRT Config> add multiaccess-port
ASRT Config> Interface number [0]? 1
ASRT Config> Port Number [5]?
ASRT Config> Segment Number for the port in hex (1 - FFF) [001]? 300
ASRT Config> Bridge Number in hex (0 - 9, A - F) [0]? 2
ASRT Config> Bridge Virtual Segment Number (1 - FFF) [001]? CCD
ASRT Config> add multiaccess-port
ASRT Config> Interface number [0]? 4
ASRT Config> Port Number [6]?
ASRT Config> Segment Number for the port in hex (1 - FFF) [001]? 400
```

**Nota:** No se le solicitará el número de puente ni el número de segmento virtual después de configurar el primer puerto de puente multiacceso.

## Interoperatividad con dispositivos IBM 2218

Si utiliza puertos multiacceso con dispositivos 2210/2212/2216 como captadores de datos, obtendrá una topología de alta densidad y alto nivel de disponibilidad para los 2218 de la red.

- La alta densidad se debe a que varios dispositivos 2218 se pueden conectar a un puente centro de datos a través de un solo puerto de puente multiacceso.
- El alto nivel de disponibilidad se debe a la configuración de un solo 2218 para establecer conexión con los puentes principal y de reserva a través de sus puertos de puente multiacceso. El 2218 puede conmutar entre los circuitos principal y de reserva en cuanto el 2218 detecta problemas en la red Frame Relay.

Para que el 2218 conmute entre los puentes principal y central sin perder las conexiones LLC entre él mismo y el puente central, debe:

- Configurar los puentes de centro de datos principal y de reserva con el mismo número de segmento virtual 1-a-N de puente.
- Configurar los puentes de centro de datos principal y de reserva con el mismo número de puente de direccionamiento de origen.
- Configurar los puentes de centro de datos principal y de reserva con el mismo número de segmento multiacceso.

**Nota:** Esta configuración sólo da soporte a la conectividad de subordinado a centro de datos.

La Figura 19 en la página 61 muestra una conexión de red típica entre dispositivos 2210 y 2218.

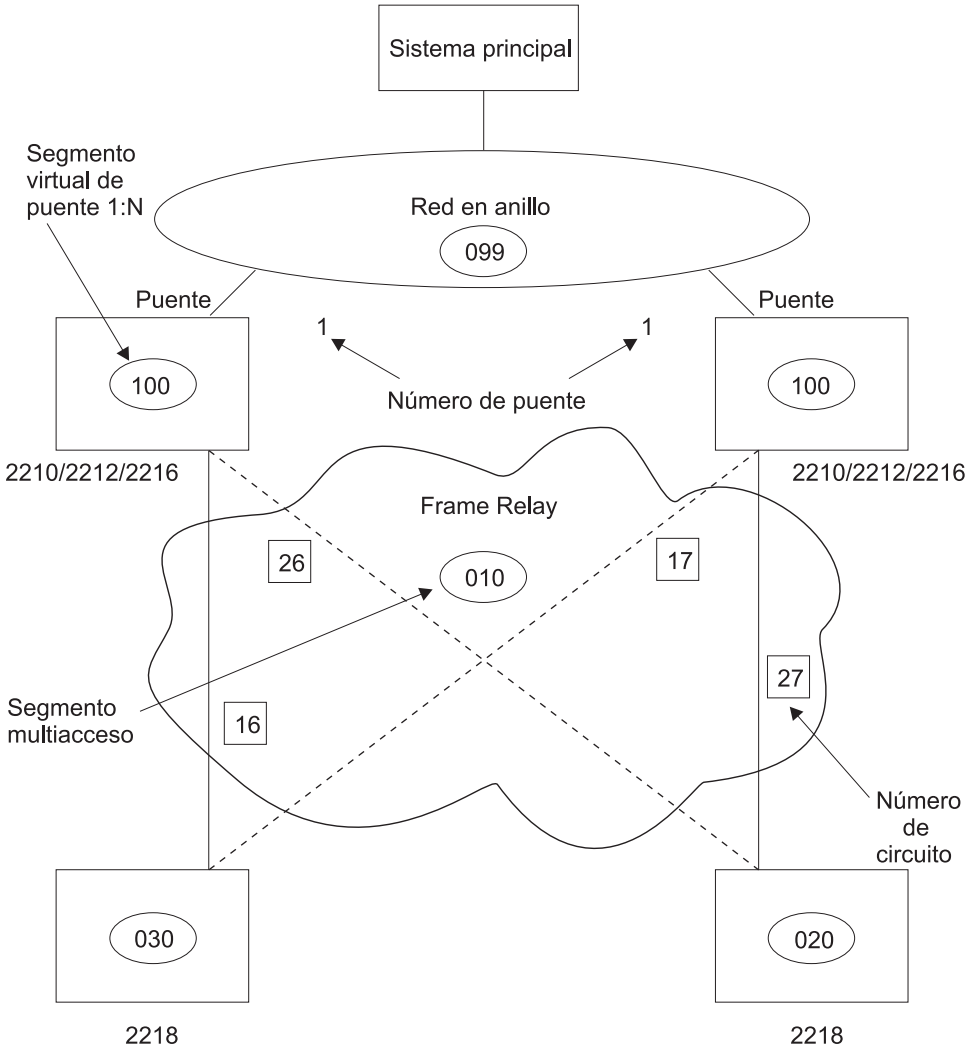



*Figura 19. Configuración de ejemplo con 2218 y puertos de puente multiacceso*

# Utilización de la característica Nodo límite de acceso (BAN)

Este capítulo describe la característica Nodo límite de acceso (BAN) del 2210. BAN ofrece un método fiable y de bajo coste de establecer comunicación entre estaciones finales de Tipo 2.0 y 2.1 conectadas a PU y el entorno SNA a través de enlaces de área amplia. Este capítulo incluye las siguientes secciones:



## Acerca de la característica Nodo límite de acceso

BAN se puede utilizar para conectar cualquiera de estos tipos de nodos SNA:

- Nodos finales
- Nodos de red
- Nodos de subárea.

El Programa de control de red (NCP) de IBM es un ejemplo de nodo de subárea y, junto con VTAM, de nodo de red APPN compuesto.

La característica BAN es una mejora de las funciones Frame Relay, DLSw y conexión por puente de ruta de origen adaptable (ASRT) del software 2210. Esta característica permite que las estaciones finales IBM Tipo 2.0 y 2.1 conectadas a un 2210 establezcan una conexión directa mediante Frame Relay a un nodo SNA que dé soporte al formato de trama RFC 1490/2427 conectado por puente 802.5 (red en anillo). La característica BAN ofrece un método mejor y más barato de establecer comunicación con el entorno IBM SNA. IBM ha modificado el software Programa de control de red (NCP) de IBM para dar soporte a esta mejora.

Si se utiliza BAN, las estaciones finales funcionan como si estuvieran directamente conectadas a un nodo SNA mediante una línea de red en anillo, Ethernet, o SDLC, tal como se muestra en la Figura 20 en la página 64. Los datos realmente pasan a través de un 2210 y sobre una red Frame Relay, pero esto resulta transparente para las estaciones finales.

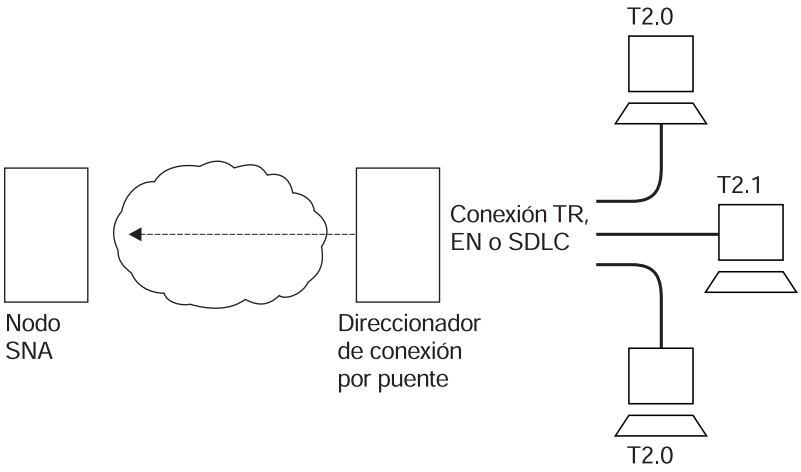



*Figura 20. Conexión directa de estaciones finales a un nodo SNA mediante BAN*

## Ventajas de BAN

Diseñado para adaptarse a las necesidades de los clientes que no necesitan una implantación DLSw completa, BAN constituye un método económico para conectar entornos IBM. Al ofrecer un método de conseguir todas las funciones de DLSw, BAN ofrece tres ventajas principales a los clientes que necesiten una interred con el entorno IBM:

1. Posibilidad de conectar por puente tráfico Ethernet o de red en anillo directamente al nodo SNA sin conversión de tramas por parte de otro direccionador DLSw. Esto permite ahorrar costes de equipo, puesto que elimina la necesidad de disponer de otro direccionador y un sistema principal en la ubicación central.
2. Posibilidad de conectar por puente tráfico Ethernet, de red en anillo o FDDI directamente al nodo SNA sin conversión de tramas por parte de otro direccionador DLSw. Esto permite ahorrar costes de equipo, puesto que elimina la necesidad de disponer de otro direccionador y un sistema principal en la ubicación central.
3. No hay límite arquitectónico en el número de conexiones LLC de Tipo 2 (*LLC2*) multiplexadas sobre un solo identificador de conexión de enlace de datos (DLCI) Frame Relay. Por el contrario, el soporte de Nodo límite (BN) de Frame Relay NCP actual limita el número de conexiones LLC2 por DLCI a 127. Esto permite ahorros significativos en los costes de suministro DLCI Frame Relay.
4. Elimina la necesidad de configurar direcciones de estaciones finales en el direccionador DLSw local a las estaciones finales. Esto facilita la configuración y gestión de la puesta a punto del BAN.

   **Nota:** Puede utilizar un BAN DLCI para tráfico IP. Esto le permite gestionar el direccionador (mediante SNMP) sobre el mismo DLCI que utiliza para SNA (mediante BAN).

## Cómo funciona BAN

La característica BAN en el direccionador funciona filtrando las tramas enviadas por las estaciones finales de Tipo 2.0 ó 2.1. El direccionador modifica cada trama BAN para que cumpla con el formato de trama de conexión por puente 802.5 (red en anillo). El direccionador examina cada trama y sólo permite que pasen sobre un DLCI al sistema principal las que tienen dirección MAC de DLCI BAN. La dirección MAC de destino de la trama 802.5 conectada por puente se sustituye por el Identificador límite de nodo en las tramas destinadas al nodo SNA.

Con BAN, sólo se necesita un DLCI. Sin embargo, BAN puede utilizar varias conexiones DLCI entre el direccionador y el entorno IBM. En algunos casos, es deseable configurar más de un DLCI para gestionar el tráfico BAN. Consulte el tema “Configuración de varios DLCI” en la página 72 para obtener más información.

Hay dos maneras de utilizar la característica BAN:

- Conexión por puente directa mediante la capacidad de conexión por puente del 2210
- Terminación DLSw, en el que BAN termina la conexión LLC2 en el direccionador que ejecuta DLSw.

Las siguientes secciones explican cómo configurar cada método.

## BAN de conexión por puente frente a DLSw

Puede implantar BAN de dos formas: con una conexión por puente directa o con terminación DLSw. Con la conexión por puente directa, configura BAN para que conecte por puente tramas LLC2 procedentes de estaciones finales de Tipo 2.0 o de Tipo 2.1 con el nodo SNA. Con la terminación DLSw, BAN termina la conexión LLC2 en el direccionador que ejecuta DLSw. En esta sección, denominaremos la conexión por puente directa como *BAN Tipo 1* y la terminación DLSw como *BAN Tipo 2*.

La Figura 21 en la página 66 muestra una conexión BAN Tipo 1 (conectada por puente). En esta figura, observe que el direccionador no termina el tráfico LLC2 recibido de las estaciones finales conectadas. En su lugar, el direccionador convierte las tramas que recibe en tramas con formato de red en anillo conectada por puente (RFC 1490/2427) y establece una conexión por puente directamente al nodo SNA.

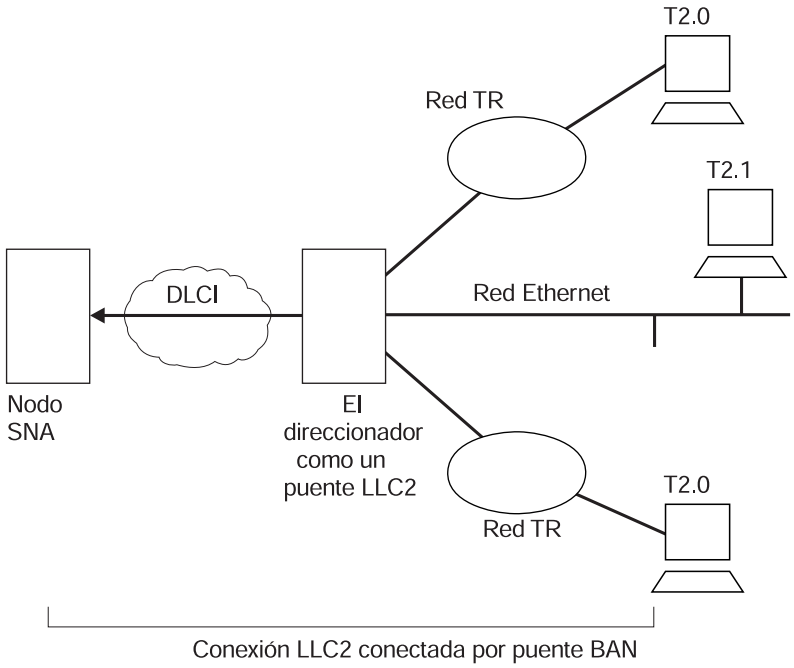



*Figura 21. BAN Tipo 1: el direccionador como un puente LLC2*

En este caso, el direccionador actúa como un puente entre el nodo SNA y las estaciones finales. DLSw no termina las sesiones LLC2 en el direccionador, como sucede en BAN Tipo 2. Las tramas de estaciones finales pueden tener formato de red en anillo o Ethernet, suponiendo que el puente esté configurado para dar soporte a este tipo de tramas.

La Figura 22 en la página 67 muestra una conexión BAN Tipo 2 (BAN DLSw virtual). En esta figura, observe que el direccionador DLSw no funciona como un puente. El direccionador termina el tráfico LLC2 que recibe de las estaciones finales conectadas. Al mismo tiempo, el direccionador establece una nueva conexión LLC2 con el nodo SNA sobre la red Frame Relay. Por lo tanto, aunque hay dos conexiones LLC2 dentro de la transacción, la interrupción entre las mismas resulta transparente tanto para el nodo SNA como para las estaciones finales. Es resultado es una conexión LLC2 virtual entre el nodo SNA y las estaciones finales.

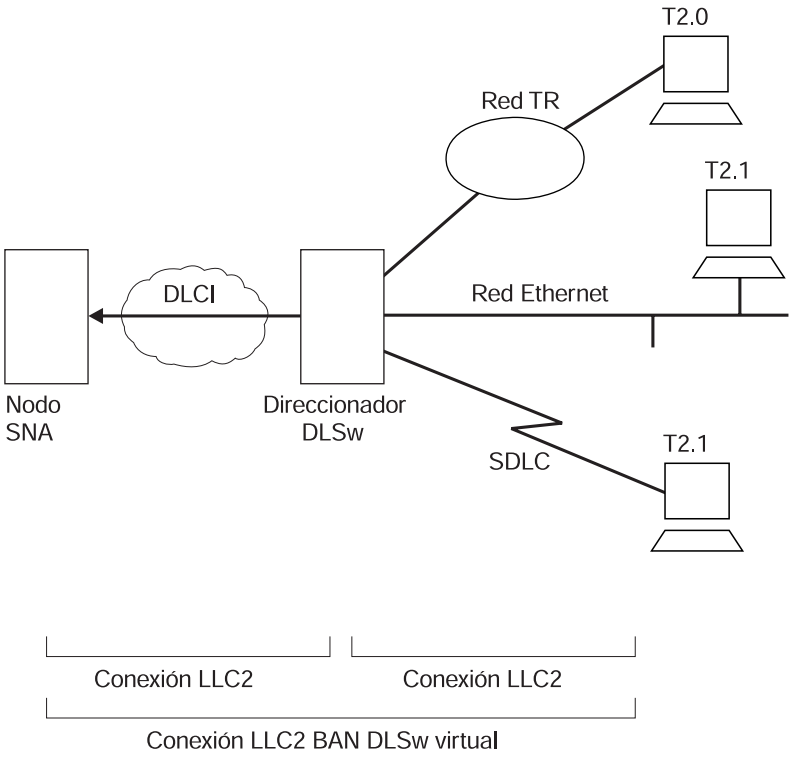



*Figura 22. BAN Tipo 2: Conversión DLSw local*

La sesión SDLC se termina en el direccionador y hay una sesión LLC2 separada entre el direccionador y el nodo SNA. La estación SDLC aparece ante el nodo SNA como una estación conectada por Frame Relay.

DLSw remoto recibe soporte para ambos tipos de BAN. Los direccionadores que funcionan como asociados DLSw para conectar estaciones finales Tipo 2.0 ó 2.1 a un nodo SNA pueden utilizar tanto conexiones BAN Tipo 1 como Tipo 2.

## ¿Qué método debe utilizar?

La conexión por puente directa de tramas (BAN tipo 1) suele ser el método preferido porque permite distribuir datos rápidamente con una mínima actividad general de la red. Sin embargo, existen excepciones. Si el nivel de utilización de un DLCI es demasiado alto, pueden excederse los tiempos de espera de sesiones en una configuración conectada por puente. Por el contrario, raramente se exceden los tiempos de espera en una configuración DLSw (BAN Tipo 2) puesto que este tipo de configuración termina y luego vuelve a crear sesiones LLC2 en el direccionador local (DLSw).

## Utilización de la característica BAN

Al configurar BAN, el sistema le solicita información. Normalmente, el sistema ofrece valores por omisión, puede aceptar pulsando **Intro**.

Para poder utilizar la característica BAN, debe:

1. Configurar el direccionador para Frame Relay (FR)
2. Configurar el direccionador para la Conexión por puente de ruta de origen adaptable (ASRT)

3. Configurar el direccionador para BAN
4. Configurar el direccionador para DLSw (sólo en BAN Tipo 2)

Estos pasos se documentan en el siguiente ejemplo. En el ejemplo se da por supuesto que está configurando un solo DLCI para que maneje tráfico BAN. En función de sus circunstancias y necesidades, quizás sea preferible configurar varios DLCI para redundancia o para aumentar el ancho de banda total en el entorno IBM. En este caso, la dirección MAC BAN DLCI del 2210 debe ser idéntica a la dirección MAC BAN DLCI del 2210 de reserva ISDN. Además, el valor del segmento de puente interno del 2210 debe ser diferente del calor del segmento de puente interno del 2210 de reserva. Consulte el tema “Configuración de varios DLCI” en la página 72 para obtener más información.

## Paso 1: Configurar el 2210 para Frame Relay

Para acceder al indicador de configuración de Frame Relay, escriba **network** *núm. interfaz* en el indicador `Config>` tal como se muestra en el siguiente ejemplo. (*núm. interfaz* es el número de la interfaz Frame Relay.)

```
Config>network 2
Frame Relay user configuration
FR Config>
```

En el indicador `FR Config>`, añada un circuito permanente tal como se muestra en el siguiente ejemplo. El direccionador le solicitará:

- El número de circuito. Es el número de DLCI.
- Una velocidad de información confirmada.

```
FR Config>add permanent
Circuit number  [16]? 20
Committed Information Rate in bps  [64000]?
Committed Burst Size(Bc) in bits (64000)?
Excess Burst Size (Be) in bits(0)?
Assign circuit name []? 20-ncp10
Is circuit required for interface operation [N]?
FR Config>
```

El DLCI que cree se convierte en el PVC que conecta el 2210 y el nodo SNA cuando se utiliza BAN . El paso siguiente consiste en configurar este PVC como un puerto de puente.

**Nota:** Si desea definir varios DLCI BAN conectados al mismo o a distintos nodos SNA, debe configurar Frame Relay por separado para cada DLCI. Consulte el tema “Configuración de varios DLCI” en la página 72 para obtener más información.

## Paso 2: Configurar el direccionador para la Conexión por puente de ruta de origen adaptable

A continuación, debe configurar el PVC como un puerto de puente. Para ello, utilice el mandato **protocol** en el indicador `Config>` tal como se muestra a continuación:

```
Config>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>
```

En el indicador `ASRT Config>`, añada un puerto tal como se muestra. El direccionador le solicitará un número de interfaz. El número que asigne será el número de interfaz FR del puente. Se le solicitará un número de puerto y un

número de circuito. El número de circuito que asigne debe coincidir con el número utilizado al configurar el dispositivo para la conexión por puente sobre Frame Relay en el Paso 1.

```
ASRT config>add port
Interface Number [0]? 2
Port Number [5]?
Assign circuit number [16]? 20
ASRT config>
```

A continuación, active el direccionamiento de origen y defina números de segmento de direccionamiento de origen para el puerto Frame Relay:

```
ASRT config>enable source routing
Port Number [3]? 5
Segment Number for the port in hex (1 - FFF) [1]? 456
Bridge Number in hex (1-9, A-F) [1]?
ASRT config>
```

Por último, desactive la conexión por puente transparente en el puerto de puente del siguiente modo:

```
ASRT config>disable transparent bridging
Port Number [3]? 5
ASRT config>
```

Si se van a utilizar conexiones BAN tipo 2, active DLSw para la conexión por puente.

```
ASRT config>enable dls
ASRT config>
```

El paso siguiente consiste en configurar el direccionador para BAN.

## Paso 3: Configurar el direccionador para BAN

Debe configurar el direccionador para BAN desde el indicador `ASRT config>`. La adición de un puerto BAN en el direccionador no se verificará hasta que vuelva a arrancar el direccionador. Observe que, al igual que en los pasos 1 y 2, el puerto de puente 5 es el puerto que se utiliza en este paso.

```
Config>protocol asrt
ASRT config>ban
BAN (Boundary Access Node) configuration
BAN config>
```

En el indicador `BAN config>`, añada el número de puerto (5) en la que desea activar la característica BAN. Se le solicitará que entre la dirección MAC de BAN DLCI y la dirección del Identificador límite de nodo, tal como se muestra a continuación:

```
BAN config>add 5
Enter the BAN DLCI MAC Address []? 400000000001
Enter the Boundary Node Identifier MAC Address [4FFF00000000]?
```

En este ejemplo, 400000000001 es la dirección MAC del DLCI. Es la dirección a la que las estaciones finales conectadas enviarán los datos. (Consulte la Figura 21 en la página 66 y la Figura 22 en la página 67). La otra dirección, 4FFF00000000, es la dirección por omisión del identificador límite de nodo. Para aceptarla, pulse **Intro**.

**Nota:** El identificador límite de nodo corresponde a la dirección MAC de destino colocada en las tramas 802.5 conectadas por puente que se envían desde el 2210 al nodo SNA. El valor por omisión, 4FFF00000000, coincide con el

valor por omisión que utiliza el Programa de control de red (NCP) de IBM. La dirección NCP se especifica en la definición de NCP mediante la palabra clave LOCADD de la sentencia LINE que define el puerto físico de Frame Relay. Para otros nodos SNA que dan soporte a tramas 802.5 conectadas por puente sobre Frame Relay, el identificador límite de nodo debe tener el valor de la dirección MAC que ha configurado el nodo SNA para este circuito virtual.

**Especificación del tipo de conexión BAN:** El siguiente indicador le solicita que especifique el tipo de conexión BAN que desea añadir: conectada por puente o con terminación DLSw. Estos dos métodos se han descrito en secciones anteriores como BAN Tipo 1 y BAN Tipo 2. El Tipo 1, la conexión por puente directa, es el valor por omisión. Debe aceptar el valor por omisión a no ser que desee que el tráfico de entrada se termine en el direccionador.

Después de entrar **b** o **t**, el direccionador le notifica que se ha añadido el puerto BAN.

```
Do you want the traffic bridged (b) or DLSw terminated (t) (b/t) [b]?
BAN port record added.
```

## Paso 4: Configurar el direccionador para DLSw (sólo BAN Tipo 2)

Si se utilizan conexiones BAN Tipo 2, se debe configurar DLSw. Esto implica activar DLSw, definir el número de segmento DLSw, añadir el asociado DLSw TCP local y abrir los puntos de acceso de servicio (SAP) asociados a la interfaz FR y a la interfaz de la LAN. Si no lleva a cabo esta configuración de DLSw, no podrá utilizar conexiones BAN Tipo 2 (con terminación DLS).

Active DLSw, mediante el mandato **enable dls** desde el indicador `DLSw config>`.

Defina el número de segmento DLSw mediante el mandato **set srb** desde el indicador `DLSw config>`.

Para añadir un asociado DLSw TCP local, haga lo siguiente en el indicador `DLSw config>`:

```
DLSw config>add tcp
Enter the DLSw neighbor IP Address [0.0.0.0.]? 128.185.236.33
Neighbor Priority (H/M/L) [M]?
DLSw config>
```

Abra los SAP desde el indicador `DLSw config>`, tal como se muestra en este ejemplo:

```
DLSw config>open
Núm. interfaz [0]?
Entrar SAP en hex (rango 0-ff) [0]? 4
DLSw config>
```

Al emitir el mandato **open** para la interfaz 0 se abre el SAP en la interfaz LAN. Emita el mismo mandato para abrir el SAP en la interfaz FR. Observe que en cualquier caso debe entrar el número **4** para abrir un SAP.

```
DLSw config>open
Interface # [2]?    [open on the FR interface]
Enter SAP in hex (range 0-ff) [0]? 4
DLSw config>
```

## Utilización de varios DLCI para tráfico BAN

Aunque un DLCI suele ser suficiente para manejar tráfico BAN procedente del entorno IBM y destinado al mismo, el configurar dos o más DLCI puede resultar útil en determinadas circunstancias.

## Escenario 1: Configuración de una conexión BAN con tolerancia de errores

Las conexiones redundantes a varios nodos SNA constituyen una protección frente a una anomalía de un solo nodo SNA. Además, la distribución del tráfico BAN entre varios DLCI reduce la posibilidad de que desbordamiento de un nodo SNA. En una configuración DLCI redundante, las estaciones finales PU Tipo 2.0 y 2.1 pueden pasar tráfico BAN a distintos nodos SNA, tal como se muestra en la Figura 23.

**Nota:** Cada DLCI está configurado en un puerto de puente FR ASRT separado con la misma dirección MAC DLCI.

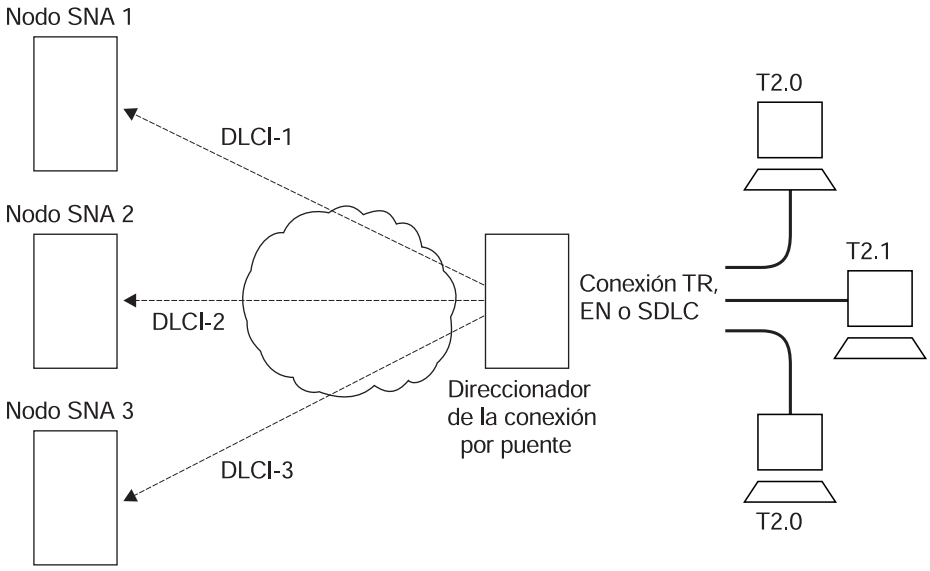



*Figura 23. Configuración BAN con varios DLCI a distintos nodos SNA*

## Escenario 2: Aumento del ancho de banda del entorno IBM

Varias conexiones al mismo nodo SNA aumentan el ancho de banda total disponible para establecer comunicación con el entorno IBM. Esto reduce la posibilidad de congestión de un solo DLCI.

Puede ser recomendable configurar dos o más DLCI si tiene gran cantidad de tráfico BAN y otra conexión FR a su disposición. Un segundo DLCI puede ofrecer un mayor ancho de banda total con el nodo SNA y le puede proteger frente a anomalías inesperadas.

## Configuración de varios DLCI

La configuración de varios DLCI es sencilla, especialmente si lo hace durante la configuración inicial de BAN. Al configurar varias conexiones, recuerde que cada DLCI Frame Relay corresponde a un determinado nodo SNA del entorno IBM. Para pasar tramas BAN a un nodo SNA, debe especificar el número de circuito correcto al establecer la conexión Frame Relay. El proveedor de Frame Relay le puede facilitar el número de circuito para cada una de sus conexiones.

Para configurar conexiones DLCI con distintos nodos SNA ( “Escenario 1: Configuración de una conexión BAN con tolerancia de errores” en la página 71), debe:

1. Emprenda una de las siguientes acciones:
   - **En la configuración ASRT**, añada un puerto de puente para este DLCI.
   - **En la configuración Frame Relay**, defina otro DLCI Frame Relay en un segundo puerto de puente.
2. Configure el puerto de puente para BAN, tal como se muestra en el “Paso 3: Configurar el direccionador para BAN” en la página 69.

Para configurar una segunda conexión DLCI con el mismo nodo SNA (consulte el “Escenario 2: Aumento del ancho de banda del entorno IBM” en la página 71) siga los mismos pasos. En el “Escenario 2: Aumento del ancho de banda del entorno IBM” en la página 71, el número de circuito suministrado para el segundo puerto Frame Relay diferirá del correspondiente al primero. Sin embargo, cada número de circuito identifica un DLCI diferente y una vía de acceso distinta al entorno IBM.

## Comprobación de la configuración de BAN

Cuando vuelva a arrancar el direccionador, este comprobará que el puerto de puente BAN es un puerto de puente Frame Relay con comportamiento de direccionamiento de origen. Debe comprobar la configuración de BAN con el mandato list, tal como se muestra a continuación:

```
BAN config>list

bridge    BAN                 Boundary              bridged or
port      DLCI MAC Address    Node Identifier       DLSw terminated
------    ----------------    ---------------       ---------------
5         40:00:00:00:00:01   4F:FF:00:00:00:00     bridged

BAN config>
```

Tal como aparece en este ejemplo, el mandato **list** muestra cada aspecto de la configuración de BAN, ofreciendo el puerto de puente (5 en este caso), la dirección MAC del DLCI y el identificador límite de nodo correspondiente al nodo SNA, y si el puerto está conectado por puente (bridged) o con terminación DLSw (DLSw terminated).

Para comprobar que BAN se ha inicializado correctamente durante el arranque, puede utilizar GWCON del siguiente modo:

```
+ protocol asrt
ASRT>ban
BAN (Boundary Access Node) console

BAN>list
bridge  BAN                Boundary           bridged or
port    DLCI MAC Address   Node Identifier    DLSw terminated   Status
----    ----------------   ---------------    ---------------   -------
5       40:00:00:00:00:01  4F:FF:00:00:00:00  bridged           Init Fail

BAN>
```

GWCON ofrece tres mensajes de estado:

- El estado `Init Fail` indica que se ha producido un problema de configuración.
- El estado `Down` indica que el DLCI no se está ejecutando.
- El estado `Up` indica que el DLCI Frame Relay está funcionando según lo previsto.

Si recibe un estado distinto de `Up`, debe comprobar los mensajes ELS del direccionador para diagnosticar el problema. El tema “Activación de mensajes del Sistema de registro cronológico de sucesos (ELS) correspondientes a BAN” explica cómo activar mensajes ELS.

## Activación de mensajes del Sistema de registro cronológico de sucesos (ELS) correspondientes a BAN

Tras la configuración inicial de BAN y después de volver a arrancar, se recomienda activar los mensajes ELS para ver si la configuración está funcionando según lo previsto. Puede activar mensajes específicos de BAN desde el indicador `Config>` tal como se muestra a continuación:

```
Config>ev
Event Logging System user configuration
ELS config>display subsystem ban all
ELS config>
```

Al entrar este mandato se muestran todos los mensajes del subsistema BAN. Esto permitirá que ELS le muestre mensajes relacionados con el comportamiento de BAN. Después de ejecutar BAN durante un rato, puede que desee desactivar algunos mensajes. Puede desactivar mensajes ELS de BAN específicos mediante el mandato **nodisplay** seguido del número de mensaje. Este ejemplo muestra cómo desactivar el mensaje ban.9:

```
ELS config>nodisplay event ban.9
```

Para ver una lista y explicaciones de todos los mensajes relacionados con BAN, consulte el manual Guía de mensajes del sistema para el registro cronológico de sucesos.

# Utilización de la conexión por puente

Este capítulo describe cómo crear configuraciones básicas para el puente transparente de direccionamiento de origen adaptable (ASRT) mediante mandatos de configuración de ASRT. Este capítulo incluye los “Procedimientos básicos de configuración de la conexión por puente”.

Si necesita más información sobre los mandatos de configuración del puente ASRT, consulte el tema “Configuración y supervisión de la conexión por puente” en la página 79.

Para ver una introducción a la modificación de la conexión por puente ASRT, consulte el tema “Filtros de bytes y nombres de NetBIOS” en la página 50.

Para ver ejemplos de cómo configurar la función de filtro de NetBIOS, consulte el tema “Procedimientos de configuración de la función de filtro de nombres de sistema principal NetBIOS y de bytes” en la página 169.

Para obtener información sobre cómo acceder al entorno de configuración de ASRT, consulte el tema “Getting Started” del manual *Guía del usuario de software*.

## Procedimientos básicos de configuración de la conexión por puente

El puente ASRT le permite realizar configuraciones básicas de conexión por puente utilizando el menor número de mandatos posible. Por ejemplo, el mandato **enable bridge** comienza este proceso dejando que todos los dispositivos configurados correctamente participen en la conexión por puente transparente. Además, todos los valores por omisión correspondientes al algoritmo de árbol de expansión están activados.

La función de conexión por puente, además de la conexión por puente transparente, se activa “por puerto”. Cuando el direccionamiento de origen está activado, se siguen necesitando entradas de usuario, como número de segmento, número de puente, etc., que se deben entrar, además de los mandatos básicos que se explican.

## Interfaces de conexión por puente

El puente ASRT da soporte a la conexión por puente sobre combinaciones de una o más de las siguientes interfaces:

- Ethernet
- Red en anillo
- Línea serie
- ATM

La interfaz Ethernet da soporte a la conexión por puente transparente, mientras que las interfaces de red en anillo dan soporte al direccionamiento de origen y a la conexión por puente transparente.

La interfaz de línea serie ofrece conectividad punto a punto para el tráfico de direccionamiento de origen y transparente. Es importante tener en cuenta que una configuración de puente sobre una línea serie debe ser coherente en ambos

puntos finales. Esto significa que ambos puntos finales se deben configurar del siguiente modo:

- Transparente a transparente
- Direccionamiento de origen a direccionamiento de origen
- Direccionamiento de origen/transparente a direccionamiento de origen/transparente

Es mejor si la línea serie está configurada para ambos métodos de conexión por puente en el caso de que se desee una conexión por puente mixta. Otro procedimiento recomendable es asegurarse de que los direccionadores de la conexión por puente son coherentes en su método de conexión por puente o en su direccionamiento de determinados protocolos.

La información que viene a continuación describe los pasos iniciales a seguir para activar las opciones de conexión por puente que ofrece el puente ASRT. Los detalles sobre cómo realizar cambios en la configuración se explican en las secciones sobre mandatos de este capítulo. Una vez realizadas estas tareas, debe volver a arrancar el direccionador para que la nueva configuración entre en vigor.

## Activación del puente transparente

Utilice los siguientes mandatos para activar la conexión por puente transparente:

- **Enable bridge** para activar la conexión por puente transparente en todas las interfaces de la red de área local (LAN). Las interfaces de red de área amplia (WAN) (como líneas serie) se pueden incluir utilizando el mandato **add port**.
- **Disable transparent** *núm. puerto* para que las interfaces de red en anillo no participen en la conexión por puente transparente. Repita el mandato para todas las interfaces que desee excluir de la configuración de conexión por puente transparente.

## Activación del puente de direccionamiento de origen

Utilice los siguientes mandatos para activar la conexión por puente de direccionamiento de origen:

- **Enable bridge** para activar la conexión por puente en todas las interfaces de la red de área local.Las interfaces de WAN (por ejemplo, líneas serie) se pueden incluir utilizando el mandato **add port**.
- **Disable transparent** *núm. puerto* para desactivar la conexión por puente transparente en todos los puertos.
- **Enable source-routing** *núm. puerto núm. segmento [núm. puente]* para activar el direccionamiento de origen para determinados puertos. Cuando el direccionamiento de origen está activado en más de dos puertos, se necesita un número de segmento adicional para asignar un segmento virtual interno necesario para configuraciones SRB 1:N.

Si el direccionamiento de origen es la única característica que necesita, desactive la conexión por puente transparente en las interfaces.

**Nota:** Debe tener cuidado de ***no*** incluir las interfaces que tradicionalmente no dan soporte al direccionamiento de origen. Por ejemplo, si la conexión por puente transparente está desactivada y el direccionamiento de origen está activado en un puerto Ethernet , el recurso de conexión por puente se desactiva para este puerto.

## Activación del puente SR-TB

Utilice los siguientes mandatos para activar la conexión por puente SR-TB:

- **Enable bridge** para activar la conexión por puente en todas las interfaces de la red de área local.Las interfaces de WAN (por ejemplo, líneas serie) se pueden incluir utilizando el mandato **add port**.
- **Disable transparent** *núm. puerto* para desactivar la conexión por puente transparente en todas las interfaces subyacentes de direccionamiento de origen.
- **Enable source routing bridge** *núm. puerto núm. segmento [núm. puente]* para activar el direccionamiento de origen para determinados puertos. Cuando el direccionamiento de origen está activado en más de dos puertos, se necesita un número de segmento adicional para asignar un segmento virtual interno necesario para configuraciones SRB 1:N.
- **Enable sr-tb-conversion** *núm. segmento* para activar la conversión de tramas direccionadas de origen a tramas transparentes y viceversa. También tiene que asignar un número de segmento de dominio y un tamaño de MTU de dominio para representar el dominio completo de la conexión por puente transparente.

Una vez realizados los procedimientos necesarios de los anteriormente descritos, se recomienda utilizar el mandato **list bridge** para visualizar la configuración de puente actual. Esto le permite verificar y comprobar la configuración.

Para obtener más información sobre los mandatos mencionados, consulte el tema “Configuración y supervisión de la conexión por puente” en la página 79.

# Configuración y supervisión de la conexión por puente

Este capítulo describe cómo configurar el protocolo de puente transparente de direccionamiento de origen adaptable (ASRT) y cómo utilizar los mandatos de configuración ASRT. Este capítulo incluye las siguientes secciones:



## Cómo acceder al entorno de configuración ASRT

Para acceder al entorno de configuración ASRT, entre el mandato **protocol asrt** en el indicador`Config>`:

```
Config>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>
```

## Mandatos de configuración ASRT

Los mandatos de configuración ASRT le permiten especificar parámetros de red correspondientes al puente ASRT y a sus interfaces de red. Estos mandatos también le permiten activar y configurar las características Túnel IP de puente, interfaz ATM y NetBIOS.

El dispositivo se tiene que volver a arrancar para que la nueva configuración entre en vigor.

**Nota:** Los mandatos de configuración ASRT no entran en vigor de forma inmediata. Permanecen pendientes hasta que vuelve a arrancar o vuelve a cargar el dispositivo.

Entre los mandatos de configuración ASRT en el indicador `ASRT config>`. Acceda a los mandatos del siguiente modo:

- Entre los mandatos de configuración correspondientes al túnel IP en el indicador `TNL config>`. El indicador `TNL config>` es un subconjunto de los principales mandatos ASRT; puede acceder al mismo entrando el mandato `ASRT config>` **tunnel** que se explica más adelante en este capítulo.
- Entre los mandatos de configuración correspondientes a NetBIOS en el indicador `NetBIOS config>`. El indicador `NetBIOS config>` es un subconjunto de los principales mandatos ASRT; puede acceder al mismo entrando el mandato `ASRT config>` **netbios** que se explica más adelante en este capítulo.
- Entre los mandatos de configuración correspondientes a la función de filtro de NetBIOS en el indicador `NetBIOS Filter config>`. Este indicador es un subconjunto de los mandatos NetBIOS.
- Entre los mandatos de configuración correspondientes a ATM en el indicador `ASRT config>`.

La Tabla 4 en la página 80 muestra los mandatos de configuración ASRT.

*Tabla 4 (Página 1 de 2). Resumen de mandatos de configuración ASRT*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Add | Añade a la base de datos permanente entradas de direcciones de estaciones, correlación específica de direcciones, puertos LAN/WAN, puertos multiacceso, filtros de protocolo, direcciones MAC duplicadas y un túnel entre las estaciones finales de la interred IP. |
| Ban | Permite acceder al indicador de configuración del nodo límite de acceso (BAN), en el que se pueden entrar mandatos de configuración de BAN. |
| Change | Permite al usuario cambiar los números de puente y de segmento. |
| Delete | Suprime entradas de direcciones de estaciones, correlación específica de direcciones, puertos LAN/WAN, filtros de protocolo, direcciones MAC duplicadas y un túnel entre las estaciones finales de una interred IP. |
| Disable | Desactiva las siguientes funciones:<br>• Conexión por puente<br>• Tramas duplicadas<br>• Correlación entre direcciones funcionales y de grupo<br>• Propagación de tramas exploradoras del árbol de expansión<br>• Direccionamiento de origen en un determinado puerto<br>• Recepción de tramas exploradoras del árbol de expansión sobre un túnel<br>• Conversión SR-TB<br>• Función de conexión por puente transparente (árbol de expansión) en un determinado puerto<br>• Túnel entre puentes<br>• Característica de direcciones MAC duplicadas<br>• Equilibrio de cargas MAC duplicadas<br>• Conversión IPX |
| Enable | Activa las siguientes funciones:<br>• Conexión por puente<br>• Tramas duplicadas<br>• Correlación entre direcciones funcionales y de grupo<br>• Propagación de tramas exploradoras del árbol de expansión<br>• Direccionamiento de origen en un determinado puerto<br>• Recepción de tramas exploradoras del árbol de expansión sobre un túnel<br>• Conversión SR-TB<br>• Función de conexión por puente transparente (árbol de expansión) en un determinado puerto<br>• Túnel entre puentes<br>• Característica de direcciones MAC duplicadas<br>• Equilibrio de cargas MAC duplicadas<br>• Conversión IPX |

*Tabla 4 (Página 2 de 2). Resumen de mandatos de configuración ASRT*

| Mandato | Función |
|---|---|
| List | Muestra información sobre la configuración completa del puente o sobre los parámetros de configuración seleccionados. |
| NetBIOS | Muestra el indicador de configuración de NetBIOS. |
| Set | Define los siguientes parámetros:<br>• Periodo de antigüedad correspondiente a entradas de direcciones dinámicas<br>• Dirección de puente<br>• Tamaño máximo de trama para la conexión por túnel<br>• Codificación de bits de la trama de mayor tamaño (LF)<br>• Tamaño máximo de trama<br>• Parámetros de puerto y puente del protocolo de árbol de expansión<br>• Valores del Descriptor de ruta (RD)<br>• Tamaño de la base de datos de la función de filtro<br>• Valor de antigüedad correspondiente a los campos de información de direccionamiento (RIF) de direcciones MAC duplicadas<br>• Valor de antigüedad correspondiente a entradas de la base de datos multiacceso<br>• Modalidad de conversión IPX<br>• Preferencia Ethernet |
| Tunnel | Permite acceder al indicador de configuración de túnel, en el que se pueden entrar mandatos de configuración del túnel. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Respuesta a mandatos de configuración ASRT

Los mandatos de configuración ASRT (Talk 6) no entran en vigor de forma inmediata. Permanecen pendientes hasta que emite el mandato **reload** o **restart**.

## Add

Utilice el mandato **add** para añadir la siguiente información a la configuración de la conexión por puente:

- Entradas de direcciones de estaciones a la base de datos permanente
- Correlación específica de direcciones para un determinado protocolo
- Puertos multiacceso
- Puertos LAN/WAN
- Filtros de protocolo que filtran paquetes de forma selectiva, en función del tipo de protocolo
- Túnel IP entre estaciones finales de segmentos de la red IP
- Un máximo de 7 direcciones MAC duplicadas

Para la característica de túnel IP del puente, el mandato **add** le permite crear un túnel IP entre las estaciones finales de la interred IP. Este túnel se cuenta como un solo salto entre las estaciones finales, independientemente de la complejidad de la vía de acceso a través de la interred IP.

**Sintaxis:**

**add** address . . .
dmac-addr
mapping . . .
multiaccess-port . . .
port . . .
prot-filter . . .
tunnel . . .

**address** *valor-dirección*
Añade entradas de direcciones de estaciones exclusivas a la base de datos permanente. Estas entradas se copian en la base de datos de la función de filtro como entradas permanentes cuando se vuelve a arrancar el puente. El *valor-dirección* es la dirección MAC de la entrada deseada. Puede ser una dirección individual, una dirección de difusión múltiple o una dirección de difusión general. También tiene la opción de especificar la correlación de puertos de reenvío de salida para cada puerto de entrada. Las entradas de la base de datos permanente no se destruyen durante el proceso de encendido/apagado y son inmunes a los valores de antigüedad. Las entradas permanentes no se pueden sustituir por entradas dinámicas.

**Valores válidos**: X'0000 0000 0000' a X'FFFF FFFF FFFF'

**Valor por omisión**: ninguno

Las siguientes secciones muestran ejemplos específicos de cómo utilizar el mandato **add address** para gestionar entradas de direcciones:

***Cómo añadir una dirección***

```
add address
Address (in 12-digit hex) []? 123456789013
    Exclude destination address from all ports?(Yes or [No]):
    Use same output port mapping for all input Ports?(Yes or [No]):
    Output port mapping:
       Input Port Number [1]?
       Bridge to all ports?(Yes or [No]):
       Bridge to  port 1  Yes or [No]:
       Bridge to  port 2  Yes or [No]:
       Bridge to  port 3  Yes or [No]:
       Bridge to  port 4  Yes or [No]:
       Bridge to  port 5  Yes or [No]:
       continue to another input port? (Yes or [No]): y
       Input Port Number [2]? 3
       Bridge to all ports?(Yes or [No]): y
       continue to another input port? (Yes or [No]): y
       Input Port Number [4]?
       Bridge to all ports?(Yes or [No]):
       Bridge to  port 1  Yes or [No]:
       Bridge to  port 2  Yes or [No]:
       Bridge to  port 3  Yes or [No]:
       Bridge to  port 4  Yes or [No]:
       Bridge to  port 5  Yes or [No]:
       continue to another input port? (Yes or [No]): n
    Source Address Filtering Applies? (Yes or No): y
    ASRT config>
```

**Nota:** Para cualquiera de las preguntas tipo “Yes o No” de los indicadores, “No” es el valor por omisión. Pulse **Intro** para aceptar el valor por omisión.

**Exclude destination address ...**
Este indicador le permite definir la función de filtro de direcciones de destino correspondiente a esta entrada. Si responde *yes* al indicador, se filtra cualquier trama que contenga esta dirección

como dirección de destino, sin tener en cuenta de qué puerto procede.

**Use same output mapping...**
Si responde *yes* a este indicador, puede crear una correlación de puerto de salida para todos los puertos de entrada, en lugar de permitir únicamente la correlación a determinados puertos. Si responde *no* a este indicador, aparece otro indicador (`Input Port Number [1]?`) para seleccionar cada puerto de entrada. Desde este indicador de puerto de entrada puede crear una correlación de puerto exclusiva para este puerto de entrada.

**Input Port 1, Port 2**
Si responde "No" al indicador anterior, el indicador de puerto de entrada por puerto de entrada (`Input Port Number [1]?`) selecciona cada puerto de entrada y sus puertos de puente de salida asociadas.

**Bridge to all ports?**
Si responde *yes* a este indicador, se crea una correlación de puerto de salida que incluye todos los puertos. Por lo tanto, cuando se recibe una trama con esta dirección como dirección de destino, se reenvía a todos los puertos de reenvío de salida excepto al puerto de entrada. A continuación se muestran ejemplos de cómo se hace según la correlación de puertos:

Si se recibe una trama en el *puerto 1* y la correlación de puerto indica 1 (para puerto 1), la trama se filtra.

Si se recibe la misma trama en el *puerto 2* y la correlación de puerto indica 1 (para puerto 1), la trama se reenvía al puerto 1. Si se recibe una trama en el puerto 1 y la correlación de puerto de la entrada de dirección coincidente indica 1, 2 ó 3, la trama se reenvía a los puertos 2 y 3.

Si la correlación de puerto indica ningún puerto (NONE/DAF), la trama se filtra. Esto recibe el nombre de función de filtro de dirección de destino (DAF).

Si no se encuentra ninguna entrada de dirección que coincida con la trama recibida, se reenvía a todos los puertos de reenvío excepto al puerto de origen.

**Bridge to Port 1, Port 2, etc.**
Este indicador le permite asociar una entrada de dirección con este puerto de puente específica. Si responde *yes*, la dirección se correlaciona con el puerto especificado para que el puerto se incluya en esta correlación de puerto de la entrada de dirección. Si responde *no*, se salta la correlación de dirección correspondiente a este puerto.

**continue to another bridge port?**
Este indicador le permite seleccionar la siguiente puerto de entrada que se tiene que configurar.

**Source address filtering**
Permite llevar a cabo la función de filtro de direcciones de origen (SAF) específica de cada puerto. Cuando se aplica SAF (se responde *yes* a este indicador), las tramas recibidas con direcciones

de origen que coinciden con entradas de direcciones de la base de datos de filtro que tienen activada la función de filtro de direcciones de origen se eliminan. Este mecanismo permite al gestor de la red aislar una estación final, prohibiendo que su tráfico se conecte por puente.

### *Activación de la función de filtro de direcciones de destino para una entrada*

Este ejemplo muestra cómo responder a los indicadores de mandatos para seleccionar la función de filtro de direcciones de destino correspondiente a una entrada:

```
ASRT config>add address 000000334455
Exclude destination address from all ports?(Yes or [No]): y
Source Address Filtering Applies? (Yes o [No]): y
ASRT config>
```

Después de añadir la entrada de dirección, puede comprobar su estado mediante el mandato **list range**. El siguiente ejemplo muestra que no existe ningún puerto para esta entrada (en negrita) y que la función de filtro de direcciones de destino (DAF) se ha desactivado.

```
ASRT config>list range
Start-Index [1]?
Stop-index [3]?
ADDRESS                 ENTRY TYPE      PORT MAP
=======                 ==========      ========
01-80-C2-00-00-00       REGISTERED      Input Port:  ALL PORTS
                                        Output ports:

00-00-00-22-33-44       PERMANENT       Input Port:  3
                                        Output ports: 1, 2
                                        Input Port:  4
                                        Output ports:  1, 2

00 00 00 33 44 55       PERMANENT       NONE/DAF
```

### *Correlación de puertos de salida creada para una entrada de dirección que tiene más de un puerto de entrada*

Este ejemplo muestra cómo responder a los indicadores de mandatos para crear correlaciones separadas de puertos de salida para una entrada de dirección que tendrá más de un puerto de entrada.

```
ASRT config> add address 000000123456
Exclude destination address from all ports?(Yes or [No]):
Use same output port mapping for all input Ports?(Yes or [No]):
Input Port Number [1]? 1
Bridge to all ports ?(Yes or [No]):
Bridge to port 1 - Yes or [No]: y
Bridge to port 2 - Yes or [No]: y
Bridge to port 3 - Yes or [No]:
continue to another input port ? (Yes or [No]): y
Input Port Number [2]?
Bridge to all Ports?(Yes or [No]):
Bridge to Port 1 - Yes or [No]:
Bridge to port 2 - Yes or [No]:
Bridge to port 3 - Yes or [No]: y
continue to another input port ? (Yes or [No]):
Source Address Filtering Applies? (Yes or [No]):
ASRT config>
```

Después de añadir la entrada de dirección, puede comprobar su estado mediante el mandato **list range**. El siguiente ejemplo muestra une entrada (en negrita) que tiene los puertos 1 y 2 como puertos de entrada y tiene distintas correlaciones de puertos para dichos puertos de entrada. La función de filtro de direcciones de origen (SAF) también se ha activado.

```
ASRT config> list range
Start-Index [1]?
Stop-index [3]?
ADDRESS                 ENTRY TYPE      PORT MAP
=======                 ==========      ========
01-80-C2-00-00-00       REGISTERED      Input Port:  ALL PORTS
                                        Output ports:

01-80-C2-00-00-01       RESERVED        NONE/DAF

00-00-00-12-34-56       PERM/SAF        Input Port:  1
                                             Output ports: 1, 2
                                             Input Port:  2
                                             Output ports: 3
```

***Una sola correlación de puertos de salida creada para todos los puertos de entrada asociados a una entrada de dirección***

Este ejemplo muestra cómo responder a los indicadores de mandatos para crear una sola correlación de puertos de salida para todos los puertos de entrada asociados a una entrada de dirección.

```
ASRT config> add address 000000556677
Exclude destination address from all ports?(Yes or [No]):
Use same output port mapping for all input Ports?(Yes or [No]): y
   Bridge to all ports?(Yes or [No]): n
   Bridge to  port 1 - Yes or [No]: y
   Bridge to  port 2 - Yes or [No]: y
   Bridge to  port 3 - Yes or [No]:
Source Address Filtering Applies? (Yes or [No]): y
ASRT config>
```

Después de añadir la entrada de dirección, puede comprobar su estado mediante el mandato **list range**. El siguiente ejemplo muestra una entrada (en negrita) que tiene una sola correlación de puertos para todos los puertos de entrada. La función de filtro de direcciones de origen (SAF) también se ha activado.

```
ASRT config> list range
Start-Index [1]?
Stop-index [3]?
ADDRESS                 ENTRY TYPE      PORT MAP
=======                 ==========      ========
01-80-C2-00-00-00       REGISTERED      Input Port:  ALL PORTS
                                        Output ports:

01-80-C2-00-00-01       RESERVED        NONE/DAF

00-00-00-55-66-77       PERM/SAF        Input Port:  ALL PORTS
                                        Output ports:  1, 2
```

**dmac-addr** *valor-dirección*

Añade un máximo de 7 entradas de direcciones MAC duplicadas a la base de datos. El *valor-dirección* es la dirección MAC de la entrada deseada. Consulte el tema “Característica de dirección MAC duplicada de SR-TB” en la página 57 para obtener información adicional sobre la característica de direcciones MAC duplicadas.

**Valores válidos**: X'0000 0000 0000' a X'FFFF FFFF FFFF'

**Valor por omisión**: ninguno

**Ejemplo:**

Después de añadir la dirección, puede comprobar la información DMAC mediante el mandato **list dmac**.

```
ASRT config>add dmac-addr
Address (in 12-digit hex) []? 10005a777701
```

```
ASRT config>list dmac
Duplicate MAC address feature is    ENABLED
Load balance feature is    ENABLED
Age value for Duplicate MAC address :000000C8
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-02
10-00-5A-66-66-05
10-00-5A-77-77-01
```

**mapping** *tipo-ced campo-tipo dirección-dg dirección-df*
Añade una determinada dirección funcional a la correlación de direcciones de grupo correspondiente a un determinado identificador de protocolo. La correlación de direcciones se convierte sólo en direcciones de destino que cruzan de Red en anillo a Ethernet o viceversa.

**Nota:** Para cada valor correlacionado tipo Ether, se debe añadir el valor correspondiente tipo SNAP. Esto es necesario para la correlación bidireccional.

**tipo-ced** (tipo cabecera-enlace-datos) es una opción para DSAP, tipo Ether o SNAP.

**campo-tipo**
Campo de tipo de protocolo.

El tipo de protocolo Punto de acceso de servicio de destino (DSAP) se entra en el rango 1–FE (hexadecimal).

**Valores válidos de DSAP**: X'1' a X'FE'

Los valores comunes son:

*Protocolo - SAP (valor hexadecimal)*
- Banyan SAP - BC (sólo se utiliza para 802.5)
- Novell IPX SAP - E0 (sólo se utiliza para 802.5)
- NetBIOS SAP - F0
- ISO Connectionless Internet - FE

**Valor por omisión de DSAP**: 1
El tipo de protocolo Ethernet (Ether) se entra en el rango 5DD–FFFF (hexadecimal).

**Valores válidos de Ethernet**: X'5DD' a X'FFFF'

*Protocolo - Tipo Ethernet (valor hex)*
- IP - 0800
- ARP - 0806
- CHAOS - 0804
- Tipo de paquete de mantenimiento - 7030
- Vuelco/carga DECnet MOP - 6000
- Consola remota DECnet MOP - 6002
- DECnet- 6003
- DEC LAT - 6004
- DEC LAVC - 6007
- XNS - 0600
- Dominio Apollo - 8019 (Ethernet)
- Novell NetWare IPX - 8137 (Ethernet)
- AppleTalk Fase 1 - 809B
- Apple ARP Fase 1 - 80F3
- Asistencia bucle de retorno - 9000

**Valor por omisión de Ethernet**: 1
El tipo de protocolo del Protocolo de acceso de subred (SNAP) se entra en formato hexadecimal de 10 dígitos.

**Valores válidos de SNAP**: X'00 0000 0000' a X'FF FFFF FFFF'

Los valores comunes son:
- AppleTalk Fase 2 08-00-07-80-9B
- Apple ARP Fase 2 00-00-00-80-F3

**Valor por omisión de SNAP**: 00 0000 0800

**dirección-dg**
Dirección de grupo/difusión múltiple de 6 bytes (hexadecimal de 12 dígitos).

**Valores válidos**: X'0000 0000 0000' a X'FFFF FFFF FFFF'

**Valor por omisión**: ninguno

**dirección-df**
Dirección funcional en formato no canónico. Las direcciones funcionales son direcciones de grupo administradas localmente. Se utilizan con más frecuencia en redes en anillo.

**Valores válidos**: X'0000 0000 0000' a X'FFFF FFFF FFFF'

**Valor por omisión**: ninguno

**Ejemplo:**
```
ASRT config> add mapping dsap

Protocol Type in hex (1 - FE) [1]?
Group-Address (in 12-digit hex) [ ]?
Functional address (in noncanonical format) [ ]?
```

**Ejemplo:**
```
ASRT config> add mapping ether

Protocol Type in hex (5DD - FFFF) [0800]?
Group-Address (in 12-digit hex) []?
Functional address (in noncanonical format) [ ]?
```

**Ejemplo:**
```
ASRT config> add mapping snap

Address (in 10-digit hex) [0000000800]?
Group-Address (in 12-digit hex) []?
Functional address (in noncanonical format) [ ]?
```

**multiaccess-port** *núm. interfaz núm. puerto núm. segmento [núm. puente] [núm. segmento-virtual]*
Añade un puerto multiacceso a la configuración de conexión por puente. Este mandato asocia un número de puerto con una interfaz Frame Relay y activa el puerto para la conexión por puente de direccionamiento de origen.

**núm. interfaz**
Especifica la interfaz Frame Relay en la que está configurando el puerto multiacceso.

**Valores válidos:** cualquier número de interfaz Frame Relay existente

**Valor por omisión:** 0

**núm. puerto**
Especifica el número de puerto del puente. Este número debe ser exclusivo entre todos los puertos de puente configurados en el dispositivo.

**Valores válidos:** 1 a 254

**Valor por omisión:** siguiente número de puerto disponible

**núm. segmento**

Especifica un número de segmento de direccionamiento de origen hexadecimal de 12 bits que representa el segmento multiacceso. Todos los puentes conectados al segmento multiacceso deben utilizar el mismo número de segmento.

**Valores válidos:** X'001' a X'FFF'

**Valor por omisión:** X'001'

**núm. puente**

Especifica un número de puente de direccionamiento de origen hexadecimal de 4 bits que representa este puente en el segmento multiacceso. Este parámetro sólo se necesita cuando se activa el direccionamiento de origen por primera vez. El número de puente debe ser exclusivo entre todos los puentes del segmento multiacceso.

**Valores válidos:** X'0' a X'F'

**Valor por omisión:** X'0'

**núm. segmento-virtual**

Especifica un número de segmento de direccionamiento de origen hexadecimal de 12 bits. Este parámetro sólo se necesita cuando se activa el direccionamiento de origen por primera vez en más de dos puertos de puente o la primera vez que se configura un puerto de puente multiacceso.

**Valores válidos:** X'001' a X'FFF'

**Valor por omisión:** X'001'

**Ejemplo:**

```
add multiaccess-port
Interface number [0]? 3
Port number [2]? 2
Segment number for the port in hex (1 - FFF) [001]? 200
Bridge number in hex (0-9, A-F) [0]? 1
Bridge Virtual Segment Number in hex (1-FFF) [001]? FFF
```

**port** *núm. interfaz núm. puerto*

Añade un puerto LAN/WAN a la configuración de conexión por puente. Este mandato asocia un número de puerto con el número de interfaz y activa la participación de dicho puerto en la conexión por puente transparente.

**Valores válidos de número de puerto**: 1 a 254

**Valor por omisión de número de puerto**: ninguno

**Ejemplo: add a port**

```
ASRT config> add port
Interface Number [0]?
Port Number [5]?
```

Consulte el tema “Mandatos de ATM” en la página 130 para obtener información sobre cómo añadir puertos ATM y el tema “Mandatos de Frame Relay” en la página 129 para obtener información sobre cómo añadir puertos Frame Relay.

**prot-filter** s**nap** e**ther** d**sap**

Permite configurar el puente de modo que pueda filtrar paquetes de forma selectiva en función del tipo de protocolo. Los filtros se pueden aplicar a todos los puertos o sólo a los puertos seleccionados.

Este parámetro especifica identificadores de protocolo para los que las tramas recibidas de este protocolo específico se eliminan exclusivamente sin aplicar la lógica del puente. Los paquetes ARP correspondientes a este tipo de protocolo también se eliminan. El filtro de protocolos se aplica sólo en los paquetes recibidos. Los filtros de protocolo disponibles incluyen:

**Paquetes SNAP**
Protocolo de acceso de subred con el tipo de protocolo entrado en formato hexadecimal de 10 dígitos.

**Paquetes Ether**
Tipo Ethernet con el tipo de protocolo entrado en el rango 5DD–FFFF (hexadecimal).

**Paquetes DSAP**
Protocolo de Punto de acceso de servicio de destino con el tipo de protocolo entrado en el rango 0–FE (hexadecimal).

**Notas:**

1. No puede filtrar todos los paquetes de formato SNAP añadiendo un filtro DSAP correspondiente al tipo X'AA'. El protocolo o protocolos SNAP encapsulados se deben filtrar individualmente. Considere la posibilidad de utilizar un filtro de ventana corredera. Consulte el capítulo “Using MAC Filtering” del manual *Utilización y configuración de las características*.
2. No puede configurar filtros de protocolo correspondientes a un protocolo que se direcciona sobre una determinada interfaz si dicha interfaz también está configurada para la conexión por puente.

Los filtros de protocolo comunes y sus respectivos valores son los siguientes.

**Tipos DSAP**

| Protocolo | SAP (valor hexadecimal) |
|---|---|
| Banyan SAP | BC (sólo se utiliza para 802.5) |
| Novell IPX SAP | E0 (sólo se utiliza para 802.5) |
| NetBIOS SAP | F0 |
| ISO Connectionless Internet | FE |

**Identificadores de protocolo SNAP**

| Protocolo | SNAP OUI/IP (10 dígitos) |
|---|---|
| AppleTalk Fase 2 | 08-00-07-80-9B |
| Apple ARP Fase 2 | 00-00-00-80-F3 |

**Tipos Ethernet**

| Protocolo | Tipo Ethernet (valor hex) |
|---|---|
| IP | 0800 |
| ARP | 0806 |
| CHAOS | 0804 |
| Tipo de paquete de mantenimiento | 7030 |
| Vuelco/carga DECnet MOP | 6000 |
| Consola remota DECnet MOP | 6002 |
| DECnet | 6003 |
| DEC LAT | 6004 |
| DEC LAVC | 6007 |
| XNS | 0600 |
| Dominio Apollo | 8019 (Ethernet) |
| Novell NetWare IPX | 8137 (Ethernet) |
| Apple ARP Fase 1 | 80F3 |
| Asistencia bucle de retorno | 9000 |

**Ejemplo:** ASRT config> **add prot-filter dsap** (utilizado para paquetes DSAP)

```
Protocol Type in hex (0 - FE) [1]?
   Filter packets arriving on all ports?(Yes or [No]):
   Filter packets arriving on  port 1 - Yes or [No]:
   Filter packets arriving on  port 2 - Yes or [No]:
   Filter packets arriving on  port 3 - Yes or [No]:
Port assignment Required, filter not added
ASRT config>
```

**Ejemplo:** ASRT config> **add prot-filter ether** (utilizado para paquetes Ethernet)

```
Protocol Type in hex (5DD - FFFF) [0800]?
   Filter packets arriving on all ports?(Yes or [No]):
   Filter packets arriving on  port 1 - Yes or [No]:
   Filter packets arriving on  port 2 - Yes or [No]:
   Filter packets arriving on  port 3 - Yes or [No]:
Port assignment Required, filter not added
ASRT config>
```

**Ejemplo:** ASRT config>**add prot-filter snap** (utilizado para paquetes SNAP)

```
Address (in 10-digit hex) [0000000800]?
Protocol Type in hex (5DD - FFFF) [0800]?
   Filter packets arriving on all ports?(Yes or [No]):
   Filter packets arriving on  port 1 - Yes or [No]:
   Filter packets arriving on  port 2 - Yes or [No]:
   Filter packets arriving on  port 3 - Yes or [No]:
Port assignment Required, filter not added
ASRT config>
```

**tunnel** *núm. puerto*

Crea el túnel IP definido por el usuario a un puerto de puente. El túnel de puente permite establecer comunicación a través de una red IP a dominios de puente de direccionamiento de origen o a dominios de puente transparente.

Para permitir que tráfico de IBM LAN y de terminal se fusionen con tráfico que no sea de IBM (es decir, Novell) a través de una sola red troncal, las características Túnel de puente de direccionamiento de origen y Transmisión SDLC (Control síncrono de enlace de datos) del

software del dispositivo de conexión por puente encapsulan el tráfico de IBM dentro de paquetes TCP/IP estándares de la industria. Luego el dispositivo de conexión por puente direcciona estos paquetes utilizando una vía de acceso IP o *túnel* a través de grandes interredes IP. Como resultado aumenta la funcionalidad y la utilización de la red, así como la disponibilidad de la red y la facilidad de uso.

Las estaciones finales ven la vía de acceso IP (el túnel) como un solo salto, independientemente de la complejidad de la red. Esto ayuda a solucionar el límite habitual de distancia de 7 saltos de las configuraciones de direccionamiento de origen. También le permite conectar estaciones finales de direccionamiento de origen a través de un soporte de direccionamiento que no es de origen, como las redes Ethernet.

El túnel de conexión por puente también ayuda a evitar problemas derivados de limitaciones normales de direccionamiento de origen, como las siguientes:

- Límite de distancia de siete saltos
- Gran cantidad de actividad general que causa el direccionamiento de origen en redes de área amplia (WAN)
- El gran impacto que causa en el direccionamiento de origen los errores de la WAN (por ejemplo, si falla una vía de acceso todos los sistemas deben reiniciar sus transmisiones)

Con la característica de túnel de conexión por puente activada, el software encapsula los paquetes en paquetes TCP/IP. Para el dispositivo, el paquete tiene el aspecto de un paquete TCP/IP. Una vez se ha encapsulado una trama en un sobre IP, el distribuidor IP es el responsable de seleccionar la interfaz de red adecuada según la dirección IP de destino. Este paquete se puede direccionar de forma dinámica a través de grandes interredes sin que se degrade y sin restricciones de tamaño de red. Las estaciones finales ven esta vía de acceso o túnel como un solo salto, independientemente de la complejidad de la interred.

El túnel resulta transparente para las estaciones finales. Los dispositivos de la conexión por puente que participan en la conexión por túnel tratan la interred IP como uno de los segmentos del puente. Cuando el paquete alcanza la interfaz de destino, las cabeceras TCP/IP se eliminan de forma automática y el paquete interno continúa como un paquete de direccionamiento de origen estándar.

**Add Tunnel** crea el túnel IP definido por el usuario a un puerto de puente. Este túnel se cuenta como un solo salto entre los puentes, independientemente de la complejidad de la vía de acceso a través de la interred IP. Para poder utilizar la característica de túnel, se debe activar el distribuidor IP.

Sólo se puede añadir un túnel. Debe utilizar un *Número de puerto* que no se utilice para ningún otro puerto de la LAN. Una vez se asigna un Número de puerto al túnel de conexión por puente, se pueden utilizar todos los demás mandatos de conexión por puente que necesiten un número de puerto como parámetro para configurar las características del túnel. Para la configuración específica del túnel, como las direcciones IP de los puntos finales, utilice el mandato **tunnel** (consulte el tema “Tunnel” en la página 122).

La conexión por puente transparente se activa en este puerto por omisión. Sin embargo, el direccionamiento de origen se puede activar utilizando la opción **Enable Source-Routing**.

**Ejemplo:** **add tunnel 3**

```
Port Number   [1] ? 3
```

**Número puerto** Un número de puerto exclusivo que el puente no esté utilizando.

## BAN

Utilice el mandato **ban** para acceder al indicador de configuración del nodo límite de acceso (BAN). Los mandatos BAN se entran en el indicador de configuración de BAN (`BAN config>`). Consulte el tema “Mandatos de configuración de BAN” en la página 123 para ver una explicación de cada uno de estos mandatos.

**Sintaxis:**

**ban**

**Ejemplo:** **ban**

```
BAN (Boundary Access Mode) configuration
BAN config>
```

## Change

Utilice el mandato **change** para cambiar números de segmento y de puente de direccionamiento de origen en la configuración de conexión por puente.

**Sintaxis:**

**change** bridge . . .
segment . . .

**bridge** *nuevo núm. puente*
Cambia el número de puente en la configuración de la conexión por puente.

**Ejemplo:** **change bridge 3**

**segment** *antiguo núm. segmento nuevo núm. segmento*
Cambia el número de segmento en la configuración de la conexión por puente.

**Ejemplo:** **change segment 2 3**

## Delete

Utilice el mandato **delete** para suprimir la siguiente información de la configuración de la conexión por puente:

- Entradas de direcciones de estaciones a la base de datos permanente
- Correlación específica de direcciones para un determinado protocolo
- Puertos LAN/WAN y multiacceso
- Filtros de protocolo que filtran paquetes de forma selectiva, en función del tipo de protocolo
- Direcciones MAC duplicadas

Para la característica de túnel IP, el mandato **delete port** con el número de puerto correspondiente al túnel elimina el túnel entre puentes a través de una interred IP.

**Sintaxis:**

de**lete** address

dmac-addr

mapping . . .

port . . .

prot-filter . . .

**address** *valor-dirección*
Suprime una entrada de dirección de la base de datos permanente. La dirección es la dirección MAC de la entrada deseada. Entre el valor-dirección (en formato hexadecimal de 12 dígitos) de la entrada que desee suprimir y pulse **Intro**. Las direcciones de difusión múltiple reservadas no se pueden suprimir. Si intenta suprimir una entrada de dirección que no existe, recibirá el mensaje

```
Record matching that address not found
```

**Valores válidos**: X'0000 0000 0000' a X'FFFF FFFF FFFF'

**Valor por omisión**: ninguno

**Ejemplo: `delete address`**

**dmac-addr** *valor-dirección*
Suprime las entradas de direcciones MAC duplicadas de la base de datos. El *valor-dirección* es la dirección MAC de la entrada que desea eliminar.

**Valores válidos**: X'0000 0000 0000' a X'FFFF FFFF FFFF'

**Valor por omisión**: ninguno

**Ejemplo:**

```
ASRT>list gamic
Duplicate MAC address feature is   DISABLED
Load balance feature is   DISABLED
Age value for Duplicate MAC address :00000096
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-00
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05

ASRT config>delete dmac-address
Address (in 12-digit hex) []? 10005a666600
Address deleted

ASRT config>list dmac
Duplicate MAC address feature is   DISABLED
Load balance feature is   DISABLED
Age value for Duplicate MAC address :00000096
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05
```

**mapping** *tipo-ced campo-tipo dirección-dg*
Suprime la correlación específica de direcciones correspondientes a un determinado protocolo.

**tipo-ced** (tipo cabecera-enlace-datos) es una opción para DSAP, tipo Ether o SNAP.

**campo-tipo**
Campo de tipo de protocolo.

El tipo de protocolo Punto de acceso de servicio de destino (DSAP) se entra en el rango 1–FE (hexadecimal).

**Valores válidos**: X'1' a X'FE'

Los valores comunes son:

*Protocolo - SAP (valor hexadecimal)*

**Valor por omisión**: 1

El tipo de protocolo Ethernet (Ether) se entra en el rango 5DD–FFFF (hexadecimal).

**Valores válidos**: X'5DD' a X'FFFF'

**Valor por omisión**: 1

El tipo de protocolo del Protocolo de acceso de subred (SNAP) se entra en formato hexadecimal de 10 dígitos.

**Valores válidos**: X'00 0000 0000' a X'FF FFFF FFFF'

Los valores comunes son:

**Valor por omisión**: 00 0000 0800

**dirección-dg**
Dirección de grupo/difusión múltiple de 6 bytes (hexadecimal de 12 dígitos).

**Valores válidos**: X'0000 0000 0000' a X'FFFF FFFF FFFF'

**Valor por omisión**: ninguno

**Ejemplo:** `delete mapping DSAP FE <dirección grupo>`

**port** *núm. puerto*
Elimina un puerto de una configuración de conexión por puente. Puesto que el mandato **enable bridge** configura por omisión todos los dispositivos de la LAN para que participen en la conexión por puente, este mandato le permite personalizar los dispositivos que deben o no deben participar en la conexión por puente. El valor de número de puerto suele ser mayor que el número de interfaz.

Este mandato seguido del número de puerto del túnel IP elimina un túnel IP de una configuración de conexión por puente.

**Ejemplo:** `delete port 2`

**prot-filter** **snap ether dsap**
Suprime los identificadores de protocolo anteriormente especificados que se utilizan en la función de filtro. Puede suprimir los filtros de todos los puertos o de los puertos seleccionados. Estos filtros incluyen:

**Paquetes SNAP**
Protocolo de acceso de subred con el tipo de protocolo entrado en formato hexadecimal de 10 dígitos.

**Paquetes Ether**
Tipo Ethernet con el tipo de protocolo entrado en el rango 5DD–FFFF (hexadecimal).

**Paquetes DSAP**
Protocolo de punto de acceso de servicio de destino con el tipo de protocolo entrado en el rango 0–FE (hexadecimal).

**Ejemplo:** ASRT config> **delete prot-filter snap** (utilizado para paquetes SNAP)

```
Address (in 10-digit hex) [0000000800]?
   Delete filter on all ports?(Yes or [No]):
   Delete filter on  port 1 - Yes or [No]:
   Delete filter on  port 2 - Yes or [No]:
   Delete filter on  port 3 - Yes or [No]:
```

**Ejemplo:** ASRT config> **delete prot-filter ether** (utilizado para paquetes Ethernet)

```
Protocol Type in hex (5DD - FFFF) [0800]?
   Delete filter on all ports?(Yes or [No]):
   Delete filter on  port 1 - Yes or [No]:
   Delete filter on  port 2 - Yes or [No]:
```

**Ejemplo:** ASRT config> **delete prot-filter dsap** (utilizado para paquetes DSAP)

```
Protocol Type in hex (0 - FE) [1]?
   Delete filter on all ports?(Yes or [No]):
   Delete filter on  port 1 - Yes or [No]:
   Delete filter on  port 2 - Yes or [No]:
   Delete filter on  port 3 - Yes or [No]:
```

## Disable

Utilice el mandato **disable** para desactivar las siguientes funciones de puente:

- Conexión por puente
- Tramas duplicadas
- Correlación entre direcciones funcionales y de grupo
- Propagación de tramas exploradoras del árbol de expansión
- Direccionamiento de origen en un determinado puerto
- Conversión SR-TB
- Función de conexión por puente transparente (árbol de expansión) en un determinado puerto
- Característica de direcciones MAC duplicadas
- Equilibrio de cargas MAC duplicadas
- DLSw

Para la característica de túnel, el mandato disable desactiva un túnel entre estaciones finales a través de una interred IP.

**Sintaxis:**

**disable** bridge
dls
duplicate . . .
dmac-addr

dmac-load-balance

ethertype-ibmrt-pc

fa-ga-mapping

ibm8209-spanning-tree

ipx-conversion . . .

spanning-tree-explorer . . .

source-routing . . .

sr-tb-conversion

stp

transparent . . .

tree

ub-encapsulation

**bridge** Desactiva por completo la función de conexión por puente. Sin embargo, este mandato no elimina los valores de conexión por puente anteriormente configurados.

**Ejemplo:** `disable bridge`

**dls** Desactiva la operación de DLSw del puente. (El dispositivo que ejecuta DLSw aparece como un puente ante las estaciones finales.) Consulte el tema “Utilización de DLSw” en la página 525 para obtener más información.

**Ejemplo:** `disable dls`

**duplicate** *tipo-trama*
Desactiva la creación de tramas duplicadas presentes en entornos mixtos de conexión por puente. Cuando la característica de conexión por puente SR-TB está activada en una interfaz 802.5 (con el direccionamiento de origen o la conexión por puente transparente activados), se generan incoherencias cuando se conectan por puente tramas a un destino desconocido (o difusión múltiple). El puente no sabe si el destino se encuentra detrás de un direccionamiento de origen (sólo) o de un puente transparente.

Para remediar esta situación, el puente envía duplicados de estas tramas (por omisión). Una trama contiene campos de direccionamiento de origen (RIF explorador del árbol de expansión) y la otra está formateada para la conexión por puente transparente (no contiene ningún RIF). El mandato **disable duplicate** le permite eliminar esta duplicación, permitiéndole desactivar la creación de uno de estos tipos de tramas. El mandato **disable duplicate** no le permitirá desactivar simultáneamente ambos tipos de tramas.

Si entra **STE** tras el mandato, indica al puente que no envíe tramas exploradoras del árbol de expansión correspondientes al entorno de direccionamiento de origen. Si entra **TSF** tras el mandato, indica al puente que no envíe tramas de expansión transparentes correspondientes al entorno de conexión por puente transparente. En ambos casos, se trata de una situación en la que normalmente no se enviarían ambos tipos de tramas. Al desactivar la conexión por puente transpa-

rente en la interfaz también se desactiva la creación de tramas transparentes.

**Ejemplo: `disable duplicate TSF`**

```
          Port Number [1]?
```

### dmac-addr

Desactiva la característica de direcciones MAC duplicadas.

**Ejemplo: `disable dmac-addr`**

```
ASRT>list dmac
Duplicate MAC address feature is    ENABLED
Load balance feature is    ENABLED
Age value for Duplicate MAC address :00000096
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-00
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05

ASRT config>disable dmac-addr

ASRT>list dmac
Duplicate MAC address feature is   DISABLED
Load balance feature is   DISABLED
Age value for Duplicate MAC address :00000096
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-00
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05
```

### dmac-load-balance

Desactiva el equilibrio de carga de MAC duplicadas para la característica de direcciones MAC duplicadas.

**Ejemplo: `disable dmac-load-balance`**

```
ASRT>list dmac
Duplicate MAC address feature is    ENABLED
Load balance feature is    ENABLED
Age value for Duplicate MAC address :00000096
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-00
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05
ASRT config>disable dmac-load-balance
ASRT>list dmac
Duplicate MAC address feature is   ENABLED
Load balance feature is   DISABLED
Age value for Duplicate MAC address :00000096
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-00
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05
```

**ethertype-ibmrt-pc**

Desactiva la conversión de tramas SNA a formato Ethernet Tipo 2, utilizado por los RT de IBM que ejecutan OS/2 EE.

**Ejemplo:** `disable ethertype-ibmrt-pc`

```
Port Number [1]?
```

**fa-ga-mapping**

Desactiva la correlación dirección de grupo a dirección funcional (y viceversa). Bajo determinadas circunstancias, es posible que desee desactivar la correlación entre entre dirección de grupo y dirección funcional de forma global.

**Ejemplo:** `disable fa-ga-mapping`

**ibm8209-spanning-tree**

Evita que los puentes participen en los protocolos de árbol de expansión con puentes IBM 8209.

**Ejemplo:** `disable ibm8209-spanning-tree`

**ipx-conversion**

Desactiva de forma global la conversión de tramas Novell IPX cuando se establece una conexión por puente entre puertos de puentes Ethernet/802.3 y Red en anillo (802.5). Cuando están desactivadas, las tramas Novell IPX se pueden conectar por puente entre estaciones finales del mismo tipo de soporte a través de una LAN troncal de un tipo de soporte distinto, pero no se pueden conectar por puente entre estaciones finales de distintos soportes.

**Ejemplo:** `disable ipx-conversion`

**spanning-tree-explorer** *port#*

Evita que un puerto permita la propagación de tramas exploradoras del árbol de expansión si el direccionamiento de origen está activado. Este mandato sólo se utiliza si la conexión por puente transparente no está activada en el puerto. En este caso, cumple automáticamente con el árbol de expansión transparente.

**Ejemplo:** `disable spanning-tree-explorer 2`

**source-routing** *núm. puerto*

Desactiva el direccionamiento de origen en un determinado puerto. Este mandato sirve para que una interfaz de puente que ya participa deje de participar en el direccionamiento de origen.

**Ejemplo:** `disable source-routing 2`

**sr-tb-conversion**

Desactiva la conversión de tramas de direccionamiento de origen a tramas transparentes y viceversa.

**Ejemplo:** `disable sr-tb-conversion`

**stp** Desactiva el protocolo del árbol de expansión en el puente. El valor por omisión es que esté activado.

**Ejemplo:** `disable stp`

**transparent** *núm. puerto*

Desactiva la función de conexión por puente transparente en un determinado puerto. Este mandato resulta útil cuando se desea un método de comunicación alternativo como el direccionamiento de origen.

**Nota:** Este mandato puede dar lugar a una configuración absurda si no se utiliza correctamente. Por ejemplo, si se utiliza en una interfaz Ethernet se desactiva la función de conexión por puente correspondiente a dicha interfaz. Este mandato sirve para generar la función de puente SRB y SR-TB.

**Ejemplo:** `disable transparent 2`

**tree** *núm. puerto*

Desactiva la participación de STP correspondiente al puente por puerto.

**Ejemplo:** `disable tree 1`

**Nota:** Al desactivar STP por puerto se pueden generar bucles de red, debido a la existencia de puentes paralelos.

**ub-encapsulation**

Desactiva la encapsulación Ungermann-Bass OUI de tramas XNS. Las tramas XNS se reenvían tanto a Ethernet como a la red en anillo con encapsulación SNAP con un OUI con todo ceros.

**Ejemplo:** `disable ub-encapsulation`

## Enable

Utilice el mandato **enable** para activar las siguientes funciones de la conexión por puente:

- Conexión por puente
- Tramas duplicadas
- Correlación entre direcciones funcionales y de grupo
- Propagación de tramas exploradoras del árbol de expansión
- Direccionamiento de origen en un determinado puerto
- Conversión SR-TB
- Función de conexión por puente transparente (árbol de expansión) en un determinado puerto
- Característica de direcciones MAC duplicadas
- Equilibrio de cargas MAC duplicadas
- DLSw

**Sintaxis:**

**enable** bridge . . .

dls

duplicate

dmac-addr

dmac-load-balance

ethertype-ibmrt-pc

fa-ga-mapping

ibm8209-spanning-tree

ipx-conversion . . .

spanning-tree-explorer . . .

source-routing . . .

sr-tb-conversion

stp

transparent . . .

tree

ub-encapsulation

**bridge** Activa la función de conexión por puente transparente en todos los dispositivos de la LAN (interfaces) configurados en el dispositivo de conexión por puente. A cada interfaz se le asigna un número de puerto igual al número de interfaz anterior más 1. Por ejemplo, si la interfaz 0 es un dispositivo de la LAN, su número de puerto será 1.

**Ejemplo:** `enable bridge`

**dls** Activa la operación de DLSw del puente. El dispositivo que ejecuta DLSw aparece como un puente ante las estaciones finales. Consulte el tema “Utilización de DLSw” en la página 525 para obtener más información.

**Ejemplo:** `enable dls`

**duplicate** *tipo-trama*
Activa la generación de tramas STE (exploradoras del árbol de expansión) o TSF (tramas de expansión) duplicadas. Este mandato sirve para inhabilitar el mandato **disable duplicate**. La generación de tramas duplicadas está activada por omisión. El mandato **enable duplicate** puede ir seguido de un tipo de trama igual a **TSF** o a **STE** para activar específicamente uno de estos tipos de tramas, o bien puede ir seguido del tipo de trama **BOTH**, lo que equivale a no especificar ningún tipo de trama con este parámetro.

**Ejemplo:** `enable duplicate STE`

```
Port Number [1]?
```

**dmac-addr**
Activa la característica de direcciones MAC duplicadas. Consulte el tema “Característica de dirección MAC duplicada de SR-TB” en la página 57 para obtener información adicional sobre la característica de direcciones MAC duplicadas.

**Ejemplo con equilibrio de carga:**

```
ASRT config>enable dmac-addr

ASRT config>list dmac
Duplicate MAC address feature is    ENABLED
Load balance feature is   DISABLED
Age value for Duplicate MAC address :000000C8
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05

ASRT config>enable dmac-load-balance

ASRT config>li dmac
Duplicate MAC address feature is    ENABLED
Load balance feature is    ENABLED
Age value for Duplicate MAC address :000000C8
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05
```

**Ejemplo (sin equilibrio de carga):**

```
ASRT config>enable dmac-addr

ASRT config>list dmac
Duplicate MAC address feature is    ENABLED
Load balance feature is   DISABLED
Age value for Duplicate MAC address :000000C8
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05
```

### dmac-load-balance

Activa el equilibrio de carga de MAC duplicadas para la característica de direcciones MAC duplicadas. Consulte el tema “Característica de dirección MAC duplicada de SR-TB” en la página 57 para ver una descripción del equilibrio de carga de MAC duplicadas.

**Ejemplo:**

```
ASRT config>enable dmac-addr

ASRT config>list dmac
Duplicate MAC address feature is    ENABLED
Load balance feature is   DISABLED
Age value for Duplicate MAC address :000000C8
Duplicate MAC ADDRESSES CONFIGURED
================================
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05

ASRT config>enable dmac-load-balance

ASRT config>li dmac
Duplicate MAC address feature is    ENABLED
Load balance feature is    ENABLED
Age value for Duplicate MAC address :000000C8
Duplicate MAC ADDRESSES CONFIGURED
================================
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05
```

**ethertype-ibmrt-pc**

Activa la conversión de tramas SNA a formato Ethernet Tipo 2, utilizado por los RT de PC IBM que ejecutan OS/2 EE. Esto da lugar a que las tramas SNA se duplican en formatos 802.3/802.2 e IBM-RT para los sistemas principales desconocidos de una red Ethernet.

**Ejemplo: `enable ethertype-ibmrt-pc`**

```
            Port Number  [4]?
```

**fa-ga-mapping**

Activa la correlación dirección de grupo a dirección funcional (y viceversa). Esta correlación se realiza cuando se reenvían tramas entre una red en anillo y otro tipo de soporte (excepto una línea serie). En el entorno de red en anillo, las direcciones funcionales se utilizan con más frecuencia, aunque son direcciones de grupo asignadas localmente debido a las restricciones de hardware. En otros tipos de soporte, se utilizan con más frecuencia las direcciones de grupo. Bajo circunstancias normales, la correlación de direcciones de grupo a direcciones funcionales resulta inevitable.

La correlación está activada por omisión se se han añadido direcciones de correlación. La posibilidad de activar y desactivar la correlación permite a los usuarios elegir cuando se tienen que suprimir los registros de correlación añadidos.

**Ejemplo: `enable fa-ga-mapping`**

**ibm8209-spanning-tree**

Permite que los puentes participen en los protocolos de árbol de expansión con puentes IBM 8209.

**Ejemplo: `enable ibm8209-spanning-tree`**

**ipx-conversion**

Activa de forma global la conversión de tramas Novell IPX cuando se establece una conexión por puente entre puertos de puentes Ethernet/802.3 y Red en anillo (802.5). Cuando están activadas, las

tramas Novell se pueden conectar por puente entre estaciones finales de distintos soportes.

**Ejemplo:** `enable ipx-conversion`

**spanning-tree-explorer** *port#*

Deja que un puerto permita la propagación de tramas exploradoras del árbol de expansión si el direccionamiento de origen está activado. Este mandato sólo es válido en puertos de red en anillo y WAN. Esta característica está activada por omisión cuando el direccionamiento de origen está configurado en el puerto.

**Ejemplo:** `enable spanning-tree-explorer 2`

**source-routing** *núm. puerto núm. segmento [núm. puente]*

Activa el direccionamiento de origen para un determinado puerto. Este mandato se suele utilizar cuando se necesita un direccionamiento de origen en parte del puente. Si el direccionamiento de origen es la única característica que desea, se debe desactivar la conexión por puente transparente en la interfaz. La primera vez que emita el mandato, debe especificar el número de puente. Las veces siguientes, esta entrada no es obligatoria.

**núm. puerto**

Puerto válido que participa en la configuración del puente.

**Valores válidos**: X'0' a X'FFF'

**Valor por omisión**: 1

**núm. segmento**

Número de 12 bits que representa la LAN/WAN a la que está conectado el soporte. Todos los soportes de los demás puentes conectados a esta LAN/WAN se deben configurar con el mismo valor. Para que la función de direccionamiento de origen funcione correctamente, es importante que todos los puentes conectados a esta LAN/WAN tengan la misma perspectiva del valor de identificación de la LAN/WAN.

**núm. puente**

Valor de 4 bits exclusivo entre todos los puentes conectados a la misma LAN/WAN. Este valor es obligatorio cuando el direccionamiento de origen está activado en la primera interfaz. Para las demás interfaces, esta entrada es opcional. Se recomienda que el número de puente sea exclusivo en el segmento.

**Valores válidos**: X'0' a X'F'

**Valor por omisión**: 1

**Nota:** Si en la configuración hay dos segmentos ya configurados (es decir, se trata de una configuración SRB 1:N), se le solicitará un parámetro *núm. segmento-virtual* adicional.

**Ejemplo:** `enable source-routing 2 1 1`

**sr-tb-conversion**

Esta opción activa la conversión de formato de trama de direccionamiento de origen a conexión por puente transparente y viceversa. Permite la compatibilidad entre dominios de direccionamiento de

origen y de conexión por puente transparente. Cuando esta característica está activada, el puente permite que se acepten tramas de direccionamiento de origen en un dominio transparente, eliminando el campo RIF y convirtiéndolas en tramas transparente.

El puente también recopila información de direccionamiento sobre las estaciones de direccionamiento de origen de las tramas de direccionamiento de origen que se pasan. Esta información se obtiene del RIF. Esta información del RIF se utiliza para convertir una trama transparente en una trama de direccionamiento de origen. Si no hay ningún RIF disponible para una estación, la trama se envía como una trama exploradora del árbol de expansión al dominio de direccionamiento de origen.

Para que la función de conversión funcione correctamente, debe suministrar al dominio de puente transparente un número de segmento. Todos los puentes SR-TB que están conectados a este dominio se deben configurar con el mismo número de segmento.

**Valores válidos para el número de segmento del dominio TB**: X'1' - X'FFF'

**Valor por omisión para el número de segmento del dominio TB**: 1

La unidad máxima de transmisión (MTU) es el número de octetos por trama de datos que se pueden transferir a través de una determinada red física. Cuando un datagrama IP viaja de un sistema principal a otro, puede atravesar distintas redes físicas. Algunas redes físicas pueden tener tener definida esta MTU, que no permitirá que los datagramas IP largos se coloquen en una trama física. Se procederá a la fragmentación cuando intente transmitir tramas de tamaño superior al que puede manejar la red física.

**Valores válidos de MTU de dominio TB**: 576 a 18000 bytes

**Valor por omisión de MTU de dominio TB**: 2048

**Ejemplo: `enable sr-tb-conversion`**

```
TB-Domain Segment Number in hex(1 - FFF) [1]? 2
Bridge Virtual Segment Number in hex[1 - FFF]? aa
TB-Domain's MTU [1470]? 1455
TB-Domain's MTU is adjusted to 1350
```

**stp** Activa el protocolo del árbol de expansión en el puente. Es el valor por omisión.

**Ejemplo: `enable stp`**

**transparent** *núm. puerto*
Activa la función de conexión por puente transparente en un determinado puerto. Bajo circunstancias normales, este mandato no es necesario.

**Ejemplo: `enable transparent`**

```
Port Number [1]?
```

**tree** *núm. puerto*
Activa la participación de STP correspondiente al puente por puerto.

**Ejemplo: `enable tree 1`**

**ub-encapsulation**

Hace que las tramas XNS Ethernet Tipo 2 se conviertan en tramas de red en anillo mediante Ungermann-Bass OUI en la cabecera SNAP. Las tramas de red en anillo que contienen la cabecera UB OUI se reenvían a redes Ethernet como tramas 0x0600 Ethernet Tipo 2 en lugar de como tramas 802.3/802.2.

**Ejemplo:** `enable ub-encapsulation`

## List

Utilice el mandato **list** para ver información sobre la configuración completa del puente o para ver información sobre los parámetros de configuración seleccionados.

**Sintaxis:**

**list** address

bridge

dmac

filtering . . .

mapping . . .

multiaccess

permanent . . .

port . . .

prot-filter . . .

protocol

range . . .

**address** *valor dirección* Lee una entrada de dirección de la base de datos permanente. El valor dirección es la dirección MAC de la entrada necesaria. Puede ser una dirección individual, una dirección de difusión múltiple o una dirección de difusión general. Las bases de datos permanentes no se destruyen durante el proceso de encendido/apagado y son inmunes a los valores de antigüedad. Las entradas permanentes no se pueden sustituir por entradas dinámicas.

**Valores válidos**: X'0000 0000 0000' a X'FFFF FFFF FFFF'

**Valor por omisión**: ninguno

**Ejemplo:** `list address 000000123456`

```
0000-00-12-34-56    PERMANENT  Input Port:  1
                               Output ports:  1, 2
                               Input port:  2
                               Output ports:  3
ASRT config>
```

**Address** Entrada de dirección en formato hexadecimal de 12 dígitos.

**Tipo de entrada**

**Permanent**

Indica que la naturaleza de la entrada es permanente y no se modificará tras un

encendido/apagado o una restauración del sistema.

**Reserved**
Indica que la entrada está reservada por el comité IEEE 802.1d para un uso futuro. Las tramas destinadas a direcciones reservadas se eliminan.

**Registered**
Indica que la entrada va destinada al puente en sí.

**SAF** Aparece tras el tipo de entrada si se ha configurado la función de filtro de direcciones de origen.

**Input Port**
Muestra los números del puerto o puertos de entrada asociados a esta entrada de dirección.

**Output Port**
Muestra los números del puerto o puertos de salida asociados a esta entrada de dirección. Muestra “NONE/DAF” para indicar que la función de filtro de direcciones de destino se aplica porque no se ha seleccionado ningún puerto a asociar con esta entrada de dirección.

**bridge** Lista toda la información general correspondiente al puente.

**Ejemplo: `list bridge`**

```
Source Routing Transparent Bridge Configuration
===============================================

Bridge:  ENABLED                        Bridge Behavior: ADAPTIVE SRT
                 +----------------------------+
-----------------| SOURCE ROUTING INFORMATION |--------------------------
                 +----------------------------+
Bridge Number:         0A               Segments:          2
Max ARE Hop Cnt:       14               Max STE Hop cnt:  14
1: N SRB:              Active           Internal Segment:  0xFF6
LF-bit interpret:      Extended
                 +-------------------+
-----------------| SR-TB INFORMATION |---------------------------------
                 +-------------------+
SR-TB Conversion:       Enabled
TB-Virtual Segment:     0x107               MTU of TB-Domain:   1470
                 +-----------------------------------+
-----------------| SPANNING TREE PROTOCOL INFORMATION |-----------------
                 +-----------------------------------+
Bridge Address:        Default          Bridge Priority:     32768/0x8000
SRB Bridge Address:    Default          SRB Bridge Priority: 32768/0x8000
STP Participation:     IEEE802.1d and IBM-8209
                 +-------------------------+
-----------------| TRANSLATION INFORMATION |----------------------------
                 +-------------------------+
FA<=>GA Conversion:    Enabled                UB-Encapsulation:  Disabled
DLS for the bridge:    Enabled
IPX Conversion:        Enabled
Conversion Mode:       Automatic
Ethernet Preference:   IEEE-802.3
                 +------------------+
-----------------| PORT INFORMATION |-----------------------------------
                 +------------------+
Number of ports added:  3
Port:   1      Interface:     0      Behavior:   STB only    STB:  Enabled
Port:   2      Interface:     1      Behavior:   STB & SRB   STB:  Enabled
 Circuit number: 16
Port:   3      Interface:     2      Behavior:   STB & SRB   STB:  Enabled
Circuit number: 18
```

**Bridge** Indica el estado actual del puente. Los valores son ENABLED o DISABLED.

**Bridge Behavior**
Indica el método de conexión por puente que utiliza este puente. Los valores incluyen STB para transparente, SRB para direccionamiento de origen y SRT ADAPTABLE para la conexión por puente de conversión de direccionamiento de origen a transparente.

**Bridge Number**
El número exclusivo que identifica un puente. Se utiliza para distinguir entre varios puentes que conectan los mismos anillos.

**Segments**
Indica el número de segmentos del puente de direccionamiento de origen configurados para el dominio de direccionamiento de origen.

**Max ARE/STE Hop cnt**
El número máximo de saltos para la transmisión de tramas desde el puente para una determinada interfaz asociada con la conexión por puente de direccionamiento de origen.

**1:N SRB** Indica el estado actual del direccionamiento de origen 1:N como ACTIVO o NO ACTIVO.

**Internal Segment**
Muestra el número de segmento virtual configurado para la conexión por puente SRB 1:N.

**LF-bit interpretation**
Indica la modalidad de interpretación de la codificación del bit de trama de mayor tamaño (LF) si el direccionamiento de origen está activado en este puente. El valor puede ser BASIC o EXTENDED.

**SR-TB Conversion**
Indica si la función de conversión de tramas de direccionamiento de origen/puente transparente está activada o desactivada.

**TB-Virtual Segment**
Indica el número de segmento del dominio de la conexión por puente transparente.

**MTU for TB-Domain**
Especifica el tamaño máximo de trama (número máximo de unidades de transmisión) que el puente transparente puede transmitir y recibir.

**Bridge address**
Dirección de puente especificada por el usuario (si está definida).

**Bridge priority**
Una dirección de puente superior de 2 octetos que se encuentra en el Identificador de puente, que puede ser la

dirección MAC obtenida del puerto de número menor o la dirección definida por el mandato Set Bridge.

**STP Participation**
Muestra los tipos de protocolos de árbol de expansión en los que participa el puente.

**FA-GA conversion**
Indica si la conversión FA-GA está activada o desactivada.

**UB Encapsulation**
Indica si la encapsulación UB está activada o desactivada.

**DLS for the bridge**
Indica si el protocolo de Conmutación de enlace de datos está activado o desactivado en el puente.

**IPX Conversion**
Indica si la conversión IPX está activada o desactivada.

**Conversion Mode**
Indica la Modalidad de conversión IPX como automática o manual.

**Ethernet Preference**
Indica el tipo de trama Ethernet preferido para la conversión IPX como IEEE-802.3 o Ethernet.

**Number of ports added**
Número de puertos de puente añadidos a la configuración de la conexión por puente.

**Port Number**
Número definido por el usuario asignado a una interfaz mediante el mandato Add Port.

**Interface Number**
Identifica los dispositivos conectados a un segmento de la red a través del puente. Debe añadir al menos dos interfaces para que participen el la conexión por puente. Se utiliza el número de interfaz 255 para la conexión por puente.

**Port Behavior**
Indica el método de conexión por puente que utiliza este puerto, STB para la conexión por puente transparente y SRB para la conexión por puente de direccionamiento de origen.

**VPI** Especifica la VPI asociada con el puerto ATM.

**VCI** Especifica la VCI asociada con el puerto ATM.

**Circuit Number**
Especifica la DLCI asociada con el puerto Frame Relay.

**dmac** Muestra las opciones configuradas para la característica de direcciones MAC duplicadas.

**Example:** `list dmac`

```
Duplicate MAC address feature is    ENABLED
Load balance feature is   DISABLED
Age value for Duplicate MAC address :000000C8
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05
```

**filtering** *opción-grupodatos* Se pueden visualizar los siguientes grupos de datos generales bajo el mandato **list filtering**:

*All* Muestra todas las entradas de la base de datos de la función de filtro.

*Ethertype* Muestra las entradas de la base de datos del filtro de tipo protocolo Ethernet.

*SAP* Muestra las entradas de la base de datos del filtro del protocolo SAP.

*SNAP* Muestra las entradas de la base de datos del filtro de identificador de protocolo SNAP.

Los siguientes ejemplos ilustran cada una de las opciones de visualización de **list filtering**.

**Ejemplo 1: `list filtering all`**

```
Ethernet type 0800 is routed on ports 1
IEEE 802.2 destination SAP 42 is routed on ports 1
IEEE 802 SNAP PID 00-00-00-08-00 is routed on ports 2-3
```

Los descriptores utilizados para explicar cómo se comunican los paquetes incluyen:

**Routed** Describe paquetes que se pasan a un distribuidor de direccionamiento para que los reenvíe.

**Filtered** Describe paquetes que son filtros de protocolo de valor de filtro administrativo que define el usuario.

**Bridged and routed**
Describe un identificador de protocolo para el que hay una entidad de protocolo dentro del sistema que no es un distribuidor. Por ejemplo, un protocolo de eco de nivel de enlace. Los paquetes de difusión individual procedentes de este protocolo se conectan por puente o se procesan localmente si se tienen que enviar a una dirección registrada. Los paquetes de difusión múltiple se reenvían y se procesan localmente para una dirección de difusión múltiple registrada.

Todos estos descriptores se aplican también a paquetes ARP con este Ethertype.

**Ejemplo 2: `list filtering ethertype`**

```
Ethernet type (in hexadecimal), 0 for all [0]? 0800
Ethernet type 0800 is routed on ports 1
```

**Ejemplo 3: `list filtering sap`**

```
SAP (in hexadecimal), 100 for all [100]? 42
IEEE 802.2 destination SAP 42 is routed on ports 1
```

**Ejemplo 4: `list filtering snap`**

```
SNAP Protocol ID, return for all [00-00-00-00-00]?
IEEE 802 SNAP PID 00-00-00-08-00 is routed on ports 2-3
```

**mapping** *tipo-añadir campo-tipo* Lista correlaciones específicas de direcciones para un determinado protocolo.

**Ejemplo: `list mapping SNAP`**

```
PROTOCOL TYPE          GROUP ADDRESS          FUNCTIONAL ADDRESS
=============          =============          ==================
123456-7890            12-34-56-78-90-12      12:34:56:78:90:12
```

**tipo-añadir**

Puede ser DSAP, Ether (Ethernet) o SNAP.

**campo-tipo**

Campo de tipo de protocolo:

- El tipo de protocolo Punto de acceso de servicio de destino (DSAP) se entra en el rango 1–FE (hexadecimal).
- El tipo de protocolo Ethernet (Ether) se entra en el rango 5DD–FFFF (hexadecimal).
- El tipo de protocolo del Protocolo de acceso de subred (SNAP) se entra en formato hexadecimal de 10 dígitos.

**multiaccess** Muestra el periodo de antigüedad de las entradas de la base de datos multiacceso y muestra los puertos del puente multiacceso. Consulte la salida del mandato **list port** para ver una descripción de los parámetros de puerto de puente.

**Ejemplo:** `list multiaccess`

```
Aging time (in seconds): 300

Port ID (dec)    : 238:02, (hex): 80-02
Port State       : Enabled
STP Participation: Disabled
Port Supports    : Source Route Bridging Only
SRB: Segment Number: 0x003       MTU:  2040     STE: Enabled
Assoc Interface  : 1
Path Cost        : 0
```

**permanent** Muestra el número de entradas de la base de datos permanente del puente.

**Ejemplo: `list permanent`**

```
Number of Entries in Permanent Database:  17
```

**port** *núm. puerto* Muestra información de puerto relacionada con los puertos que ya están configurados. Núm. puerto selecciona el puerto que desea listar. Si no especifica ningún número, se seleccionan todos los puertos.

**Ejemplo: `list port`**

```
Port Id (dec)    : 128: 5, (hex): 80-05
Port State       : Enabled
STP Participation: Enabled
Port Supports    : NO Bridging
Assoc Interface  : 1
Path Cost        : 0
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Port Id (dec)    : 128: 6, (hex): 80-06
Port State       : FORWARDING
STP Participation: Enabled
Port Supports: Source Routing Bridging Only
SRB: Segment Number:  Ox116     MTU:  1979
STE Forwarding:  Auto
Assoc Interface #/name : 1/FR/0   Circuit number 16
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Port Id (dec)    : 128: 7, (hex): 80-07
Port State       : FORWARDING
STP Participation: Enabled
Port Supports: Source Routing Bridging Only
SRB: Segment Number:  Ox117     MTU:  1979
STE Forwarding:  Auto
Assoc Interface #/name : 1/FR/0   Circuit number 17
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Port ID (dec)    : 128: 2, (hex): 80-02
Port State       : Enabled
STP Participation: Enabled
Port Supports    : Transparent Bridging Only
Assoc Interface  : 0  VPI  0  VCI:    78
Path Cost        : 0
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Port ID (dec)    : 128: 3, (hex): 80-03
Port State       : Enabled
STP Participation: Enabled
Port Supports    : Transparent Bridging Only
Assoc Interface  : 2
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
 Port ID (dec)    : 128: 1, (hex): 80-01
 Port State       : Enabled
 STP Participation: Enabled
 Port Supports    : Transparent Bridging Only
 Assoc Interface  : 0  VPI:   0  VCI:   795
 Path Cost        : 0
 ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
 Port ID (dec)    : 128: 4, (hex): 80-04
 Port State       : Enabled
 STP Participation: Enabled
 Port Supports    : Transparent Bridging Only
 Assoc Interface  : 0  Dest ATM Addr: 391122334455667788990011223344
                                                              5566778899
 Path Cost        : 0
 ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

**Port ID** El ID consta de dos partes: la prioridad de puerto y el número de puerto. En el ejemplo, 128 es la prioridad y 1, 2 y 3 son los números de puerto. En formato hexadecimal, el byte inferior indica el número de puerto y los bytes superiores indican la prioridad.

**Port state**

Muestra el estado actual del puerto o puertos especificados. Puede ser ENABLED o DESABLES.

**Port supports**

Muestra el método de conexión al que da soporte este puerto (por ejemplo, conexión por puente transparente).

**SRB** Sólo se muestra cuando SRB está activado y muestra información sobre la conexión por puente de direccionamiento de origen. Esto incluye el número de segmento SRB (in hex), el tamaño máximo de unidad de transmisión y si está activada o desactivada la transmisión de tramas exploradoras del árbol de expansión.

**Duplicate Frames Allowed**
Muestra un desglose y el número de tipos de tramas duplicadas permitidas.

**Assoc interface**
Muestra el número de la interfaz asociada al puerto visualizado. También muestra la VPI/VCI o la dirección ATM de destino si hay un puerto en una interfaz ATM.

**Path Cost**
Coste asociado al puerto que se utiliza para un posible coste de vía de acceso raíz. El rango es de 1 a 65535.

**prot-filter** *núm. puerto* Lee una lista actual de los tipos de protocolos de filtro. Los filtros se pueden listar de forma selectiva por puerto o se pueden visualizar todos los puertos simultáneamente. Núm puerto selecciona el número de puente que desea listar.

**Ejemplo:** **`list prot-filter 1`**

```
PORT 1
Protocol Class   :  DSAP
Protocol Type    :  01
Protocol State:  :  Filtered
Port Map         :  1, 2, 3
```

**Número puerto**
Se visualiza el número de puerto correspondiente a cada puerto, en el caso de que se seleccionen todos los puertos.

**Protocol Class**
Muestra la clase de protocolo (SNAP, Ether o DSAP).

**Protocol Type**
Muestra el ID de protocolo en formato hexadecimal.

**Protocol State**
Indica que se está filtrando el protocolo correspondiente al puerto seleccionado.

**Port Map** Muestra los números de los puertos en los que está presente este tipo de filtro de protocolos.

**protocol** Muestra información de puente relacionada con el protocolo del árbol de expansión.

**Ejemplo:** **`list protocol`**

```
IEEE 802.1d Spanning Tree Configuration:
 Bridge Identifier                : 32768/000000000000 (using port address)
 Bridge-Max-Age (in seconds)      : 20
 Bridge-Hello-Time (in seconds)   : 2
 Bridge-Forward-Delay (in seconds): 15

SRB Spanning Tree Configuration:
 Bridge Identifier                : 32768/000000000000 (using port address)
 Bridge-Max-Age (in seconds)      : 20
 Bridge-Hello-Time (in seconds)   : 2
 Bridge-Forward-Delay (in seconds): 15
```

**Nota:** Cada uno de estos parámetros relacionados con el puente se describen con detalle en el capítulo anterior.

**Bridge Identifier**
Valor de 8 bytes en formato ASCII. Si no ha definido la dirección del puente antes de visualizar esta información, los 6 bytes inferiores aparecerán con el valor cero, lo que indica que se utiliza la dirección MAC por omisión de un puerto. Cuando se ha seleccionado un puente como puente raíz, el puente transmite su antigüedad máxima de puente y su tiempo Hello de puente a todos los puentes de la red mediante BPDU tipo Hello.

**Bridge-Max-Age**
Antigüedad máxima (periodo de tiempo) que se debe utilizar para calcular el tiempo de espera de la información relacionada con el árbol de expansión.

**Bridge-Hello-Timer**
Intervalo de tiempo entre BPDU tipo HELLO.

**Bridge-Forward-Delay**
Intervalo de tiempo empleado antes de pasar a otro estado (si este puente tiene que convertirse en raíz).

**range** *índice-inicio índice-detención* Lee un rango de entradas de direcciones de la base de datos permanente. Para especificarlo, antes debe determinar el tamaño de la base de datos mediante el mandato **list permanent**. A partir de este valor puede determinar un valor "índice-inicio" para su rango inicial. El índice de inicio está en el rango comprendido entre 1 y el tamaño de la base de datos. Luego puede elegir un "índice-detención" para visualizar un número limitado de entradas. Esta entrada es opcional. Si no especifica el índice de detención, el valor por omisión es el tamaño de la base de datos.

Las entradas de direcciones contienen la siguiente información:

**Ejemplo: `list range`**

```
Start-Index [1]? 1
Stop-index [17]? 6
ADDRESS                 ENTRY TYPE      PORT MAP

=======                 ==========      ========
01-80-C2-00-00-00       REGISTERED      Input Port:  ALL PORTS
                                        Output ports:

01-80-C2-00-00-01       RESERVED        NONE/DAF
01-80-C2-00-00-02       RESERVED        NONE/DAF
01-80-C2-00-00-03       RESERVED        NONE/DAF
01-80-C2-00-00-04       RESERVED        NONE/DAF
01-80-C2-00-00-05       RESERVED        NONE/DAF
```

**Address** Dirección MAC de 6 bytes de la entrada.

**Type of Entry**
Especifica uno de los siguientes tipos:

- Reserved - entradas reservadas por el comité IEEE 802.1d
- Registered - entradas que constan de direcciones de difusión individual que pertenecen al hardware de comunicaciones conectado al recuadro o de direcciones de difusión múltiple activadas por distribuidores de protocolos

- Permanent - entradas que especifica el usuario en el proceso de configuración y que no se modifican tras procesos de encendido/apagado o de restauración del sistema.
- Static - entradas que especifica el usuario en el proceso de supervisión, que no se conservan tras un proceso de encendido/apagado o de restauración del sistema y que no tienen antigüedad
- Dynamic - entradas “aprendidas” por el puente “de forma dinámica” que no se conservan tras un proceso de encendido/apagado o de restauración del sistema y que tienen una “antigüedad” asociada
- Free - ubicaciones de la base de datos que están libres y se pueden rellenar con entradas de direcciones

**Port Map** Muestra una correlación de puertos de salida para todos los puertos de entrada.

## NetBIOS

Muestra el indicador de configuración de NetBIOS. Entre **netbios** en el indicador `ASRT config>` para que aparezca el indicador de configuración de NetBIOS. Consulte el tema “Mandatos de NetBIOS” en la página 178 para ver una explicación de cada uno de los mandatos de configuración de NetBIOS.

**Sintaxis:**

netbios

**Ejemplo:** **`netbios`**

```
NetBIOS Support User Configuration
NetBIOS config>
```

**Nota:** Si no ha adquirido la característica de función de filtro de NetBIOS, recibirá el siguiente mensaje si utiliza este mandato:

```
NetBIOS Filtering is not available in this load.
```

## Set

Utilice el mandato **set** para definir determinados valores, funciones y parámetros asociados a la configuración del puente. Estos incluyen:

- Periodo de antigüedad correspondiente a entradas de direcciones dinámicas de la base de datos de la función de filtro
- Dirección de puente
- Modalidad de conversión IPX y preferencia Ethernet
- Interpretación de la codificación de bits de la trama de mayor tamaño (LF) para el direccionamiento de origen
- Tamaño de la unidad de datos del servicio MAC (MSDU)
- Parámetros de puerto y puente del protocolo de árbol de expansión
- Límite del Descriptor de ruta (RD)
- Tamaño de la base de datos de la función de filtro del puente
- Periodo de antigüedad correspondiente a los RIF asociados a direcciones MAC duplicadas
- Periodo de antigüedad correspondiente a las entradas de la base de datos multiacceso

**Sintaxis:**

| | |
|---|---|
| s**et** | age |
| | bridge |
| | conversion-mode |
| | ethernet-preference |
| | dmac-age |
| | filtering |
| | lf-bit-interpretation . . . |
| | maximum-packet-size . . . |
| | multiaccess-age . . . |
| | port |
| | protocol bridge |
| | protocol port . . . |
| | route-descriptor-limit . . . |

**age** *seconds resolution*

Define el periodo de caducidad de las entradas dinámicas de la base de datos de la función de filtro cuando el puerto con la entrada está en el estado de reenvío. Esta antigüedad también se utiliza para la caducidad de las entradas RIF de la base de datos adaptable en el caso de una personalidad de puente SR-TB.

Entre el valor que desee después de cada indicador y pulse **Intro**.

**Valores válidos de periodo de antigüedad**: 10 a 1000000

**Valor por omisión de periodo de antigüedad**: 30

El valor de resolución especifica la frecuencia con que las entradas dinámicas de la base de datos de la función de filtro se deben explorar para determinar si han superado su límite de antigüedad, definido por el temporizador de caducidad.

**Valores válidos de resolución**: 1 a 60 segundos

**Valor por omisión para la resolución**: 5 segundos

**Ejemplo:** **`set age`**

```
seconds [300]  ?  400
resolution [5] ?  6
```

**bridge** *bridge-address*

Define la dirección del puente. Se trata de la dirección del puente de los 6 octetos inferiores del identificador del puente. Por omisión, el valor de dirección de puente se define en el control de acceso al medio (MAC) dirección del puerto que número menor en el momento de la inicialización. Puede utilizar este mandato para alterar temporalmente la dirección por omisión y entrar su propia dirección exclusiva.

Entre *srb* o *tb* para especificar si esto debe afectar a la dirección del puente de direccionamiento de origen (srb) o del puente transparente (tb).

**Nota:** Cada puente de la red debe tener una dirección exclusiva para que el protocolo de árbol de expansión funcione correctamente.

**Atención:** En el caso de que la interfaz de línea serie (o túnel) sea el puerto con número menor, es obligatorio utilizar este mandato para que el puente tenga una dirección exclusiva cuando se vuelva a arrancar. Este proceso es necesario porque las línea serie no tienen su propia dirección MAC.

En el indicador, entre la dirección del puente en formato hexadecimal de 12 dígitos y pulse **Intro**.

Si entra la dirección en un formato incorrecto, recibirá el mensaje `Illegal Address`. Si no entra ninguna dirección en el indicador, recibirá el mensaje `Zero length address supplied` y el puente conservará su valor anterior. Para volver a suministrar al puente el valor por omisión, entre una dirección que sólo contenga ceros.

**Valores válidos**: 12 dígitos hexadecimales

No utilice guiones ni símbolos de dos puntos para separar cada octeto. Cada puente de la red debe tener una dirección exclusiva para que el protocolo de árbol de expansión funcione correctamente.

**Valor por omisión**: 000000000000

**Ejemplo:** **`set bridge`**

```
Bridge Address (in 12-digit hex)[]?
```

**conversion-mode** *modalidad*

Especifica la modalidad de conversión IPX, que puede ser automática o manual.

**modalidad**

Cuando se define una modalidad de conversión automática, el tipo de trama IPX de cada estación final Ethernet/802.3 se aprende y se guarda en la base de datos de la función de filtro, y se utilizará en las siguientes conversiones al formato de MAC Ethernet/802.3. El parámetro Preferencia Ethernet determina qué tipo de trama IPX se debe utilizar al convertir al formato de MAC Ethernet /802.3 en el caso de que no se haya aprendido ninguna.

Cuando el valor de la modalidad de conversión es manual, el valor del parámetro Preferencia Ethernet especifica en qué tramas IPX Ethernet/802.3 se debe realizar la conversión.

**Valores válidos de modalidad de conversión**: automatic o manual

**Valor por omisión de la modalidad de conversión**: automatic

**Ejemplo:** **`set conversion-mode manual`**

**ethernet-preference** *preferencia*

Especifica el tipo de trama IPX preferida, que puede ser IEEE-802.3 o Ethernet.

**preferencia** Cuando el valor de la modalidad de conversión es automatic, el tipo de trama IPX de cada estación final Ethernet/802.3 se aprende y se guarda en la base de datos de la función de filtro, y se utiliza en las futuras conversiones al formato de MAC Ethernet/802.3. El parámetro Preferencia

Ethernet determina qué tipo de trama IPX se debe utilizar al convertir al formato de MAC Ethernet /802.3 en el caso de que no se haya aprendido ninguna.

Cuando el valor de la modalidad de conversión es manual, el valor del parámetro Preferencia Ethernet especifica en qué tramas IPX Ethernet/802.3 se debe realizar la conversión.

**Valores válidos de preferencia Ethernet**: ieee-802.3 o ethernet

**Valor por omisión de preferencia Ethernet**: ieee-802.3

**Ejemplo:** `set ethernet-preference ethernet`

**dmac-age** *segundos*

Define el periodo de caducidad de las entradas RIF de la tabla RIF correspondiente a direcciones MAC duplicadas. Este valor sólo se utiliza para las direcciones MAC duplicadas aprendidas. Para las demás direcciones, se utiliza el valor del mandato **set age** para calcular el periodo de caducidad.

Entre el valor que desee después de cada indicador y pulse **Intro**.

**Valores válidos de periodo de caducidad DMAC**: 10 a 1000000

**Valor por omisión de periodo de caducidad DMAC**: 300

**Ejemplo:** `set dmac-age`

```
seconds [300]? 200
ASRT config>list dmac
Duplicate MAC address feature is   DISABLED
Load balance feature is   DISABLED
Age value for Duplicate MAC address :000000C8
Duplicate MAC ADDRESSES CONFIGURED
================================
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05
```

**filtering** *database-size*

Define el número de entradas que se pueden conservar en la base de datos de función de filtro del puente.

**Valor por omisión**: 1024 multiplicado por el número de puertos del puente.

Para obtener más información, consulte el mandato **list filtering** en la página 109.

**Ejemplo:** `set filtering`

```
database-size [2048]?
```

**lf-bit-interpretation** *modalidad-codificación*

Define la interpretación de la codificación del bit de Trama de mayor tamaño (LF) si el direccionamiento de origen está activado en este puente.

**Ejemplo:** `set lf-bit-interpretation basic`

**modalidad-codificación**

Puede tener el valor **basic** o **extended**. En la modalidad basic, sólo se utilizan 3 bits del campo de control de direccionamiento. Es el valor que se suele utilizar en los puentes de direccionamiento de origen actuales. En la modalidad extended, se utilizan 6 bits del campo de control de direccionamiento para representar la unidad máxima de datos a la que da soporte el puente. El valor por omisión es **extended**. Los nodos tipo extended y tipo basic son compatibles.

**maximum-packet-size** *núm. puerto tamaño-msdu*

Define el tamaño mayor posible de la unidad de datos de servicio MAC (MSDU) para el puerto, si el direccionamiento de origen está activado en este puerto. El valor de MSDU no tiene ningún efecto sobre el soporte transparente tradicional. Un valor de MSDU superior al tamaño del paquete configurado en el dispositivo se tratará como un error.

Si no se define este parámetro, el valor por omisión utilizado es el tamaño configurado como tamaño de paquete para esta interfaz.

**Valores válidos**: Especifique un entero comprendido entre 16 y 65535

**Valor por omisión**: tamaño de paquete definido para este puerto

**Ejemplo:** `set maximum-packet-size 1 4399`

**multiaccess-age** *segundos*

Define el periodo de caducidad correspondiente a las entradas de la base de datos multiacceso. La base de datos se explora a la velocidad definida por el parámetro *resolution* del mandato **set age**.

**Valores válidos:** 1 a 1 000 000

**Valor por omisión:** 300

**Ejemplo:** set multiaccess-age

```
seconds [300]? 500
```

**port** *block* **o** *disable*

Comienza la participación del puerto en el protocolo del árbol de expansión. Esto se lleva a cabo entrando un valor de estado igual a “block”, lo que coloca en puerto en el estado “bloqueado” como punto de inicio. El estado real del puerto lo determina posteriormente el protocolo del árbol de expansión cuando determina su topología. Si entra un valor igual a “disable”, el puerto no participa en el árbol de expansión.

**Ejemplo:** **set port block**

```
Port Number [1]?
```

**protocol** *bridge* **o** *port*

Modifica los parámetros de puerto o de puente del protocolo de árbol de expansión correspondientes a una nueva configuración, o bien ajusta los parámetros de configuración para que se ajusten a una determinada topología.

Entre “bridge” como opción para modificar parámetros del puente. Los parámetros relacionados con el puente que se pueden modificar con este mandato se muestran a continuación.

Entre **srb** o **tb** para especificar si esto debe afectar a los parámetros de protocolo de árbol de expansión del puente de direccionamiento de origen (srb) o del puente transparente (tb).

Al definir estos valores, asegúrese de que existen las siguientes relaciones entre los parámetros o la entrada se rechazará:

*2 X (Bridge Forward Delay - 1 segundo) ≥ Bridge Maximum Age*
*Bridge Maximum Age ≥ 2 X (Bridge Hello Time + 1 segundo)*

**Ejemplo:** **set protocol bridge tb**

```
Bridge Max-Age [20]  25
Bridge Hello Time [2]   3
Bridge Forward Delay [15] 20
Bridge Priority [32768]    1
```

**Bridge Maximum Age**

Antigüedad máxima (periodo de tiempo) que se debe utilizar para calcular el tiempo de espera de la información relacionada con el árbol de expansión.

Cuando se selecciona este dispositivo de conexión por puente como el puente raíz de un árbol de expansión, el valor de este parámetro especifica el intervalo de tiempo que los demás puentes activos deben guardar las unidades de datos del protocolo de puente (BPDU) de configuración que reciben. Cuando una BPDU alcanza su límite máximo de antigüedad sin que se sustituya, los puentes activos de la

red la eliminan y dan por supuesto que el puente raíz ha fallado. A continuación se selecciona un nuevo puente raíz.

**Dependencias**

El valor de este parámetro se puede ver afectado por el valor del parámetro Tiempo Hello del puente. Además, el valor de este parámetro puede afectar al valor del parámetro Retraso reenvío del puente.

**Valores válidos**: 6 a 40 segundos

**Valor por omisión**: 20 segundos

**Bridge Hello Timer**

Intervalo de tiempo entre BPDU tipo HELLO.

Cuando se selecciona este dispositivo de conexión por puente como el puente raíz del árbol de expansión, este parámetro especifica la frecuencia con que este puente transmite unidades de datos del protocolo de puente (BPDU) de configuración. Las BPDU contienen información sobre la topología del árbol de expansión y reflejan los campos efectuados en la topología.

**Dependencias**

El valor de este parámetro puede afectar al valor del parámetro Antigüedad máxima.

**Valores válidos**: 1 a 10 segundos

**Valor por omisión**: 2

**Bridge Forward Delay**

Intervalo de tiempo empleado antes de pasar a otro estado (si este puente tiene que convertirse en raíz).

Cuando se selecciona este dispositivo de conexión por puente como el puente raíz de un árbol de expansión, el valor de este parámetro especifica el tiempo en que los puertos activos de todos los puentes permanecen en un *estado de escucha*. Una vez transcurrido el intervalo de retraso de reenvío, los puertos que se encuentran en estado de escucha pasan al *estado de reenvío*. El estado cambia como resultado de cambios en la topología del árbol de expansión, como por ejemplo cuando un puente activo falla o se concluye.

El puente raíz transmite este valor a todos los puentes. Este proceso asegura que todos los puentes son coherentes entre cambios.

**Dependencias**

El valor de este parámetro se puede ver afectado por el valor del parámetro Antigüedad máxima del puente SRB.

**Valores válidos**: 4 a 30 segundos

**Valor por omisión**: 15

**Bridge Priority**

Una dirección de puente superior de 2 octetos que se encuentra en el Identificador de puente, que puede ser la dirección MAC obtenida del puerto de número menor o la dirección definida por el mandato **Set Bridge**.

La prioridad del puente indica la probabilidad de que este puente se convierta en el puente raíz del árbol de expansión. Cuanto menor sea el valor numérico del parámetro de prioridad de puente, mayor es la prioridad del puente y más probable es que sea seleccionado. El algoritmo del árbol de expansión selecciona como puente raíz el puente con el valor numérico menor de este parámetro.

**Valores válidos**: 0 a 65535

**Valor por omisión**: 32768

Entre **port** como opción para modificar los parámetros de puerto del protocolo de árbol de expansión. Entre el valor que desee en cada indicador y pulse **Intro**.

**Ejemplo:** `set protocol port`

```
Port Number [1] ?
Port Path-Cost (0 for default) [0] ?   1
Port Priority [128] ?   1
```

**Port Number**

Número del puerto del puente; selecciona el puerto para que el que se modificarán el coste de vía de acceso y la prioridad de puerto.

**Path Cost**

Coste asociado al puerto que se utiliza para un posible coste de vía de acceso raíz.

Cada interfaz de puerto tiene un coste de vía de acceso asociado, que es el valor relativo de utilizar dicho puerto para alcanzar el puente raíz de una red conectada por puente. El algoritmo de árbol de expansión utiliza el coste de vía de acceso para calcular la vía de acceso que minimiza el coste desde el puente raíz a los demás puentes de la topología de red.

Este parámetro especifica el coste asociado a pasar tramas a través de esta interfaz de puerto, en el caso de que este dispositivo de conexión por puente se convierta en el puente raíz. Aplique un factor a este valor al determinar rutas del árbol de expansión entre dos estaciones cualesquiera. Un valor igual a 0 indica al dispositivo de conexión por puente que calcule de forma automática un coste de vía de acceso correspondiente a este puerto utilizando su propia fórmula.

**Valores válidos**: 1 a 65535

**Valor por omisión**: 0 (significa que el coste se calculará de forma automática)

**Port Priority**

Identifica la prioridad de puerto correspondiente al puerto especificado. El algoritmo del árbol de expansión utiliza este valor para realizar comparaciones para la selección del puerto (qué puerto ofrece el menor coste de vía de acceso al puente raíz) y para tomar decisiones sobre bloqueos.

**Valores válidos**: 0 a 255

**Valor por omisión**: 128

**route-descriptor-limit** *tipo-límite*

Permite al usuario asociar una longitud máxima del Descriptor de ruta (RD) para todas las tramas exploradoras de ruta (ARE) o exploradoras del árbol de expansión (STE) que reenvía el puente si el direccionamiento de origen está activado.

**Ejemplo:** `set route-descriptor-limit ARE`

**Tipo-límite**

Puede adoptar el valor ARE o STE, en función de si se aplica el valor-límite-RD a todas las tramas exploradoras de ruta (ARE) o exploradoras del árbol de expansión (STE). Luego se le solicitará un valor-límite-RD.

**Valor-límite-RD**

Especifica el número máximo de RD que puede contener el campo de información de direccionamiento (RIF) del tipo de trama especificado por el tipo de límite RD.

El número de saltos correspondiente a cada trama es el número de puentes por los que ha viajado la trama hasta el momento. Se añade un RD al Campo de información de direccionamiento cada vez que la trama pasa a través de un puente. Por lo tanto, el número de RD es igual al número de saltos. Cuando el número de RD (saltos) supera el número de saltos permitido por este parámetro, la trama se elimina.

**Valores válidos**: 0 a 14

**Valor por omisión**: 14

# Tunnel

Utilice el mandato **tunnel** para acceder al indicador de configuración de túnel. Los mandatos de configuración de túnel se entran en este indicador. Consulte el tema “Mandatos de configuración de túnel” en la página 124 para ver una explicación de cada uno de estos mandatos.

**Sintaxis:**

**tunnel**

## Mandatos de configuración de BAN

Esta sección describe todos los mandatos de configuración de BAN (nodo límite de acceso). Estos mandatos le permiten configurar BAN como una característica añadida de la conexión por puente ASRT o de DLSw.

**Nota:** Los mandatos de configuración de BAN no entran en vigor de forma inmediata. Permanecen pendientes hasta que vuelve a arrancar o vuelve a cargar el dispositivo.

Los mandatos de configuración se entran en el indicador `BAN config>`. Para acceder a este indicador, entre el mandato ban en el indicador `ASRT config>` o en el indicador `DLSw config`. La Tabla 5 muestra los mandatos de configuración de BAN.

*Tabla 5. Mandatos de configuración de BAN*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Add | Añade un puerto de BAN. |
| Delete | Suprime un puerto de BAN. |
| List | Muestra toda la información sobre los puertos de BAN. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Respuesta a mandatos de configuración de BAN

Los mandatos de configuración de BAN (Talk 6) no entran en vigor de forma inmediata. Permanecen pendientes hasta que emite el mandato **reload** o **restart**.

## Add

Utilice el mandato **add** para añadir un puerto de BAN a la configuración de BAN. Si no especifica un número de puerto con este mandato, se le solicitará el número de puerto.

**Sintaxis:**

a**dd** *núm. puerto*

**Ejemplo:** **add**

```
Port Number [0]? 3.
Enter the BAN DLCI MAC Address []? 400012345678
Enter the Boundary Node Identifier MAC Address [4FFF00000000]?
Do you want the traffic bridged (b) or DLSw terminated (t) (b/t) [b]
```

## Delete

Utilice el mandato **delete** para suprimir un puerto de BAN de la configuración de BAN. Si no especifica un número de puerto con este mandato, se le solicitará el número de puerto.

**Sintaxis:**

d**elete** *núm. puerto*

**Ejemplo:** `delete 3`

## List

Utilice el mandato **list** para listar información sobre todos los puertos de BAN. La información que se muestra incluye el número de puerto de BAN, la dirección MAC correspondiente a BAN DLCI y si las tramas manejadas por el puerto se conectan por puente o el LLC se termina con DLSw.

**Sintaxis:** list

l**ist**

**Ejemplo:** `list`

```
bridge  BAN                Boundary           bridged or
port    DLCI MAC Address   Node Identifier    DLSw terminated
2       40:00:11:22:33:44  4F:FF:00:00:00:00  bridged
3       40:00:55:66:77:88  4F:FF:00:00:00:00  bridged
```

# Mandatos de configuración de túnel

Esta sección describe los mandatos de configuración de túnel. Los mandatos de configuración de túnel le permiten especificar parámetros de red correspondientes a un túnel que transmite tramas de conexión por puente sobre IP.

**Nota:** Los mandatos de configuración de túnel no entran en vigor de forma inmediata. Debe volver a arrancar o volver a cargar el dispositivo para que entren en vigor.

Los mandatos de configuración del túnel se entran en el indicador `TNL config>`. Para acceder a este indicador, entre el mandato **tunnel** en el indicador `ASRT config>`.La Tabla 6 en la página 125 muestra los mandatos de configuración de túnel.

*Tabla 6. Mandatos de configuración de túnel*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Add | Añade la dirección IP de puentes de destino que participan en una configuración de direcciones de difusión múltiple o difusión individual IP para conectar por puente sobre IP. |
| Delete | Suprime la dirección IP de un puente de destino que participa en una configuración de direcciones de difusión múltiple o difusión individual IP para conectar por puente sobre IP. |
| Join | Configura el dispositivo como un miembro de uno o más grupos de difusión múltiple. |
| Leave | Elimina el dispositivo como miembro de grupos de difusión múltiple. |
| List | Muestra las direcciones IP de las estaciones finales que participan en una configuración de direcciones de difusión múltiple o difusión general para conectar por puente sobre IP. También muestra el tamaño (en número de bytes) de los paquetes de conexión por puente que se direccionan a través de un túnel IP y si el direccionamiento de difusión múltiple está activado o desactivado. |
| Set | Define una dirección IP base de difusión múltiple para la conexión por túnel de difusión múltiple en el dispositivo. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Respuesta a mandatos de configuración de túnel

Los mandatos de configuración de túnel (Talk 6) no entran en vigor de forma inmediata. Permanecen pendientes hasta que emite el mandato **reload** o **restart**.

## Conexión por túnel y paquetes de difusión múltiple

El túnel de conexión por puente se puede definir como un túnel de difusión individual o como un túnel de difusión múltiple. Para definir un túnel de difusión individual, utilice el mandato **add** para configurar la dirección IP del punto final del túnel. Para definir un túnel de difusión múltiple, utilice los mandatos **set** y **join**. Para las configuraciones de túnel en las que intervienen paquetes de difusión múltiple, la dirección de origen de los paquetes de difusión múltiple deben estar en un segmento de la red que dé soporte al Protocolo de gestión de grupos de Internet (IGMP).

IGMP no está definido en algunas interfaces como ATM, X.25 y Frame Relay. Esto significa que cuando defina un túnel de difusión múltiple en el dispositivo (por ejemplo, el túnel MOSPF), debe asegurarse de que se cumple una de las siguientes condiciones:

- El origen es una de las direcciones de segmento de la LAN
- El origen es la dirección IP interna

La primera condición se puede comprobar utilizando el mandato de configuración **set router-id** de IP. La segunda condición se puede comprobar utilizando el mandato de configuración **set internal-ip-address** de IP.

En cualquier caso, la segunda opción es preferible y la primera sólo se debe utilizar si alguno de los dispositivos de la red no acepta direcciones de sistema principal (esto sucedería en redes mixtas de distintos proveedores).

## Add

Utilice el mandato **add** para añadir la dirección IP de estaciones finales que participan en una configuración de direccionamiento IP de difusión individual.

Para el direccionamiento de difusión individual IP, la configuración de la conexión por túnel requiere que especifique direcciones IP de puentes de destino. El software del dispositivo utilizará este registro para convertir el número de segmento del campo de información de direccionamiento (RIF) de una trama direccionada de origen en la dirección IP correspondiente del puente de destino. Para tramas de conexión por puente transparente, identifica el otro punto final del túnel.

**Sintaxis:** add

add**dress** *dirección-IP*

**Valores válidos**: una dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `add address 128.185.144.37`

## Delete

Utilice el mandato **delete** para suprimir la dirección IP de los puentes que participan en una configuración de direccionamiento IP de difusión individual o de difusión general.

**Sintaxis:**

del**ete** address *dirección-IP*

**Valores válidos**: una dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `delete address 128.185.144.37`

## Join

Utilice el mandato **join** para definir el dispositivo como un miembro de uno o más grupos de difusión múltiple. Un grupo de túnel puede ser de uno de estos tres tipos: peer, client o server. El grupo de túnel se define mediante un identificador que es un entero. Un puente sólo puede pertenecer a un tipo de grupo por cada identificador. Por ejemplo, un puente no puede pertenecer simultáneamente al *peer group 1* y al *server group 1*.

**Sintaxis:**

j**oin** client-group *número-grupo*

peer-group *número-grupo*

server-group *número-grupo*

**client-group** *número-grupo*
Une el grupo cliente con el número de grupo especificado.

**Valores válidos**: 0 a 64

**Valor por omisión**: 0

**Ejemplo:** `join client-group 3`

**peer-group** *número-grupo*
Une el grupo similar con el número de grupo especificado.

**Valores válidos**: 0 a 64

**Valor por omisión**: 0

**Ejemplo:** `join peer-group 5`

**server-group** *número-grupo*
Une el grupo servidor con el número de grupo especificado.

**Valores válidos**: 0 a 64

**Valor por omisión**: 0

**Ejemplo:** `join server-group 7`

## Leave

Utilice el mandato **leave** para retirar el dispositivo de grupos de difusión múltiple.

**Sintaxis:**

| | |
|---|---|
| le**ave** | server-group *número-grupo* |
| | client-group *número-grupo* |
| | peer-group *número-grupo* |

**server-group** *número-grupo*
Retira el grupo servidor con el número de grupo especificado.

**Valores válidos**: 0 a 64

**Valor por omisión**: 0

**Ejemplo:** `leave server-group 7`

**client-group** *número-grupo*
Retira el grupo cliente con el número de grupo especificado.

**Valores válidos**: 0 a 64

**Valor por omisión**: 0

**Ejemplo:** `leave client-group 3`

**peer-group** *número-grupo*
Retira el grupo similar con el número de grupo especificado.

**Valores válidos**: 0 a 64

**Valor por omisión**: 0

**Ejemplo:** `leave peer-group 5`

## List

Utilice el mandato **list** para visualizar las direcciones IP de los puentes que participan en una configuración de direccionamiento de difusión múltiple o difusión individual IP correspondiente a una conexión por túnel sobre IP. Este mandato también sirve para visualizar el tamaño actual de los paquetes IP que se envían a través del túnel y muestra si IP está activado o desactivado.

**Sintaxis:**

**list** address

all

**address** Lista todas las direcciones IP de los puentes que participan en una configuración de direccionamiento de difusión múltiple o difusión individual IP correspondiente a una conexión por túnel sobre IP.

**Ejemplo:** `list address`

```
IP Tunnel Addresses
128.185.179.51      128.185.170.51      128.185.142.39
128.185.143.39       224.0.0.5
```

**all** Lista todas las direcciones IP de difusión individual, las direcciones de difusión múltiple configuradas y el tamaño de los paquetes del túnel.

**Ejemplo:** `list all`

```
IP Tunnel Addresses
128.185.179.51      128.185.170.51      128.185.142.39
128.185.143.39       224.0.0.5
Frame size for the tunnel 2120
```

## Set

Utilice el mandato **set** para definir la dirección de difusión múltiple base del dispositivo.

Para un direccionamiento de difusión múltiple IP, la configuración de la conexión por túnel sólo necesita la dirección de difusión múltiple IP reservada para la conexión por túnel. La función de encapsulamiento utiliza tres grupos de direcciones de difusión múltiple IP. El primer grupo sirve para enviar tramas exploradoras de todas las rutas (ARE), el segundo grupo para enviar tramas exploradoras del árbol de expansión (STE) y el tercer grupo para tramas direccionadas específicamente (SRF).

**Sintaxis:**

**set** base-multicast-address

base-multicast-address

Define la dirección IP de difusión múltiple base para la conexión por túnel de difusión múltiple.

**Valores válidos**: cualquier dirección IP de clase D válida cuyo valor de los dos últimos bytes sea 0.

**Valor por omisión**: 224.186.0.0

**Ejemplo:** `set base-multicast-address 224.10.0.0`

## Mandatos de Frame Relay

Para activar la conexión por puente sobre la interfaz Frame Relay, debe asociar un número DLCI (también denominado número de circuito) a un puerto del puente. Este recibe el nombre de puerto del puente punto a punto de Frame Relay. También puede definir un puerto de puente multiacceso asociado a la interfaz Frame Relay. Para obtener más información, consulte el tema “Configuración de puertos de puente multiacceso” en la página 59.

Una vez configurado un puerto del puente, todas las funciones asociadas a los puertos del puente, incluidas las funciones de filtro de protocolos y filtro de direcciones, están disponibles.

Por cada puerto de puente punto a punto Frame Relay debe especificar PVC o SVC. Para el soporte PVC debe especificar el número DLCI asociado. Para el soporte SVC debe especificar el nombre del circuito SVC.

## Respuesta a mandatos de configuración de Frame Relay

Los mandatos de configuración de Frame Relay (Talk 6) no entran en vigor de forma inmediata. Permanecen pendientes hasta que emite el mandato **reload** o **restart**.

En el indicador `ASRT config>`, utilice el siguiente mandato para activar la conexión por puente correspondiente a un circuito Frame Relay:

**add port** *núm. interfaz núm. puerto id-circuito*

**núm. interfaz**
El número de interfaz de la interfaz Frame Relay.

**núm. puerto**
El número exclusivo específico del puente asociado al circuito.

**Rango válido**: 1 a 254

**Valor por omisión**: ninguno

**id-circuito**
El número DLCI correspondiente al PVC en el que se está activando la conexión por puente o el nombre del circuito del SVC en el que se está activando la conexión por puente.

El mandato asocia un número de puerto al PVC Frame Relay identificado en *número circuito* o al SVC Frame Relay identificado mediante el nombre del circuito y activa la participación del circuito en la conexión por puente transparente.

**Ejemplo: add a port on a Frame Relay interface (PVC)**

```
ASRT config> add port
Interface Number [0]? 5
Port Number [7]? 7
Use FR PVC? [Yes]: yes
Frame Relay Circuit number [16]? 17
```

**Ejemplo: add a port on a Frame Relay interface (SVC)**

```
ASRT config> add port
Interface Number [0]? 5
Port Number [8]? 8
Use FR PVC? [Yes]: no
Frame Relay SVC Circuit Name []? 05svc020
```

## Mandatos de ATM

Para activar la conexión por puente sobre la interfaz ATM, debe asociar un VCC al puerto del puente.

Una vez configurado un puerto de puente, todas las funciones asociadas a los puertos del puente, incluidas las funciones de filtro de protocolos y filtro de direcciones, están disponibles.

Tiene que especificar el soporte PVC o SVC. Para el soporte PVC, debe especificar el VPI y VCI para el PVC. Para el soporte SVC, debe especificar la dirección ATM remota y el byte selector local.

En el indicador `ASRT config>`, utilice el siguiente mandato para activar la conexión por puente en la interfaz ATM:

**add port** *núm. interfaz  núm. puerto  id-VCC*

**núm. interfaz**
El número de interfaz de la interfaz ATM.

**núm. puerto**
El número exclusivo específico del puente asociado al VCC.

**Rango válido**: 1 a 254

**Valor por omisión**: ninguno

Una vez se ha añadido el puerto a la interfaz ATM, el número de puerto identificará el puerto ante el cliente ATM ARP y ante el VCC asociado a este puerto.

Consulte el tema “Utilización de ARP” en la página 627 para obtener información sobre la configuración del cliente ATM ARP.

**id-vcc** Para definir un PVC, especifique la información sobre VPI y VCI. Para definir un SVC, especifique la dirección de destino y la información sobre el selector.

**VPI** El VPI del PVC en el que se activa la conexión por puente.

**Valores válidos de VPI**: 0 a 255

**Valor por omisión de VPI**: 0

**VCI** El VCI del PVC en el que se activa la conexión por puente.

**Valores válidos de VCI**: 0 a 65535

**Valor por omisión de VCI**: 0

**dirección-destino**
La dirección ATM de destino del SVC.

**Valores válidos de dirección ATM de destino**: cualquier dirección ATM válida de 20 bytes

**Valor por omisión de dirección ATM de destino**: ninguno

**selector** El selector de la dirección ATM de destino del SVC.

**Valores válidos del selector**: X'00' – X'FF'

**Valor por omisión del selector**: X'00'

**Ejemplo: add a port on an ATM interface (PVC)**

```
ASRT config> add port
Interface number [0]?
Port number [1]?
Use PVC? [Yes]:
VPI, Range 0..255 [0]? 0
VCI, Range 0..65535 [0]? 795
```

**Ejemplo: add a port on an ATM interface (SVC)**

```
ASRT config> add port
Interface number [0]?
Port number [2]?
Use PVC? [Yes]:No
Destination ATM Address []? 39112233445566778899001122334455667788 99
Selector, Range 00..FF [00]? 0A
ASRT config>
```

## Cómo acceder al entorno de supervisión de ASRT

Para acceder al entorno de supervisión ASRT, entre el mandato **protocol asrt** en el indicador + (GWCON):

```
+protocol asrt
ASRT>
```

## Mandatos de supervisión de ASRT

Esta sección describe los mandatos de supervisión de ASRT. Estos mandatos le permite ver y modificar parámetros de la supervisión activa. La información que modifica con los mandatos de supervisión se restaura en la configuración SRAM cuando vuelve a arrancar el dispositivo de conexión por puente.

Puede utilizar estos mandatos para modificar de forma temporal la configuración sin perder la información de configuración de la memoria del puente. El indicador ASRT> se visualiza para todos los mandatos de supervisión de ASRT.

Los mandatos de supervisión para NetBIOS se entran en el indicador de supervisión NetBIOS>. El indicador de NetBIOS es un subconjunto de los principales mandatos ASRT y se accede al mismo entrando el mandato de ASRT **netbios** que se explica más adelante en este capítulo.

Los mandatos de supervisión para NetBIOS se entran en el indicador de supervisión NetBIOS>. El indicador de la función de filtro de NetBIOS es un subconjunto de los principales mandatos ASRT.

**Nota:** Para los mandatos en los que tiene que especificar direcciones MAC, las direcciones se pueden entrar en los siguiente formatos:

Orden de bits canónico IEEE 802 00-00-00-12-34-56
Orden de bits canónico IEEE 802 (formato abreviado) 000000123456
Orden de bits nativo de red en anillo de IBM (no canónico)
00:00:00:12:34:56

La Tabla 7 muestra los mandatos de supervisión de ASRT.

*Tabla 7. Resumen de mandatos de supervisión de ASRT*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Add | Añade entradas de direcciones permanentes (estáticas) en la base de datos permanente del dispositivo de conexión por puente. |
| BAN | Le permite acceder al indicador de supervisión del nodo límite de acceso (BAN), en el que puede entrar mandatos de supervisión específicos de BAN. Consulte la Tabla 8 en la página 151 para obtener más información. |
| Cache | Muestra las entradas de la antememoria correspondientes a un puerto especificado. |
| Delete | Suprime entradas de direcciones MAC de la base de datos del dispositivo de conexión por puente. |
| Flip | Alterna direcciones MAC de orden de bits canónico a orden de bits 802.5 (no canónico o IBM). |
| List | Muestra información sobre la configuración completa del puente o sobre las opciones seleccionadas de la configuración. |
| NetBIOS | Muestra el indicador de supervisión de NetBIOS. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Add

Utilice el mandato **add** para añadir entradas de direcciones estáticas y filtros de direcciones de destino a la base de datos del dispositivo de conexión por puentes. Estas adiciones a la base de datos se pierden cuando se vuelve a arrancar el dispositivo.

**Sintaxis:**

a**dd** destination-address-filter

static-entry

**destination-address-filter** *dirección-mac*
Añade un filtro de direcciones de destino a la base de datos permanente del dispositivo de conexión por puentes. Entre el mandato seguido de la dirección MAC de la entrada.

**Ejemplo:** **add destination-address-filter**

```
Destination MAC address [00-00-00-00-00-00]?
```

**static-entry** *dirección-mac puerto-entrada [puertos-salida]*

Añade entradas de direcciones estáticas a la base de datos permanente del dispositivo de conexión por puentes. Entre el mandato seguido de la dirección MAC de la entrada estática y del número de puerto de entrada (también se pueden entrar números de puertos de salida si se desea). Para crear una entrada estática con varias correlaciones de puertos (1 por puerto de entrada), utilice este mandato varias veces.

**Ejemplo:** **add static-entry**

```
MAC address [00-00-00-00-00-00]?  400000012345
Input port, 0 for all [0]? 2
Output port, 0 for none [0]? 3
Output port, 0 to end [0]?
```

## BAN

Utilice el mandato **ban** para acceder al indicador de supervisión de BAN (Nodo límite de acceso). Entre el mandato **ban** desde el indicador ASRT>.

**Sintaxis:** ban

**Ejemplo:** ASRT>**ban**

```
BAN>
```

Una vez haya accedido al indicador de supervisión de BAN, puede empezar a entrar mandatos específicos de supervisión. Para volver al indicador ASRT> en cualquier momento, entre el mandato **exit**.

## Cache

Utilice el mandato **cache** para visualizar el contenido de la antememoria de direccionamiento del puerto de conexión por puente seleccionado. Si el puerto no posee una antememoria, aparecerá el mensaje El puerto X no tiene antememoria.

**Sintaxis:**

c**ache** *núm. puerto*

**Ejemplo:** **cache**

```
Port number [1]? 3

MAC Address    MC*   Entry Type       Age  Port(s)

00-00-93-00-C0-D0   PERMANENT          0  3 (TKR/1)
00-00-00-11-22-33   STATIC             0  3 (TKR/1)
```

**MAC Address**

Dirección MAC de 6 bytes de la entrada.

**Entry Type**

Especifica uno de los siguientes tipos de entradas de dirección:

**Reserved** - entradas reservadas por el Estándar IEEE 802.1d.

**Registered** - entradas que constan de direcciones de difusión individual que pertenecen al hardware de comunicaciones conectado al recuadro

o de direcciones de difusión múltiple activadas por distribuidores de protocolos.

**Permanent** - entradas que especifica el usuario en el proceso de configuración y que no se modifican tras procesos de encendido/apagado o de restauración del sistema.

**Static** - entradas que entra el usuario en el proceso de supervisión, que no se conservan tras un proceso de encendido/apagado o de restauración del sistema y que no se ven afectadas por el temporizador de caducidad.

**Dynamic** - entradas “aprendidas” por el puente “de forma dinámica” que no se conservan tras un proceso de encendido/apagado o de restauración del sistema y que tienen una “antigüedad” asociada.

**Free** - ubicaciones de la base de datos que están libres y se pueden rellenar con entradas de direcciones

**Unknown** - tipos de entradas desconocidas para el puente. Pueden ser errores y/o direcciones no válidas.

**Age** Antigüedad en segundos de cada entrada dinámica. La antigüedad se reduce en cada intervalo de resolución.

**port(s)** Especifica el número de puerto asociado a esta entrada y muestra el nombre de la interfaz (que siempre será la interfaz que tiene la antememoria).

## Delete

Utilice el mandato **delete** para suprimir entradas de direcciones (incluidas direcciones MAC) de estación de la base de datos permanente del dispositivo.

**Sintaxis:**

del**ete mac-address**

**Ejemplo:** `delete 00-00-93-10-04-15`

## Flip

Utilice el mandato **flip** para ver direcciones MAC específicas en formato canónico o no canónigo “alternando” el orden de los bits de la dirección. Este mandato resulta útil para convertir direcciones IEEE 802.5 con su formato típico no canónico en el formato canónico utilizado universalmente por la supervisión del puente y ELS (y viceversa).

**Sintaxis:**

**flip** *MAC-address*

**Ejemplo:** `flip`

```
MAC address [00-00-00-00-00-00]? 00-00-00-33-44-55
IEEE 802 canonical bit order:    00-00-00-33-44-55
IBM Token-Ring native bit order: 00:00:00:CC:22:AA
```

## List

Utilice el mandato **list** para visualizar información sobre la configuración completa del dispositivo de conexión por puente o para visualizar información sobre opciones seleccionadas de configuración o de conexión por puente.

**Sintaxis:**

list
- adaptive . . .
- bridge . . .
- conversion . . .
- database . . .
- dmac
- filtering . . .
- multiaccess-database . . .
- port
- source-routing . . .
- spanning-tree-protocol . . .
- transparent . . .
- tunnel . . .

**adaptive** *opción-grupodatos [sub-opción]*

Lista toda la información general sobre el puente SR-TB que efectúa la conversión entre tipos de conexión por puente. Hay varias opciones generales de grupo de datos que se pueden visualizar bajo **list adaptive**. Estas opciones incluyen:

- Config - Muestra información general sobre el puente SR-TB.
- Counters - Muestra todos los contadores del puente SR-TB.
- Database - Muestra el contenido de la base de datos de RIF del puente SR-TB.

**Ejemplo:** **`list adaptive config`**

```
  Adaptive bridge:            Enabled
  Translation database size:  0
  Aging time:                 320 seconds
  Aging granularity           5 seconds

Port  Segment  Interface   State     MTU
   1  001      TKR/1      Enabled   2052
   -  002      Adaptive   Enabled   1470
```

**Adaptive bridge**

Muestra el estado actual del puente adaptable SR-TB. Puede adoptar el Valor Activado o Desactivado.

**Translation database size**

Muestra el tamaño actual de la base de datos SR-TB, que contiene direcciones MAC y RIF asociados correspondientes al dominio de direccionamiento de origen.

**Aging time**

Muestra el valor del temporizador de caducidad en segundos. Todas las entradas de la base de datos de RIF de SR-TB que superan este límite de tiempo se eliminan.

**Aging granularity**
Muestra la frecuencia con que se exploran las entradas para ver se caducan en función de temporizador de caducidad.

**Port** Muestra el número de un puerto asociado a esta conexión por puente de conversión.

**Segment** Muestra el número de segmento de direccionamiento de origen asignado al puerto asociado con la conexión por puente de conversión.

**Interface** Identifica el dispositivo conectado a un segmento de la red del puente de conversión. Además, muestra el VPI/VCI si es un puerto ATM y el DCI si es un puerto Frame Relay.

**State** Indica el estado actual del puerto del puente de conversión.

**MTU** Especifica el tamaño máximo de trama (desde el final del RIF al principio del FCS) que puede transmitir y recibir el puente de conversión.

**Ejemplo:**

```
list adaptive counters
Hash collision count: 28
Adaptive database entry count: 0
Adaptive database overflow  count: 0
```

**Hash Collision Count**
Muestra el número de direcciones que se han guardado (hash) en la misma ubicación de la tabla hash. Este número es acumulativo y refleja el número total de incidentes de colisión hash producidos. Un aumento de este número puede indicar un problema potencial de tamaño de la tabla.

**Adaptive Database Entry Count**
Muestra el número de entradas actualmente guardadas en la base de datos del puente adaptable.

**Adaptive Database Overflow Count**
Muestra el número de veces que se ha sobregrabado una dirección porque la tabla de la base de datos de conversión no tenía espacio.

La opción *database* del mandato **list adaptive** le permite seleccionar partes de la base de datos de RIF del puente adaptable para que se visualicen. Esto se debe al tamaño potencial de la base de datos. Las opciones de visualización incluyen las siguientes:

- Address - Muestra la parte de la base de datos del puente de conversión relacionada a las direcciones MAC especificadas
- All - Muestra toda la base de datos.
- Port - Muestra todas las entradas del puente de conversión correspondientes al puerto especificado.
- Segment - Muestra todas las entradas del puente de conversión asociadas con el puerto que tiene el número de segmento especificado.

Los siguientes ejemplos ilustran cada una de las opciones del mandato **list adaptive database**.

**Nota:** Sólo se visualizan si la conexión por puente adaptable está activada.

**Ejemplo:** `list adaptive database address` ***dirección-mac***

**Ejemplo:** `list adaptive database all`

**Ejemplo:** `list adaptive database port` ***núm. segmento***

**Ejemplo:** `list adaptive database segment` ***núm. segmento***

Cada entrada se visualiza en dos líneas seguidas de una línea en blanco. Para cada entrada se visualiza la siguiente información:

**Canonical address**
Lista las direcciones MAC del nodo correspondiente a esta entrada. Se visualiza en formato canónico IEEE 802 (hexadecimal).

**Interface** Muestra el nombre de la interfaz de red que ha aprendido esta entrada.

**Port** Muestra el número de puerto del puerto que ha aprendido esta entrada de dirección.

**Seg** Muestra el número del segmento que ha aprendido esta dirección.

**Age** Muestra la antigüedad de la entrada en segundos.

**RIF Type** Muestra el tipo de RIF, que puede ser SRF, STE o ARE.

**RIF Direction**
Muestra la dirección de RIF, que puede ser Reenviar o Invertir.

**RIF Length**
Muestra la longitud del RIF en bytes.

**RIF LF** Muestra el valor de la trama de mayor tamaño codificada en el RIF.

**IBM MAC Address**
Muestra la dirección MAC del nodo correspondiente a esta entrada. Esto se visualiza en el orden de bits no canónico de “IBM” que suele aparecer en las interfaces 802.5 y se utiliza en los protocolos IP/ARP, IPX y NetBIOS.

**RIF** Muestra el Campo de información de direccionamiento aprendido a partir de este nodo.

**adaptive database duplicate**
Lista la entrada de base de datos de todas las direcciones MAC duplicadas. Muestra los RIF principal y secundario para cada dirección MAC duplicada.

**Ejemplo:** `list adaptive database duplicate`

```
Canonical Address  Interface  Port  Seg    Age  RIF: Type Direct   Length  LF IBM MAC Address    RIF

08-00-5a-ee-ee-ee  TKR/0         3  001    180       SRF  Forward  14  1470 90:00:5a:77:77:77  0e10fef0dcab001b960395029001  PRI. RIF(3)

                   TKR/2         5  003    185       SRF  Reverse  14  1470                    0c9070087109003bdcabfef00000  SEC. RIF(3)
```

**bridge** Lista toda la información general sobre la configuración del dispositivo de puente.

### Ejemplo: `list bridge`

```
Bridge ID (prio/add):  32768/10-00-5A-63-01-00
Bridge state:          Enabled
UB-Encapsulation:      Disabled
Bridge type:           STB
Number of ports:       2
STP Participation:     IEEE802.1d
IPX Conversion:        Enabled
Conversion Mode:       Automatic
Ethernet Preference:   IEEE-802.3
**Bridge is enabled for Data Link Switching**

                                                        Maximum
Port  Interface      State  MAC Address         Modes   MSDU   Segment Flags

   1  Eth /0            Up  10-00-5A-63-01-00       T    1514          RD
   2  FR /0:16          Up  00-00-00-00-00-00     SRT    2038     001  RD
   2  FR /0:18          UP  00-00-00-00-00-00     SR     2038     002  RD

Flags: RE = IBMRT PC behavior Enabled, RD = IBMRT PC behavior Disabled


SR bridge number:      00a
SR virtual segment:    ff6 (1 : N SRB Active)
Adaptive segment:      107
```

**Bridge ID**
ID exclusivo que utiliza el algoritmo de árbol de expansión para determinar el árbol de expansión. A cada puente de la red se le asigna un identificador de puente exclusivo. La prioridad del puente se muestra en formato decimal seguido de la dirección hex.

**Bridge State**
Indica si la conexión por puente está activada o desactivada.

**UB-Encapsulation**
Indica si la encapsulación UB está activada o desactivada.

**Bridge Type**
Muestra el tipo de puente configurado. Puede tener el valor NONE, SRB, TB, SRT, ADAPT, A/SRB, A/TB o ASRT.

**Number of Ports**
Muestra el número de puertos configurados para este puente.

**STP Participation**
Describe los tipos de protocolos de árbol de expansión en los que participa un puente.

**IPX Conversion**
Indica si la conversión IPX está activada o desactivada.

**Conversion Mode**
Indica la Modalidad de conversión IPX como automática o manual.

**Ethernet Preference**
Indica el tipo de trama Ethernet preferido para la conversión IPX como IEEE 802.3 o Ethernet.

**Port** Especifica un número definido por el usuario asociado a una interfaz mediante el mandato **add port**.

**Interface** Identifica los dispositivos conectados a un segmento de la red a través del puente.

**State** Indica el estado actual del puerto. Puede tener el valor UP o DOWN.

**MAC address**
Muestra la dirección MAC asociada a este puerto en orden de bits canónico.

**Modes** Muestra la modalidad de conexión por puente correspondiente a este puerto. T indica conexión por puente transparente. SR indica direccionamiento de origen. A indica conexión por puente adaptable.

**MSDU** Especifica el tamaño máximo de trama (unidad de datos) (incluida la cabecera MAC pero no el campo FCS) que puede transmitir y recibir el puente en esta interfaz.

**Segment** Muestra el número de segmento del puente de direccionamiento de origen asignado a este puerto (si lo hay).

**SR bridge number**
Muestra el número de puente de direccionamiento de origen asignado por el usuario.

**SR virtual segment**
Muestra el número de segmento virtual del puente de direccionamiento de origen (si lo hay).

**Adaptive segment**
Muestra el número del segmento que se utiliza en el dominio de direccionamiento de origen para direccionar al dominio transparente (mediante conversión).

**conversion** *opción-grupodatos*

- Muestra información general sobre las reglas del puente para convertir formatos de tramas en función del tipo de trama. Hay varios grupos de datos que se pueden visualizar bajo el mandato **list conversion**. Incluyen los siguientes:
  - All - Muestra todas las reglas.
  - Ethertype - Muestra las reglas para todos los tipos Ethernet o para un tipo Ethernet específico.
  - SAP - Muestra las reglas para todos los identificadores de protocolo SAP o para un tipo SAP 802.2 específico.
  - SNAP - Muestra las reglas para todos los identificadores de protocolo SNAP o para un tipo SNAP 802.2 específico.

Los siguientes ejemplo muestran cada una de las opciones de visualización del mandato conversion.

**Ejemplo:** list conversion all

**Ejemplo:** list conversion ethertype

```
Ethernet type (in hexadecimal), 0 for all [0]?
```

**Ejemplo:** list conversion SAP

```
SAP (in hexadecimal), 100 for all [100]?
```

**Ejemplo:** list conversion SNAP

```
SNAP Protocol ID, return for all [00-00-00-00-00]?
```

**database** *opción-grupodatos*
Lista el contenido de las bases de datos de la función de filtro transparente. Hay varios grupos de datos que se pueden visualizar bajo el mandato database. Incluyen los siguientes:

- All - Muestra toda la base de datos de conexión por puente transparente.
- Dynamic - Muestra todas las entradas dinámicas (aprendidas) de la base de datos de direcciones.
- Local - Muestra todas las entradas locales (reservadas) de la base de datos de direcciones.
- Permanent - Muestra todas las entradas permanentes de la base de datos de direcciones.
- Port - Muestra todas las entradas de direcciones correspondientes a un determinado puerto.
- Range - Muestra un rango de entradas de la base de datos completa de direcciones de la función de filtro de conexión por puente transparente. Se especifica una dirección MAC inicial y final para definir el rango. Se muestran todas las entradas que están dentro de este rango.
- Static - Muestra las entradas estáticas de la base de datos de direcciones.

Los siguientes ejemplos muestran algunas opciones del mandato database. El primer ejemplo muestra también la salida relacionada.

**Ejemplo:** `list database all`

```
MAC Address    MC*  Entry Type       Age  Port(s)
00-00-00-00-AA-AA   Dynamic          295  4 (Eth/2)
00-00-00-12-34-56   Perm/Source filter    2 (TKR/1)  ->  3-4
                                         1-2
00-00-00-22-33-44   Permanent            1-2
                                         1-2
00-00-00-33-44-55   Perm Dest filter     All
00-00-00-55-66-77   Perm/Source filter   1-2,4

00-00-93-10-04-15   Registered           1 (Eth/1)
00-00-93-10-E4-F9   Dynamic          300 1 (Eth/1)
00-00-93-90-04-A6   Dynamic          300 1 (Eth/1)
00-00-A7-10-68-28   Dynamic          270 1 (Eth/1)
01-80-C2-00-00-00*  Registered           1,3
01-80-C2-00-00-01*  Reserved             All
01-80-C2-00-00-02*  Reserved             All
01-80-C2-00-00-03*  Reserved             All
01-80-C2-00-00-0D*  Reserved             All
01-80-C2-00-00-0E*  Reserved             All
03-00-00-00-80-00*  Reserved             All
08-00-17-00-35-F9   Dynamic/ETH-II       300  1 (Eth/1)
08-00-17-00-4D-DA   Dynamic              300  1 (Eth/1)
```

**Ejemplo: `list database range`**

```
First MAC address [00-00-00-00-00-00]? 00-00-93-00-C0-D0
Last MAC address [FF-FF-FF-FF-FF-FF]? 01-80-C2-00-00-00

MAC Address    MC* Entry Type      AGE  Port(s)
00-00-93-10-04-15  Registered          1 (Eth/2)
01-80-C2-00-00-00  Registered          1,3
```

**Ejemplo: `list database dynamic`**

```
MAC Address    MC* Entry Type      AGE  Port(s)
00-00-00-00-AA-AA  Dynamic         295  4 (Eth/2)
00-00-93-10-E4-F9  Dynamic         300  1 (Eth/1)
00-00-93-90-04-A6  Dynamic         300  1 (Eth/1)
00-00-A7-10-68-28  Dynamic         270  1 (Eth/1)
08-00-17-00-35-F9  Dynamic/ETH-II  300  1 (Eth/1)
08-00-17-00-4D-DA  Dynamic         300  1 (Eth/1)
```

**Nota:** Los siguientes campos se visualizar para todas las opciones del mandato **list database**.

**MAC Address** Especifica la entrada de dirección en formato hexadecimal de 12 dígitos (orden de bits canónico).

**MC*** Un asterisco seguido de una entrada de dirección indica que la dirección se ha marcado como una dirección de difusión múltiple.

**Entry Type** Especifica uno de los siguientes tipos:

**Reserved**

Entradas reservadas por el estándar IEEE 802.1d.

**Registered**

Entradas que consisten en direcciones de difusión individual pertenecientes a interfaces que participan en el puente o en direcciones de difusión múltiple activadas por distribuidores de protocolos

**Permanent**

Entradas que especifica el usuario en el proceso de configuración y que no se modifican tras procesos de encendido/apagado o de restauración del sistema

**Static** Entradas que especifica el usuario en el proceso de supervisión, que no se conservan tras un proceso de encendido/apagado o de restauración del sistema y que no tienen antigüedad.

**Dynamic** Entradas “aprendidas” por el puente “de forma dinámica” que no se conservan tras un proceso de encendido/apagado o de restauración del sistema y que tienen una “antigüedad” asociada

Si la conversión IPX está activada y la entrada se ha “aprendido” durante el proceso de reenvío de una trama Novell IPX, el tipo de trama Ethernet/802.3 (encapsulado) también se muestra con uno de los siguientes valores:

- **ETH-II** - Ethernet-V2.0 (tipo de trama IPX ETHERNET_II)
- **802.3** - 802.3/Novell Proprietary (tipo de trama IPX ETHERNET_8023)
- **802.2** - 802.3/LLC (tipo de trama IPX ETHERNET_8022)
- **SNAP** - 802.3/SNAP (tipo de trama IPX ETHERNET_SNAP)

**Free** Este tipo no se utiliza y normalmente no aparece, excepto en condiciones ocasionales de “contención” entre la supervisión y el puente.

**Unknown** Tipo de entrada desconocido. Puede indicar un error en el software. Notifique el tipo de entrada en hexadecimal al Servicio al cliente.

**Age** Hace referencia a la antigüedad (en segundos) de cada entrada dinámica. La antigüedad se reduce en cada intervalo de resolución.

**Port(s)** Especifica el número o números de puertos de salida correspondientes a esta entrada. También se muestra el tipo de dispositivo para las entradas de puertos.

**dmac** Muestra información sobre las opciones configuradas para la característica de direcciones MAC duplicadas.

**Ejemplo: `list dmac`**

```
ASRT>list dmac
          Duplicate MAC address feature is    ENABLED
          Load balance feature is    ENABLED
          Age value for Duplicate MAC address :00000096
          Duplicate MAC ADDRESSES CONFIGURED
          ==================================
          10-00-5A-66-66-00
          10-00-5A-66-66-01
          10-00-5A-66-66-02
          10-00-5A-66-66-03
          10-00-5A-66-66-04
          10-00-5A-66-66-05
```

**filtering** *opción-grupodatos*

Muestra información general sobre las bases de datos de la función de filtro de protocolos del puentes. Hay varios grupos de datos generales que se pueden visualizar con el mandato **list filtering**. Incluyen los siguientes:

- All - Muestra todas las entradas de la base de datos de la función de filtro.
- Ethertype - Muestra las entradas de la base de datos del filtro de tipo protocolo Ethernet.
- SAP - Muestra las entradas de la base de datos del filtro del protocolo SAP.
- SNAP - Muestra las entradas de la base de datos del filtro de identificador de protocolo SNAP.

Los siguientes ejemplos muestran cada una de las opciones de visualización de la función de filtro.

**Ejemplo: `list filtering all`**

```
Ethernet type 0800 is routed on ports 1
IEEE 802.2 destination SAP 42 is routed on ports 1
IEEE 802 SNAP PID 00-00-00-08-00 is routed on ports 2-3
```

Los descriptores utilizados para explicar cómo se comunican los paquetes incluyen los siguientes:

- Routed - Describe paquetes que se pasan a un distribuidor de direccionamiento para que los reenvíe
- Filtered - Describe los paquetes que filtran de forma administrativa los valores de usuario de los filtros de protocolos
- Bridged and routed - Describe un identificador de protocolo para el que hay una entidad de protocolo dentro del sistema que no es un distribuidor. Por ejemplo, un protocolo de eco de nivel de enlace. Los paquetes de difusión individual procedentes de este protocolo se conectan por puente o se procesan localmente si se tienen que enviar a una dirección registrada. Los paquetes de difusión múltiple se reenvían y se procesan localmente para una dirección de difusión múltiple registrada.

Todos estos descriptores se aplican también a paquetes ARP con este Ethertype.

**Ejemplo: `list filtering ethertype`**

```
Ethernet type (in hexadecimal), 0 for all [0]? 0800
Ethernet type 0800 is routed on ports 1
```

**Ejemplo: `list filtering SAP`**

```
SAP (in hexadecimal), 100 for all [100]? 42
IEEE 802.2 destination SAP 42 is routed on ports 1
```

**Ejemplo: `list filtering SNAP`**

```
SNAP Protocol ID, return for all [00-00-00-00-00]?
IEEE 802 SNAP PID 00-00-00-08-00 is routed on ports 2-3
```

**multiaccess-database** *núm. puerto*

Muestra el contenido de la base de datos multiacceso. Esta base de datos correlaciona un número de segmento de direccionamiento de origen con un número de circuito Frame Relay.

**all-ports** Especifica que se deben visualizar todas las entradas de la base de datos.

**Ejemplo:** list multiaccess-database

```
Aging Time (in seconds): 300

4 entries used out of 512

Segment  Age    Port  Interface   Circuit
204      100    2     FR/0        16
267      200    3     FR/1        16
375      120    2     FR/0        18
400      220    3     FR/1        18
```

**port** *núm. puerto* Muestra las entradas de la base de datos correspondientes a un determinado puerto del puente.

**Ejemplo:** list multiaccess-database

```
Aging Time (in seconds): 300

4 entries used out of 512

Segment  Age    Port  Interface   Circuit
204      100    2     FR/0        16
375      120    2     FR/0        18
```

En la información mostrada:

**Segment** Es el número de segmento de destino de direccionamiento de origen.

**Age** Es el periodo de duración de la entrada en segundos.

**Port** Es el número de puerto del puerto del puente multiacceso que ha generado esta entrada.

**Interface** Es el nombre de la interfaz de red que ha generado esta entrada.

**Circuit** Es el número de circuito Frame Relay que ha generado esta entrada.

**port** *núm. puerto*

Muestra información sobre puertos.

**Ejemplo: list port**

```
Port Id (dec)    : 128: 3, (hex): 80-03
Port State       : Forwarding
STP Participation: Enabled
Port Supports    : Transparent Bridging Only
Assoc Interface #/name : 5/Eth/1
```

**Ejemplo: list port 1**

```
Port Id (dec)    : 128: 4, (hex): 80-04
Port State       : Disabled
STP Participation: Enabled
Port Supports    : Transparent Bridging Only
Assoc Interface #/name : 1/FR/0  PVC Circuit name:
  PVC Circuit number: 16
```

**Ejemplo: list port 2**

```
Port Id (dec)    : 128: 5, (hex): 80-05
Port State       : Disabled
STP Participation: Enabled
Port Supports    : Source Route Bridging Only
SRB: Segment Number: 0x004       MTU:  1979     STE Forwarding: Auto
Assoc Interface #/name : 10/PPP/1
```

**Port** Especifica un número definido por el usuario asociado a una interfaz mediante el mandato **add port**.

**Interface** Identifica los dispositivos conectados a un segmento de la red a través del puente.

**State** Indica el estado actual del puerto. Puede tener el valor UP o DOWN.

**MAC address**
Muestra la dirección MAC asociada a este puerto en orden de bits canónico.

**Modes** Muestra la modalidad de conexión por puente correspondiente a este puerto. **T** indica conexión por puente transparente. **SR** indica direccionamiento de origen. **A** indica conexión por puente adaptable.

**MSDU** Especifica el tamaño máximo de trama (unidad de datos) (incluida la cabecera MAC pero no el campo FCS) que puede transmitir y recibir el puente en esta interfaz.

**Segment** Muestra el número de segmento del puente de direccionamiento de origen asignado a este puerto (si lo hay).

**source-routing** *opción-grupodatos*
Muestra información sobre la configuración del puente de direccionamiento de origen. Hay varias opciones de grupos de datos generales que se pueden visualizar con el mandato source-routing. Incluyen las siguientes:

- Configuration - Muestra información general sobre el puente SRB.
- Counters - Muestra todos los contadores del puente SRB .
- State - Muestra el contenido de todas las bases de datos relacionadas con el puente SR-TB.

Los siguientes ejemplos ilustran cada una de las opciones de visualización del mandato source-routing.

**Ejemplo:** **`list source-routing configuration`**

```
Bridge number:              1
Bridge state:               Enabled
Maximum STE hop count       14
Maximum ARE hop count       14
Virtual segment:            003
Port  Segment  Interface   State     MTU    STE Forwarding  LNM
2     001      TKR/1       Enabled   4399   Yes             ENA
3     002      TKR/2       Enabled   4399   Yes
```

**Bridge number**
El número de puente (en hexadecimal) asignado a este puente.

**Bridge State**
Indica si la conexión por puente está activada o desactivada.

**Maximum STE hop count**
El número máximo de saltos para la transmisión de tramas exploradoras del árbol de expansión desde el puente a una determinada interfaz asociada con la conexión por puente de direccionamiento de origen.

**Maximum ARE hop count**
El número máximo de saltos para la transmisión de tramas exploradoras de todas las rutas desde el puente a una determinada interfaz asociada a la conexión por puente de direccionamiento de origen.

**Virtual segment**
El número de segmento virtual asignado para la conexión por puente 1:N.

**Port** El número de puertos asociados a la conexión por puente de direccionamiento de origen.

**Segment** Los números de segmento asignados a puertos asociados a la conexión por puente de direccionamiento de origen.

**Interface** Los nombres de las interfaces asociadas. Se muestra VPI/VCI para ATM. Se muestra DLCI para FR.

**State** El estado actual del puente (Enabled o Disabled).

**MTU** El tamaño de MTU definido para este puerto.

**STE Forwarding**
Indica si las tramas exploradoras del árbol de expansión que se reciben en este puerto se reenvían (Yes) o si las tramas STE procedentes de otros puertos pasan por este puerto.

**LNM** Indica si los agentes del Gestor de red de la LAN (LNM) están activados (ENA) o desactivados (DIS) en este puerto específico.

La opción counters tiene más subgrupos de información que se pueden visualizar con el mandato source-routing. Incluyen los siguientes:

- All-ports - Muestra contadores correspondientes a todos los puertos.
- Port - Muestra contadores para un determinado puerto.
- Segment - Muestra contadores para el puerto correspondiente a un determinado segmento.

Los siguientes ejemplos ilustran cada una de las opciones de visualización del mandato source-routing.

**Ejemplo:** `list source-routing counters all-ports`

```
ASRT>list source counters all-ports
Counters for port 2, segment 001, interface TKR/1
SRF frames received:          0    sent:          0
STE frames received:          0    sent:          0
ARE frames received:        648    sent:          0
SR frames sent as TB:                               0
TB frames sent as SR:                            2057
Dropped, input queue overflow:                      0
Dropped, source address filtering:                  0
Dropped, dest address filtering:                    0
Dropped, invalid RIF length:                        0
Dropped, duplicate segment:                      2594
Dropped, segment mismatch:                          0
Dropped, Duplicate LAN ID or tree error:            0
Dropped, STE hop count exceeded:                    0
Dropped, ARE hop count exceeded:                    0
Dropped, no buffer available to copy:               0
Dropped, MTU exceeded:                              0


Counters for port 3, segment 002, interface TKR/2:
SRF frames received:          0    sent:          0
STE frames received:          0    sent:          0
ARE frames received:        825    sent:          0
SR frames sent as TB:                               0
TB frames sent as SR:                            2041
Dropped, input queue overflow:                      0
Dropped, source address filtering:                  0
Dropped, dest address filtering:                    0
Dropped, invalid RIF length:                        0
Dropped, duplicate segment:                      3300
Dropped, segment mismatch:                          0
Dropped, Duplicate LAN ID or tree error:            0
Dropped, STE hop count exceeded:                    0
Dropped, ARE hop count exceeded:                    0
Dropped, no buffer available to copy:               0
Dropped, MTU exceeded:                              0
```

**Port** Lista los números de puertos asociados con la conexión por puente de direccionamiento de origen

**Segment** Lista los números de segmento de direccionamiento de origen en hex.

**Interface** Lista el nombre de la interfaz de red.

**SRF Frames Received/Sent**
Lista el número de tramas direccionadas específicamente recibidas y enviadas a través de este puente.

**STE Frames Received/Sent**
Lista el número de tramas exploradoras del árbol de expansión recibidas y enviadas a través de este puente.

**ARE Frames Received/Sent**
Lista el número de tramas exploradoras de todas las rutas recibidas y enviadas a través de este puente.

**SR Frames Sent as TB**
Lista el número de tramas de direccionamiento de origen recibidas en esta interfaz que se enviaron como tramas de puente transparente.

**TB Frames Sent as SR**
Lista el número de tramas de puente transparente recibidas en esta interfaz que se enviaron como tramas de direccionamiento de origen.

**Dropped, input queue overflow**
Lista el número de tramas que han llegado a esta interfaz que no se conectaron por puente por motivos de control de flujo. La cola de entrada del distribuidos se ha desbordado.

**Dropped, source address filtering**
Lista el número de tramas que han llegado a esta interfaz que no se conectaron por puente porque esta dirección de origen coincidía con un filtro de direcciones de origen de la base de datos de la función de filtro.

**Dropped, destination address filtering**
Lista el número de tramas que han llegado a esta interfaz que no se conectaron por puente porque esta dirección de destino coincidía con un filtro de direcciones de destino de la base de datos de la función de filtro.

**Dropped, protocol filtering**
Lista el número de tramas que han llegado a esta interfaz que no se conectaron por puente porque su identificador de protocolo es uno de los que se filtran de forma administrativa.

**Dropped, invalid RIF length**
Lista el número de tramas que han llegado a esta interfaz que se eliminaron porque la longitud de RIF era que de 2 o mayor que 30.

**Dropped, duplicate segment**
Lista el número de tramas que han llegado a esta interfaz que se eliminaron debido a un segmento duplicado en el RIF. Es lo normal para tramas ARE.

**Dropped, segment mismatch**
Lista el número de tramas que han llegado a esta interfaz que se eliminaron porque el número de segmento de salida no coincidía con ninguno de este puente.

**Dropped, Duplicate LAN ID or tree error:**
El número de ID de LAN duplicados o de errores de árbol. Esto ayuda en la detección de problemas de redes que contienen puentes de direccionamiento de origen de IBM antiguos.

**Dropped, STE hop count exceeded:**
El número de tramas exploradoras que ha eliminado este puerto porque el Campo de información de direccionamiento excedía la longitud máxima del descriptor de ruta.

**Dropped, ARE hop count exceeded:**
El número de tramas exploradoras que ha eliminado este puerto porque el Campo de información de direccionamiento excedía la longitud máxima del descriptor de ruta.

**Dropped, no buffer available to copy:**
El número de veces que no se ha podido reenviar una trama a una interfaz porque no había recursos de almacenamiento intermedio disponibles para copiar la trama. (Las tramas enviadas a destinos de difusión múltiple y a destinos desco-

nocidos se tienen que copiar para transmitirlas a todos los puertos activos.)

**Dropped, MTU exceeded:**
El número de tramas que ha eliminado este puerto por su excesivo tamaño.

**Ejemplo: `list source-routing counters port 3`**

```
Counters for port 3, segment 002, interface TKR/1:
SRF frames received:          0    sent:           0
STE frames received:          0    sent:           0
ARE frames received:       1140    sent:           0
SR frames sent as TB:                                0
TB frames sent as SR:                             2931
Dropped, input queue overflow:                       0
Dropped, source address filtering:                   0
Dropped, dest address filtering:                     0

Dropped, invalid RIF length:                         0
Dropped, duplicate segment:                       4560
Dropped, segment mismatch:                           0
Dropped, Duplicate LAN ID or tree error:             0
Dropped, STE hop count exceeded:                     0
Dropped, ARE hop count exceeded:                     0
Dropped, no buffer available to copy:                0
Dropped, MTU exceeded:                               0
Dropped, dest address filtering:                     0
Dropped, protocol filtering:                         0
```

**Ejemplo: `list source-routing counters segment 2`**

```
Counters for port 3, segment 002, interface TKR/2:
SRF frames received:          0    sent:           0
STE frames received:          0    sent:           0
ARE frames received:       1249    sent:           0
SR frames sent as TB:                                0
TB frames sent as SR:                             3200
Dropped, input queue overflow:                       0
Dropped, source address filtering:                   0
Dropped, dest address filtering:                     0
Dropped, protocol filtering:                         0
Dropped, invalid RI length:                          0
Dropped, duplicate segment:                       4996
Dropped, segment mismatch:                           0
Dropped, Duplicate LAN ID or tree error:             0
Dropped, STE hop count exceeded:                     0
Dropped, ARE hop count exceeded:                     0
Dropped, no buffer available to copy:                0
Dropped, MTU exceeded:                               0
```

**spanning-tree protocol** *opción-grupodatos*

- Muestra información sobre el protocolo del árbol de expansión. El puente transparente utiliza el protocolo del árbol de expansión para formar una topología libre de bucles. Hay varias opciones de grupos de datos generales que se pueden visualizar con el mandato **list spanning-tree-protocol**. Incluyen las siguientes:
  - Configuration - Muestra información sobre el protocolo del árbol de expansión.
  - Counters - Muestra contadores del protocolo del árbol de expansión.
  - State - Muestra información sobre el estado actual del protocolo del árbol de expansión.
  - Tree - Muestra información actual sobre el árbol de expansión, que incluye puerto, interfaz y coste.

  Los siguientes ejemplos ilustran cada una de las opciones de visualización del mandato spanning-tree-protocol.

  **Ejemplo: `list spanning-tree-protocol configuration`**

```
Bridge ID (prio/add):  32768/0000-93-00-84-EA
Bridge state:          Enabled
Maximum age:           20 seconds
Hello time:            2 seconds
Forward delay:         15 seconds
Hold time:             1 seconds
Filtering age:         320 seconds
Filtering resolution:  5 seconds

Port  Interface  Priority  Cost   State
  4   Eth/1      128    100     Enabled
128   Tunnel     128    65535   Enabled
```

### Ejemplo: `list spanning-tree-protocol counters`

```
  Time since topology change (seconds)        0
  Topology changes:                           1
  BPDUs received:                             0
  BPDUs sent:                             14170

Port  Interface  BPDUs received  BDPU input overflow  Forward transitions

   1  TKR/1             0              0              1
```

### Ejemplo: `list spanning-tree-protocol state`

```
Designated root (prio/add):    32768/00-00-93-00-84-EA
Root cost:                     0
Root port:                     Self
Current (root) maximum age:    20 seconds
Current (root) hello time:     2 seconds
Current (root) Forward delay:  15 seconds
Topology change detected:      FALSE
Topology change:               FALSE

Port  Interface   State
  4   Eth/1       Forwarding
128   Tunnel      Forwarding
```

### Ejemplo: `list spanning-tree-protocol tree`

```
Port                 Designated   Desig.         Designated   Des.
No.  Interface             Root     Cost             Bridge   Port

1  TKR/1  32768/12-34-56-78-90-12    0 32768/12-34-56-78-90-12 90-01
```

**tunnel** *opción-grupodatos*

Muestra información sobre la configuración del túnel. Hay varias opciones de grupos de datos generales que se pueden visualizar bajo el mandato tunnel. Incluyen las siguientes:

- Bridges - Muestra información sobre el puente del túnel.
- Config - Muestra información sobre la configuración del túnel.

## NetBIOS

Utilice el mandato **netbios** para acceder al indicador `NetBIOS>`. Los mandatos de supervisión de NetBIOS se pueden entrar en el indicador `NetBIOS>`.

Consulte el tema “Mandatos de NetBIOS” en la página 178 para ver los mandatos de supervisión de NetBIOS.

**Sintaxis:**

**netbios**

## Cómo acceder al indicador de supervisión de BAN

Utilice el mandato **ban** desde el indicador de supervisión `ASRT>` o `DLSw>` para acceder a los mandatos de BAN.

Para acceder al indicador de supervisión de BAN, entre el mandato **ban** desde el indicador de supervisión de ASRT o desde el indicador de supervisión de DLSw. Por ejemplo:

```
ASRT> ban
BAN>

   o

DLSw> ban
BAN>
```

Una vez haya accedido al indicador de supervisión de BAN, puede empezar a entrar mandatos específicos de supervisión. Para volver al indicador de supervisión desde que ha emitido el mandato, entre el mandato **exit**.

## Mandatos de supervisión de BAN

Esta sección describe los mandatos de supervisión de BAN. Entre los mandatos en el indicador BAN>.

*Tabla 8. Resumen de los mandatos de supervisión de BAN*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| List | Muestra toda la información sobre los puertos BAN. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## List

Utilice el mandato **list** para listar información sobre todos los puertos de BAN. La información que se muestra incluye el número de puerto de BAN, la dirección MAC correspondiente a BAN DLCI, si las tramas manejadas por el puerto se conectan por puente o el LLC se termina con DLSw y el estado del puerto.

El estado del puente puede tener uno de los siguientes valores:

- Init Fail - Indica que existe un problema de configuración.
- Up - Indica que la DLCI Frame Relay está funcionando.
- Down - Indica que la DLCI no está activa.

**Sintaxis:**

**list**

**Ejemplo: `list`**

```
bridge  BAN                Boundary            bridged or
port    DLCI MAC Address   Node Identifier     DLSw terminated  Status
2       40:00:12:34:56:78  4F:FF:00:00:00:00   bridged          Up
```

# Utilización de NetBIOS

Este capítulo describe la implantación de IBM de NetBIOS sobre redes conectadas por puente y sobre redes DLSw. Incluye los siguientes temas:



## Acerca de NetBIOS

El protocolo NetBIOS fue diseñado para utilizarse en una LAN de Red en anillo. Es un protocolo direccionable, pero se puede conectar por puente o conmutar mediante DLSw. Se da soporte a estos dos métodos de manejar el tráfico de NetBIOS.

NetBIOS se basa en tramas de difusión general para la mayoría de sus funciones que no sean la transferencia de datos. Aunque puede no presentar problemas en entornos de LAN, si no se controla puede presentar problemas en entornos de WAN.

Las siguientes secciones describen los nombres NetBIOS y los distintos tipos de comunicación de difusión general de NetBIOS.

## Nombres NetBIOS

La clave de la comunicación entre estaciones NetBIOS son los nombres NetBIOS. Cada entidad NetBIOS tiene asignado un nombre NetBIOS. Para poder establecer comunicación con otra entidad NetBIOS, su nombre NetBIOS debe ser conocido. Los nombres se utilizan en las tramas NetBIOS de difusión general para indicar la entidad NetBIOS de origen de la trama y la entidad NetBIOS de destino a la que va destinada la trama.

Todos los nombres de las tramas NetBIOS tienen 16 caracteres ASCII. Hay dos tipos de nombres NetBIOS:

**Individual (o exclusivo)**
Representa un solo servidor o cliente NetBIOS. Este nombre debe ser exclusivo dentro de la red NetBIOS.

Este nombre sirve para establecer comunicación con esta entidad NetBIOS concreta.

**Grupo** Representa un grupo de estaciones NetBIOS (un dominio de OS/2 LAN Server, por ejemplo). Este nombre no puede coincidir con ningún nombre NetBIOS individual de la red.

Este nombre sirve para permitir la comunicación entre un grupo de entidades NetBIOS.

Una sola estación NetBIOS (una sola dirección MAC) puede tener asociados varios nombres individuales y/o de grupo. La aplicación NetBIOS genera estos nombres

en función de un nombre o nombres configurados en la estación NetBIOS por el administrador de la red.

## Resolución de conflictos de nombres NetBIOS

Cuando una entidad NetBIOS se está preparando para utilizar un nombre NetBIOS individual como suyo propio, comprueba la red para asegurarse de que no haya ninguna otra estación NetBIOS que ya utilice este nombre.

Comprueba el nombre NetBIOS efectuando difusiones generales repetidas de una trama UI NetBIOS a todas las estaciones NetBIOS. Si ninguna estación responde, se da por supuesto que el nombre es exclusivo y se puede utilizar. Si una estación responde, la nueva estación no debe intentar utilizar este nombre.

## Procedimiento de configuración de sesiones NetBIOS

Para establecer una sesión NetBIOS a fin de realizar operaciones de transferencia de datos, el cliente NetBIOS resuelve en primer lugar la dirección MAC del servidor NetBIOS y la ruta LLC al servidor NetBIOS.

Para ello, efectúa difusiones generales repetidas de una determinada trama UI NetBIOS a todas las estaciones NetBIOS. Esta trama contiene el nombre NetBIOS del servidor con el que este cliente está estableciendo una sesión. Cuando el servidor recibe esta trama que contiene su nombre NetBIOS, responde con una trama correspondiente UI NetBIOS de difusión general al cliente. Cuando el cliente recibe la trama de respuesta, la trama contiene la dirección MAC y la ruta al servidor NetBIOS.

Para algunas aplicaciones NetBIOS, la búsqueda del servidor NetBIOS constituye un proceso de varios pasos. Por ejemplo, el primer paso puede ser buscar un controlador de dominio que indique al cliente qué servidor de dominio utilizar. Luego el cliente busca este servidor de dominio.

Cuando se han encontrado la dirección MAC del servidor NetBIOS y la ruta al servidor NetBIOS, el cliente NetBIOS puede emprender una de las siguientes acciones:

- Establecer una conexión LLC2 con el servidor NetBIOS para comunicarse con el servidor mediante tramas-I.
- Empezar la comunicación con el servidor NetBIOS utilizando tramas UI NetBIOS direccionadas específicamente.

## Flujos de datos de difusión general NetBIOS

Para algunas aplicaciones NetBIOS, resulta común efectuar difusiones generales periódicas de tramas de datos. Esto se puede realizar si una estación tiene datos de una sola trama que valga la pena enviar a otra estación NetBIOS. Puede hacerlo realizando una difusión general de una determinada trama UI NetBIOS (que contenga el nombre de la estación NetBIOS de destino) a todas las estaciones NetBIOS.

Otro caso es cuando estaciones NetBIOS de un grupo (o dominio) tienen que establecer comunicación entre sí. Esto puede realizarse efectuando una difusión general de una determinada trama UI NetBIOS (que contenga el nombre del grupo NetBIOS de destino) a todas las estaciones NetBIOS. Esto se realiza con frecuencia.

## Flujos de estados de NetBIOS

Una función de NetBIOS menos utilizada es la posibilidad de obtener estados desde cualquier estación NetBIOS. Esto se realiza efectuando una difusión general de una determinada trama NetBIOS (que contenga el nombre de la estación NetBIOS de destino) a todas las estaciones NetBIOS. Cuando la estación NetBIOS de destino recibe la trama, responde con una trama correspondiente de respuesta de NetBIOS de difusión general.

## Tramas de difusión general a todas las estaciones NetBIOS

Hay dos tipos de funciones de NetBIOS que se utilizan con poca frecuencia. En ambas funciones se realiza una difusión general de una trama NetBIOS a todas las estaciones NetBIOS. Las tramas no contienen ningún nombre NetBIOS de destino. Estas dos funciones son:

- Función de difusión general de NetBIOS – envía una trama de datos a todas las estaciones NetBIOS de la red.
- Función de terminación de rastreo de NetBIOS – permite a un administrador de la red terminar las funciones de rastreo de NetBIOS de todas las estaciones NetBIOS de la red desde un solo punto. Se efectúa una difusión general de una determinada trama NetBIOS a todas las estaciones NetBIOS de la red.

## Reducción del tráfico NetBIOS

Para estabilizar una red, el objetivo es reducir la cantidad de tráfico NetBIOS de difusión general que se reenvía a través de las redes conectadas por puente o conmutadas DLSw. Esto se puede realizar de dos modos:

- Filtrando tantas tramas NetBIOS de difusión general como sea posible antes de conectarlas por puente o conmutarlas DLSw.
- Reenviando tramas UI NetBIOS no filtradas en el menor número posible de puertos de puente o de sesiones TCP DLSw.

La Tabla 9 contiene los filtros que suministra IBM.

*Tabla 9. Filtros NetBIOS*

| Tipo de filtro | Filtra |
|---|---|
| Dirección MAC | Tramas según la dirección MAC de origen o de destino. |
| Byte | Tramas según el desplazamiento de bytes y la longitud de campo de una trama. |
| Nombre | Tramas por nombres de origen y de destino de NetBIOS. |
| Trama duplicada | Tramas duplicadas. |
| Respuesta | Respuestas para las que el direccionador no reenvió una trama de difusión general NetBIOS. |

Una vez el direccionador filtra tramas, las listas nombres NetBIOS y las funciones de colocación en antememoria de nombres NetBIOS y de rutas controlan el modo en que se deben reenviar las tramas restantes. Los temas “Función de filtro de byte de NetBIOS” en la página 52 y “Función de filtro de nombre de sistema prin-

cipal de NetBIOS” en la página 51 describen la función de filtro de byte y de nombre respectivamente. El manual *Guía del usuario de software* describe la función de filtro de direcciones MAC.

Para ver una introducción a la función de filtro de nombre de sistema principal y a la función de filtro de byte, consulte el tema “Filtros de bytes y nombres de NetBIOS” en la página 50.

Las siguientes secciones describen tipo de trama, trama duplicada, función de filtro de trama de respuesta, listas de nombres NetBIOS y colocación en antememoria de rutas y nombres NetBIOS.

## Función de filtro de tipo de trama

La función de filtro de tipo de trama permite filtrar por completo determinadas categorías de tramas para tráfico de puente, tráfico DLSw y ambos.

Las tres categorías de tramas NetBIOS que se pueden filtrar son las siguientes:

- Tramas de resolución de conflictos de nombres

  Son las tramas NetBIOS de difusión general que sirven para asegurarse de que un nombre NetBIOS es exclusivo en la red.

  En redes NetBIOS, es importante que los nombres NetBIOS de las estaciones con las que se establece una sesión NetBIOS (generalmente los servidores NetBIOS) sean exclusivos. También es importante que los nombres NetBIOS individuales de estaciones del mismo grupo (o dominio) sean exclusivos. Pero generalmente no es tan importante que los nombres NetBIOS de las estaciones para las que se configura una sesión NetBIOS (generalmente los clientes NetBIOS) sean exclusivos, especialmente entre dominios.

  Por este motivo, las redes en las que hay un buen control sobre los nombres de servidor pueden beneficiarse de la función de filtro de tramas de resolución de conflictos de nombres. Esto es especialmente cierto en las redes conmutadas DLSw.

  Las tramas de resolución de conflictos de nombres NetBIOS son Add-Name-Query, Add-Group-Name-Query y Add-Name-Response.

- Tramas generales de difusión general

  Son las tramas NetBIOS de difusión general que sirven para enviar datos a todas las estaciones NetBIOS de una red. Este tipo de trama no se suele utilizar y generalmente se puede filtrar.

  La trama general de difusión general NetBIOS es Datagram-Broadcast.

- Tramas de terminación de rastreo

  Son las tramas NetBIOS de difusión general que sirven para terminar rastreos NetBIOS en todas las estaciones NetBIOS de una red. Estas tramas no se suelen utilizar y generalmente se pueden filtrar.

  La trama de terminación de rastreo NetBIOS es Terminate-Trace.

El valor por omisión consiste en no filtrar ninguno de los tipos de tramas anteriores para el tráfico NetBIOS conectado por puente y filtrar todos los tipos de tramas anteriores para el tráfico NetBIOS conmutado DLSw. Sin embargo, puede resultar beneficioso filtrar los tipos de tramas anteriores si el tráfico NetBIOS se conecta por puente en enlaces WAN.

Para la conexión por puente, entre **set filters bridge** para activar y desactivar la función de filtro de tipo de trama. Para DLSw, entre **set filters dlsw** para activar o desactivar la función de filtro de tipo de trama.

Por ejemplo:

```
NetBIOS config>set filters bridge

Filter Name Conflict frames? [Yes]:

Name conflict filtering is              ON

Filter General Broadcast frames? [Yes]:

General broadcast filtering is          ON

Filter Trace Control frames? [Yes]:

Trace control filtering is              ON
```

## Función de filtro de tramas duplicadas

La estación NetBIOS de origen envía todas las tramas NetBIOS de difusión general que han obtenido respuesta un número fijo de veces (el valor por omisión es 6), a intervalos fijos (el valor por omisión es 1/2 segundo). En la siguiente explicación, estas tramas reciben el nombre de tramas de *mandato NetBIOS* y las posibles tramas de respuesta reciben el nombre de *tramas de respuesta de NetBIOS*

Las tramas de mandato NetBIOS son las:

- Tramas de resolución de conflictos de nombres – Add-Name-Query y Add-Group-Name-Query
- Tramas de configuración de sesiones NetBIOS – Name-Query
- Tramas de estados de NetBIOS – Status-Query

Las tramas de mandato se envían varias veces para aumentar la probabilidad de distribución satisfactoria (estas tramas son tramas sin conexión). Cada trama de respuesta se envía sola una vez en respuesta a cada trama de mandato recibida.

En una red conmutada DLSw, el reenvío de cada reintento a través de sesiones de WAN puede resultar muy caro. Por lo tanto, cuando se recibe la primera trama de mandato, se reenvía a los puertos de puente y DLSw contiguos adecuados y se guarda una copia. Todos los reintentos de la misma trama de mandato NetBIOS recibidos durante un periodo de tiempo que se puede configurar se eliminan.

Sólo hay un periodo de tiempo que se puede configurar para la red de puente y un periodo de tiempo que se puede configurar para la red DLSw.

El periodo de tiempo que se puede configurar para la red de puente se controla mediante dos mandatos:

- **enable duplicate-filtering / disable duplicate-filtering**, que controla si las tramas de mandato NetBIOS duplicadas se filtran o no en la red del puente.
- **set general** (parámetro “Duplicate frame filter timeout value in seconds”)

  Si la función de filtro de tramas duplicadas está activada para la red de puente, este valor especifica la duración del periodo para eliminar tramas duplicadas de mandato NetBIOS una vez conectada por puente la trama de mandato NetBIOS.

Si se recibe una trama duplicada de mandato NetBIOS una vez transcurrido este periodo, la trama se reenvía a la red de puente.

El periodo de tiempo que se puede configurar para la red DLSw se controla mediante un solo parámetro:

- **set cache-parms** (parámetro “Reduced search timeout value in seconds”)

  Este valor especifica la duración del periodo para eliminar tramas duplicadas de mandato NetBIOS una vez la trama de mandato NetBIOS se ha reenviado a la red DLSw.

  Si se recibe una trama duplicada de mandato NetBIOS una vez transcurrido este periodo, la trama se reenvía a la red DLSw.

  **Nota:** La función de filtro de tramas duplicadas de mandato NetBIOS a una red DLSw está siempre activada.

Cuando un DLSw contiguo recibe una trama de mandato NetBIOS, la trama se reenvía a la red de puente y se guarda una copia. En un intervalo que se puede configurar (1/2 segundo) y durante un número de veces que se puede configurar (el valor por omisión es 6), la función DLSw contigua reenvía un reintento de la trama de mandato a la función de puente. La función de puente maneja la trama de mandato según los parámetros configurados de tramas duplicadas de puente.

El número de reintentos y el intervalo, ambos configurables, se controlan mediante el siguiente mandato y parámetros:

- **set general** (parámetros “Command frame retry count” y “Command frame retry timeout value in seconds”)

Hay al menos un parámetro que controla el periodo de tiempo en que se guarda la trama de mandato a fin de realizar la función de reenvío de red DLSw y de puente:

- **set general** (parámetro "Duplicate frame detect timeout value in seconds")

  Este parámetro indica el periodo de tiempo que se guarda una trama de mandato NetBIOS recibida para el proceso de tramas duplicadas y tramas de respuesta. Una vez transcurrido este periodo, la trama de mandato se suprime y los temporizadores de filtro de tramas duplicadas y de búsqueda reducida asociados se cancelan. La primera trama de mandato duplicada recibida una vez transcurrido el periodo es trata como la primera trama de mandato recibida. Todas las tramas de respuesta recibidas después del periodo de tiempo de espera se eliminan.

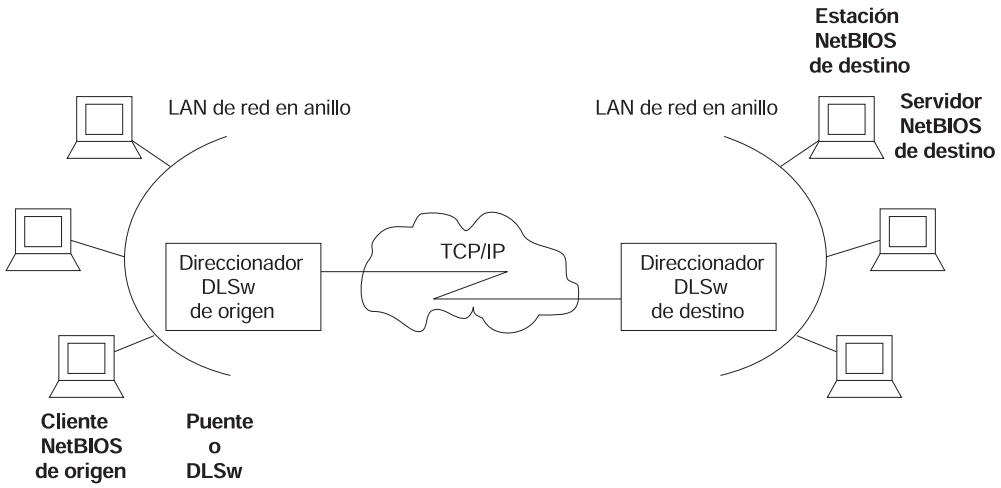
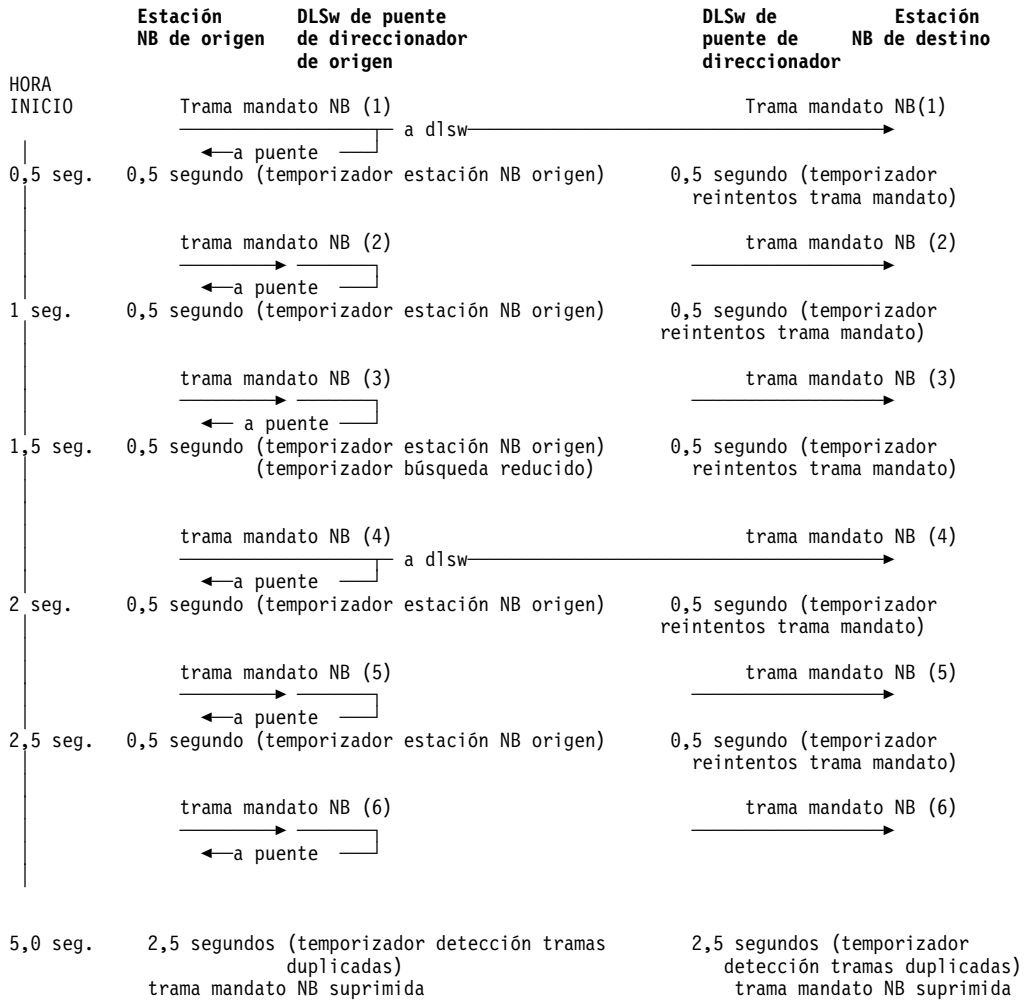



*Figura 24. Configuración de una sesión NetBIOS sobre DLSw. La función de filtrado de duplicados reduce el número de tramas de difusión general que se reenvían sobre una WAN DLSw.*

La Figura 24, junto con la siguiente secuencia, muestra cómo funciona el proceso, con los valores por omisión. Para simplificar la explicación, se da por supuesto que no se recibe ninguna trama de respuesta.




La secuencia de sucesos es la siguiente:

1. La primera trama de mandato NetBIOS se recibe en un puerto de puente en el direccionador DLSw de origen. Se guarda una copia de la trama de mandato NetBIOS. Puesto que la conexión por puente está activada, la trama se reenvía por la red de puente. Puesto que, por omisión, la función de filtro de duplicados está desactivada en el puente, no se arranca el temporizador de filtro de tramas duplicadas. Puesto que NetBIOS DLSw está activado, la trama se reenvía por la red DLSw y se arranca el temporizador de búsqueda reducida (valor por omisión, 1-1/2 segundos). El temporizador de detección de tramas duplicadas (valor por omisión, 5 segundos) también se arranca.
2. La función DLSw del direccionador de destino recibe la primera trama de mandato NetBIOS. Se guarda una copia de la trama de mandato NetBIOS. Puesto que la conexión por puente está activada, la trama se reenvía por la red de puente. Puesto que, por omisión, la función de filtro de duplicados está desactivada en el puente, no se arranca el temporizador de filtro de tramas duplicadas. El temporizador de mandato de reintento (valor por omisión, 1/2 segundo) y el temporizador de detección de tramas duplicadas (valor por omisión, 5 segundos) se arrancan.
3. En el direccionador de origen, se recibe la segunda trama de mandato NetBIOS (segundo reintento). Puesto que, por omisión, la función de filtro de duplicados está desactivada en la red de puente, la trama se reenvía a la red de puente. Puesto que no ha transcurrido el tiempo de espera de búsqueda reducida, la trama no se reenvía a la red DLSw.
4. En el direccionador de destino, la función DLSw reenvía un primer reintento de la trama de mandato NetBIOS (generada localmente) a la función de puente. Puesto que, por omisión, la función de filtro de duplicados está desactivada en la red de puente, la trama se reenvía a la red de puente. El temporizador de mandato de reintento (valor por omisión, 1/2 segundo) se arranca.
5. En el direccionador de origen, la tercera trama de mandato NetBIOS (segundo reintento) se gestiona del mismo modo que la segunda trama de mandato NetBIOS.
6. En el direccionador de destino, el segundo reintento de la trama de mandato NetBIOS se gestiona del mismo modo que el primer reintento.
7. En el direccionador de origen, se recibe la cuarta trama de mandato NetBIOS (tercer reintento). Puesto que, por omisión, la función de filtro de duplicados está desactivada en la red de puente, la trama se reenvía a la red de puente. Puesto que ahora ha transcurrido el tiempo de espera de búsqueda reducida, la trama se reenvía a la red DLSw. Se arranca el temporizador de búsqueda reducida.
8. En el direccionador de destino, la función DLSw reenvía un tercer reintento de la trama de mandato NetBIOS (generada localmente) a la función de puente. Puesto que, por omisión, la función de filtro de duplicados está desactivada en la red de puente, la trama se reenvía a la red de puente. El temporizador de mandato de reintento (valor por omisión, 1/2 segundo) se arranca. El direccionador de destino recibe también la trama de mandato NetBIOS reenviada desde el direccionador de origen, pero la elimina como duplicado.
9. En el direccionador de origen, la quinta trama de mandato NetBIOS (cuarto reintento) se gestiona del mismo modo que la segunda trama de mandato NetBIOS.
10. En el direccionador de destino, el cuarto reintento de la trama de mandato NetBIOS se gestiona del mismo modo que el primer reintento.

11. En el direccionador de origen, se recibe la sexta trama de mandato NetBIOS (quinto reintento). Puesto que, por omisión, la función de filtro de duplicados está desactivada en la red de puente, la trama se reenvía a la red de puente. Puesto que no ha transcurrido el tiempo de espera de búsqueda reducida, la trama no se reenvía a la red DLSw.
12. En el direccionador de destino, la función DLSw reenvía un quinto reintento de la trama de mandato NetBIOS (generada localmente) a la función de puente. Puesto que, por omisión, la función de filtro de duplicados está desactivada en la red de puente, la trama se reenvía a la red de puente. Puesto que ya se ha agotado el número máximo de reintentos, el temporizador de reintentos de mandato no se vuelve a arrancar.
13. Transcurridos otros 2-1/2 segundos, en el direccionador de origen el temporizador de detección de tramas duplicadas caduca y la trama de mandato NetBIOS guardada se suprime.
14. Transcurridos otros 2-1/2 segundos, en el direccionador de destino el temporizador de detección de tramas duplicadas caduca y la trama de mandato NetBIOS guardada se suprime.

## Función de filtro de tramas de respuesta

Tanto la trama de mandato de configuración de sesiones NetBIOS como la trama de mandato de estados de NetBIOS esperan una trama de respuesta de NetBIOS correspondiente. Si no se recibe ninguna trama de respuesta, se vuelve a intentar la trama de mandato como en el ejemplo anterior.

Cuando se recibe la primera trama de respuesta de NetBIOS en la red de puente en el direccionador de destino, se reenvía al direccionador de origen y la trama de mandato NetBIOS guardada se suprime. Las siguientes tramas de respuesta que se reciban en el direccionador de destino se eliminan puesto que no se encuentra ninguna trama de mandato NetBIOS correspondiente.

En el direccionador de origen, la trama de respuesta recibida se reenvía por la red de puente y la trama de mandato NetBIOS guardada se suprime. Las siguientes tramas de respuesta que se reciban en el direccionador de origen (procedentes de la red de puente o DLSw) se suprimen.

Las tramas de mandato de conflictos de nombres NetBIOS pueden originar, aunque no la necesitan, una trama de respuesta de NetBIOS correspondiente. Además, se utilizan todas las tramas de respuesta recibidas (para determinar si hay más de un conflicto).

Por lo tanto, todas las tramas de conflictos de nombres NetBIOS se reenvían, pero la trama de mandato NetBIOS no se suprime hasta que caduca el temporizador de detección de tramas duplicadas.

## Listas de nombres NetBIOS

Las listas de nombres NetBIOS constituyen un método, sólo de DLSw, para limitar el número de asociados DLSw a los que se reenvía una trama UI NetBIOS.

Se puede configurar una lista de nombres NetBIOS en cada direccionador. Esta lista de nombres representa todos los nombres NetBIOS conectados a la red conectada por puente localmente del direccionador a los que pueden acceder los asociados DLSw. El direccionador envía la lista de nombres NetBIOS local a todos

los asociados DLSw. Estos asociados utilizan la lista para limitar el tráfico NetBIOS que envía el asociado a este direccionador.

Las listas de nombres NetBIOS resultan útiles en entornos en los que se mantiene un buen control sobre los nombres NetBIOS, especialmente en entornos a los que se debe acceder de forma remota a través de DLSw.

## Configuración de listas de nombres NetBIOS locales

Una lista de nombres NetBIOS es un conjunto de entradas de lista de nombres NetBIOS. Para configurar la lista de nombres NetBIOS local hay que:

- Añadir un máximo de 30 entradas a la lista de nombres
- Configurar si esta lista representa todos los nombres NetBIOS que pueden alcanzar los asociados DLSw del direccionador.

Las entradas de la lista de nombres se configuran en el indicador `NetBIOS config>` con el mandato *add name-list*. Cada entrada contiene la siguiente información:

**calificador de nombre**

Un calificador de nombre representa uno o más nombres NetBIOS. Cada calificador de nombre puede tener un máximo de 16 caracteres. Puede representar varios nombres NetBIOS especificando comodines (un ? intercalado o un * final) en el nombre.

El ? (símbolo de interrogación) significa que el carácter de dicha posición del nombre NetBIOS puede tener cualquier valor.

El * (asterisco) como último carácter de un nombre significa que todos los caracteres restantes del nombre NetBIOS pueden tener cualquier valor.

**Nota:** En la mayoría de las aplicaciones NetBIOS de cliente/servidor, los únicos nombres necesarios en las listas de nombres son los de los servidores o los dominios. No hace falta que los nombres de los clientes se configuren en las listas de nombres.

**tipo de calificador de nombre**

Los nombres NetBIOS pueden ser nombres individuales o nombres de grupo. Cada calificador de nombre representa un conjunto de nombres NetBIOS individuales o un conjunto de nombres NetBIOS de grupo. El tipo de calificador de nombre especifica el tipo de nombres NetBIOS (individual o grupo) que representa el calificador de nombre correspondiente.

Como normal general, los nombres de dominios son nombres de grupos y los nombres de clientes y servidores son nombres individuales.

La propia lista de nombres tiene un atributo que se configura en el indicador `NetBIOS config>` mediante el mandato SET NAME-LIST. Este atributo es *exclusividad de lista de nombres*

El atributo indica si el conjunto de entradas de la lista de nombres representa todos los nombres NetBIOS que pueden alcanzar los asociados DLSw de este direccionador (exclusivo) o representa algunos, pero no necesariamente todos, nombres NetBIOS que pueden alcanzar los asociados DLSw de este direccionador (no exclusivo).

Una lista de nombres exclusiva funciona mejor en cuanto a la limitación de tráfico DLSw NetBIOS de la red. Sólo las tramas destinadas a un nombre NetBIOS repre-

sentado por la lista de nombres exclusiva de un direccionador se reenvían a este direccionador.

Una lista de nombres no exclusiva ayuda a limitar el tráfico DLSw NetBIOS de la red, aunque no de forma tan eficaz como la lista de nombres exclusiva. Las tramas destinadas a un nombre NetBIOS representado por una lista de nombres no exclusiva de un direccionador se reenviarán primero a dicho direccionador.

Si el direccionador recibe una trama destinada a un nombre NetBIOS que no está representado en ninguna lista de nombres del direccionador, el direccionador reenvía la trama a todos los direccionadores con listas de nombres no exclusivas.

Se puede controlar el modo en que un determinado direccionador utiliza su lista de nombres NetBIOS local y las listas de nombres recibidas de sus asociados DLSw mediante los siguientes parámetros:

**use local NetBIOS name list**

Esta función se configura con el mandato **enable name-list local** o **disable name-list local** en el indicador `NetBIOS config>`.

Si activa la opción utilizar lista de nombres NetBIOS local, el direccionador envía la lista de nombres NetBIOS local configurada en el direccionador a todos los asociados DLSw.

Si desactiva la opción utilizar lista de nombres NetBIOS local, el direccionador no envía la lista de nombres NetBIOS configurada en el direccionador a todos los asociados DLSw.

**use remote NetBIOS name lists**

Esta función se configura con el mandato **enable name-list remote** o **disable name-list remote** en el indicador `NetBIOS config>`.

Si activa la opción utilizar listas de nombres NetBIOS remotas, el direccionador utiliza todas las listas de nombres NetBIOS que recibe de los asociados DLSw del direccionador para determinar el modo de reenviar determinadas tramas NetBIOS.

Si desactiva la opción utilizar listas de nombres NetBIOS remotas, el direccionador para por alto todas las listas de nombres NetBIOS recibidas de los asociados DLSw del direccionador.

## Confirmación de cambios de listas de nombres NetBIOS

Puede cambiar todos los parámetros de las listas de nombres NetBIOS de forma permanente en el indicador `NetBIOS config>` o de forma temporal en el indicador `NetBIOS>`.

Puesto que por cada cambio efectuado el direccionador debe enviar información a cada asociado DLSw, puede indicar que los cambios de las listas de nombres están listos para ser utilizados entrando **set name-list** en el indicador `NetBIOS>`.

## Utilización de listas de nombres NetBIOS

El direccionador utilizar listas de nombres NetBIOS para determinar el modo de reenviar las siguientes tramas NetBIOS:

- Trama de mandato de configuración de sesiones NetBIOS (Name-Query)
- Trama de mandato de estados de NetBIOS (Status-Query)
- Trama de transferencia de datos sin conexión de NetBIOS (Datagram)

***Utilización de listas de nombres NetBIOS exclusivas de forma eficiente:*** Configure listas de nombres NetBIOS exclusivas siempre que le sea posible. Si configura y envía una lista de nombres exclusiva a todos los asociados DLSw, las únicas tramas NetBIOS que se recibirán de los asociados DLSw serán las tramas cuyos nombres de destino coincidan con una de las entradas de la lista de nombres.

Una lista de nombres NetBIOS exclusiva muy útil es la lista de nombres NetBIOS vacía. Si un determinado direccionador no tiene definido ningún servidor NetBIOS al que deba acceder ninguno de sus asociados DLSw, utilice una lista de nombres exclusiva vacía.

***Utilización de listas de nombres NetBIOS no exclusivas:*** Si un direccionador tiene muchos asociados DLSw en distintas redes conectadas por puente, puede utilizar listas de nombres no exclusivas. Se pueden configurar entradas de listas de nombres para los servidores que se utilizan con más frecuencia de modo que el tráfico destinado a estos servidores pase primero por este direccionador. La posibilidad de especificar la lista de nombre como no exclusiva permite que el tráfico vaya a los servidores que se utilizan con menos frecuencia sin tener que configurar los servidores en la lista de nombres. Utilice este configuración en una red sin un buen control de los nombres NetBIOS; especialmente los servidores a los que se tiene que acceder de forma remota a través de DLSw.

También puede utilizar listas de nombres NetBIOS no exclusivas en configuraciones que contienen vías de acceso DLSw paralelas entre redes conectadas por puente. Si hay dos direccionadores en la misma red conectada por puente, un direccionador puede configurar una lista de nombres NetBIOS que represente un grupo de servidores a los que se tiene que acceder de forma remota a través de DLSw en la red conectada por puente y el otro direccionador puede configurar una lista de nombres NetBIOS que represente otro grupo de servidores. Cuando ambos direccionadores están activos, el tráfico NetBIOS se distribuye entre los dos direccionadores. Si un direccionador está inactivo, todo el tráfico NetBIOS pasará a través del otro direccionador puesto que tiene una lista no exclusiva.

La lista de nombres por omisión es una lista de nombres NetBIOS no exclusiva vacía. Esto indica que un direccionador desea que sus asociados DLSw envían al direccionador todo el tráfico NetBIOS que no puedan reenviar.

## Colocación en antememoria de nombres NetBIOS y colocación en antememoria de rutas

La Colocación en antememoria de nombres NetBIOS es la función del direccionador que clasifica el tipo de nombre NetBIOS y la información necesaria para alcanzar el nombre NetBIOS. Esta información sirve para determinar del mejor modo de reenviar las tramas NetBIOS no filtradas al menor número posible de DLSw contiguos y al menor número posible de puertos de puente. Los posibles tipos de nombres NetBIOS y la información que se guarda para cada uno de ellos se muestra a continuación

**Remoto individual**

Es un nombre NetBIOS que se sabe que se puede alcanzar de forma remota a través de una sesión TCP DLSw determinada. Las mejores sesiones TCP se guardan.

**Local individual**
Es un nombre NetBIOS que se sabe que se puede alcanzar de forma local a través de la red de puente. La dirección MAC asociada al nombre se guarda. Si la colocación en antememoria de rutas está activada, también se guarda la mejor ruta LLC entre el direccionador y la estación NetBIOS.

**Grupo**
Es un nombre NetBIOS que se sabe es un nombre de grupo. Se puede alcanzar de forma remota y/o local y puede representar varias estaciones NetBIOS. No se guarda ninguna otra información.

**Desconocido**
La información sobre el nombre NetBIOS aún no se conoce, lo que indica que la búsqueda del nombre no ha finalizado. No se guarda ninguna otra información.

Cuando se reciben tramas de configuración de sesiones NetBIOS o tramas de transferencia de datos sin conexión, la antememoria de nombres sirve para determinar el modo de reenviar la trama. Si una de estas tramas se recibe en la red de puente en el direccionador, se emprende una de las siguientes acciones:

- Si el nombre de destino de la trama NetBIOS no está en la antememoria de nombres NetBIOS del direccionador, se busca una coincidencia en las listas de nombres de todos los asociados DLSw.

  Si se encuentran coincidencias con calificadores de nombres de grupos, se crea una entrada de antememoria de nombres NetBIOS con el tipo de nombre *grupo.* La trama se reenvía a todos los puertos de puente y a todos los asociados DLSw con listas de nombres no exclusivas o listas de nombres exclusivas con una entrada coincidente de la lista de nombres.

  Si se encuentran coincidencias con calificadores de nombres individuales, se crea una entrada de antememoria de nombres NetBIOS con el tipo de nombre *remoto individual.* La trama se reenvía a cada asociado DLSw con una entrada coincidente de su lista de nombres.

  Si no se encuentran coincidencias, se crea una entrada de antememoria de nombres NetBIOS con el tipo de nombre *desconocido.* La trama se reenvía a todos los puertos de puente y a todos los asociados DLSw con listas de nombres no exclusivas.

- Si el nombre de destino de la trama NetBIOS está en la antememoria de nombres NetBIOS del direccionador y está clasificado como remoto individual, la trama re reenvía a la mejor sesión TCP DLSw aprendida.

  Si existen varias sesiones TCP de igual nivel, se utilizarán de forma alternativa en distintas tramas de configuración de sesiones NetBIOS.

- Si el nombre de destino de la trama NetBIOS está en la antememoria de nombres NetBIOS del direccionador y está clasificado como local individual, la dirección MAC guardada sustituirá a la dirección MAC de destino de la trama NetBIOS.

  Si la colocación en antememoria de rutas está desactivada, la información de direccionamiento de la trama NetBIOS no se toca y la trama se reenvía a todos los puertos de puente.

  Si la colocación en antememoria de rutas está activada, la información de direccionamiento de la trama NetBIOS se actualiza con la información de

direccionamiento guardada y la trama se reenvía al puerto de puente adecuado (determinado por la dirección MAC y la ruta).

- Si el nombre de destino de la trama NetBIOS está en la antememoria de nombres NetBIOS del direccionador y está clasificado como grupo o desconocido, la trama se reenvía a todos los puertos de puente o a todos los DLSw contiguos.

## Cómo aprender nombres NetBIOS

Los nombres NetBIOS se aprenden y clasifican a partir de la información de las tramas de configuración de sesiones NetBIOS (Name-Query y Name-Recognized).

## Configuración de entradas de la antememoria de nombres NetBIOS

Se pueden configurar nombres NetBIOS remotos individuales y asociarlos a una determinada sesión TCP DLSw. Esto puede reducir significativamente la actividad general de búsqueda. Para mejorar el rendimiento, se recomienda configurar los servidores NetBIOS remotos a los que acceden normalmente los clientes NetBIOS en la red de puente local del direccionador.

No se pueden configurar nombres NetBIOS locales individuales y asociarlos a una determinada dirección MAC y ruta.

Hay tres tipos de entradas de la antememoria de nombres NetBIOS:

- Las entradas permanentes son aquellas que se añaden en el indicador de configuración de NetBIOS (`NetBIOS config>`). El direccionador guarda las entradas permanentes en su configuración cuando se vuelve a arrancar el direccionador.

  Entre **add cache-entry** en el indicador `NetBIOS config>` para añadir una entrada permanente. Se le solicitará que entre el nombre NetBIOS y la dirección IP asociada.

- Las entradas estáticas son aquellas que se añaden en el indicador de supervisión de NetBIOS (consola `NetBIOS>`). El direccionador no tiene entradas estáticas cuando se vuelve a arrancar.

  Entre **add cache-entry** en el indicador de consola `NetBIOS>` para añadir una entrada estática. Se le solicitará que entre el nombre NetBIOS y la dirección IP asociada.

- Las entradas dinámicas son aquellas que ***no*** se añaden en los indicadores de configuración ni de supervisión de NetBIOS, sino que se aprenden de forma dinámica a partir de las tramas de configuración de sesiones NetBIOS. El direccionador no guarda las entradas dinámicas cuando se vuelve a arrancar el direccionador.

## Configuración de parámetros de antememoria de nombres

Para evitar que un tipo de nombre NetBIOS llene toda la antememoria de nombres, hay dos límites de antememoria de nombres NetBIOS que se pueden configurar:

- Número máximo de entradas de la antememoria de nombres locales especifica el número máximo de entradas de antememoria de nombres NetBIOS locales individuales que se pueden colocar en antememoria simultáneamente. Las entradas que hace tiempo que no se utilizan se sobregraban con entradas nuevas.

- Número máximo de entradas de antememoria de nombres remotos especifica el número máximo combinado de entradas de antememoria de nombres NetBIOS remotos individuales, de grupo y desconocidos que se pueden colocar en antememoria simultáneamente. Las entradas que hace tiempo que no se utilizan se sobregraban con entradas nuevas.

Si no se hace referencia a una entrada durante un periodo de tiempo que se puede configurar, la entrada se suprime de forma automática. Este periodo de tiempo de espera es el valor de tiempo de espera de la entrada a la que no se ha hecho referencia.

La asociación de un nombre NetBIOS con una sesión TCP o una dirección MAC y una ruta se hace de instancia en instancia. Puesto que las redes cambian y la mejor vía de acceso a un nombre NetBIOS puede cambiar, la asociación entre un nombre NetBIOS y una sesión TCP o una dirección MAC y una ruta sólo se guarda durante un periodo de tiempo que se puede configurar. Una vez transcurrido este periodo de tiempo, se aprende una nueva y mejor asociación de vía de acceso. El parámetro que controla este periodo de tiempo que se puede configurar es el valor de tiempo de espera de caducidad de la mejor vía de acceso.

Otro parámetro de configuración muy útil es el valor de tiempo de espera de búsqueda reducida. Además de controlar el periodo de tiempo en que las tramas de mandato duplicadas se filtran a la red DLSw, controla también el periodo de tiempo que debe esperar antes de expandir la búsqueda de un nombre NetBIOS. Si se recibe una trama de configuración de sesión NetBIOS y el nombre NetBIOS de destino se encuentra en la antememoria de nombres NetBIOS del direccionador como una trama remota individual, la trama se reenvía a la sesión TCP correspondiente. Si no se recibe ninguna respuesta para esta trama, puede deberse a que ya no se puede acceder al nombre a través de esta vía de acceso. La primera trama duplicada de configuración de sesión NetBIOS recibida una vez transcurrido el periodo de búsqueda reducida se envía a todas las sesiones TCP DLSw, con lo que se expande la búsqueda de una vía de acceso mejor.

El último parámetro, caracteres significativos del nombre, controla cuántos de los 16 caracteres de un nombre NetBIOS se necesitan para poder considerarlo un nombre NetBIOS exclusivo. Algunas aplicaciones NetBIOS utilizan el carácter número 16 del nombre NetBIOS para distinguir entre determinadas entidades asociadas a un solo nombre NetBIOS (por ejemplo, servidor de impresión y servidor de archivos). En estos casos, es mejor no especificar más de 15 caracteres significativos en el nombre. Esto hace que cualquier trama cuyos 15 primeros caracteres del nombre NetBIOS de destino coincidan con los 15 primeros caracteres de una entrada de la antememoria de nombres NetBIOS del direccionador se reenvíe de acuerdo a la información de la entrada de la antememoria de nombres. Por lo tanto, se pueden representar varios nombres NetBIOS con una sola entrada de la antememoria de nombres NetBIOS.

Todos los parámetros anteriores relacionados con la antememoria de nombres NetBIOS se pueden configurar mediante el mandato **set cache-parms**, como en el siguiente ejemplo:

```
NetBIOS config>set cache-parms

Significant characters in name [15]?
Best path aging timeout value in seconds [60.0]?
Reduced search timeout value in seconds [1.5]?
Unreferenced entry timeout value in minutes [5000]?
Max nbr local name cache entries [500]?
Max nbr remote name cache entries [100]?

Cache parameters set
```

Consulte el tema “Mandatos de NetBIOS” en la página 178 para obtener más información sobre el mandato **set cache-parms**.

## Cómo visualizar entradas de la antememoria

El direccionador proporciona los siguientes mandatos que le permiten ver las entradas de la antememoria. Desde el indicador de configuración de NetBIOS, puede utilizar los mandatos **list cache** que aparecen en la Tabla 10.

*Tabla 10. Mandatos de configuración de antememoria List Cache de NetBIOS*

| Mandato | Muestra . . . |
|---|---|
| list cache all | Todas las entradas permanentes. No muestra las entradas estáticas ni las dinámicas. |
| list cache entry-number | Una entrada de la antememoria permanente que coincide con el número de entrada |
| list cache NetBIOS-name | Una entrada de la antememoria permanente correspondiente a un determinado nombre NetBIOS. |
| list cache ip-address | Una entrada de la antememoria permanente correspondiente a una determinada dirección IP. |

Desde el indicador de supervisión de NetBIOS, puede utilizar los mandatos list cache que aparecen en la Tabla 11.

*Tabla 11. Mandatos de supervisión List Cache de NetBIOS*

| Mandato | Muestra . . . |
|---|---|
| list cache active | Todas las entradas de la antememoria de nombres del direccionador, que incluyen entradas permanentes, estáticas y dinámicas. |
| list cache config | Entradas estáticas y permanentes No muestra las entradas dinámica. |
| list cache group | Entradas existentes para nombres de grupo NetBIOS. |
| list cache local | Entradas locales de la antememoria. Las entradas locales de la antememoria son aquellas que el direccionador aprende sobre la red conectada por puente. |
| list cache name | Una entrada de la antememoria correspondiente a un determinado nombre NetBIOS. |
| list cache remote | Entradas remotas de la antememoria. Son las entradas que el direccionador aprende sobre la WAN DLSw. |
| list cache unknown | Entradas cuyo tipo de entrada NetBIOS es desconocido. El direccionador que todas las entradas son desconocidas hasta que aprende el tipo de entrada. |

## Procedimientos de configuración de la función de filtro de nombres de sistema principal NetBIOS y de bytes

Las siguientes secciones contienen ejemplos sobre cómo configurar la función de filtro de NetBIOS. La primera sección explica cómo crear un filtro de nombres de sistema principal. La segunda indica cómo configurar un filtro de bytes. Para obtener más información sobre los mandatos utilizados en estos ejemplos, consulte el tema “Mandatos de NetBIOS” en la página 178.

Para crear un filtro de nombres de sistema principal, entre los mandatos en el indicador `NetBIOS Filter config>`.

```
Config>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>NetBIOS

NetBIOS Support User Configuration

NetBIOS config>set filter name
NetBIOS Filtering configuration
NetBIOS Filter config>
```

## Cómo crear un filtro de nombres de sistema principal

Utilice el siguiente procedimiento para crear un filtro de nombres de sistema principal.

1. Cree una lista vacía de filtros de nombres.

   ```
   NetBIOS Filter config>create name-filter-list
   Handle for Name Filter List []? boston
   ```

2. Añada los elementos de filtro a la lista de filtros de nombres.

   Entre **update** para obtener el indicador para esta lista específica de filtros. Desde este indicador puede añadir elementos de filtro a la lista de filtros.

   ```
   NetBIOS Filter config>update
   Handle for Filter List []? boston
   Name Filter List Configuration
   NetBIOS Name boston config>
   ```

3. Añada los elementos de filtro a la lista de filtros con el mandato **add**. El modo en que se configuran los elementos de filtro determina qué paquetes NetBIOS se conectan por puente o se eliminan. Configure los elementos de filtro de nombres de sistema principal con los siguientes parámetros especificados en este orden:

   - *Inclusive* (conectado por puente) o *Exclusive* (eliminado).
   - *ASCII* o *HEX* - cómo se representa el nombre del sistema principal.
   - *host name* - el nombre real del sistema principal representado en una serie ASCII o hex (consulte el tema “Mandatos de NetBIOS” en la página 178 para ver la sintaxis).

     **Nota:** Esta entrada es sensible a mayúsculas y minúsculas.

   - <*ÚLTIMO-número-hex*> - un parámetro opcional para ser utilizado con series ASCII que contienen menos de 16 caracteres.

   El siguiente ejemplo añade un elemento de filtro a la lista de filtros de nombres de sistema principal **boston**, que permite que los paquetes que contienen el nombre del sistema principal **westboro** (una serie ASCII) se conecten por puente (se configuran como *inclusive*). No se ha configurado ningún parámetro <*ÚLTIMO-número-hex*> para esta entrada.

```
NetBIOS Name boston config>add inclusive ascii
Hostname []? westboro
Special 16th character in ASCII hex (<CR> for no special char) []?
```

Puede entrar todos los parámetros como una serie en la línea de mandatos si no desea que se le solicite información. Asegúrese de especificar un espacio entre cada parámetro.

4. Compruebe la entrada del elemento de filtro.

   Escriba **list** para comprobar la entrada:

```
NetBIOS Name boston config>list

NAME Filter List Name: boston
NAME Filter List Default: Inclusive

 Item #   Type    Inc/Ex    Hostname         Last Char

   1      ASCII    Inc      westboro
```

5. Añada más elementos de filtro a la lista de filtros.

   Repita los cuatro primeros pasos para añadir elementos de filtro a la lista de filtros. El orden en que especifica los elementos de filtro es importante porque determina el modo en que el direccionador aplica los elementos de filtro a un paquete. La primera coincidencia detiene la aplicación de elementos de filtro y el direccionador reenvía o elimina el paquete, en función de si el elemento de filtro es Inclusive o Exclusive.

   Si entra los elementos de filtro más comunes en primer lugar, el proceso de la función de filtro será más eficaz porque habrá más probabilidades de que el software encuentre una coincidencia al principio de la lista.

   Si el paquete no coincide con ninguno de los elementos de filtro, el direccionador utiliza la condición por omisión (Inclusive o Exclusive) de la lista de filtros. Puede cambiar la condición por omisión de la lista entrando **default inclusive** o **default exclusive** en el indicador de configuración de lista de filtros. Por ejemplo:

```
NetBIOS Name boston config> default exclusive
```

6. Cuando termine de añadir elementos de filtro a la lista de filtros, entre **exit** para volver al indicador `NetBIOS Filter config>`.

```
NetBIOS Name boston config>exit
NetBIOS Filter config>
```

7. Añada el filtro a su configuración.

   La lista de filtros que contiene los elementos de filtro ya se puede añadir como un filtro a la configuración del direccionador de conexión por puente. Para ello, utilice el mandato **filter-on**. Configure los filtros de nombres de sistema principal con los siguientes parámetros (especificados en este orden):

   - *Input* (para filtrar todos los paquetes NetBIOS recibidos en este puerto) o salida (para filtrar todos los paquetes NetBIOS transmitidos en este puerto).
   - *Port Number*, que es el número de puerto de puente configurado deseado del direccionador.
   - *Filter-list*, que es el nombre de la lista de filtros (que contiene elementos de filtro) que desea incluir en este filtro.

- Un operador opcional que se especifica como AND u OR, en mayúsculas. Si hay un operador, debe ir seguido de un nombre de lista de filtros. Los filtros con más de una lista de filtros reciben el nombre de filtros complejos.

El siguiente ejemplo añade un filtro de nombres de sistema principal que afectará a la entrada de paquetes en el puerto 3. Consta de la lista de filtros de nombres de sistema principal **boston**. Todos los paquetes que entran en el puerto 3 se examinan de acuerdo con las reglas suministradas por los elementos de filtro contenidos en la lista de filtros **boston**. Esto significa que todos los paquetes que entran en el puerto 3 que contienen el nombre de sistema principal **westboro** se conectan por puente.

```
NetBIOS Filter config>filter-on input
Número puerto [1] ? 3
Lista filtros []? boston
```

8. Compruebe el filtro que acaba de crear.

   Entre **list** para comprobar la entrada:

```
NetBIOS Filter config>list

NetBIOS Filtering: Disabled

NetBIOS Filter Lists
--------------------

    Handle           Type
    nlist            Name
    newyork          Name
    HELLO            Byte
    boston           Name

NetBIOS Filters
---------------

    Port #      Direction      Filter List Handle(s)
       3          Output       nlist
       1          Input        newyork OR HELLO
       3          Input        boston
```

9. Active de forma global la función de filtro de NetBIOS.

   Utilice el mandato **enable** para activar de forma global la función de filtro de NetBIOS en el direccionador.

```
NetBIOS Filter config>enable NetBIOS-filtering
```

10. Vuelva a arrancar el direccionador para activar todos los cambios en la configuración de la función de filtro de NetBIOS.

    Entre **exit** seguido de **Control-P** para volver al indicador *. Desde este indicador, entre **restart** para activar todos los cambios de software efectuados durante el proceso de configuración de la función de filtro de NetBIOS.

```
NetBIOS Filter config>exit
ASRT config>exit
Config> Ctrl-P
* restart
```

## Cómo crear un filtro de bytes

Utilice el siguiente procedimiento como guía para crear un filtro de bytes. Entre todos los mandatos en el indicador `NetBIOS filtering config>`.

```
Config>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>NetBIOS

NetBIOS Support User Configuration

NetBIOS config> set filter byte
NetBIOS Filtering configuration
NetBIOS Filter config>
```

1. Cree una lista de filtros vacía mediante el mandato **create byte-filter-list**.

   ```
   NetBIOS Filter config>create byte-filter-list
   Handle for Byte Filter List []? westport
   ```

2. Añada los elementos de filtro a la lista de filtros de bytes.

   Entre **update** para obtener el indicador para esta lista específica de filtros. Desde este indicador puede añadir elementos de filtro a la lista de filtros.

   ```
   NetBIOS Filter config>update
   Handle for Filter List []? westport
   Byte Filter List Configuration
   NetBIOS Byte westport config>
   ```

   Empiece a añadir elementos de filtro a la lista de filtros con el mandato **add**. El modo en que se configuran los elementos de filtro determina qué paquetes NetBIOS se conectan por puente o se eliminan. Los elementos de filtros de bytes se configuran con los siguientes parámetros (especificados en este orden):

   - Inclusive (conectado por puente) o Exclusive (eliminado).
   - Byte Offset - el número de bytes (en decimal) a desplazar en el paquete que se filtra. Comienza en la cabecera NetBIOS del paquete. Cero especifica que el direccionador examinará todos los bytes del paquete.
   - Hex pattern - un número hexadecimal utilizado para comparar con los bytes que comienzan en el desplazamiento de bytes de la cabecera NetBIOS. Consulte el tema “Mandatos de NetBIOS” en la página 178 para ver las reglas de sintaxis.
   - Hex mask - (si la hay) debe tener la misma longitud que el patrón hex y se le suman (AND) de forma lógica los bytes del paquete que comienzan en el desplazamiento de bytes antes de compararse el resultado con el patrón hex. Si se omite el argumento *máscara-hex*, se considera que todos son unos binarios.

   El siguiente ejemplo añade un elemento de filtro a la lista de filtros de bytes **westboro** que permite que los paquetes con un patrón hex 0x12345678 en el desplazamiento de bytes 0 se conecten por puente (configurado como inclusive). No hay máscara hex.

   ```
   NetBIOS Byte westport config>add inclusive
   Byte Offset [0]? 0
   Hex Pattern []? 12345678
   Hex Mask (<CR> for no mask) []?
   ```

3. Compruebe la entrada del elemento de filtro con el mandato **list**.

   ```
   NetBIOS Byte westport config>list

   BYTE Filter List Name: westport
   BYTE Filter List Default: Inclusive

    Item #   Inc/Ex   Offset  Pattern        Mask

      1       Inc        0    0x12345678     0xFFFFFFFF
   ```

4. Añada más elementos de filtro a la lista de filtros.

Repita los tres primeros pasos para añadir elementos de filtro a la lista de filtros.

5. Cuando termine de añadir elementos de filtro a la lista de filtros, escriba **exit** para volver al indicador `NetBIOS Filter config>`.

```
NetBIOS Byte westport config>exit
NetBIOS Filter config>
```

El orden en que especifica los elementos de filtro es importante porque determina el modo en que el direccionador aplica el filtro a un paquete. La primera coincidencia detiene la aplicación de elementos de filtro y el direccionador reenvía o elimina el paquete, en función de si el elemento de filtro es Inclusive o Exclusive.

Si entra los elementos de filtro más comunes en primer lugar, el proceso de la función de filtro será más eficaz porque habrá más probabilidades de que el software encuentre una coincidencia al principio de la lista, en lugar de tener que comprobar toda la lista para encontrar una coincidencia.

Si el paquete no coincide con ninguno de los elementos de filtro, el direccionador utiliza la condición por omisión (Inclusive o Exclusive) de la lista de filtros. Puede cambiar la condición por omisión de la lista entrando **default inclusive** o **default exclusive** en el indicador de configuración de lista de filtros. Por ejemplo:

```
NetBIOS Byte westport config> default exclusive
```

6. Añada el filtro a su configuración.

La lista de filtros que contiene los elementos de filtro ya se puede añadir como un filtro a la configuración del direccionador de conexión por puente. Para ello, utilice el mandato **filter-on**. Configure los filtros de nombres de sistema principal con los siguientes parámetros (especificados en este orden):

- *Input* (para filtrar todos los paquetes recibidos en este puerto) o salida (para filtrar todos los paquetes transmitidos en este puerto).
- *Port Number* - el número del puerto de puente configurado.
- *Filter-list* - el nombre de la lista de filtros (que contiene elementos de filtro) que desea incluir en este filtro.
- Un operador opcional que se especifica como AND u OR, en mayúsculas. Si hay un operador, debe ir seguido de un nombre de lista de filtros. Los filtros con más de una lista de filtros reciben el nombre de filtros complejos. Estos se explican con más detalle en el tema “Acerca de los mandatos de configuración y supervisión de NetBIOS” en la página 175.

El siguiente ejemplo añade un filtro de nombres de sistema principal que afectará a los paquetes de salida del puerto 3. Consta de la lista de filtros de bytes **westboro**. Todos los paquetes de salida del puerto 3 se comprobarán en función de las reglas suministradas por los elementos de filtro contenidos en la lista de filtros **westboro**.

```
NetBIOS Filter config>filter-on output
Port Number [1]? 3
Filter List []? westboro
```

7. Compruebe el filtro que acaba de crear.

Entre **list** para comprobar la entrada:

```
NetBIOS Filter config>list

NetBIOS Filtering: Disabled

NetBIOS Filter Lists
--------------------

    Handle           Type
    nlist            Name
    newyork          Name
    HELLO            Byte
    westboro         Byte

NetBIOS Filters
---------------

    Port #      Direction      Filter List Handle(s)
       3          Output       nlist
       1          Input        newyork OR HELLO
       3          Output       westboro
```

8. Active de forma global la función de filtro de NetBIOS.

   Entre **enable** para activar de forma global la función de filtro de NetBIOS en el direccionador de la conexión por puente.

```
NetBIOS Filter config>enable NetBIOS-filtering
```

9. Vuelva a arrancar el direccionador para activar todos los cambios en la configuración de la función de filtro de NetBIOS.

   Entre **exit** seguido de **Control-P** para volver al indicador *. Entre **restart**.

```
NetBIOS Filter config>exit
ASRT config>exit
Config> Ctrl-P
* restart
```

# Configuración y supervisión de NetBIOS

Este capítulo describe la configuración y supervisión de IBM de NetBIOS sobre redes conectadas por puentes y sobre redes DLSw. Incluye los siguientes temas:



## Acerca de los mandatos de configuración y supervisión de NetBIOS

Los mandatos de configuración de NetBIOS se emiten desde el indicador `ASRT/DLSW config>`. Los cambios que se hacen en la configuración del direccionador no entran en vigor de forma inmediata. Pasan a formar parte de la memoria de configuración del direccionador hasta que lo vuelve a arrancar. Este capítulo trata los cambios en la configuración como permanentes.

Los mandatos de supervisión de NetBIOS se emiten en el indicador `ASRT/DLSW>`. Los mandatos de supervisión entran en vigor de forma inmediata, pero no se guardan en la memoria de configuración no volátil del direccionador. Por lo tanto, aunque los mandatos de supervisión le permiten efectuar cambios en tiempo real en la configuración del direccionador, estos cambios son temporales. La memoria de configuración del supervisor los sobregraba cuando se vuelve a arrancar el direccionador. Este capítulo trata los cambios que efectúa en el indicador de supervisión como estáticos.

## Cómo acceder al entorno de configuración de NetBIOS

Puede visualizar el indicador `NetBIOS config>` desde el entorno de configuración ASRT o desde el entorno de configuración DLSw. Los cambios que efectúe en el indicador `NetBIOS config>` afectan tanto a la conexión por puente como a DLSw.

**Nota:** Los mandatos de configuración de NetBIOS no entran en vigor de forma inmediata. Debe volver a arrancar o volver a cargar el dispositivo para que entren en vigor.

Para visualizar el indicador `NetBIOS config>` desde el entorno de configuración ASRT:

```
Config>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>NetBIOS

NetBIOS Support User Configuration

NetBIOS config>
```

Para visualizar el indicador `NetBIOS config>` desde el entorno de configuración DLSw:

```
Config>protocol dls
DLSw protocol user configuration
DLSw config>NetBIOS

NetBIOS Support User Configuration

NetBIOS config>
```

## Cómo acceder al entorno de supervisión de NetBIOS

Puede visualizar el indicador NetBIOS> desde el entorno de supervisión ASRT o desde el entorno de supervisión DLSw.

Los cambios que efectúe en el indicador de supervisión NetBIOS> afectan tanto a la conexión por puente como a DLSw.

Para visualizar el indicador de supervisión NetBIOS> desde el entorno de supervisión ASRT:

```
+ protocol asrt
ASRT>NetBIOS

NetBIOS Support User Console

NetBIOS>
```

Para visualizar el indicador NetBIOS> desde el entorno de supervisión DLSw:

```
+ protocol dls
DLSw>NetBIOS

NetBIOS Support User Console

NetBIOS>
```

## Configuración de NetBIOS para DLSw

Si va a enviar tráfico NetBIOS sobre DLSw, utilice este procedimiento desde el indicador DLSw config>:

- Abra SAP de NetBIOS.
- Defina una prioridad para sesiones SNA y NetBIOS.
- Defina el tamaño máximo de trama NetBIOS.
- Defina el número de bytes a asignar para tramas UI NetBIOS.

### Cómo abrir SAP de NetBIOS

Abra SAP de NetBIOS a ambos extremos del enlace para permitir que DLSw transmita tramas NetBIOS.

```
DLSw config> open-sap
Interface # [0]?
Enter SAP in hex(range 0-F0),'SNA', or 'NB'[4]? nb
SAP F0 opened on interface 0
```

### Definición de una prioridad para sesiones SNA y NetBIOS

Puede definir una prioridad para el tráfico SNA y NetBIOS para evitar que un tipo de sesión utilice demasiado ancho de banda durante una congestión de red. Para ello, entre **priority** para definir una prioridad para sesiones SNA y sesiones NetBIOS. También debe definir la asignación de mensajes correspondiente a una prioridad de sesión.

Utilice el mandato **set priority** tal como se muestra en el siguiente ejemplo:

```
DLSw config> set priority
Default priority for SNA DLSw session traffic (C/H/M/L) [M]?  C
Default priority for NetBIOS DLSw session traffic (C/H/M/L) [M]? L
Default priority for SNA DLSw explorer traffic (C/H/M/L) [M]?  H
Default priority for NetBIOS DLSw explorer traffic (C/H/M/L) [M]? M
Message allocation by C/H/M/L priority (4 digits) [4/3/2/1]?
Maximum NetBIOS frame size (516, 1470, 2052, or 4399) [2052]? 516
```

La asignación de mensajes por omisión, 4/3/2/1, ofrece la siguiente asignación a las sesiones:

4 - Crítica
3 - Alta
2 - Media
1 - Baja

El direccionador utiliza la prioridad y la asignación de mensajes para limitar de forma selectiva la longitud de ráfaga de determinados tipos de tráfico. Por ejemplo:

- Si asigna al tráfico SNA la prioridad Crítica y las sesiones Críticas tienen un valor de asignación de mensajes igual a 4

  ***y***

- Asigna al tráfico NetBIOS una prioridad Media y las sesiones Medias tienen un valor de asignación de mensajes igual a 2,

el direccionador procesa cuatro tramas SNA antes de procesar dos tramas NetBIOS. Después de procesar dos tramas NetBIOS, el direccionador procesa cuatro tramas SNA, y así sucesivamente.

En este escenario, el direccionador dedica dos terceras partes del ancho de banda disponible al tráfico SNA (una proporción de 4 a 2). Tenga en cuenta que el direccionador cuenta tramas, no bytes, al asignar ancho de banda en función de las prioridades asignadas.

Puede cambiar la asignación de mensajes por omisión (4/3/2/1) correspondiente a las sesiones. Siempre debe entrar cuatro dígitos, comprendidos entre 9 y 1, en orden descendente. Por ejemplo, si la prioridad SNA es Crítica y el tráfico NetBIOS es Medio, y cambia la asignación de mensajes por 8/7/6/5, el direccionador procesa ocho tramas SNA antes de procesar seis tramas NetBIOS.

## Definición del tamaño máximo de trama NetBIOS

También puede utilizar el mandato **set priority** de DLSw para cambiar el tamaño máximo de trama NetBIOS. El valor por omisión es 2052. Defina este parámetro con el valor del tamaño mayor de trama que espera necesitar; no defina un valor superior. Si define un tamaño de trama superior al necesario, reduce el número de almacenamientos intermedios disponibles.

## Definición de la asignación de memoria para tramas UI NetBIOS

Utilice el mandato **set memory** de DLSw para definir el número de bytes que asigna el direccionador como un almacenamiento intermedio para tramas UI NetBIOS. Si el almacenamiento intermedio de transmisión de TCP se llena, el direccionador utiliza este almacenamiento intermedio para las tramas UI NetBIOS.

Tenga en cuenta que el número de bytes asignado para NetBIOS es global, no por sesión.

```
DLSw config> set memory
Number of bytes to allocate for DLSw (at least 26368) [141056]?
Number of bytes to allocate per LLC session [8192]?
Number of bytes to allocate per SDLC session [4096]?
Number of bytes to allocate for NetBIOS UI-frames [40960]?
```

# Mandatos de NetBIOS

La Tabla 12 contiene los mandatos de configuración y supervisión de NetBIOS.

*Tabla 12. Mandatos de configuración y supervisión de NetBIOS*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Add | Añade entradas de antememoria a la antememoria de nombres del direccionador y añade entradas de lista de nombres a la lista de nombres locales del direccionador. |
| Delete | Suprime entradas de antememoria o entradas de lista de nombres añadidas mediante el mandato **add**. |
| Disable | Desactiva la función de filtro de tramas duplicadas, la colocación en antememoria de rutas y la utilización de listas de nombres NetBIOS locales y remotas. |
| Enable | Activa la función de filtro de tramas duplicadas, la colocación en antememoria de rutas y la utilización de listas de nombres NetBIOS locales y remotas. |
| List | Muestra información de configuración de antememoria de nombres y de lista de nombres NetBIOS, en función de si se encuentra en el indicador de configuración o en el indicador de supervisión. |
| Set | Configura parámetros para la colocación en antememoria de nombres, la función de filtro de tramas duplicadas, la función de filtro de tipos de tramas y las listas de nombres. También muestra el indicador `NetBIOS Filter config>`. |
| Test | Este mandato sólo está disponible en el indicador de supervisión y compara un determinado nombre NetBIOS con las listas actuales de nombres y antememoria de nombres NetBIOS. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

# Respuesta a mandatos de configuración de NetBIOS

Los mandatos de configuración de NetBIOS (Talk 6) no entran en vigor de forma inmediata. Permanecen pendientes hasta que emite el mandato **reload** o **restart**.

# Add

Añade una nueva entrada de antememoria de nombres a la configuración estática o permanente del direccionador o bien añade una entrada de lista de nombres NetBIOS que sirve para limitar el acceso de estaciones remotas a DLSWs locales. Sólo Puede añadir entradas de antememoria de nombres para DLSw contiguos. El direccionador pasa por alto las entradas añadidas para el tráfico ASRT.

**Sintaxis:**

| | |
|---|---|
| a**dd** | cache-entry |
| | name-list |

**cache-entry**

Añade una nueva entrada a la antememoria de nombres del direccionador.

- Desde el indicador de configuración, añade una entrada permanente.
- Desde el indicador de supervisión, añade una entrada temporal.

El direccionador le solicitará el carácter número 16 en hex sólo si ha indicado mediante **set cache-parms** que 16 caracteres del nombre NetBIOS son relevantes.

Se pueden añadir varias entradas con distintas direcciones IP para un solo nombre NetBIOS. Esto permite acceder al nombre a través de distintos DLSw contiguos.

**Nota:** El nombre NetBIOS es sensible a mayúsculas y minúsculas y debe tener las mismas mayúsculas y minúsculas que el nombre NetBIOS de la red.

**Ejemplo: `add cache-entry`**

```
Enter up to 15 characters of NetBIOS name (no wild cards)
Enter NetBIOS name[]? Accounting
Enter last character of NetBIOS name in hex [0]? 01
Enter IP Address [0.0.0.0]? 20.2.1.3
Name cache entry has been created
```

**name-list** Añade una nueva entrada a la lista de nombres local del direccionador.

***Desde el indicador de configuración,*** añade una entrada de lista de nombres permanente. El cambio no entra en vigor hasta que se vuelve a arrancar el direccionador o se confirma el cambio desde el indicador `NetBIOS>` mediante el mandato **set name-list**.

***Desde el indicador de supervisión,*** añade una entrada de lista de nombres temporal. El cambio no entra en vigor hasta que se confirma desde el indicador `NetBIOS>` mediante el mandato **set name-list**. El cambio se pierde cuando se vuelve a arrancar el direccionador.

El calificador de nombre NetBIOS representa uno o más nombres NetBIOS a los que se puede acceder en esta red conectada por puente de forma local del direccionador a los que deben poder acceder otros direccionadores a través de DLSw.

El calificador de nombre NetBIOS puede contener dos tipos de comodines:

**? (signo de interrogación)**
Indica que un solo carácter de un nombre NetBIOS real puede tener cualquier valor.

*** (asterisco)**
Al final de un calificador de nombre indica que el resto de los caracteres de un nombre NetBIOS real pueden tener cualquier valor.

**Notas:**

1. Si no aparece ningún asterisco al final de un calificador de nombre, el resto del calificador de nombre hasta llegar al máximo de 16 caracteres se rellena con nulos (ceros hex).
2. El calificador de nombres NetBIOS es sensible a mayúsculas y minúsculas y debe tener las mismas mayúsculas y minúsculas que los nombres NetBIOS de la red.

**Ejemplo: `add name-list`**

```
Enter up to 16 characters of NetBIOS name qualifier (wild cards OK).
  Enter name qualifier []? NY_SERV*
NetBIOS name qualifier type (I=individual, G=group) [I]?

Name list entry has been created

For the new entry to take effect, restart or commit the change using
  't 5' : 'SET NAME-LIST'.
```

## Delete

Suprime entradas de la antememoria de nombres o entradas de la lista de nombres NetBIOS.

**Sintaxis:**

| | |
|---|---|
| de**lete** | cache-entry<br>name-list |

**cache-entry**

***Desde el indicador de configuración***, suprime entradas de la antememoria de nombres de la configuración permanente del direccionador. El indicador solicita un número de registro, que es el número de la entrada que desea suprimir. Para ver una lista de números de entradas, especifique **list cache all**.

***Desde el indicador de supervisión***, suprime entradas de la antememoria de nombres de la configuración estática del direccionador o de la antememoria activa. El direccionador solicita un nombre de entrada de antememoria. Para ver una lista de entradas, especifique **list cache conf** o **list cache active**.

**Nota:** El nombre NetBIOS es sensible a mayúsculas y minúsculas.

**Ejemplo de configuración `delete cache-entry`**

```
Enter name cache record number [1]? 2

Name cache entry has been deleted
```

**Ejemplo de supervisión: `delete cache-entry`**

```
Enter up to 15 characters of NetBIOS name (no wild cards)
  Enter NetBIOS name []? ADMIN

Name cache entry NOT found in Active list for name entered
Name cache entry has NOT been deleted from Active list

Static name cache entry deleted from Config list
```

**name-list** Suprime una entrada de la lista de nombres local del direccionador.

***Desde el indicador de configuración,*** suprime una entrada de la lista de nombres permanente. El indicador solicita un número de registro que

es el número de la entrada que desea suprimir. Para ver una lista de números de entradas, especifique el mandato **list name-list all**. El cambio no entra en vigor hasta que se vuelve a arrancar el direccionador o se confirma el cambio desde el indicador de supervisión mediante el mandato **set name-list**.

***Desde el indicador de supervisión,*** suprime temporalmente una entrada de la lista de nombres. El indicador solicita un número de registro que es el número de la entrada que desea suprimir. Para ver una lista de números de entradas, especifique el mandato **list name-list config**. El cambio no entra en vigor hasta que se confirma el cambio desde el indicador de supervisión mediante el mandato **set name-list**. El cambio se pierde cuando se vuelve a arrancar el direccionador.

**Ejemplo: `delete name-list`**

```
Enter name list record number [1]? 1

Name list entry NY_SERV*         / INDIVIDUAL has been deleted.

For the deletion to take effect, restart or commit the change using
  't 5' : 'SET NAME-LIST'.
```

## Disable

Desactiva la función de filtro de tramas duplicadas, el uso de listas de nombres NetBIOS o la colocación en antememoria de rutas.

**Sintaxis:**

**disable** duplicate-filtering
name-list local
name-list remote
route-caching

**duplicate-filtering**

Desactiva la función de filtro de tramas duplicadas correspondiente a la conexión por puente. No puede desactivar la función de filtro de tramas duplicadas para el tráfico DLSw.

**Ejemplo: `disable duplicate-filtering`**

```
Duplicate frame filtering is          OFF
```

**name-list local**

Desactiva la utilización de la lista de nombres local. Las entradas de lista de nombres local no se enviarán a ningún asociado DLSw.

Desde el indicador de configuración, desactiva de forma permanente el uso de la lista de nombres local. El cambio no entra en vigor hasta que se vuelve a arrancar el direccionador o se confirma el cambio desde el indicador de supervisión mediante el mandato **set name-list**.

Desde el indicador de supervisión, desactiva de forma temporal el uso de la lista de nombres local. El cambio no entra en vigor hasta que se confirma el cambio desde el indicador de supervisión mediante el mandato **set name-list**. El cambio se pierde cuando se vuelve a arrancar el direccionador.

**Ejemplo: `disable name-list local`**

```
Use of local NetBIOS name list is  DISABLED

For the change to take effect, restart or commit the change using
  't 5' : 'SET NAME-LIST'.
```

**name-list remote**

Desactiva el uso de listas de nombres remotas. No se utilizan las listas de nombres NetBIOS recibidas de asociados DLSw.

***Desde el indicador de configuración,*** desactiva de forma permanente el uso de listas de nombres remotas. El cambio no entra en vigor hasta que se vuelve a arrancar el direccionador o se confirma el cambio desde el indicador de supervisión mediante el mandato **set name-list**.

***Desde el indicador de supervisión,*** desactiva de forma temporal el uso de listas de nombres remotas. El cambio no entra en vigor hasta que se confirma el cambio desde el indicador de supervisión mediante el mandato **set name-list**. El cambio se pierde cuando se vuelve a arrancar el direccionador.

**Ejemplo: `disable name-list remote`**

```
Use of remote NetBIOS name list is  DISABLED

For the change to take effect, restart or commit the change using
  't 5' : 'SET NAME-LIST'.
```

**route-caching**

Desactiva la colocación en antememoria de rutas correspondientes a conexión por puente y a DLSw. La colocación en antememoria de rutas es el proceso de convertir tramas de difusión general en tramas direccionadas específicamente (SRF) utilizando las entradas de la antememoria de nombres NetBIOS.

**Ejemplo: `disable route-caching`**

```
Route caching is                    OFF
```

## Enable

Activa la función de filtro de tramas duplicadas, el uso de listas de nombres NetBIOS o la colocación en antememoria de rutas.

**Sintaxis:**

| | |
|---|---|
| en**able** | duplicate-filtering |
| | name-list local |
| | name-list remote |
| | route-caching |

**duplicate-filtering**

Activa la función de filtro de tramas duplicadas correspondiente a la conexión por puente. La función de filtro de tramas duplicadas siempre está activada para DLSw. No puede activarla ni desactivarla.

**Ejemplo: `enable duplicate-filtering`**

```
Duplicate frame filtering is           ON
```

**name-list local**

Activa la utilización de la lista de nombres local. Las entradas de lista de nombres local se enviarán a todos los asociados DLSw.

Desde el indicador de configuración, activa de forma permanente el uso de la lista de nombres local. El cambio no entra en vigor hasta que se vuelve a arrancar el direccionador o se confirma el cambio desde el indicador de supervisión mediante el mandato **set name-list**.

Desde el indicador de supervisión, activa de forma temporal el uso de la lista de nombres local. El cambio no entra en vigor hasta que se confirma el cambio desde el indicador de supervisión mediante el mandato **set name-list**. El cambio se pierde cuando se vuelve a arrancar el direccionador.

**Ejemplo: `enable name_list local`**

```
Use of local NetBIOS name list is   ENABLED

For the change to take effect, restart or commit the change using
  't 5' : 'SET NAME-LIST'.
```

**name-list remote**

Activa el uso de listas de nombres remotas. Se utilizan todas las listas de nombres NetBIOS recibidas de asociados DLSw.

***Desde el indicador de configuración,*** activa de forma permanente el uso de listas de nombres remotas. El cambio no entra en vigor hasta que se vuelve a arrancar el direccionador o se confirma el cambio desde el indicador de supervisión mediante el mandato **set name-list**.

***Desde el indicador de supervisión,*** activa de forma temporal el uso de listas de nombres remotas. El cambio no entra en vigor hasta que se confirma el cambio desde el indicador de supervisión mediante el mandato **set name-list**. El cambio se pierde cuando se vuelve a arrancar el direccionador.

**Ejemplo: `enable name_list remote`**

```
Use of remote NetBIOS name list is   ENABLED

For the change to take effect, restart or commit the change using
  't 5' : 'SET NAME-LIST'.
```

**route-caching**

Activa la colocación en antememoria de rutas correspondientes a conexión por puente y a DLSw. La colocación en antememoria de rutas es el proceso de convertir tramas de difusión general en tramas direccionadas específicamente (SRF) utilizando la antememoria de nombres NetBIOS.

**Ejemplo: `enable route-caching`**

```
Route caching is                    ON
```

## List (Configuración)

Muestra todas las entradas de antememoria o muestra las entradas de antememoria por tipo de entrada. Muestra información sobre la configuración de filtro o información general de configuración. Muestra entradas de la lista local de nombres NetBIOS.

**Sintaxis:**

| | |
|---|---|
| **list** | cache all<br>cache entry-number<br>cache name<br>cache ip-address<br>filters all<br>filters bridge<br>filters dlsw<br>general<br>name-list all |

name-list *entry-number*

**cache all** Muestra todas las entradas permanentes de la antememoria de nombres del direccionador. No muestra las entradas estáticas ni dinámicas.

**Ejemplo: `list cache all`**

```
Entry  Name                IP Address
-----  ------------------  ---------------

    1  ACCOUNTING     <00>  20.2.1.3
    2  NOTES          <00>  20.2.3.4
```

**cache entry-number** *núm. registro*

Muestra una entrada de la antememoria en función de su número de entrada. Entre **list cache all** para ver una lista de números de entradas.

**Ejemplo: `list cache entry-number`**

```
Enter name cache record number [1]? 1

Entry  Name                IP Address
-----  ------------------  ---------------
    1  ACCOUNTING     <00>  20.2.1.3
```

**cache name** *nombre*

Muestra una entrada de antememoria correspondiente a un determinado nombre NetBIOS. Puede utilizar los siguientes comodines para simplificar la búsqueda:

***** (asterisco) puede sustituir a cero o más ocurrencias de cualquier carácter. Por ejemplo, San* puede dar como resultado:

- San Francisco
- Santa Fe
- San Juan

**?** (símbolo de interrogación) puede sustituir un carácter cualquiera.

**$** (símbolo de dólar) sólo tiene efecto cuando el número de caracteres significativos del nombre NetBIOS no es 16 y cuando el argumento de búsqueda no comienza con un asterisco (*).

Puede utilizar tantos comodines como desee, con un máximo igual al número máximo de caracteres de un nombre NetBIOS (15 ó 16, en función de la configuración).

**Nota:** El nombre NetBIOS es sensible a mayúsculas y minúsculas.

**Ejemplo: `list cache name`**

```
Enter up to 15 characters of NetBIOS name (wild cards ok) []? Acc*

Entry  Name                IP Address
-----  ------------------  ---------------
    1  Accounting     <00>  20.2.1.3
```

**cache ip-address**

Le permite visualizar todas las entradas con una determinada dirección IP.

**Ejemplo: `list cache ip-address`**

```
Enter IP Address [0.0.0.0]? 20.2.1.3

Entry  Name                IP Address
-----  ------------------  ---------------
    1  Accounting     <00>  20.2.1.3
```

**filters all** Muestra si la función de filtro de tipos de tramas está activa o inactiva tanto para la conexión por puente como para DLSw. Utilice los mandatos **set filters bridge** para activar y desactivar estos filtros.

**Ejemplo: `list filters all`**

```
Bridge name conflict filtering is       OFF
Bridge general bcast filtering is       OFF
Bridge trace control filtering is       OFF

DLS name conflict filtering is          ON
DLS general bcast filtering is          ON
DLS trace control filtering is          ON
```

**filters bridge**

Muestra si la función de filtro de tipos de tramas está activa o inactiva para la conexión por puente. Utilice el mandato **set filters bridge** para activar y desactivar estos filtros.

**Ejemplo: `list filters bridge`**

```
Bridge name conflict filtering is       OFF
Bridge general bcast filtering is       OFF
Bridge trace control filtering is       OFF
```

**filters dlsw**

Muestra si la función de filtro de tipos de tramas está activa o inactiva para DLSw. Utilice el mandato **set filters dlsw** para activar y desactivar estos filtros.

**Ejemplo:**

```
list filters dlsw
DLS name conflict filtering is          ON
DLS general bcast filtering is          ON
DLS trace control filtering is          ON
```

**general** Muestra la configuración actual de función de filtro y colocación en antememoria de NetBIOS.

**Ejemplo:**

```
list general
Bridge-only Information:

Bridge duplicate filtering is          OFF
Bridge duplicate frame filter t/o      1.5 seconds

DLS-only Information:
DLS command frame retry count            5
DLS max remote name cache entries      100
DLS command frame retry timeout        0.5 seconds
DLS type of local name list  NON-EXCLUSIVE
DLS use of local name list is     DISABLED
DLS use of remote name list is     ENABLED
```

**name-list all**

Muestra todas las entradas de la lista de nombres NetBIOS local configurada de forma permanente. No muestra entradas estáticas.

**Ejemplo:**

```
list name-list all
Entry  Name Qualifier    Type
-----  ----------------  ----------
  1    NY_SERV*          INDIVIDUAL
  2    NY_DOMAIN*             GROUP
```

**name-list** *número-entrada*

Muestra una entrada de la lista de nombres NetBIOS local configurada de forma permanente.

**Ejemplo:**

```
list name-list entry-number
Enter name list record number [1]? 1

Entry  Name Qualifier    Type
-----  ----------------  ----------
  1    NY_SERV*          INDIVIDUAL
```

## List (Supervisión)

Muestra varios tipos de entradas de la antememoria, configuración de filtros, información general de configuración, listas de nombres NetBIOS o estadísticas sobre otros temas.

**Sintaxis:**

**list**

cache active
cache config
cache group
cache local
cache name
cache remote
cache unknown
filters all
filters bridge
filters dlsw
general
name-list all
name-list config
name-list local
name-list remote
statistics cache
statistics frames bridge
statistics frames dlsw
statistics general bridge
statistics general dlsw

**cache active**

Muestra todas las entradas activas de la antememoria de nombres del direccionador.

El número que aparece entre codillos es el carácter número 16 del nombre NetBIOS. Algunas aplicaciones NetBIOS utilizan este carácter, que puede especificar en hexadecimal si crea la entrada de antememoria, con objetivos especiales.

Si el campo Tipo nombre no especifica LOCAL, se trata de una entrada remota.

**Ejemplo: `list cache active`**

```
Cnt  NetBIOS Name         Name Type          Entry Type
---  -------------------  -----------------  ----------
  1  HYPERION       <01>  INDIVIDUAL LOCAL   DYNAMIC
  2  LANGROUP       <00>  UNKNOWN            STATIC
  3  ACCOUNTING     <00>  GROUP              PERMANENT
```

**cache config**

Muestra todas las entradas estáticas y permanentes de la antememoria de nombres. No muestra las entradas dinámica.

El número que aparece entre codillos es el carácter número 16 del nombre NetBIOS. Algunas aplicaciones NetBIOS utilizan este carácter, que puede especificar en hexadecimal si crea la entrada de antememoria, con objetivos especiales.

**Ejemplo: `list cache config`**

```
Name               IP Address      Source     Last Mod
-----------------  --------------  ---------  ---------
Admin         <00>  20.3.120.8      STATIC     ADDED
Finance       <01>  20.4.96.8       PERMANENT  MODIFIED
Notes         <00>  20.8.210.3      PERMANENT  UNCHANGED
```

**cache group**

Muestra entradas de la antememoria correspondientes a nombres de grupos NetBIOS.

**Ejemplo: `list cache group`**

```
Cnt  NetBIOS Name         Entry Type  Loc Path State  Rem Path State
---  -------------------  ----------  --------------  --------------
  2  HYPERION       <01>  DYNAMIC     UNKNOWN         GROUP
  3  EXCEL          <00>  DYNAMIC     GROUP           GROUP
```

**cache local**

Muestra entradas locales de la antememoria. Las entradas locales de antememoria son las que aprende el direccionador a través de la red local de puente.

Para clientes NetBIOS, el Estado vía local es siembre Desconocido y los campos Dirección MAC e Información de direccionamiento siempre están vacíos.

**Ejemplo: `list cache local`**

```
Cnt  NetBIOS Name     Loc Path State  MAC Address  Routing Information
---  ---------------  --------------  -----------  -------------------
  2  HYPERION   <01>  UNKNOWN
```

**Cnt** Número de la entrada de la antememoria.

**NetBIOS Name**
El nombre NetBIOS de la entrada.

**Loc Path State**
Estado de la vía de acceso local.

**MAC Address**
Si la entrada es un servidor, muestra la dirección MAC del servidor.

**Routing Information**
Muestra información RIF estándar.

**cache name** *nombre*

Muestra una entrada de antememoria correspondiente a un determinado nombre NetBIOS. Puede utilizar los siguientes comodines para simplificar la búsqueda:

***** (asterisco) puede sustituir a cero o más ocurrencias de cualquier carácter. Por ejemplo, San* puede dar como resultado:

- San Francisco
- Santa Fe
- San Juan

**?** (símbolo de interrogación) puede sustituir un carácter cualquiera.

**$** (símbolo de dólar) sólo tiene efecto cuando el número de caracteres significativos del nombre NetBIOS no es 16 y cuando el argumento de búsqueda no comienza con un asterisco (*).

Puede utilizar tantos comodines como desee, con un máximo igual al número máximo de caracteres de un nombre NetBIOS (15 ó 16, en función de la configuración).

**Nota:** Los nombres NetBIOS son sensibles a mayúsculas y minúsculas.

**Ejemplo: `list cache name`**

```
    NetBIOS Name         Name Type          Entry Type
    -------------------  -----------------  ----------
    HYPERION       <01>  INDIVIDUAL REMOTE  DYNAMIC

Count of name cache entry hits ............................. 20

Age of name cache entry ..................................... 689
Age of name cache last reference ............................ 85

Local path information:

  Loc Path State  Timestamp  MAC Address    LFS   Routing Information
  --------------  ---------  ------------  -----  -------------------
  UNKNOWN         689

Remote path information:

  Rem Path State  Timestamp   LFS   IP Address(es)
  --------------  ---------  -----  --------------
  BEST FOUND      85         2052   20.3.120.8
```

**cache remote**

Muestra entradas de la antememoria que el direccionador aprende sobre la WAN DLSw.

**Ejemplo: `list cache remote`**

```
Cnt  NetBIOS Name         Entry Type  Rem Path State  IP Address(es)
---  -------------------  ----------  --------------  --------------
  2  HYPERION       <01>  STATIC      BEST FOUND      20.3.120.8
  3  EXCEL          <00>  DYNAMIC     SEARCH ALL
```

**Cnt** Número de la entrada de la antememoria.

**NetBIOS Name**

El nombre NetBIOS de la entrada.

**Rem Path State**

Estado de la vía de acceso remota. Los estados posibles son:

Best Found
: El direccionador ha encontrado la mejor ruta a esta estación.

Unknown
: El direccionador aún no ha encontrado la mejor ruta a esta estación.

Group
: El direccionador no busca una vía de acceso mejor para nombres de grupos.

Search Limited
El direccionador realiza una búsqueda limitada de este nombre NetBIOS. Consulte el mandato **set cache-parms** para obtener más información sobre la búsqueda reducida.

Search All
El direccionador lleva a cabo una búsqueda completa. Cuando caduca el temporizador de búsqueda reducida del mandato **set cache-parms**, el direccionador lleva a cabo una búsqueda completa.

**IP Address(es)**
Si se ha encontrado la mejor vía de acceso, muestra la dirección o direcciones IP asociadas al DLSw contiguo que puede alcanzar la estación NetBIOS.

**cache unknown**

Muestra las entradas de la antememoria cuyo tipo de nombres NetBIOS es desconocido. El direccionador entra todas las entradas dinámicas como Desconocidas hasta que aprende el tipo de nombre. Luego marca las entradas como locales, remotas o de grupo.

**Ejemplo: `list cache unknown`**

```
Cnt  NetBIOS Name     Entry Type      Loc Path State  Rem Path State
---  ---------------  --------------  --------------  --------------
  2  HYPERION   <01>  STATIC          UNKNOWN          UNKNOWN
  3  EXCEL      <00>  STATIC          UNKNOWN          UNKNOWN
```

**filters all**

Muestra si la función de filtro de tipos de tramas está activa o inactiva tanto para la conexión por puente como para DLSw.

Utilice los mandatos **set filters bridge** y **set filters dlsw** para activar y desactivar estos filtros.

**Ejemplo: `list filters all`**

```
Bridge name conflict filtering is       OFF
Bridge general bcast filtering is       OFF
Bridge trace control filtering is       OFF

DLS name conflict filtering is          ON
DLS general bcast filtering is          ON
DLS trace control filtering is          ON
```

**filters bridge**

Muestra si la función de filtro de tipos de tramas está activa o inactiva para la conexión por puente. Utilice el mandato **set filters bridge** para activar y desactivar estos filtros.

**Ejemplo: `list filters bridge`**

```
Bridge name conflict filtering is       OFF
Bridge general bcast filtering is       OFF
Bridge trace control filtering is       OFF
```

**filters dlsw**

Muestra si la función de filtro de tipos de tramas está activa o inactiva para DLSw. Utilice el mandato **set filters dlsw** para activar y desactivar estos filtros.

**Ejemplo: `list filters dlsw`**

```
DLS name conflict filtering is          ON
DLS general bcast filtering is          ON
DLS trace control filtering is          ON
```

**general** Muestra la configuración actual de configuración de filtro y colocación en antememoria de NetBIOS.

**Ejemplo: `list general`**

```
Bridge-only Information:

Bridge duplicate filtering is          OFF
Bridge duplicate frame filter t/o      1.5 seconds

DLS-only Information:


DLS command frame retry count            5
DLS max remote name cache entries      100
DLS command frame retry timeout        0.5 seconds
DLS type of local name list  NON-EXCLUSIVE
DLS use of local name list is     DISABLED
DLS use of remote name list is     ENABLED

DLS-Bridge Common Information:

Route caching is                        OFF
Significant characters in name           15
Max local name cache entries            500
Duplicate frame detect timeout          5.0 seconds
Best path aging timeout                60.0 seconds
Reduced search timeout                  1.5 seconds
Unreferenced entry timeout             5000 minutes
```

**name-list all**

Muestra todas las entradas activas de la lista de nombres NetBIOS, tanto locales como remotas. Si no se han confirmado las entradas de la lista de nombres local o el uso de listas de nombres locales está desactivada, las entradas de la lista de nombres local no aparecerán en la lista. Si el uso de listas de nombres remotas está desactivada, las entradas remotas de la lista de nombres no aparecerán en la lista.

**Ejemplo: `list name-list all`**

```
Name Qualifier    Type        IP Address
----------------  ----------  ---------------
LA_DOMAIN*             GROUP  20.2.1.3
LA_SERV*          INDIVIDUAL  20.2.1.3
NY_DOMAIN*             GROUP  Local
NY_SERV*          INDIVIDUAL  Local
SF_DOMAIN*             GROUP  20.2.3.4
SF_SERV*          INDIVIDUAL  20.2.3.4
TEMP_DOMAIN            GROUP  Local
TEMP_SERV01       INDIVIDUAL  Local
```

**name-list config**

Muestra todas las entradas de la lista de nombres NetBIOS local configuradas de forma permanente o temporal.

El campo de origen puede tener uno de los siguientes valores:

**PERMANENT**
Entradas configuradas de forma permanente.

**STATIC** Entradas configuradas de forma temporal.

El campo LastMod puede tener uno de los siguientes valores:

**ADDED** La entrada de la lista de nombres local se ha añadido, pero el cambio no se ha confirmado.

**DELETED**
La entrada de la lista de nombres local se ha suprimido, pero el cambio no se ha confirmado.

**UNCHANGED**

La entrada de la lista de nombres local se ha añadido y el cambio se ha confirmado.

**Ejemplo: `list name-list config`**

```
Entry  Name Qualifier    Type        Source     LastMod
-----  ----------------  ----------  ---------  ---------
  1    NY_SERV*          INDIVIDUAL  PERMANENT  UNCHANGED
  2    NY_DOMAIN*             GROUP  PERMANENT  UNCHANGED
  3    TEMP_SERV01       INDIVIDUAL  STATIC     ADDED
  4    TEMP_DOMAIN            GROUP  STATIC     ADDED
```

### name-list local

Muestra todas las entradas de la lista de nombres NetBIOS local actualmente activa. Si no se han confirmado las entradas de la lista de nombres local o el uso de listas de nombres locales está desactivada, las entradas la lista de nombres local no aparecerán en la lista.

**Ejemplo: `list name-list local`**

```
LOCAL Name List
Type of Name List (active) .......     EXCLUSIVE
Type of Name List (pending) ...... NON-EXCLUSIVE

Name Qualifier    Type
----------------  ----------
NY_DOMAIN*             GROUP
NY_SERV*          INDIVIDUAL
TEMP_DOMAIN            GROUP
TEMP_SERV01       INDIVIDUAL
```

### name-list remote

Muestra todas las entradas actualmente activas de la lista de nombres NetBIOS remota correspondiente a un determinado asociado DLSw. Si el uso de las listas de nombres remotas se ha desactivado, no aparecerá ninguna entrada.

**Ejemplo: `list name-list remote`**

```
Enter IP Address [0.0.0.0]? 20.2.1.3

Partner IP Address ........... 20.2.1.3

Type of Name List .............     EXCLUSIVE
    Use of remote name lists ..... ENABLED

Name Qualifier    Type
----------------  ----------
LA_DOMAIN*             GROUP
LA_SERV*          INDIVIDUAL
```

### statistics cache

Lista las siguientes estadísticas sobre la antememoria de nombres.

**Ejemplo: `list statistics cache`**

```
Local name cache entries                1
Remote name cache entries               1
Local individual names                  1
Remote individual names                 0
Group names                             0
Unknown names                           1
Name cache hits                      2194
Name cache misses                       2
```

### statistics frames bridge

Lista las siguientes estadísticas sobre la antememoria de nombres correspondientes a la conexión por puente.

**Ejemplo: `list statistics frames bridge`**

```
Frames in cache                         0
Name query frames                       0
Status query frames                     0
Add name frames                         0
Add group name frames                   0
Name in conflict frames                 0
Frames not filtered as duplicates       0
```

**statistics frames dlsw**

Lista las siguientes estadísticas sobre la antememoria de nombres correspondientes a DLSw.

**Ejemplo: `list statistics frames dlsw`**

```
Name query frames                       0
Status query frames                     0
Add name frames                         0
Add group name frames                   0
Name in conflict frames                 0
Frames not filtered as duplicates       0
```

**statistics general bridge**

Muestra contajes de tramas correspondientes a la conexión por puente.

**Ejemplo: `list statistics general bridge`**

```
Frames received                      1339
Frames discarded                        0
Frames forwarded to bridge           1339
Frames forwarded to DLS              1339
```

**statistics general dlsw**

Muestra contajes de tramas para DLSw.

**Ejemplo: `list statistics general dlsw`**

```
Frames received                      1339
Frames discarded                        0
Frames forwarded to bridge           1339
```

## Set

Define parámetros de la colocación en antememoria de nombres, activa y desactiva la función de filtro de tipos de tramas para la conexión por puente o DLSw, ajusta temporizadores de la función de filtro de tramas duplicadas y temporizadores de reintentos de tramas y define parámetros de lista de nombres NetBIOS. También muestra el indicador de función de filtro de bytes y de nombres NetBIOS.

**Sintaxis:**

**set** cache-parms
filters bridge
filters byte
filters dlsw
filters name
general
name-list

**cache-parms**

Define parámetros de la colocación en antememoria de nombres que se aplican a la conexión por puente o a la conmutación.

### Ejemplo: `set cache-parms`

```
Significant characters in name [15]?
Best path aging timeout value in seconds [60.0]?
Reduced search timeout value in seconds [1.5]?
Unreferenced entry timeout value in minutes [5000]?
Max nbr local name cache entries [500]?
Max nbr remote name cache entries [100]?

Cache parameters set
```

*Significant characters in name*
: Determina si el direccionador tiene en cuenta 15 ó 16 caracteres cuando busca el nombre NetBIOS. Si especifica 15, el direccionador pasa por alto el carácter número 16. Si selecciona 16, el direccionador incluye el carácter número de 16 al buscar entradas en la antememoria.

  El valor por omisión es 15.

*Best path aging timeout*
: Periodo de tiempo que en que el direccionador considera la dirección y la ruta correspondiente a una entrada de la antememoria de nombres como la mejor vía de acceso a esta estación. Cuando transcurre este periodo, el direccionador suprime la entrada de la antememoria de nombres e intenta descubrir una nueva vía de acceso mejor para el nombre NetBIOS.

  Para determinar la mejor vía de acceso, el direccionador considera el periodo de transmisión entre nodos en todas las rutas posibles que conectan estos nodos, así como el tamaño de la trama de mayor tamaño. El direccionador considera que una vía de acceso no es adecuada si no puede soportar a la trama NetBIOS de mayor tamaño que se puede transmitir a través de la vía de acceso.

  El valor por omisión es 60 segundos. El rango es el comprendido entre 1.0 y 100000.0 segundos.

*Reduced search timeout*
: Cuando el direccionador recibe una trama Name-Query, Status-Query o Datagram durante el periodo de tiempo de espera, lleva a cabo una búsqueda basada en la información actual de la antememoria de nombres NetBIOS.

  Si el direccionador recibe una trama duplicada una vez transcurrido este periodo, da por supuesto que la ruta anterior ya no es válida y amplía su búsqueda. El direccionador reenvía la trama duplicada tanto a los puentes como a DLS. DLS realiza una difusión general del mensaje SSP correspondiente a todos los asociados DLS posibles.

  El valor por omisión es 1.5 segundos. El rango es el comprendido entre 1.0 y 100.0 segundos.

*Unreferenced entry timeout*
: El direccionador mantiene un nombre al que no se hace referencia en su antememoria durante este periodo de tiempo antes de suprimirlo. Si la antememoria se llena, el direccionador elimina entradas antes.

  El valor por omisión es de 5000 minutos. El rango es el comprendido entre 1 y 100000 minutos

*Max nbr local name cache entries*
El número máximo de entradas aprendidas de forma local que el direccionador guarda en la antememoria de nombres.

El valor por omisión es 500. El rango es el comprendido entre 100 y 30000. Puede reducir este valor para utilizar menos memoria del direccionador. Para optimizar el uso de la memoria, el uso del procesador y la cantidad de tráfico de difusión general, defina para el número de entradas de la antememoria de nombres local un valor lo más cercano posible al número total de estaciones NetBIOS (servidores y clientes) activas en esta red de puente local del direccionador.

*Max nbr remote name cache entries*
El número máximo de entradas aprendidas de forma remota, entradas de nombres de grupo y entradas desconocidas que el direccionador guarda en la antememoria de nombres.

El valor por omisión es 100. El rango es el comprendido entre 100 y 30000. Puede reducir este valor para utilizar menos memoria del direccionador. Para optimizar el uso de la memoria, el uso del procesador y la cantidad de tráfico de difusión general, defina para el número de entradas de la antememoria de nombres remotos un valor igual al número de servidores NetBIOS remotos a los que van a acceder los clientes NetBIOS en esta red de puente local del direccionador más un 25% aproximadamente.

**filters bridge**
Activa y desactiva la función de tipos de tramas para la conexión por puente.

**Ejemplo: `set filters bridge`**

```
Filter Name Conflict frames? [No]: y
Name conflict filtering is             ON
Filter General Broadcast frames? [No]:
General broadcast filtering is         OFF
Filter Trace Control frames? [No]:
Trace control filtering is             OFF
```

**filters byte**
Desde el indicador `NetBIOS config>`, muestra el indicador de configuración de la función de filtro de NetBIOS (`NetBIOS Filter config>`). La configuración de la función de filtro de NetBIOS se explica en el tema “Configuración y supervisión de la función de filtro de NetBIOS” en la página 199.

Desde el indicador de supervisión `NetBIOS >`, muestra el indicador de supervisión de la función de filtro de NetBIOS (`NetBIOS Filter>`). La supervisión de la función de filtro de NetBIOS se explica en el tema “Supervisión de la función de filtro de NetBIOS” en la página 209.

Este parámetro le permite acceder a la función de filtro de bytes de NetBIOS.

**Ejemplo: `set filters byte`**

```
NetBIOS Filtering configuration
NetBIOS Filter config>
```

**filters dlsw**
Define los filtros de tipos de trama para el tráfico DLSw.

**Ejemplo: `set filters dlsw`**

```
Filter Name Conflict frames? [Yes]:
Name conflict filtering is              ON
Filter General Broadcast frames? [Yes]:
General broadcast filtering is          ON
Filter Trace Control frames? [Yes]:
Trace control filtering is              ON
```

**filters name**

Desde el indicador `NetBIOS config>`, muestra el indicador de configuración de la función de filtro de NetBIOS (`NetBIOS Filter config>`). La configuración de la función de filtro de NetBIOS se explica en el tema “Configuración y supervisión de la función de filtro de NetBIOS” en la página 199.

Desde el indicador de supervisión `NetBIOS >`, muestra el indicador de supervisión de la función de filtro de NetBIOS (`NetBIOS Filter>`). La supervisión de la función de filtro de NetBIOS se explica en el tema “Supervisión de la función de filtro de NetBIOS” en la página 209.

Este parámetro le permite acceder a la función de filtro de nombres NetBIOS.

**Ejemplo: `set filters name`**

```
NetBIOS Filtering configuration
NetBIOS Filter config>
```

**general** Define el tiempo de espera de tramas duplicadas, el tiempo de espera de detección de tramas duplicadas y el tiempo de espera y el número de reintentos de tramas de mandato. Consulte el tema “Función de filtro de tramas duplicadas” en la página 157 para obtener más información sobre cómo funcionan los filtros de tramas duplicadas.

**Ejemplo: `set general`**

```
ATTENTION! Setting Duplicate Frame Filter Timeout to zero...
disables duplicate frame checking!
Duplicate frame filter timeout value in seconds [1.5]?
Duplicate frame detect timeout value in seconds [5.0]?
General parameters set
```

Si DLSw está activado, el indicador también le solicita:

```
Command frame retry count [5]?
Command frame retry timeout value in seconds [0.5]?
```

**Duplicate frame filter timeout**

Sólo se aplica al tráfico conectado por puente si la función de filtro de duplicados está activada. Durante el periodo de tiempo de espera, el direccionador filtra todas las tramas duplicadas que recibe.

El rango es el comprendido entre 0.0 y 100.0 segundos. Cero desactiva la comprobación de tramas duplicadas. El valor por omisión es 1.5 segundos.

**Duplicate frame-detect timeout**

De aplica al tráfico conectado por puente y DLSw. Es el periodo de tiempo durante el cual el direccionador guarda entradas en su base de datos de filtro de tramas duplicadas. Cuando transcurre este periodo, el direccionador crea nuevas entradas para las nuevas tramas que recibe.

El rango es el comprendido entre 0.0 y 100.0 segundos. El valor por omisión es 5 segundos.

**Command frame retry count**

Sólo se aplica al tráfico DLSw.

Es el número de tramas UI NetBIOS duplicadas que el direccionador DLSw de destino envía a su LAN conectada localmente. Estas tramas se envían a intervalos especificados por el tiempo de espera de reintentos de trama de mandato.

El rango es el comprendido entre 0 y 10. El valor por omisión es 5.

**Command frame retry timeout**

Sólo se aplica al tráfico DLSw. Es el intervalo con el que un direccionador DLSw contiguo reintenta enviar tramas UI NetBIOS duplicadas a su red de puente local.

El rango es el comprendido entre 0.0 y 10.0 segundos. El valor por omisión es 0.5 segundos.

**name-list** Define parámetros relacionados con la lista de nombres NetBIOS local. Actualmente el único parámetro relacionado con la lista de nombres NetBIOS local es el parámetro de exclusividad de lista de nombres NetBIOS local.

***Desde el indicador de configuración,*** define de forma permanente los parámetros de lista de nombres NetBIOS local. El cambio no entra en vigor hasta que se vuelve a arrancar el direccionador o se confirma el cambio desde el indicador de supervisión mediante el mandato **set name-list**.

***Desde el indicador de supervisión,*** este mandato define de forma temporal los parámetros de lista de nombres NetBIOS local. El mandato también confirma los cambios en la lista de nombres NetBIOS que se han efectuado desde los indicadores de configuración o de supervisión.

## Test (sólo supervisión)

Permite comparar los nombres NetBIOS reales con la antememoria de NetBIOS actual o la lista de nombres NetBIOS.

**Sintaxis:**

**test** cache
name-list

**test cache**

Muestra una lista de asociados DLSw actuales a los que se reenviaría una trama DLSw con un determinado nombre NetBIOS de destino y el modo en que se reenviaría la trama.

**Ejemplo (no hay entrada correspondiente en la antememoria de NetBIOS): `test cache ABC`**

```
Destination NetBIOS name being tested .... ABC           <20>

Name cache entry NOT found.

How frame destined for this NetBIOS name is forwarded to DLSw partners .....
  Send to all partners.
```

### Ejemplo (hay una entrada correspondiente en la antememoria NetBIOS): `test cache LA_SERV01`

```
Destination NetBIOS name being tested .... LA_SERV01      <00>

Name cache entry found:
  Name type = INDIVIDUAL REMOTE;   Entry type = DYNAMIC

How frame destined for this NetBIOS name is forwarded to DLSw partners .....
  Send to all name list learned and dynamically learned partners.

List of DLSw partners to which frame destined for this name is forwarded .....

  Send via TCP           to 20.2.1.3 ( Name list, Learned )
```

## test name-list

Muestra una lista de entradas de la lista de nombres NetBIOS (local o remota) que coinciden con el nombre NetBIOS especificado.

### Ejemplo: `test name-list`

```
Enter up to 15 characters of NetBIOS name (no wild cards).
  Enter NetBIOS name []? LA_SERV01
Enter last character of NetBIOS name in hex [0]?

Name Qualifier    Type        IP Address
----------------  ----------  ---------------
LA_SERV*          INDIVIDUAL  20.2.1.3
```

# Configuración y supervisión de la función de filtro de NetBIOS

Este capítulo describe los mandatos de configuración de la función de filtro de NetBIOS. Estos mandatos le permiten configurar la función de filtro de NetBIOS como característica añadida de la conexión por puente ASRT. Puede acceder a los mandatos de configuración desde el indicador `NetBIOS config>`.

Este capítulo contiene las siguientes secciones:

- "Cómo acceder a los entornos de configuración ASRT y DLSW"
- "Mandatos de configuración de la función de filtro de NetBIOS"

## Cómo acceder a los entornos de configuración ASRT y DLSW

Para visualizar el indicador de función de filtro de NetBIOS desde el entorno ASRT, entre los mandatos que se muestran en el siguiente ejemplo:

```
Config> protocol asrt
Adaptive Source Routing Transparent Bridge user configuration

ASRT config> netbios
NetBIOS Support User Configuration

NetBIOS config> set filters name o byte
NetBIOS filtering configuration

NetBIOS filter config>
```

Para visualizar el indicador `NetBIOS config>` desde el entorno de configuración DLSw:

```
Config> protocol dls
DLSw protocol user configuration

DLSw config> netbios
NetBIOS Support User Configuration

NetBIOS config> set filters name o byte
NetBIOS filtering configuration

NetBIOS filter config>
```

La Tabla 13 muestra los mandatos de configuración de la función de filtro de NetBIOS.

## Mandatos de configuración de la función de filtro de NetBIOS

**Nota:** Los mandatos de configuración de la función de filtro de NetBIOS no entran en vigor de forma inmediata. Debe volver a arrancar o volver a cargar el dispositivo para que entren en vigor.

*Tabla 13 (Página 1 de 2). Mandatos de configuración de la función de filtro de NetBIOS*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxxi. |

*Tabla 13 (Página 2 de 2). Mandatos de configuración de la función de filtro de NetBIOS*

| Mandato | Función |
|---|---|
| Create | Crea listas de filtros de bytes y de filtros de nombres de sistema principal para la función de filtro de NetBIOS. |
| Delete | Suprime listas de filtros de bytes y de filtros de nombres de sistema principal para la función de filtro de NetBIOS. |
| Disable | Desactiva la función de filtro de NetBIOS en el direccionador de conexión por puente. |
| Enable | Activa la función de filtro de NetBIOS en el direccionador de conexión por puente. |
| Filter-on | Asigna un filtro creado a un determinado puerto. Luego este filtro se puede aplicar a la entrada ***o*** salida de todos los paquetes NetBIOS del puerto especificado. |
| List | Muestra toda la información sobre los filtros creados. |
| Update | Añade información o suprime información de una lista de filtros de bytes o de nombres de sistema principal. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Respuesta a mandatos de configuración de NetBIOS

Los mandatos de configuración de NetBIOS (Talk 6) no entran en vigor de forma inmediata. Permanecen pendientes hasta que emite el mandato **reload** o **restart**.

## Create

Utilice el mandato **create** para crear una lista de filtros de bytes o una lista de filtros de nombres de sistema principal.

**Sintaxis:**

**create** byte-filter-list *lista-filtros*
name-filter-list *lista-filtros*

**byte-filter-list** *lista-filtros*

Crea un nombre de lista de filtros de bytes para la función de filtro de NetBIOS. Puede utilizar un máximo de 16 caracteres para identificar la lista que se está creando. *Lista-filtros* debe ser un nombre exclusivo que no se haya utilizado anteriormente con el mandato **create byte-filter-list** o con el mandato **create name-filter-list**.

**Ejemplo:** `create byte-filter-list newyork`

**name-filter-list** *lista-filtros*

Crea un nombre de lista de filtros de nombres de sistema principal para la función de filtro de NetBIOS. Puede utilizar un máximo de 16 caracteres para identificar la lista de filtros que se está creando. *Lista-filtros* debe ser un nombre exclusivo que no se haya utilizado anteriormente con el mandato **create byte-filter-list** o con el mandato **create name-filter-list**.

**Ejemplo:** `create name-filter-list atlanta`

## Delete

Utilice el mandato **delete** para suprimir listas de filtros de bytes, listas de filtros de nombres de sistema principal y filtros creados mediante el mandato **filter-on input** o el mandato **filter-on output**. El mandato elimina toda la información asociada con listas de filtros de bytes y de nombres de sistema principal. También deja libre la serie de caracteres definida por el usuario como nombre para una nueva lista de filtros.

**Sintaxis:**

d**elete** byte-filter-list *lista-filtros*
name-filter-list *lista-filtros*
filter input *núm. puerto*
filter output *núm. puerto*

**byte-filter-list** *lista-filtros*
Suprime una lista de filtros de bytes creada para la función de filtro de NetBIOS. *Lista-filtros* es la serie de caracteres definida por el usuario que sirve para identificar la lista de filtros de bytes que se va a suprimir.

**Ejemplo:** `delete byte-filter-list newyork`

**name-filter-list** *lista-filtros*
Suprime una lista de filtros de nombres de sistema principal creada para la función de filtro de NetBIOS. *Lista-filtros* es la serie de caracteres definida por el usuario que sirve para identificar la lista de filtros de nombres que se va a suprimir.

**Ejemplo:** `delete name-filter-list atlanta`

**filter input** *núm. puerto*
Suprime un filtro creado mediante el mandato **filter-on input**. El mandato elimina toda la información asociada al filtro y rellena los vacíos resultantes en números de filtros.

**Ejemplo:** `delete filter input 2`

**filter output** *núm. puerto*
Suprime un filtro creado mediante el mandato **filter-on output**. El mandato elimina toda la información asociada al filtro y rellena los vacíos resultantes en números de filtros.

**Ejemplo:** `delete filter output 2`

## Disable

Utilice el mandato **disable** para desactivar de forma global la función de filtro de nombres y de bytes de NetBIOS en el direccionador.

**Sintaxis:**

d**isable** netbios-filtering

**Ejemplo:** `disable netbios-filtering`

## Enable

Utilice el mandato **enable** para activar de forma global la función de filtro de nombres y de bytes de NetBIOS en el direccionador.

**Sintaxis:**

**enable** netbios-filtering

**Ejemplo:** `enable netbios-filtering`

## Filter-on

Este mandato asigna una o más listas de filtros configuradas anteriormente a la entrada o salida de un determinado puerto.

**Sintaxis:**

**filter-on** input *núm. puerto lista-filtros <lista-filtros operador . . . >*
output *núm. puerto lista-filtros <lista-filtros operador . . . >*

**input** *núm. puerto lista-filtros <lista-filtros operador . . . >*

Este mandato asigna una o más listas de filtros a paquetes que entran en un determinado puerto. El filtro resultante se aplica a toda la entrada de paquetes NetBIOS en el puerto especificado.

Núm. puerto es un número de puerto de puente configurado en el direccionador. El número de puerto identifica este filtro. Entre **list** para ver una lista de números de puertos. Lista-filtros es una serie de caracteres entrada anteriormente mediante el mandato **create**. Para añadir listas de filtros a este puerto, entre AND u OR en mayúsculas seguido del nombre de la lista de filtros.

**Nota:** Se pueden utilizar varios operadores para crear un filtro complejo. Si entra varios operadores, debe especificarlos todos simultáneamente en la misma línea de mandatos.

El filtro creado por este mandato se aplica a todos los paquetes NetBIOS que entran en el puerto especificado. Cada lista de filtros de la línea de mandatos se evalúa de izquierda a derecha junto con los operadores especificados. Una evaluación tipo Inclusive de una lista de filtros equivale a una condición de Verdadero y una evaluación tipo Exclusive equivale a una condición de Falso. Si el resultado de la evaluación de las listas de filtros es Verdadero, el paquete se conecta por puente. Si no es así, el paquete se filtra (elimina).

Si el tipo de paquete no recibe soporte de la función de filtro de NetBIOS, todas las listas de filtros de nombres de sistema principal correspondientes a este filtro se designan como de tipo “Inclusive” (Verdadero). Si un filtro de entrada ya existe para el número de puerto especificado, se muestra un mensaje de error.

**Ejemplo:** `filter-on input 2 newyork AND boston`

**output** *núm. puerto lista-filtros <lista-filtros operador . . . >*

Este mandato asigna uno o más filtros a los paquetes que salen de un puerto. Luego se aplica este filtro a toda la salida de paquetes NetBIOS de este puerto.

Núm. puerto es un número de puerto de puente configurado en el direccionador. El número de puerto identifica este filtro. Entre **list** para ver una lista de números de puertos. Lista-filtros es una serie de caracteres entrada anteriormente mediante el mandato create. Puede entrar los operadores opcionales AND u OR, en mayúsculas. Si hay un operador, debe ir seguido de un nombre de lista de filtros. El número de puerto sirve para identificar este filtro.

**Nota:** Se pueden utilizar varios operadores. Esto crea un filtro complejo. Si se especifican uno o más operadores, se deben entrar simultáneamente en la misma línea de mandatos.

El filtro creado por este mandato se aplica a toda la salida de paquetes NetBIOS del número de puerto especificado. Cada lista de filtros de la línea de mandatos se evalúa de izquierda a derecha junto con los operadores presentes. Una evaluación tipo Inclusive de una lista de filtros equivale a una condición de Verdadero y una evaluación tipo Exclusive equivale a una condición de Falso. Si el resultado de la evaluación de las listas de filtros es Verdadero, el paquete se conecta por puente. Si no es así, el paquete se filtra (elimina).

Si el tipo de paquete no recibe soporte de la función de filtro de NetBIOS, todas las listas de filtros de nombres de sistema principal correspondientes a este filtro se designan como de tipo “Inclusive” (Verdadero). Si un filtro de salida ya existe para el número de puerto especificado, se muestra un mensaje de error.

**Ejemplo:** `filter-on output 2 newyork OR boston`

## List

Utilice el mandato de función de filtro de NetBIOS **list** para visualizar toda la información sobre los filtros creados.

**Sintaxis:**

**list**

**Ejemplo:** `list`

```
NetBIOS Filtering: Disabled

NetBIOS Filter Lists
--------------------

Handle           Type

nlist            Name
newyork          Byte

NetBIOS Filters
---------------

Port #      Direction      Filter List Handle(s)

3           Output         nlist
```

**Función de filtro de NetBIOS:**
Muestra si la función de filtro de NetBIOS está activada o desactivada.

**Listas de filtros de NetBIOS**
Visualiza el nombre definido por el usuario (manejador) de las listas de filtros configuradas. Para tipo, “Nombres” indica una lista de filtros de

nombres de sistema principal y “Bytes” indica una lista de filtros de bytes.

**Filtros de NetBIOS**
Visualiza el número de puerto y dirección (entrada o salida) asignados de cada filtro. Manejador(es) listas filtros muestra los nombres de las listas de filtros que componen el filtro.

## Update

Utilice el mandato **update** para añadir o suprimir información de listas de filtros de nombres de sistema principal o de bytes. Lista-filtros es una serie de caracteres anteriormente especificada mediante el mandato create byte (o name) filter-list. Este mandato le lleva al indicador `NetBIOS Byte (o Name) filter-list Config>`, desde el que puede llevar a cabo tareas de actualización en la lista de filtros especificada. En este indicador puede añadir, suprimir, listar o mover elementos de filtro de listas de filtros de bytes y de nombres de sistema principal. En este indicador también puede definir el valor por omisión de cada lista de filtros, que puede ser Inclusive o Exclusive.

Mediante el submandato add puede crear un elemento de filtro dentro de una lista de filtros. Al primer elemento de filtro creado se le asigna el número 1, al segundo el número 2, y así sucesivamente. Después de entrar un submandato add satisfactoriamente, el direccionador muestra el número del elemento de filtro que se acaba de añadir.

**Nota:** Al añadir elementos de filtro a listas de filtros aumenta el tiempo de proceso (porque se tarda más en evaluar cada elemento de filtro de la lista), lo que puede afectar al rendimiento cuando hay mucho tráfico NetBIOS.

El orden en el que se especifican los elementos de filtro correspondientes a una determinada lista de filtros resulta importante puesto que determina el modo en que se aplican los elementos de filtro a un paquete. La primera coincidencia que se produce detiene la aplicación de elementos de filtro, y se evalúa la lista de filtros como Inclusive o Exclusive (en función de la designación Inclusive o Exclusive del elemento de filtro coincidente). Si ninguno de los elementos de filtro de una lista de filtros genera una coincidencia, se devuelve la condición por omisión (Inclusive o Exclusive) de la lista de filtros.

El submandato delete especifica el número de un elemento de filtro a suprimir de la lista de filtros. Cuando se especifica un submandato delete, los vacíos creados en la lista se rellenan. Por ejemplo, si existen los elementos de filtro 1, 2, 3 y 4 y se suprime el elemento de filtro 3, el elemento de filtro 4 pasa a tener el número 3.

El submandato default le permite cambiar el valor por omisión de la lista de filtros, que puede ser Inclusive o Exclusive. Si una lista de filtros se evalúa como Inclusive, el paquete se conecta por puente. Si no es así, el paquete se filtra.

El submandato move sirve para cambiar los números de elementos de filtro dentro de una lista de filtros. El primer argumento del submandato move es el número de la lista de filtros que se ve a mover. El segundo argumento del submandato move es el número de la lista de filtros tras la que se debe colocar la primera lista de filtros.

**Sintaxis:**

**update** byte-filter-list . . .
name-filter-list . . .

**byte-filter-list** *lista-filtros*
Actualiza información perteneciente a una lista de filtros de bytes. El parámetro filter-list es una serie de caracteres anteriormente especificada mediante el mandato **create byte-filter-list**. Este mandato le lleva al siguiente nivel de mandato `NetBIOS BYTE filter-list Config>` (consulte el ejemplo). A este nivel puede llevar a cabo tareas de actualización de la lista de filtros especificada.

**Ejemplo:** **`update byte-filter-list newyork`**

```
NetBIOS Byte newyork Config>
```

A este nivel de indicador puede ejecutar varios mandatos. Cada mandato disponible aparece listado bajo "Opciones del mandato **Update Byte-Filter**".

**name-filter-list** *lista-filtros*
Actualiza información perteneciente a una lista de filtros de nombres. este mandato es idéntico al mandato byte-filter-list, excepto en que especifica una lista de filtros de nombres en lugar de una lista de filtros de bytes. El parámetro filter-list es una serie de caracteres anteriormente especificada mediante el indicador create name-filter-list. Este mandato le lleva al siguiente nivel del mandato `NetBIOS Name filter-list Config>` (consulte el ejemplo). A este nivel puede llevar a cabo tareas de actualización de la lista de filtros especificada.

**Ejemplo:** **`update name-filter-list accounting`**

```
NetBIOS Name accounting Config>
```

A este nivel de indicador puede ejecutar varios mandatos. Cada mandato disponible aparece listado bajo "**Update Name-Filter** (Opciones de mandato)".

## Update Byte-Filter-List (Opciones de mandato)

Esta sección describe las opciones de mandato disponibles para el mandato **update byte-filter-list**:

**add inclusive** *despl-bytes patrón-hex <máscara-hex>*
Añade un elemento de filtro a la lista de filtros de bytes. Si el elemento del filtro de bytes que se añade genera una coincidencia con un paquete NetBIOS, la lista de filtros a la que pertenece evaluará como Inclusive (Verdadero).

- Despl-bytes especifica el número de bytes (en decimal) a desplazar en el paquete que se está filtrando. Comienza en la cabecera NetBIOS del paquete.
- Patrón-hex es un número hexadecimal que se compara con los bytes que comienzan en el desplazamiento de bytes de la cabecera NetBIOS. Entre las reglas de sintaxis del patrón-hex se encuentran las siguientes: no puede comenzar por 0x, puede tener un máximo de 32 números y un número par de dígitos hex.
- Máscara hex, si la hay, debe tener la misma longitud que el patrón-hex y se le suman (AND) de forma lógica los bytes del

paquete que comienzan en el desplazamiento de bytes antes de compararse el resultado con el patrón-hex. Si se omite el argumento máscara-hex, se considera que todos son 1 binarios.

Si el desplazamiento y el patrón de un elemento de filtro de bytes representan bytes que no existen en un paquete NetBIOS (es decir, si el paquete es más corto de lo que se esperaba cuando se definió una lista de filtros de bytes), no se aplicará el elemento de filtro al paquete y este no se filtrará. Si se utiliza una serie de elementos de filtros de bytes para definir una sola lista de filtros de NetBIOS, no se comprobará si se debe filtrar un paquete si alguno de los elementos de filtro de bytes de la lista de filtros de NetBIOS representa bytes que no existen en el paquete NetBIOS.

**Ejemplo: `add inclusive`**

```
Byte Offset  [0] ?
Hex Pattern  [] ?
Hex Mask (<CR> for no mask)  [] ?
```

**add exclusive** *despl-bytes patrón-hex* <*máscara-hex*>

Añade un elemento de filtro a la lista de filtros de bytes. Este mandato es idéntico al mandato add inclusive, excepto en que si el resultado de la comparación entre el elemento de filtro y un paquete NetBIOS es una coincidencia, la lista de filtros evalúa como Exclusive (Falso). Se puede especificar que se eliminen los paquetes de difusión general de datagramas con este mandato especificando un desplazamiento de bytes de 4 y un patrón de bytes de 09.

- Despl-bytes especifica el número de bytes (en decimal) a desplazar en el paquete que se está filtrando. Comienza en la cabecera NetBIOS del paquete.
- Patrón-hex es un número hexadecimal que se compara con los bytes que comienzan en el desplazamiento de bytes de la cabecera NetBIOS. Entre las reglas de sintaxis del patrón-hex se encuentran las siguientes: no puede comenzar por 0x, puede tener un máximo de 32 números y un número par de dígitos hex.
- Máscara hex, si la hay, debe tener la misma longitud que el patrón-hex y se le suman (AND) de forma lógica los bytes del paquete que comienzan en el desplazamiento de bytes antes de compararse el resultado con el patrón-hex. Si se omite el argumento máscara-hex, se considera que todos son 1 binarios.

Si el desplazamiento y el patrón de un elemento de filtro de bytes representan bytes que no existen en un paquete NetBIOS (es decir, si el paquete es más corto de lo que se esperaba cuando se definió una lista de filtros de bytes), no se aplicará el elemento de filtro al paquete y este no se filtrará. Si se utiliza una serie de elementos de filtros de bytes para definir una sola lista de filtros de NetBIOS, no se comprobará si se debe filtrar un paquete si alguno de los elementos de filtro de bytes de la lista de filtros de NetBIOS representa bytes que no existen en el paquete NetBIOS.

**Ejemplo: `add exclusive`**

```
Byte Offset  [0] ?
Hex Pattern  [] ?
Hex Mask  (<CR> for no mask)  [] ?
```

**default include**

Cambia el valor por omisión de la lista de filtros por “inclusive.” Este mandato indica que si ningún elemento de filtro de la lista de filtros coincide con el contenido del paquete que se está evaluando para ver si se filtra, la lista de filtros se evaluará como Inclusive. Este es el valor por omisión.

**default exclude**

Cambia el valor por omisión de la lista de filtros por “exclusive.” Este mandato indica que si ningún elemento de filtro de la lista de filtros coincide con el contenido del paquete que se está evaluando para ver si se filtra, la lista de filtros se evaluará como Exclusive.

**delete** *elemento-filtro*

Suprime un elemento de filtro de la lista de filtros.

Elemento-filtro es un número decimal que representa un elemento de filtro creado anteriormente con el mandato add.

**list** Muestra información relacionada con los elementos de filtro de la lista de filtros especificada.

```
BYTE Filter List Name:     Engineering
BYTE Filter List Default:  Exclusive
Filter Item # Inc/Ex       Byte Offset    Pattern          Mask
1          Inclusive        14         0x123456         0xFFFF00
2          Exclusive         0         0x9876           0xFFFF
3          Exclusive        28         0x1000000        0xFF00FF00
```

**move** *elemento-filtro1 elemento-filtro2*

Reorganiza los elementos de filtro de una lista de filtros. El elemento de filtro cuyo número se especifica como elemento-filtro1 se coloca justo detrás del elemento-filtro2 y se le cambia el número.

**exit** Sale del nivel anterior del indicador de mandatos.

## Update Name-Filter-List (Opciones de mandato)

La siguiente sección lista las opciones de mandato disponibles para el mandato update name-filter-list:

**add inclusive** *nombre sist.pral ASCII <último número-hex>*

Añade un elemento de filtro a la lista de filtros de nombres de sistema principal. Con este mandato, los campos de nombres de sistema principal de los paquetes NetBIOS se comparan con el nombre de sistema principal especificado en este mandato. La siguiente lista muestra cómo se efectúan las comparaciones:

- ADD_GROUP_NAME_QUERY: Se examina el campo nombre NetBIOS de origen
- ADD_NAME_QUERY: Se examina el campo nombre NetBIOS de origen
- DATAGRAM: Se examina el campo nombre NetBIOS de destino
- NAME_QUERY: Se examina el campo nombre NetBIOS de destino

Si se produce una coincidencia (teniendo en cuenta los comodines de este mandato), la lista de filtros evalúa como Inclusive. Si no es así, se aplica al paquete el siguiente elemento de filtro de la lista de filtros (si lo hay) del filtro. Si el paquete no es de uno de los cuatro tipos a los que da soporte la función de filtro de nombres de NetBIOS, el paquete se conecta por puente.

- Nombre-sist.pral. es una serie de caracteres ASCII con una longitud máxima de 16 caracteres. Se puede utilizar un símbolo de interrogación (?) en el nombre de sistema principal como comodín que sustituye a un solo carácter. Se puede utilizar un asterisco (*) como carácter final del nombre de sistema principal, lo que indica un comodín correspondiente al resto del nombre de sistema principal. Si el nombre de sistema principal contiene menos de 15 caracteres, se rellena hasta el carácter número 15 con espacios ASCII. El nombre del sistema principal puede contener cualquier carácter excepto los siguientes:

  . / \ [ ] : | < > + = ; , <espacio>

  **Nota:** El nombre de sistema principal es sensible a mayúsculas y minúsculas.

- Puede utilizar último-número-hex si el nombre del sistema principal contiene menos de 16 caracteres. Es un número hexadecimal (que no puede comenzar por 0x) que indica el valor a utilizar para el último carácter. Si no se especifica el último argumento en un nombre de sistema principal con menos de 16 caracteres, se utiliza un comodín “?” para el carácter número 16.

**add inclusive HEX** *seriehex*

Añade un elemento de filtro a la lista de filtros de nombres de sistema principal. Este mandato es funcionalmente equivalente al mandato add inclusive ASCII. Sin embargo, la representación del nombre de sistema principal es diferente. Este mandato muestra el nombre de sistema principal como una serie de números hexadecimal (que no comienzan por 0x).

- Seriehex debe constar de un número par de números hexadecimal. Si no especifica una serie completa de 32 números hexadecimales, se rellenan con blancos ASCII los números 29 y 30 y con un comodín los números 31 y 32 (byte número 16). Se puede especificar un comodín para un solo byte como **??**.

**add exclusive ASCII** *nombre-sist.pral. <ÚLTIMO-número-hex>*

Añade un elemento de filtro a la lista de filtros de nombres de sistema principal. Este mandato es idéntico al mandato add inclusive ASCII, excepto en que los paquetes para los que se encuentran coincidencias con este elemento de filtro generan un resultado Exclusive para la lista de filtros.

- Nombre-sist.pral. es una serie de caracteres ASCII con una longitud máxima de 16 caracteres. Se puede utilizar un símbolo de interrogación (?) en el nombre de sistema principal como comodín que sustituye a un solo carácter. Se puede utilizar un asterisco (*) como carácter final del nombre de sistema principal, lo que indica un comodín correspondiente al resto del nombre de sistema principal. Si el nombre de sistema principal contiene menos de 15 caracteres, se rellena hasta el carácter número 15 con espacios ASCII. El nombre del sistema principal puede contener cualquier carácter excepto los siguientes:

  . / \ [ ] : | < > + = ; , <espacio>

- Puede utilizar último-número-hex si el nombre del sistema principal contiene menos de 16 caracteres. Es un número hexadecimal (que no puede comenzar por 0x) que indica el valor a utilizar para el último carácter. Si no se especifica el último argumento en un nombre de sistema principal con menos de 16 caracteres, se utiliza un comodín **?** para el carácter número 16.

**add exclusive HEX** *seriehex*

Añade un elemento de filtro a la lista de filtros de nombres. Este mandato es funcionalmente equivalente al mandato add inclusive hex, excepto en que los paquetes para los que se encuentra una coincidencia con este elemento de filtro generan un resultado Exclusive para la lista de filtros.

- Seriehex debe constar de un número par de números hexadecimal. Si no especifica una serie completa de 32 números hexadecimales, se rellenan con blancos ASCII los números 29 y 30 y con un comodín los números 31 y 32 (byte número 16). Se puede especificar un comodín para un solo byte como **??**.

**default include**

Cambia el valor por omisión de la lista de filtros por “inclusive.” Este mandato indica que si ningún elemento de filtro de la lista de filtros coincide con el contenido del paquete que se está evaluando para ver si se filtra, la lista de filtros se evaluará como Inclusive. Este es el valor por omisión.

**default exclude**

Cambia el valor por omisión de la lista de filtros por “exclusive.” Este mandato indica que si ningún elemento de filtro de la lista de filtros coincide con el contenido del paquete que se está evaluando para ver si se filtra, la lista de filtros se evaluará como Exclusive.

**delete** *elemento-filtro*

Suprime un elemento de filtro de la lista de filtros.

- Elemento-filtro es un número decimal que representa un elemento de filtro creado anteriormente con el mandato add.

**list**

Muestra información relacionada con los elementos de filtro de la lista de filtros especificada.

```
NAME Filter List Name: nlist
NAME Filter List Default: Exclusive

Filter Item #   Type    Inc/Ex        Hostname       Last Char

      1         ASCII   Inclusive     EROS
      2         ASCII   Inclusive     ATHENA
      3         ASCII   Exclusive     FOOBAR
```

**move** *elemento-filtro1 elemento-filtro2*

Reorganiza los elementos de filtro de una lista de filtros. El elemento de filtro cuyo número se especifica como elemento-filtro1 se coloca justo detrás del elemento-filtro2 y se le cambia el número.

**exit**

Sale del nivel anterior del indicador de mandatos.

## Supervisión de la función de filtro de NetBIOS

Esta sección describe los mandatos de supervisión de la función de filtro de NetBIOS. Estos mandatos le permiten supervisar y visualizar información sobre filtros de NetBIOS como característica añadida de la conexión por puente ASRT. Los mandatos de supervisión se entran en el indicador de supervisión `NetBIOS >`.

Los cambios que efectúe en el indicador de supervisión `NetBIOS>` afectan tanto a la conexión por puente como a DLSw.

## Cómo acceder a los entornos de supervisión de la función de filtro de NetBIOS ASRT y DLSw

Para visualizar el indicador de supervisión NetBIOS> desde el entorno de supervisión ASRT, entre el mandato **netbios** en el indicador ASRT>:

```
+ protocol asrt

ASRT> netbios
NetBIOS Support User monitoring

NetBIOS monitoring> set filters name o byte

NetBIOS filter>
```

Para visualizar el indicador de supervisión de NetBIOS> desde el entorno de supervisión DLSw:

```
+ protocol dls
DLSw> netbios
NetBIOS Support User monitoring

NetBIOS Console> set filters name o byte
NetBIOS filtering

NetBIOS filter>
```

## Mandatos de supervisión de la función de filtro de NetBIOS

La Tabla 14 lista los mandatos de la función de filtro de NetBIOS.

*Tabla 14. Resumen de mandatos de supervisión de la función de filtro de NetBIOS*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| List | Muestra toda la información sobre los filtros creados. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

### List

Utilice el mandato de función de filtro de NetBIOS **list** para visualizar toda la información sobre los filtros creados.

**Sintaxis:**

**list** byte-filter-lists
filters
name-filter-lists

**byte-filter-lists**

Muestra información relacionada con los elementos de filtro de la lista de filtros de bytes especificada.

**Ejemplo:** `list byte-filter-lists`

```
BYTE Filter-List Name:  Engineering
BYTE Filter-List Default:  Exclusive

Filter Item # Inc/Ex     Byte Offset  Pattern      Mask

1             Inclusive     14        0x123456    0xFFFF00
2             Exclusive      0        0x9876      0xFFFF
3             Exclusive     28        0x1000000   0xFF00FF00
```

**Filter Item#**

Especifica el número de elemento de filtro del elemento de filtro. Los elementos de filtro se evalúan en orden numérico al determinar el estado de Inclusive/Exclusive de la lista de filtros.

**Inc/Ex** Especifica el estado por omisión del elemento de filtro.

**Byte-offset**

Especifica el número de bytes (en decimal) a desplazar en el paquete que se está filtrando. Comienza en la cabecera NetBIOS del paquete.

**Pattern** El número hexadecimal utilizado para comparar con los bytes que comienzan en el desplazamiento de bytes de la cabecera NetBIOS. Entre las reglas de sintaxis del patrón-hex se encuentran las siguientes: no puede comenzar por 0x, puede tener un máximo de 32 números y un número par de números hex.

**Mask** Si la hay, debe tener la misma longitud que el patrón-hex y se le suman (AND) de forma lógica los bytes del paquete que comienzan en el desplazamiento de bytes antes de compararse el resultado con el patrón-hex para ver si son iguales. Si se omite el argumento máscara-hex, se considera que todos son 1 binarios.

**filters** Muestra información relacionada con todos los filtros configurados.

**Ejemplo: `list filters`**

```
NetBIOS Filtering: Enabled

    Port #      Direction      Filter List Handle(s)   Pkts Filtered

       1          Input        valencia                      0
       2          Output       raleigh                       0
```

**name-filter-lists**

Muestra información relacionada con los elementos de filtro de la lista de filtro de nombres especificada.

**Ejemplo: `list name-filter-lists`**

```
NAME Filter List Name: nlist
NAME Filter List Default: Exclusive


Filter Item #   Type    Inc/Ex     Hostname   Last Char

 1              ASCII   Inclusive  EROS       <0x03>
 2              ASCII   Inclusive  ATHENA
 3              ASCII   Exclusive  FOOBAR
```

**Filter Item#**

Especifica el número de elemento de filtro del elemento de filtro. Los elementos de filtro se evalúan en orden numérico al determinar el estado de Inclusive/Exclusive de la lista de filtros.

**Inc/Ex** Especifica el estado por omisión del elemento de filtro.

**Type** “ASCII” indica un elemento de filtro de nombres de sistema principal añadido como caracteres ASCII.“Hex” indica un elemento de filtro de nombres de sistema principal añadido como números hexadecimales

**Host-name**

Serie ASCII con un máximo de 16 caracteres de longitud. Se puede utilizar un símbolo de interrogación (?) en el nombre del sistema principal para indicar un comodín de un solo carácter. Se puede utilizar un asterisco (*) como carácter final del nombre de sistema principal, lo que indica un comodín correspondiente al resto del nombre de sistema principal. Si el nombre de sistema principal contiene menos de 15 caracteres, se rellena hasta el carácter número 15 con espacios ASCII. El nombre del sistema principal puede contener cualquier carácter excepto los siguientes:

. / \ [ ] : | < > + = ; , <espacio>

**Last char**

Se utiliza si el nombre del sistema principal contiene menos de 16 caracteres. Es un número hexadecimal (que no puede comenzar por 0x) que indica el valor a utilizar para el último carácter. Si no se especifica el último argumento en un nombre de sistema principal con menos de 16 caracteres, se utiliza un comodín “?” para el carácter número 16.

# Utilización del LAN Network Manager (LNM)

Este capítulo describe el LAN Network Manager (LNM) ASRT de IBM. Incluye las siguientes secciones:



## Acerca de LNM

Utilice LNM para gestionar redes en anillo interconectadas mediante puentes de direccionamiento de origen. Le permite supervisar el funcionamiento de anillos, puentes y estaciones de los anillos.

Las estaciones de gestión LNM pueden acceder a la información recopilada por los agentes de software del puente. En concreto, los agentes LNM reenvían la información recopilada a través de otro agente denominado Mecanismo de notificación de la (LRM), un protocolo propiedad de IBM. El reenvío de información se realiza mediante una conexión LLC2 a una estación del LAN Network Manager.

## Agentes y funciones LNM

Los agentes LNM y sus funciones incluyen:

- Servidor de informes de configuración (CRS) - Notifica cambios en la topología del anillo y estado de las estaciones del anillo a LNM.
- Servidor de parámetros de anillo (RPS) - solicitudes de servicios procedentes de estaciones del anillo sobre información de parámetros del anillo como número de anillo, el valor del temporizador de informes de error de software y la ubicación física.
- Supervisor de errores de anillo (REM) - recopila informes de errores procedentes de estaciones del anillo y los analiza. Cuando se superan umbrales, REM puede reenviar información de error al LNM.
- Mecanismo de notificación de la LAN (LRM) - controla el establecimiento de enlaces de notificación procedentes de estaciones LNM con los agentes el puente. También gestiona la transferencia de información procedente y destinada a los demás agentes sobre estos enlaces.

La Figura 25 en la página 214 ilustra la conexión entre el puente IBM, agentes LNM y la estación LNM de IBM.

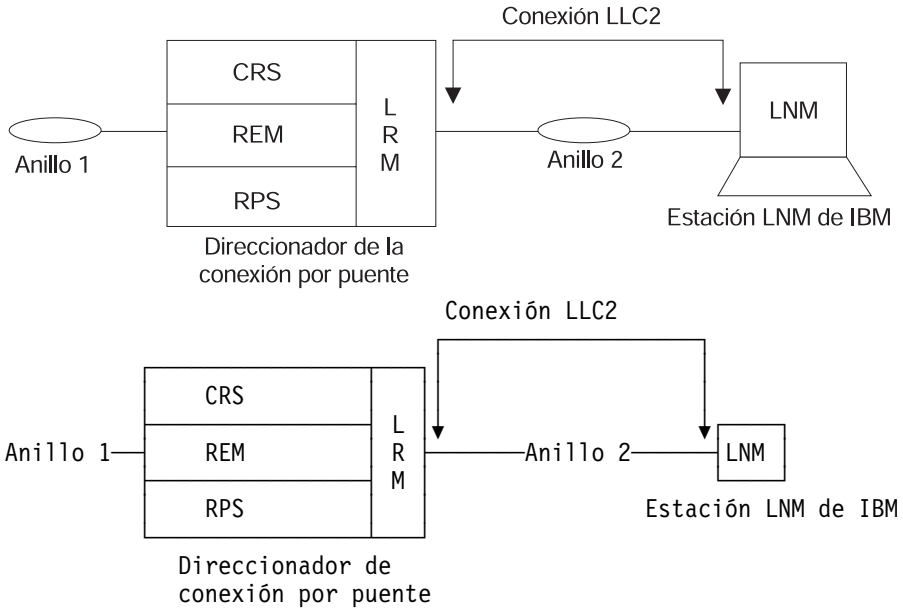



*Figura 25. Estación y agentes LNM*

Las siguientes secciones describen con detalle cada agente LNM.

## Servidor de informes de configuración

Bajo petición de LNM, CRS obtiene y reenvía el estado de las estaciones del anillo a LNM. Utilice CRS para definir parámetros de las estaciones del anillo y para eliminar una estación del anillo.

La información de configuración que generan las estaciones del anillo se reenvía a LNM. Cuando LNM solicita el estado de una estación del anillo, CRS crea y envía tramas MAC a la estación para obtener la información. Luego CRS envía las siguientes tramas a la estación del anillo:

- Trama MAC de solicitud de dirección de la estación del anillo
- Trama MAC de solicitud del estado de la estación del anillo
- Trama MAC de solicitud de conexiones de la estación del anillo

Cuando la estación del anillo responde, CRS coloca la información en una trama LLC2 formateada adecuadamente y la reenvía a LNM.

CRS también puede eliminar una estación del anillo bajo petición de LNM. Para eliminar una estación del anillo, CRS envía una trama MAC de eliminación de estación al anillo. CRS también devuelve una respuesta a LNM que indica si la eliminación se ha llevado a cabo satisfactoriamente o si se ha producido algún error.

Cuando CRS recibe una trama MAC de notificación de nuevo supervisor activo, reenvía la información a LNM. Cuando se recibe una trama MAC de notificación de cambio de NAUN (Siguiente continua activa de donde proceden los datos), esta información también se notifica. El agente CRS tiene su propia dirección funcional, que pueden utilizar las capas MAC de las estaciones del anillo para reenviar tramas MAC a CRS.

## Servidor de parámetros del anillo

RPS inserta estaciones de anillo en el anillo. Cuando se inserta una estación de anillo en el anillo:

- La nueva estación envía una trama MAC de solicitud de inicialización a RPS correspondiente a este anillo. Esta trama MAC incluye cierta información sobre la estación.
- RPS responde con una trama MAC de inicialización de estación de anillo que contiene el número del anillo y el intervalo de tiempo a esperar entre envíos de tramas MAC de notificación de errores de software. La información obtenida de la trama de solicitud de inicialización se pasa a LNM para que pueda mantener una base de datos de todas las estaciones del anillo.
- RPS también responde a una solicitud de estado procedente de LNM. El número de anillo, la información sobre versión de RPS y el valor del temporizador de notificación de errores de software se devuelven a LNM.

La función RPS tiene una dirección funcional asociada para recibir las tramas MAC que le envían otras estaciones del anillo.

**Atención:** Cuando una estación intenta insertarse en un anillo, envía una trama MAC de solicitud de inicialización al Servidor de parámetros del anillo (RPS) correspondiente a este anillo. Si RPS copia satisfactoriamente esta trama, la estación espera recibir una trama MAC de inicialización de la estación del anillo procedente de RPS. Si no recibe dicha trama, la estación no se inserta en el anillo.

Puede que una estación no se pueda insertar en el anillo si el dispositivo está configurado para LNM, se convierte en el Servidor de parámetros del anillo y entra en un estado congestionado que no le permite enviar la trama MAC de inicialización de la estación del anillo. La solución a este problema consiste en desactivar RPS en el puerto afectado. Si RPS no está activado y ningún servidor copia la trama de solicitud de inicialización, la estación que la envía no espera ninguna respuesta y se inserta en el anillo.

## Supervisor de errores del anillo

REM observa el funcionamiento de la red en anillo conectada, buscando errores de hardware o de software. Luego los notifica a LRM y ayuda a identificar la causa de los errores. Durante la detección de errores de hardware realiza las siguientes tareas:

- Los errores de hardware se detectan en el anillo mediante la recepción de tramas MAC de baliza.
- Las estaciones del dominio en el que se ha producido el error intentan corregir el problema eliminándose a ellas mismas del anillo.
- REM determina si la condición de error de hardware se corrige o no y luego notifica los resultados a LNM.

REM supervisa los errores de software del siguiente modo:

- Las estaciones del anillo envían periódicamente tramas MAC de error de software a REM para informarle sobre el número de veces que se han producido errores intermitentes, por ejemplo, errores de CRC, y la frecuencia de los errores.

- Cuando el número de errores de software correspondiente a una estación sobrepasa un determinado umbral, REM notifica esta condición a LNM.
- REM también supervisa las tramas MAC de notificación de errores de software para ver si hay condiciones de congestión en el receptor. La congestión del receptor indica que una estación del anillo ha eliminado tramas porque no tenía suficientes almacenamientos intermedios de recepción.
- Si el número de veces que una estación notifica una congestión del receptor supera un determinado umbral, REM notifica esta condición a LNM. Cuando la condición de congestión del receptor vuelve a la normalidad, LNM recibe una notificación que indica que la condición de congestión del receptor ha finalizado.

### Mecanismo de notificación de la LAN

LRM controla la conexión de LNM con los agentes. LRM establece enlaces de notificación entre él mismo y cada LNM conectado. Un *enlace de notificación* es una conexión LLC2 entre LNM y LRM.

Toda la comunicación entre LNM y los agentes se lleva a cabo a través de un enlace de notificación. LRM pasa datos de gestión procedentes y destinados a los agentes adecuados a los enlaces de notificación. Se da soporte a un máximo de cuatro enlaces de notificación. Uno se denomina *enlace de control* y los otros tres se denominan *enlaces de observación*.

Un LNM conectado a través del enlace de control puede llevar a cabo todas las operaciones disponibles. Los LNM conectados mediante enlaces de observación sólo pueden llevar a cabo un grupo limitado de las operaciones disponibles.

## Restricciones de la configuración de LNM

IBM 2210 da soporte a configuraciones de red en anillo de varios puertos y de dos redes en anillo.

El agente LNM y la estación LNM siempre dan por supuesto que los mensajes se pasan a un modelo de dos participantes. Sin embargo, LNM se activa por puerto de puente por cuestiones de coherencia con la configuración existente.

En una configuración de varios puertos, LNM se puede activar en cualquier puerto del puente de la red en anillo de direccionamiento de origen. Se crea una instancia de LNM para cada puerto sobre el que se activa LNM.

En una configuración de dos redes en anillo, el otro puerto se designa siempre mediante una seudo dirección. Esto recibe el nombre de puente de varios puertos. Puede corresponder a un anillo virtual o a una interfaz de línea serie.

Sólo en el caso en que el puente IBM 2210 tenga dos puertos de red en anillo de direccionamiento de origen, el otro puerto del puente del modelo de dos puertos es una red en anillo con una dirección real.

Para obtener las direcciones MAC necesarias para configurar el Gestor LNM, entre **`list lnm ports`** en el indicador `ASRT>`.

El Servidor de puente de la LAN (LBS) puede notificar estadísticas con datos de rendimiento sobre paquetes reenviados y paquetes eliminados cuando se lo solicite

la estación del gestor. No se dan soporte a las actualizaciones de configuraciones remotas desde la estación del gestor.

## Soporte de enlace lógico de Clase 2

En las LAN, la capa de enlace de datos consta de dos subcapas: El control de acceso al medio (MAC) y el control de la capa de enlace (LLC). LLC ofrece dos tipos de servicios:

- LLC1 (Tipo 1) - un servicio sin conexión sin acuse de recibo
- LLC2 (Tipo 2) - una serie de servicios orientados a la conexión

El LAN Network Manager (LNM) necesita servicios orientados a conexión LLC2. LLC2 ofrece capacidad para:

- Iniciar nuevas conexiones de enlace de datos
- Gestionar conexiones de enlace de datos
- Intercambiar datos en orden secuencial (de forma garantizada)
- Ejecutar un nivel de control de flujo en las conexiones establecidas
- Terminar conexiones de enlace bajo petición del usuario del servicio o por errores de enlace no recuperables.

La subcapa LLC cumple con el estándar IEEE 802.5.

# Configuración y supervisión del LAN Network Manager (LNM)

Este capítulo describe la implantación ASRT de IBM del LAN Network Manager (LNM). Incluye las siguientes secciones:



## Configuración de LNM

Esta sección resume el procedimiento para la configuración básica de la característica LNM en el direccionador de conexión por puente.

1. Obtenga la dirección MAC necesaria para el software del gestor de la red.

   Entre el mandato **list lnm ports** en el indicador ASRT> para obtener las direcciones MAC que necesita el software Network Manager que se ejecuta en la Estación del gestor de la red. Por ejemplo:

   ```
   ASRT> list lnm ports
   Port Number [1]? 1
   Port 1
   LNM Agents Enabled: RPS CRS REM
   Reporting Link          State          LNM Station Address
   0                       ACTIVE         10:00:5A: F1:02:37
   1                       AVAILABLE
   2                       AVAILABLE
   3                       AVAILABLE
   MAC Addresses to use when configuring LNM Manager:
   00:00:C9:08:35:47
   40:00:D9:08:35:47
   LNM not enabled on port 4
   LNM not enabled on port 5
   ```

   El Network Manager utiliza las direcciones MAC que se visualizan (en el ejemplo se muestran en negrita) para configurarlas para los agentes LNM que hay en el direccionador.

   **Nota:** Estas direcciones se deben entrar exactamente tal como aparecen en la salida; si no es así, LNM no se configurará correctamente.

2. Active los agentes LNM en el direccionador. Escriba **enable lnm** en el indicador LNM config> para activar los agentes LNM en el puerto deseado del direccionador de conexión por puente. Por ejemplo:

   ```
   LNM config>enable lnm
   Port Number [1]? 1
   ```

   El valor por omisión es que todos los agentes LNM estén activados.

3. Compruebe la configuración visualizando los agentes LNM activados. Escriba **list port** en el indicador LNM config> para visualizar los agentes LNM que están activados en el puerto configurado. Por ejemplo:

   ```
   LNM config>list port
   Port Number [1]? 1
   LNM Agents Enabled: RPS CRS REM
   ```

# Mandatos de LNM

Esta sección describe los mandatos de configuración y de supervisión de LNM. Estos mandatos le permiten configurar y supervisar parámetros de la red correspondientes a LNM.

**Nota:** Los mandatos de configuración de LNM no entran en vigor de forma inmediata. Debe volver a arrancar o volver a cargar el dispositivo para que entren en vigor.

Entre los mandatos de configuración en el indicador `LNM config>`. Acceda al indicador del siguiente modo:

```
Config>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>lnm
LNM configuration
LNM config>
```

Entre los mandatos de supervisión en el indicador `LNM>`. Visualice este indicador del siguiente modo:

```
+protocol asrt
ASRT>lnm
LNM>
```

La Tabla 15 en la página 221 lista los mandatos de LNM.

*Tabla 15. Resumen de mandatos de LNM*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Disable | Desactiva todos los agentes LNM de un determinado puerto o los agentes LNM especificados (RPS, CRS, or REM) de un determinado puerto.<br><br>Desactiva el establecimiento de determinados parámetros de LNM de la aplicación LNM remota conectada al puente. Se aplica de forma global a todas las instancias de LNM dentro del puente.<br><br>Este mandato sólo se utiliza para la configuración. |
| Enable | Activa todos los agentes LNM de un determinado puerto o los agentes LNM especificados (RPS, CRS, or REM) de un determinado puerto.<br><br>Activa el establecimiento de determinados parámetros de LNM de la aplicación LNM remota conectada al puente. Se aplica de forma global a todas las instancias de LNM dentro del puente.<br><br>Este mandato sólo se utiliza para la configuración. |
| List | Muestra los agentes LNM que se han activado para el puerto especificado. Muestra las contraseñas configuradas para el puente.<br><br>Este mandato se utiliza tanto para la configuración como para la supervisión. |
| Set | Define la contraseña para el número de enlace de notificación especificado.<br><br>Este mandato sólo se utiliza para la configuración. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Respuesta a mandatos de configuración de LNM

Los mandatos de configuración de LNM (Talk 6) no entran en vigor de forma inmediata. Permanecen pendientes hasta que emite el mandato **reload** o **restart**.

## Disable

Utilice el mandato **disable** para desactivar todos los agentes LNM (RPS, CRS o REM) de un determinado puerto.

Este mandato también desactiva el establecimiento de contraseñas de enlace de notificación procedentes de las aplicaciones LNM remotas conectadas al puente.

**Sintaxis:**

disable agent *núm. puerto*
lnm . . .
configuration-remote-change

**agent** *núm. puerto*
Desactiva el agente LNM especificado (RPS, CRS o REM) en el puerto especificado. Si el puerto no está configurado, aparece el mensaje `LNM not configured for port XX` y el mandato no tiene efecto.

**Ejemplo:** `disable REM 1`

**lnm** Desactiva LNM en el puerto especificado. Si el puerto no está configurado, aparece el mensaje `LNM not configured for port XX` y el mandato no tiene efecto.

**Ejemplo:** `disable lnm`

```
Port number [1]? 1
LNM not configured for Port 1
```

**configuration-remote-change**
Desactiva el establecimiento de contraseñas de enlace de notificación procedentes de las aplicaciones LNM remotas conectadas al puente. Este mandato se aplica de forma global a todas las instancias de LNM dentro del puente.

**Ejemplo:** `disable configuration-remote-change`

```
CONFIGURATION-REMOTE-CHANGE: disabled
```

## Enable

Activa todos los agentes LNM en un determinado puerto o activa los agentes LNM especificados (CRS, REM o RPS) en un determinado puerto.

Si la interfaz no es una red en anillo, aparece el mensaje `Port number XX is not token-ring` y el mandato no tiene efecto.

Si el puerto no está configurado, aparece el mensaje `Por number XX does not exist` y el mandato no tiene efecto.

Si el agente especificado ya está activado para el puerto especificado, aparece el mensaje `Already enabled`.

Este mandato también activa el establecimiento de contraseñas de enlace de notificación procedentes de las aplicaciones LNM remotas conectadas al puente.

**Sintaxis:**

**enable** agent *núm. puerto*
lnm . . .
configuration-remote-change

**agent** *núm. puerto*
Activa el agente LNM especificado (RPS, CRS o REM) en el puerto especificado.

**Ejemplo:** `enable CRS 1`

**lnm** *núm. puerto*
Activa todos los agentes LNM en el puerto especificado.

**Ejemplo:** `enable lnm`

```
Port number [1]? 1
```

**configuration-remote-change**
Activa el establecimiento de contraseñas de enlace de notificación procedentes de las aplicaciones LNM remotas conectadas al puente. El valor por omisión desactiva el establecimiento de parámetros de configuración de LNM de forma remota.

Este mandato se aplica de forma global a todas las instancias de LNM dentro del puente.

**Ejemplo:** **`enable configuration-remote-change`**

```
CONFIGURATION-REMOTE-CHANGE: Enabled
```

## List (mandato de configuración)

Muestra los agentes LNM activados para el puerto especificado y también muestra las contraseñas que se han configurado para el puente. El mandato se entra en el indicador ASRT>.

**Sintaxis:**

**list** password
port . . .

**password**

Muestra las contraseñas que se han configurado para los enlaces de notificación del puente. Muestra si la aplicación LNM remota puede o no modificar las contraseñas.

**Ejemplo:** **`list password`**

```
Reporting Link     Password
0             87654321
1             MADRAS
2             ABC1234
3             123ABC
CONFIGURATION-REMOTE-CHANGE: Disabled
```

**port** *núm. puerto*

Muestra los agentes LNM activados para el puerto especificado si el puerto es un puerto de red en anillo que da soporte a la Conexión por puente de direccionamiento de origen.

**Ejemplo:** **`list port`**

```
Port Number [1]? 1
LNM Agents Enabled: RPS CRS REM
```

## List (mandato de supervisión)

Muestra información sobre el estado de la configuración de LNM. El mandato se entra en el indicador ASRT>.

**Sintaxis:**

**list** bridge
lnm ports
source-routing configuration

**bridge** Muestra si LNM está activado en un determinado puerto.

**Ejemplo:** **`list bridge`**

```
Bridge ID (prio/add):  32768/00-00-00-00-00-38
Bridge state:          Enabled
UB-Encapsulation:      Disabled
Bridge type:           SR-TB
Bridge capability:     ASRT
Number of ports:       5
STP Participation:     IEEE802.1d on TB ports and IBM-8209 on SR ports
Maximum
Port  Interface State MAC Address      Modes   MSDU  Segment  Flags
2  TKR/0       Up  00-00-93-90-4C-F7    T    2096            RD
3  TKR/1     Down  00-00-00-00-00-00 SR          0 223         RD,LE
5  Eth/0     Down  AA-00-04-00-26-14             0            RD
Flags: RE =IBMRT PC behaviour Enabled, RD = IBMRT PC behaviour Disabled
LE = LNM Enabled, LD = LNM Disabled, LF = LNM Failed
SR bridge number:      8
SR virtual segment:    812
Adaptive segment:      214
```

### lnm ports

Muestra información sobre la configuración del LNM activado en el direccionador de la conexión por puente.

**Ejemplo:** **`list LNM ports`**

```
LNM not enabled on port 1
LNM not enabled on port 2
Port 3
LNM Agents Enabled: RPS CRS REM
Reporting Link          State          LNM Station
Address
0                AVAILABLE
1                AVAILABLE
2                AVAILABLE
3                AVAILABLE
MAC Addresses to use when configuring LNM Manager:
00:00:00:00:00:00
00:00:00:00:00:00
LNM not enabled on port 4
LNM not enabled on port 5
```

### source-routing configuration

Muestra si LNM está activado en un determinado puerto.

**Ejemplo:** **`list source-routing configuration`**

```
Bridge number:              8
Bridge state:               Enabled
Maximum STE hop count       14
Maximum ARE hop count       14
Virtual segment:            812
Port  Segment  Interface  State    MTU   STE Forwarding   LNM
   3  223      TKR/1      Enabled  4399  Auto             ENA
   -  214      Adaptive   Enabled  1470  Yes
```

## Set

Define la contraseña para el número de enlace de notificación especificado. El número de enlace puede ser 0, 1, 2 ó 3. El enlace 0 se utilizar para el enlace de control. Los enlaces 1, 2 y 3 se utilizan para enlaces de observación.

La contraseña debe constar de entre seis y ocho caracteres y debe coincidir con la contraseña que utiliza LNM al establecer un enlace de notificación con el puente. Si no se define la contraseña para un enlace, adopta el valor por omisión 00000000.

**Sintaxis:**

**set password** *núm. enlace contraseña*
**Ejemplo:** **`set password`**

**Ejemplo:** **`set password`**

```
Link Number [0]? 1
Enter new password :  [ABCDEFGH]? guesswho
```

# Configuración y supervisión de Servicios de sistema principal en TCP/IP

Este capítulo describe cómo configurar el protocolo Servicios de sistema principal en TCP/IP (Sistema principal en TCP/IP) y cómo utilizar los mandatos de configuración de Sistema principal en TCP/IP. Este capítulo incluye las siguientes secciones:

- "Cómo acceder al entorno de configuración de Sistema principal en TCP/IP"
- "Procedimientos básicos de configuración"
- "Mandatos de configuración de Sistema principal en TCP/IP" en la página 226
- "Cómo acceder al entorno de supervisión de Sistema principal en TCP/IP" en la página 230
- "Mandatos de supervisión de Sistema principal en TCP/IP" en la página 230

Consulte el tema "Servicios de sistema principal en TCP/IP (gestión sólo de puentes)" en la página 49 si desea obtener más información sobre razones para utilizar Servicios de sistema principal en TCP/IP.

No consulte este capítulo si está configurando el dispositivo para el direccionamiento IP; en su lugar, consulte el tema "Utilización de IP" en la página 241.

**Nota:** Para configurar Host Services, no puede tener ninguna dirección IP configurada en las interfaces. El dispositivo no se puede configurar como un direccionador para IP. Host Services son sólo para la conexión por puente.

## Cómo acceder al entorno de configuración de Sistema principal en TCP/IP

Para acceder al entorno de configuración de Sistema principal en TCP/IP, entre el siguiente mandato en el indicador `Config>`:

```
Config> protocol hst
TCP/IP-Host Services user configuration
TCP/IP-Host Config>
```

## Procedimientos básicos de configuración

Las siguientes secciones describen los procedimientos básicos de configuración para activar Servicios de sistema principal en TCP/IP en el 2210.

### Definición de la dirección IP

Para llevar a cabo una configuración mínima de Servicios de sistema principal en TCP/IP, asigne al 2210 una dirección IP mediante el mandato **set ip-host**. Esta dirección IP se asocia al 2210 como conjunto, en lugar de asociarse a una sola interfaz.

## Activación de Servicios de sistema principal en TCP/IP

Utilice el mandato **enable services** para activar Servicios de sistema principal en TCP/IP.

## Cómo añadir una pasarela por omisión

El 2210 utiliza su pasarela por omisión para comunicarse con los sistemas principales y pasarelas que no se encuentran en la red conectada por puente a la que se conecta directamente el 2210. El 2210 puede aprender de forma dinámica su pasarela por omisión mediante la función de Descubrimiento de rutas ICMP (consulte el mandato **enable router-discovery** en este capítulo) o mediante RIP (consulte el mandato **enable rip-listening** en este capítulo). También puede especificar de forma estática una o más pasarelas por omisión mediante el mandato **add default gateway**. El 2210 sólo utiliza una pasarela por omisión simultáneamente; las demás pasarelas por omisión se utilizan como reserva.

Para guardar la dirección IP asignada y la información sobre la pasarela por omisión,

1. Salga del indicador `TCP/IP-Host config>` par ir al indicador `Config>`.
2. Utilice el mandato **write** en el indicador `Config>` para grabar la configuración actual en memoria.
3. Entre **CONTROL-P** para llegar al indicador OPCON y utilice el mandato de OPCON **restart** para cargar una nueva copia del software.
4. Después de volver a arrancar el 2210, vuelva al indicador `TCP/IP-Host config>`.

---

## Mandatos de configuración de Sistema principal en TCP/IP

Esta sección describe los mandatos de configuración de Sistema principal en TCP/IP. Los mandatos de configuración de Sistema principal en TCP/IP le permiten especificar parámetros de la red para el puente Sistema principal en TCP/IP. Vuelva a arrancar el dispositivo para activar los mandatos de configuración.

**Nota:** Los mandatos de configuración de Sistema principal en TCP/IP no entran en vigor de forma inmediata. Permanecen pendientes hasta que vuelve a arrancar o vuelve a cargar el dispositivo.

Entre los mandatos de configuración de Sistema principal en TCP/IP en el indicador `TCP/IP-Host config>`.La Tabla 16 en la página 227 muestra los mandatos.

*Tabla 16. Resumen de mandatos de configuración de Sistema principal en TCP/IP*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Add | Añade una pasarela por omisión. |
| Delete | Suprime una pasarela por omisión. |
| Disable | Desactiva Servicios de sistema principal en TCP/IP, los procesos de descubrimiento de rutas y la función de escucha de RIP. |
| Enable | Activa Servicios de sistema principal en TCP/IP, los procesos de descubrimiento de rutas y la función de escucha de RIP. |
| List | Lista la configuración de Sistema principal en TCP/IP actual. |
| Set | Define la dirección IP del 2210. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Respuesta a mandatos de configuración de Sistema principal en TCP/IP

Los mandatos de configuración de Sistema principal en TCP/IP (Talk 6) no entran en vigor de forma inmediata. Permanecen pendientes hasta que emite el mandato **reload** o **restart**.

## Add

Utilice el mandato **add** para añadir pasarelas por omisión (es decir, direccionadores) a la configuración.

Las pasarelas por omisión se utilizan cuando se intenta enviar paquetes a direcciones IP de destino que quedan fuera de la subred local. Se crea una tabla de direccionamiento a través del proceso de redireccionar. Se intenta detectar los direccionadores que desaparecen. Si el 2210 se ha arrancado sobre la red (mediante TFTP/BootP), la pasarela por omisión se configura utilizando la información del proceso de arranque.

**Sintaxis:**

a**dd** default-gateway *dirección-IP-pasarela-omis*

**Ejemplo: `add default-gateway`**

```
Default-Gateway address [0.0.0.0]?  123.45.67.89
```

## Delete

Utilice el mandato **delete** para suprimir las pasarelas por omisión de la configuración del 2210. Entre la dirección IP de la pasarela por omisión que desea eliminar tras el mandato **delete**.

**Sintaxis:**

de**lete** default-gateway *dirección-IP-pasarela-omis*

**Ejemplo: `delete default-gateway`**

```
Enter address to be deleted [0.0.0.0]?  123.45.67.89
```

## Disable

Utilice el mandato **disable** para desactivar las siguientes funciones de TCP/IP:

- Servicios de sistema principal en TCP/IP
- Procesos de descubrimiento de rutas
- Función de escucha de RIP

**Sintaxis:**

| | |
|---|---|
| di**sable** | rip-listening<br>router-discovery<br>services |

**rip-listening**

Desactiva la creación de entradas de la tabla de direccionamiento que se han obtenido escuchando el protocolo RIP. Por omisión, la función de escucha de RIP está desactivada.

**Ejemplo:** `disable rip-listening`

**router-discovery**

Desactiva la capacidad de aprender pasarelas por omisión, recibiendo mensajes de descubrimiento de rutas ICMP. Por omisión, el descubrimiento de rutas está activado.

**Ejemplo:** `disable router-discovery`

**services** Desactiva por completo el protocolo Servicios de sistema principal en TCP/IP. Si el direccionamiento IP no está activado, Servicios de sistema principal en TCP/IP está activado por omisión.

**Ejemplo:** `disable services`

## Enable

Utilice el mandato **enable** para activar las siguientes funciones de TCP/IP:

- Servicios de sistema principal en TCP/IP
- Procesos de descubrimiento de rutas
- Función de escucha de RIP

**Sintaxis:**

| | |
|---|---|
| en**able** | rip-listening<br>router-discovery<br>services |

**rip-listening**

Activa la creación de entradas de la tabla de direccionamiento que se han obtenido “escuchando” el protocolo RIP. La función de escucha de RIP está desactivada por omisión.

**Ejemplo:** `enable rip-listening`

**router-discovery**

Activa la capacidad de aprender pasarelas por omisión a través de la recepción de mensajes de descubrimiento de rutas ICMP. Por omisión, el descubrimiento de rutas está activado.

**Ejemplo:** `enable router-discovery`

**services** Activa el protocolo Servicios de sistema principal en TCP/IP. Si el direccionamiento IP no está activado, Servicios de sistema principal en TCP/IP está activado por omisión.

**Ejemplo: `enable services`**

## List

Utilice el mandato **list** para visualizar información sobre la configuración actual de Sistema principal en TCP/IP.

**Sintaxis:**

**list**

**Ejemplo: `list`**

```
TCP/IP-Host config>list

TCP/IP Host SERVICES    : enabled
IP-HOST Address         : 128.185.142.1
        Mask            : 255.255.255.0
DEFAULT-GATEWAY Address : 128.185.142.47
RIP-LISTENING           : disabled
ROUTER-DISCOVERY        : enabled

TCP/IP-Host config>
```

| | |
|---|---|
| TCP/IP Host SERVICES | Muestra si TCP/IP Host SERVICES está activado o desactivado. |
| IP-HOST Address | Muestra la dirección IP-HOST actual. |
| IP-HOST Mask | Muestra la máscara IP-HOST actual. |
| DEFAULT-GATEWAY Address | Muestra la dirección actual de la pasarela por omisión. |
| RIP-LISTENING | Muestra si la función de escucha de RIP está activada o desactivada. |
| ROUTER DISCOVERY | Muestra si el descubrimiento de rutas está activado o desactivado. |

## Set

Utilice el mandato **set** para definir la dirección IP del 2210. Debe asignar al 2210 una dirección IP antes de activar Servicios de sistema principal en TCP/IP.

**Nota:** Si la dirección IP no está aún configurada, se define (por omisión) utilizando la información de arranque. Este proceso sólo se aplica si el 2210 es un sistema principal de red que funciona como un sistema principal IP.

**Sintaxis:**

**set** ip-host address *dirección-sist.pral.-IP*

**Ejemplo: `set ip 123.45.67.89`**

```
Address mask [255.255.0.0]?
IP-Host Address set.
```

## Supervisión de Servicios de sistema principal en TCP/IP

Esta sección describe cómo supervisar Servicios de sistema principal en TCP/IP en el IBM 2210.

## Cómo acceder al entorno de supervisión de Sistema principal en TCP/IP

Para acceder al entorno de supervisión de Sistema principal en TCP/IP, entre el siguiente mandato en el indicador + (GWCON):

```
+ protocol hst
TCP/IP-Host>
```

## Mandatos de supervisión de Sistema principal en TCP/IP

Esta sección describe los mandatos de supervisión de Sistema principal en TCP/IP. Estos mandatos le permiten ver parámetros y entrar peticiones de información desde el terminal activo. Entre estos mandatos en el indicador TCP/IP-Host>. La Tabla 17 muestra los mandatos.

*Tabla 17. Resumen de mandatos de supervisión de Sistema principal en TCP/IP*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Dump | Muestra la tabla actual de direccionamiento IP. Aparece una línea para cada destino. |
| Interface | Muestra la dirección IP del IBM 2210. |
| Ping | Emite mandatos ping continuos a un determinado destino y muestra una línea por cada respuesta recibida. |
| Traceroute | Muestra la ruta salto a salto a un determinado destino. |
| Routers | Muestra la lista de todos los direccionadores IP que conoce el 2210. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Dump

Utilice el mandato **dump** para visualizar la tabla actual de direccionamiento IP. Aparece una línea para cada destino. Muchas de las entradas que se muestran son el resultado de redireccionamientos ICMP.

**Sintaxis:**

d**ump**

**Ejemplo:**

```
TCP/IP Host> dump
Type   Dest net         Mask      Cost     Age       Next hop(s)

Stat   0.0.0.0          00000000  0        51        128.185.142.47
 Dir*  128.185.142.0    FFFFFF00  1        50        BDG/0

Default gateway in use.
Type Cost     Age       Next hop
Stat 0        51        128.185.142.47

Routing table size: 768 nets (52224 bytes), 2 nets known
                     0 nets hidden, 0 nets deleted, 0 nets inactive
                     0 routes used internally, 766 routes free
```

| | |
|---|---|
| Type | Tipo de ruta que indica el modo en que se ha obtenido la ruta:<br>RIP - la ruta se ha aprendido a través del protocolo RIP.<br>Stat - una ruta configurada de forma estática.<br>Dir - una red o subred conectada directamente. |
| Dest net | Muestra la dirección IP de la red/subred de destino. |
| Mask | Muestra la máscara de la dirección IP. |
| Cost | Muestra el coste de la ruta. |
| Age | Para rutas RIP muestra el periodo de tiempo, en segundos, desde que se renovó la ruta. Para otros tipos de rutas muestra el periodo de tiempo, en segundos, desde que se instaló la ruta. |
| Next Hop | Muestra la dirección IP del siguiente dispositivo de la vía de acceso hacia el sistema principal de destino. También se muestra el tipo de interfaz utilizada por el dispositivo emisor para reenviar el paquete. |
| Default gateway | Muestra la dirección IP de la pasarela por omisión junto con información sobre tipo de ruta, coste, antigüedad y siguiente salto asociada a esta entrada. |
| Routing table size | Muestra el tamaño actual (en redes y bytes) de la tabla actual. También identifica el número de redes que conoce el sistema principal. |

## Interface

Utilice el mandato **interface** para visualizar la dirección IP del IBM 2210. Cuando Servicios de sistema principal en TCP/IP se está ejecutando sobre el puente, se muestra una sola dirección en el terminal como BDG/0.

### Sintaxis:

**interface**

### Ejemplo:

```
TCP/IP Host> interface
Interface     MTU    IP Address(es)   Mask(s)          Address-MTU
  BDG/0      1500    128.185.142.16   255.255.255.0    Unspecified
```

| | |
|---|---|
| Interface | Muestra el tipo de interfaz. Para Servicios de sistema principal en TCP/IP, siempre es BDG/0, lo que indica el puente. |
| IP Address | Muestra la dirección IP de la interfaz Servicios de sistema principal en TCP/IP. |
| Mask | Muestra la máscara de subred de la dirección IP. |

## Ping

Utilice el mandato **ping** para que el dispositivo envíe peticiones de eco ICMP a un determinado destino una vez por segundo (“pinging”) y espere una respuesta. Este mandato sirve para aislar un problema en un entorno de interredes.

El proceso se lleva a cabo continuamente, aumentando el número de secuencia de ICMP con cada paquete adicional. Las respuestas coincidentes de eco ICMP recibidas se notifican junto con su número de secuencia y el tiempo de envío y respuesta. La granularidad (resolución de tiempo) del cálculo del periodo de tiempo de envío y respuesta depende de cada plataforma, y suele ser unos 20 milisegundos.

Para detener el proceso de ping, escriba cualquier carácter en el terminal. En ese momento aparecerá un resumen de paquetes perdidos, periodos de tiempo de envío y respuesta y número de destinos ICMP que no se han podido alcanzar.

Cuando se especifica una dirección de difusión múltiple como destino, pueden aparecer varias respuestas por cada paquete enviado, una por cada miembro del grupo. Cada respuesta recibida se muestra junto con la dirección de origen del emisor de la respuesta.

El usuario puede configurar el tamaño de ping (número de bytes de datos del mensaje ICMP, excluida la cabecera ICMP), el valor TTL y la velocidad de ping. Los valores por omisión son: tamaño de 56 bytes, TTL de 64 y velocidad de 1 ping por segundos.

**Sintaxis:**

p**ing** *destino origen tamaño ttl velocidad*

**Ejemplo:**

```
TCP/IP Host> ping
Destination IP address [0.0.0.0]? 128.185.142.11
Source IP address [128.185.142.16]?
Ping data size in bytes [56]?
Ping TTL [64]?
Ping rate in seconds [1]?
PING 128.185.142.16 -> 128.185.142.11: 56 data bytes, ttl=64, ... every 1 sec.
56 data bytes from 128.185.142.11: icmp_seq=0. ttl=254. time=0. ms
56 data bytes from 128.185.142.11: icmp_seq=1. ttl=254. time=0. ms
56 data bytes from 128.185.142.11: icmp_seq=2. ttl=254. time=0. ms
56 data bytes from 128.185.142.11: icmp_seq=3. ttl=254. time=0. ms
56 data bytes from 128.185.142.11: icmp_seq=4. ttl=254. time=0. ms
56 data bytes from 128.185.142.11: icmp_seq=5. ttl=254. time=0. ms

----128.185.142.11 PING Statistics----
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

## Traceroute

Utilice el mandato **traceroute** para visualizar la vía de acceso completa a un determinado destino, salto a salto. Para cada salto sucesivo, el mandato traceroute envía tres pruebas y muestra la dirección IP del emisor de la respuesta junto con el tiempo de envío y respuesta asociado a la respuesta. Si una determinada punta de prueba no recibe respuesta, se muestra un asterisco (*). Cada línea de la pantalla está relacionada con esta serie de tres pruebas; el número que hay más a la izquierda indica la distancia desde el dispositivo que ejecuta el mandato (en saltos de dispositivos de red).

El mandato traceroute termina cuando se alcanza el destino, se recibe un mensaje No se puede alcanzar destino ICMP o la longitud de la vía de acceso alcanza 32 saltos de dispositivos de red.

**Sintaxis:**

t**raceroute** *destino origen tamaño pruebas espera ttl*

**Ejemplo:**

```
TCP/IP Host> traceroute
Destination IP address [0.0.0.0]? 128.185.144.239
Source IP address [128.185.142.16]?
Data size in bytes [56]?
Number of probes per hop [3]?
Wait time between retries in seconds [3]?
Maximum TTL [32]?
TRACEROUTE 128.185.142.16 -> 128.185.144.239: 56 data bytes
 1 128.185.142.11 16 ms 0 ms 0 ms
 2 128.185.143.33 16 ms 0 ms 0 ms
 3 128.185.144.239 16 ms 0 ms 0 ms
```

En la pantalla:

| | |
|---|---|
| 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 de envío y respuesta que ha tardado el paquete en alcanzar el destino y volver. Se efectúan tres rastreos del paquete. |
| Destination unreachable | Indica que no hay ninguna ruta disponible hasta el destino. |
| 1 * * * 2 * * * | Indica que el dispositivo espera algún tipo de respuesta del destino, pero el destino no responde. |

Cuando una punta de prueba recibe un resultado inesperado (consulte el ejemplo de salida anterior), pueden aparecer diversos indicadores. Estos indicadores se explican en la siguiente tabla.

| | |
|---|---|
| !N | Indica que se ha recibido un mensaje No se puede alcanzar el destino ICMP (no se puede alcanzar la red). |
| !H | Indica que se ha recibido un mensaje No se puede alcanzar el destino ICMP (no se puede alcanzar el sistema principal). |
| !P | Indica que se ha recibido un mensaje No se puede alcanzar el destino ICMP (no se puede alcanzar el protocolo ). |
| ! | Indica que se ha alcanzado el destino, pero la respuesta enviada por el destino se ha recibido con un TTL igual a 1. Esto suele indicar un error en el destino, frecuente en algunas versiones de UNIX, por el que el destino inserta un TTL de prueba en sus respuestas. Esto genera una serie de líneas que solo contienen asteriscos antes de alcanzar finalmente el destino. |

## Routers

Utilice el mandato **routers** para visualizar la lista de todos los direccionadores IP que conoce el IBM 2210. Los direccionadores se pueden aprender a través de:

- Configuración estática (mediante el mandato **add default-gateway** que se explica en la página “Add” en la página 227).
- Redireccionamiento ICMP recibidos

- Mensajes de descubrimiento de rutas ICMP (si está configurado)
- Actualizaciones RIP (si está configurado)

Cada direccionador se muestra con su origen, su prioridad (utilizada al seleccionar la ruta por omisión) y su tiempo de vida (el número se segundos que transcurrirán hasta que el direccionador se declare no válido a no ser que se le vuelva a escuchar).

**Sintaxis:**

**routers**

**Ejemplo:** `routers`

# Configuración y supervisión de protocolos de direccionador

# Visión general del direccionamiento sobre ATM

**Nota:** Consulte el glosario para ver definiciones de las abreviaturas y los términos que se utilizan en este capítulo. Este capítulo describe el direccionamiento sobre ATM nativo.

## Visión general del direccionamiento

La visión general del direccionamiento que se presenta en esta sección es breve porque las relaciones entre Emulación de LAN (LE), IP clásico (CIP) y los protocolos de direccionamiento soportados son sencillas. El direccionador da soporte al direccionamiento IP e IPX, tal como se ilustra en la Figura 26 y en la Figura 27.

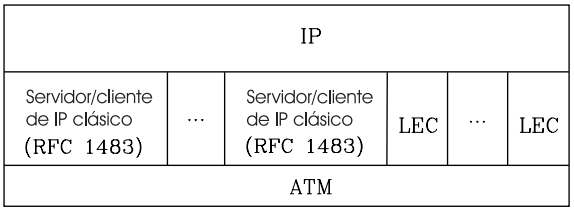



*Figura 26. Direccionamiento IP*

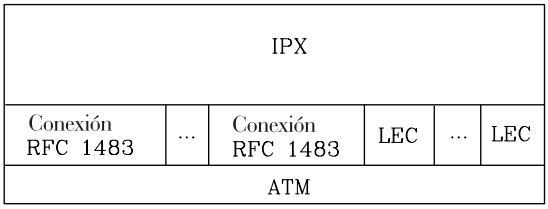



*Figura 27. Direccionamiento IPX*

Se da soporte al direccionamiento IP entre combinaciones arbitrarias de redes de IP clásico (CIP) y de emulación de LAN (LE), donde el direccionamiento IPX recibe soporte sobre interfaces de LAN emuladas y conexiones RFC 1483 [1] con otros direccionadores. Estos protocolos tratan a las interfaces emuladas implantadas por clientes de emulación de LAN (LE) como si fueran interfaces Ethernet o de red en anillo. Cuando se crea un cliente LE, se le asigna un número de interfaz exclusivo.

## Visión general sobre el Soporte RFC 1483

RFC 1483 (Encapsulación multiprotocolo sobre capa 5 de adaptación ATM) ofrece los detalles sobre la encapsulación de las tramas conectadas por puente y direccionadas. Se da soporte al direccionamiento de tráfico IP e IPX. El software también ofrece una amplia gama de posibilidades de conexión por puente, permitiendo que el tráfico conectado por puente se transmita de forma nativa sobre ATM.

[1] J. Heinanen, “Multiprotocol Encapsulation over ATM Adaptation Layer 5,” RFC 1483, Telecom Finland, Julio de 1993.

RFC 1483 especifica la encapsulación LLC/SNAP para transferir el tráfico multiprotocolo sobre ATM. Se especifica un valor de LLC igual a 0xAA-AA-03 para indicar la presencia de una cabecera SNAP. La parte OUI de la cabecera SNAP es 0x00-00-00 para los protocolos direccionados y 0x00-80-C2 para los protocolos conectados por puente.

## Visión general del Soporte RFC 1483 para el direccionamiento

IP clásico utiliza el formato LLC/SNAP para los protocolos direccionados definidos en RFC 1483. El direccionador también da soporte a las conexiones con direccionadores IPX que utilizan encapsulación LLC/SNAP. El diseño de soporte IPX se basa en IP clásico.

## Soporte RFC 1483 para el direccionamiento IPX

Los direccionadores IPX utilizan el protocolo de información de direccionamiento (RIP) y el protocolo de anuncio de servicios (SAP) para propagar las tablas de información de direccionamiento y de dispositivos. En LAN o LAN emuladas, estos protocolos utilizan tramas de difusión general para propagar la información a los partícipes interesados. El direccionador también propaga información de direccionamiento y de dispositivos destinada y procedente de todas las conexiones RFC 1483 con otros direccionadores IPX.

Al igual que otros direccionadores que dan soporte a la encapsulación LLC/SNAP de RFC 1483 en ATM, el direccionador se puede interconectar en mallas completas o parciales mediante conexiones RFC 1483 configuradas de forma manual.

En una red de *malla completa*, cada direccionador tiene una conexión directa con cada uno de los demás direccionadores. En una red de *malla parcial*, no todos los direccionadores tienen una conexión directa con cada uno de los demás direccionadores; sin embargo, existe la conectividad suficiente como para que cada direccionador alcance a cualquier otro direccionador, directamente o a través de otro direccionador. En una red de malla parcial, algunos direccionadores deben llevar a cabo el direccionamiento intermedio. Un direccionador intermedio ofrece conectividad entre direccionadores que no están directamente conectados entre sí.

Se da soporte tanto a los circuitos virtuales permanentes (PVC) como a los circuitos virtuales conmutados (SVC) configurados. Sin embargo, las conexiones de canal virtual (VCC) con direccionadores IPX deben estar dedicados a IPX; no se pueden compartir con otros protocolos, como IP.

Al igual que en IP clásico, se pueden especificar características de Calidad de servicio configurando parámetros de tráfico VCC, como velocidades punta y sostenida, y se pueden configurar varios circuitos en una sola interfaz ATM.

El direccionador da soporte a una sola red IPX por interfaz ATM. Esto significa que sólo hay un cliente ATM ARP por interfaz para IPX, el cual se debe configurar de forma explícita. Por lo tanto, todos los direccionadores interconectados de una interfaz ATM deben formar parte de la misma red IPX.

Las direcciones ATM de IPX deben ser exclusivas entre todos los componentes que utilizan la encapsulación RFC 1483, incluidos los componentes de IP clásico. Las partes de identificador del sistema final (ESI) y de selector de las direcciones ATM de IPX se configuran del mismo modo que las direcciones ATM de IP clásico. Cuando el direccionador no inicia el SVC, al menos el selector se debería especi-

ficar de forma explícita a fin de ofrecer una dirección fija que se puede configurar en el direccionador que emite la llamada.

Las direcciones del protocolo IPX tienen dos partes: un número de red de 4 bytes y un número de sistema principal (o ID de sistema principal) de 6 bytes. Los números de red deben ser exclusivos dentro de los dominios de direccionamiento IPX, y los números de sistema principal deben ser exclusivos dentro de una determinada red. El direccionador define el número de sistema principal IPX ante el componente ESI de la dirección ATM asociada. Si no configura de forma explícita el ESI, adopta por omisión la dirección MAC marcada en el hardware de la interfaz ATM.

Puede especificar números de sistema principal IPS de destino durante la configuración de VCC o puede dejar que se aprendan de forma dinámica mediante InATMARP. Debe configurar de forma manual los números de sistema principal IPX de los direccionadores de destino que no dan soporte a InATMARP. El direccionador utiliza también de forma periódica InATMARP para renovar su conocimiento del número de sistema principal IPS del direccionador asociado.

Los direccionadores interconectados en una malla parcial y que ofrecen direccionamiento intermedio entre direccionadores de la misma interfaz ATM deberían desactivar el horizonte de división IPS de la interfaz ATM. De este modo se asegura que RIP y SAP informan correctamente a los direccionadores interconectados sobre los direccionadores y servicios disponibles. Los direccionadores interconectados en una malla completa no necesitan desactivar el horizonte de división.

La implantación del direccionador del soporte RFC 1483 para direccionamiento IPX necesita una configuración mínima. El número de red IPX y el número de sistema principal IPX (cliente IPX ATM ARP) son la única información necesaria. Si desea abrir una conexión con un direccionador IPX remoto, debe configurar adicionalmente las conexiones de canal virtual (VCC) que desee. Aunque la combinación de encapsulación RFC 1483 e InATMARP aún no se ha estandarizado, se especifica la combinación para IPX sobre Frame Relay en RFC 1490/2427. [2]

[2] T. Bradley, C. Brown, and A. Malis, “Multiprotocol Interconnect Over Frame Relay,” RFC 1490/2427, Wellfleet Communications Inc. and Ascom Timeplex Inc., Julio de 1993.

# Utilización de IP

Este capítulo describe cómo configurar el Protocolo Internet (IP). Incluye las siguientes secciones:



## Procedimientos básicos de configuración

Esta sección describe los pasos iniciales a seguir para poner a punto el protocolo IP. Los detalles sobre cómo realizar cambios en la configuración se explican en otras secciones de este capítulo. Los detalles sobre cada uno de los mandatos de configuración se encuentran en la sección de mandatos de este capítulo. La siguiente línea contiene las tareas iniciales de configuración a llevar a cabo para configurar IP en el direccionador. Una vez realizadas estas tareas, debe volver a arrancar el direccionador para que la nueva configuración entre en vigor.

1. Acceda al entorno de configuración de IP. (Consulte el tema "Cómo acceder al entorno de configuración de IP" en la página 273.)
2. Asigne direcciones IP a las interfaces de red. (Consulte el tema "Cómo asignar direcciones IP a interfaces de red".)
3. Active el direccionamiento dinámico. (Consulte el tema "Activación del direccionamiento dinámico" en la página 245.)
4. Añada información sobre el direccionamiento estático, si es necesario. (Consulte el tema "Cómo añadir información de direccionamiento estático" en la página 247.)
5. Active el direccionamiento de subred ARP, si es necesario. (Consulte el tema "Activación del direccionamiento de subred ARP" en la página 250.)
6. Configure parámetros ARP, si es necesario. (Consulte el tema "Puesta a punto de la configuración ARP" en la página 250.)
7. Salta del proceso de configuración de IP.
8. Vuelva a arrancar el direccionador para activar los cambios en la configuración.

## Cómo asignar direcciones IP a interfaces de red

Utilice el mandato **add address** de configuración de IP para asignar direcciones IP a las interfaces de red. Los argumentos de este mandato incluyen el número de interfaz (que se obtiene mediante el mandato `Config>` **list devices**) y la dirección IP con su máscara de dirección asociada.

En el siguiente ejemplo, se ha asignado a la interfaz de red 2 la dirección 128.185.123.22 con la máscara de dirección asociada 255.255.255.0 (utilizando el tercer byte para las subredes).

```
IP config> add address 2 128.185.123.22 255.255.255.0
```

Se pueden asignar varias direcciones IP a una sola interfaz de red.

Por omisión, las direcciones IP asignadas a las interfaces de red deben estar en distintas redes o subredes. El mandato **enable same-subnet** elimina esta restricción.

IP le permite utilizar una interfaz de línea serie para el tráfico IP sin asignar a la línea una dirección IP real. Sin embargo, tiene que asignar a cada línea serie una seudo dirección IP; el direccionador utiliza esta dirección para hacer referencia a la interfaz, pero nunca se utiliza de forma externa. Utilice el mandato **add address** para asignar a la línea serie una dirección con el formato 0.0.0.*n*, donde *n* es el número de interfaz (que se obtiene mediante el mandato `Config>` **list devices**). Este formato de dirección indica al direccionador que la interfaz es una *línea serie no numerada*.

Para activar IP en la interfaz de línea serie número 2 sin asignar a la interfaz ninguna dirección IP, utilice el siguiente mandato:

```
IP config> add address 2 0.0.0.2
```

## Utilización de Dirección dinámica

Se puede utilizar una Dirección dinámica para identificar una interfaz que aprenderá su dirección IP desde el extremo remoto de un enlace de Protocolo punto a punto (PPP) que utilice un Protocolo de control de protocolos Internet (IPCP). Primero se debe añadir la interfaz como una línea serie no numerada (0.0.0.n). Cuando termine IPCP, se le notificará a IP y la dirección IP negociada se instalará en la interfaz especificada. Para activar la Dirección dinámica, siga los siguientes pasos:

- PPP debe estar configurado para solicitar una dirección IP del siguiente modo:

```
PPP 3 Config>set ipcp
IP COMPRESSION [no]:
Request an IP address [no]: yes
Interface remote IP address to offer if requested (0.0.0.0 for none) [0.0.0.0]?
```

- IP debe estar configurado en la interfaz PPP como una línea serie no numerada:

```
IP config>add address
Which net is this address for [0]? 3
New address []? 0.0.0.3
Address mask [0.0.0.0]? 255.255.255.255
```

- IP debe activar la Dirección dinámica en la misma interfaz:

```
IP config>enable dynamic-address
Interface address []? 0.0.0.3

IP config>list address
IP addresses for each interface:
intf  0   192.168.8.1      255.255.255.0    Local wire broadcast, fill 1
intf  1                                     IP disabled on this interface
intf  2                                     IP disabled on this interface
intf  3   0.0.0.3          255.255.255.0    Local wire broadcast, fill 1
                                            DYNAMIC-ADDRESS Enabled
```

## Cómo asignar direcciones IP a la interfaz de red de puente

El 2210 direcciona los paquetes IP a las interfaces de red a las que se han asignado direcciones IP (*interfaces de direccionamiento*) y conecta por puente paquetes IP a las interfaces de red en las que está configurada la conexión por puente, pero a las que no se ha asignado ninguna dirección IP (*interfaces de conexión por puente*). El 2210 puede recibir datagramas IP procedentes de interfaces de conexión por puente, enviar datagramas IP a las interfaces de conexión por puente y direccionar paquetes IP entre las interfaces de conexión por puente y las interfaces de direccionamiento. Puede activar estas funciones en el 2210 añadiendo una o más direcciones IP a la Interfaz de red de puente. La Interfaz de red de puente es una interfaz lógica que conecta IP a la red conectada por puente a la que está conectado el 2210.

Para añadir direcciones IP a la Interfaz de red de puente, utilice el mandato **add address**, especificando **bridge** como la interfaz de red:

```
IP config> add address bridge dirección-ip máscara-dirección-ip
```

Este mandato no asigna una dirección IP a ninguna interfaz individual de conexión por puente sino, de hecho, a todas las interfaces de conexión por puente.

Al asignar direcciones IP a la Interfaz de red de puente se puede liberar una de las interfaces de red físicas (puertos físicos) del 2210. Para comprenderlo, consulte la Figura 28, que ilustra una interred IP con distintos dispositivos que llevan a cabo las funciones de direccionador y de puente. La LAN 2 y la LAN 3 están conectadas mediante el puente para formar una red conectada por puente; ante el direccionador, esta red conectada por puente es una sola subred IP definida por la dirección IP 9.67.5.1 y la máscara 255.255.255.0.

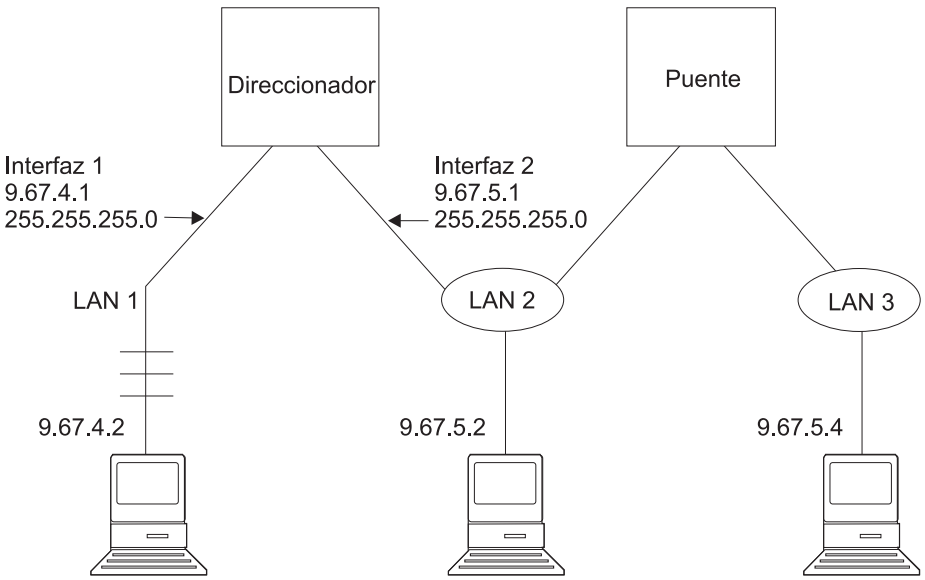



*Figura 28. Direccionamiento a una red conectada por puente - Alternativa 1*

La Figura 29 en la página 244 ilustra la misma interred con las funciones de direccionador y puente fusionadas en un solo dispositivo. En esta figura, el direccionador sigue teniendo su propia interfaz de red física (Interfaz 2) con la red conectada por puente.

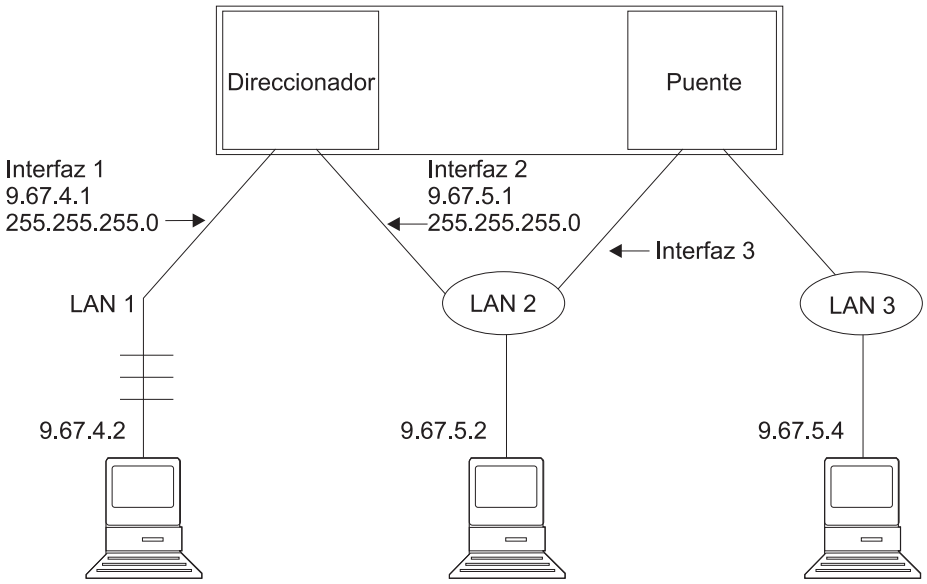



*Figura 29. Direccionamiento a una red conectada por puente - Alternativa 2*

Finalmente, en la Figura 30, la interfaz de red física del direccionador con la red conectada por puente se ha sustituido por la Interfaz de red de puente, que es una interfaz interna. Es la misma interred que aparece en la 28 y en la 29, pero el direccionador ya no necesita su propia interfaz de red física con la red conectada por puente.

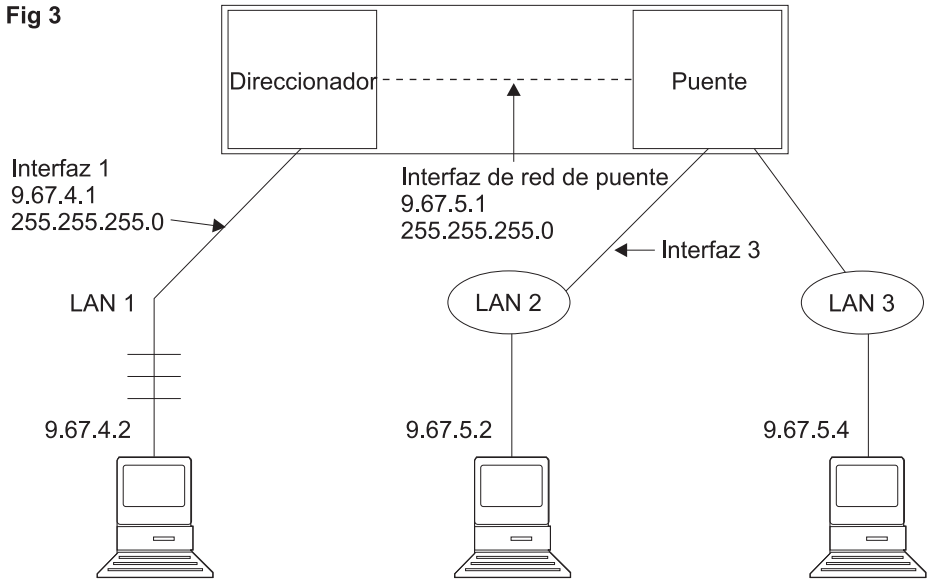



*Figura 30. Direccionamiento a una red conectada por puente - Alternativa 3*

**Nota:** Si hay direcciones IP configuradas en la interfaz de red de puente, no puede configurar direcciones IP en ninguna interfaz de red en anillo en la que se haya configurado una conexión por puente de direccionamiento de origen.

## Definición de la dirección IP interna

Es una dirección IP que no depende del estado de ninguna interfaz y se define sin referencia a ninguna otra interfaz. Algunas configuraciones IP lo necesitan. Consulte el mandato **set internal-IP-address** en la página 326 para obtener más información.

## Activación del direccionamiento dinámico

Siga los siguientes procedimientos para activar el direccionamiento dinámico en el direccionador. El software del direccionador da soporte a OSPF, RIPv1 y RIPv2 para protocolos de pasarela interior (IGP) así como a BGP, que es un protocolo de pasarela externa.

Todos los protocolos de direccionamiento se pueden ejecutar simultáneamente. Sin embargo, la mayoría de los direccionadores sólo se ejecutarán probablemente en un protocolo de direccionamiento (uno de los IGP). Se recomienda el protocolo OSPF debido a su potencia y a las características IP adicionales (como como múltiples vías de acceso al mismo coste y subredes de longitud variable) a las que da soporte.

### Definición del tamaño de la tabla de direccionamiento

El tamaño de la tabla de direccionamiento determina el número de entradas de la tabla de direccionamiento procedentes de todos los posibles orígenes, incluidos los protocolos de direccionamiento dinámico y las rutas estáticas. El tamaño por omisión es 768 entradas.

Para cambiar el tamaño de la tabla de direccionamiento, utilice el mandato de configuración **set routing table-size**. Si define un tamaño de tabla de direccionamiento insuficiente, se eliminarán rutas. Si define un tamaño excesivo, se utilizarán de forma poco eficiente los recursos de memoria. Tras la ejecución, utilice el mandato de consola **dump** para ver el contenido de la tabla y luego ajuste el tamaño según sea necesario, dejando espacio para una posible expansión.

### Activación del protocolo OSPF

La configuración OSPF se realiza a través de su propia consola de configuración (en la que se entra mediante el mandato `Config>` **protocol ospf**). Para activar OSPF, utilice el siguiente mandato:

```
OSPF Config> enable OSPF
```

Después de activar el protocolo OSPF, se le solicitará una estimación del tamaño de la base de datos de estado de enlace OSPF. Esto ofrece al direccionador una idea de la cantidad de memoria que se debe reservar para OSPF. Debe especificar los dos siguientes valores que se utilizarán para estimar el tamaño de la base de datos de estado de enlace OSPF:

- Número total de direccionadores externo importados en el dominio de direccionamiento OSPF.
- Número total de direccionadores OSPF del dominio de direccionamiento.

Entre estos valores en los siguientes indicadores (se han ofrecido valores de ejemplo):

```
OSPF Config> enable ospf
Estimated # external routes[0]? 200
Estimated # OSPF routers [50]? 60
Maximum LSA size [2048]?
```

A continuación, configure cada interfaz IP que deba participar en el direccionamiento OSPF. Para configurar una interfaz IP para OSPF, utilice el siguiente mandato:

```
OSPF Config> set interface
```

Se le solicitará que entre una serie de parámetros operativos. A cada interfaz se le asigna un coste, además de otros parámetros operativos de OSPF.

Cuando se ejecutan otros protocolos de direccionamiento IP además de OSPF, es posible que desee activar el intercambio de rutas entre OSPF y los otros protocolos. Para ello, utilice el siguiente mandato:

```
OSPF Config> enable AS-boundary-routing
```

Para obtener más información sobre el proceso de configuración de OSPF, consulte el tema “Utilización de OSPF” en la página 359.

## Activación del protocolo RIP

Esta sección describe cómo configurar inicialmente el protocolo RIP. Al configurar el protocolo RIP, puede especificar qué grupo de rutas anunciará y/o aceptará el direccionador en cada interfaz IP.

RIP no recibe soporte en interfaces de red X.25 ni ATM (RFC 1577) nativas. Para estos tipos de interfaces, utilice OSPF en lugar de RIP como protocolo de pasarela interior (IGP). RIP recibe soporte en las interfaces de red de emulación de LAN ATM.

Primero, active el protocolo RIP con el siguiente mandato:

```
IP config> enable RIP
```

Cuando RIP está activado, se establece el siguiente comportamiento por omisión:

- El direccionador incluye todas las rutas de red y subred en actualizaciones de RIP que se envían a cada una de sus interfaces IP configuradas. Esto no incluye la ruta estática ni la ruta por omisión.
- El direccionador procesa todas las actualizaciones RIP recibidas en cada una de sus interfaces IP configuradas.
- RIP no alterará temporalmente la ruta estática ni la ruta por omisión.

Para cambiar alguno de los comportamientos de envío o recepción por omisión, utilice los siguientes mandatos de configuración de IP, que se definen por interfaz IP.

```
IP config> enable/disable sending net-routes
IP config> enable/disable sending subnet-routes
IP config> enable/disable sending static-routes
IP config> enable/disable sending host-routes
IP config> enable/disable sending default-routes
IP config> enable/disable receiving rip
IP config> enable/disable receiving dynamic nets
IP config> enable/disable receiving dynamic subnets
IP config> enable/disable receiving host-routes
IP config> enable/disable override default
IP config> enable/disable override static-routes
IP config> set originate-rip-default
```

**Nota:** Estos mandatos no se visualizan cuando se han configurado políticas de direccionamiento IP. Consulte el tema “Función de filtro de rutas con políticas” en la página 259 para obtener más información.

### Activación del protocolo BGP

El protocolo BGP se activa desde su propio indicador de configuración, `BGP Config>`. Para obtener más información sobre cómo configurar BGP, consulte el tema sobre utilización y configuración de BGP4 en el manual *Consulta de configuración y supervisión de protocolos Volumen 1*.

## Cómo añadir información de direccionamiento estático

Este procedimiento sólo es necesario para información de direccionamiento que no puede obtener de ninguno de los protocolos de direccionamiento dinámico anteriores. La información de direccionamiento estático sobrevive a anomalías en la alimentación y se utiliza para rutas que nunca cambian o que no se pueden aprender de forma dinámica.

El destino de una ruta estática se describe mediante una dirección IP (*dirección-dest*) y una máscara de dirección IP (*máscara-dest*). La máscara indica el rango de direcciones IP al que se aplica la ruta; por ejemplo, una ruta con una dirección IP 10.0.0.0 y una máscara 255.0.0.0 se aplica a las direcciones IP comprendidas entre la 10.0.0.0 y la 10.255.255.255. La ruta al destino se describe mediante la dirección IP del direccionador del siguiente salto (*siguiente-salto*) y coste de reenviar un paquete a través de esta ruta (*coste*).

Para crear, modificar o suprimir una ruta estática, utilice los siguientes mandatos:

```
IP config> add route dirección-dest máscara-dest
siguiente-salto  coste
IP config> change route dirección-dest  máscara-dest siguiente-salto coste
IP config> delete route dirección-dest  máscara-dest
```

Estos mandatos le permite definir un máximo de cuatro rutas estáticas por destino IP, lo que permite disponer de rutas alternativas si una o más rutas fallan. Estos mandatos entran en vigor inmediatamente, sin tener que volver a arrancar el direccionador.

### Regla de coincidencia más larga

Puesto que el destino de una ruta incluye la máscara de dirección IP, es posible que haya más de una ruta que coincida con una determinada dirección IP; por ejemplo, para la dirección IP 10.1.2.3, coincidirían tanto una ruta con dirección IP 10.0.0.0 y máscara 255.0.0.0 como una con dirección IP 10.1.0.0 y máscara 255.255.0.0. Para determinar qué ruta utilizar, se aplica la regla de la coincidencia más larga. Se utiliza la ruta que tenga la máscara más larga (en este caso, la ruta con la dirección IP 10.1.0.0 y la máscara 255.255.0.0).

## Rutas por omisión, de red, de subred y de sistema principal

Las rutas se puede clasificar como rutas *por omisión*, *de red*, *de subred* o *de sistema principal*, en función de su dirección IP y su máscara de destino.

Una ruta *por omisión* tiene una dirección IP/máscara igual a 0.0.0.0/0.0.0.0. Esta ruta coincide con todas las direcciones IP de destino, pero puesto que se aplica la regla de coincidencia más larga, sólo se utiliza si no hay ninguna otra ruta que coincida. El siguiente mandato crea una ruta por omisión estática:

```
IP config> add route
IP destination [ ]? 0.0.0.0
Address mask [255.0.0.0]? 0.0.0.0
Via gateway 1 at [ ]? 192.9.1.4
Cost [1]? 5
Via gateway 2 at [ ]?
IP config>
```

La ruta por omisión estática también se puede definir mediante el mandato **set default network-gateway**; sin embargo, este mandato no entra en vigor de forma inmediata y sólo le permite definir una ruta estática por omisión. El siguiente ejemplo crea la misma ruta estática por omisión que el mandato **add route** anterior:

```
IP config> set default network-gateway
Default gateway [ ]? 192.9.1.4
gateway's cost [1]? 5
IP config>
```

Una *ruta de red* tiene una máscara que depende del valor de la dirección IP de destino de la ruta, tal como se ha especificado en las clases de direcciones IP IP definidas en RFC 791:

| Clase de direcciones IP | Rango de direcciones IP | Máscara de red |
|---|---|---|
| A | 0.0.0.0 - 127.255.255.255 | 255.0.0.0 |
| B | 128.0.0.0 - 191.255.255.255 | 255.255.0.0 |
| C | 192.0.0.0 - 223.255.255.255 | 255.255.255.0 |

Los mandatos **add route**, **change route** y **delete route** utilizan la máscara de red que corresponde a la dirección IP de destino como el valor de máscara por omisión. El siguiente mandato crea una ruta de red estática:

```
IP config> add route 172.16.0.0
Address mask [255.255.0.0]?
Via gateway 1 at [ ]? 192.9.1.4
Cost [1]? 5
Via gateway 2 at [ ]?
IP config>
```

Una ruta de red estática también se puede definir con el mandato **set default subnet-gateway**; sin embargo, este mandato no entra en vigor de forma inmediata y sólo le permite añadir una ruta estática por destino. El siguiente ejemplo crea la misma ruta de red estática que el mandato **add route** anterior:

```
IP config> set default subnet-gateway
For which subnetted network [ ]? 172.16.0.0
Default gateway [ ]? 192.9.1.4
gateway's cost [1]? 5
IP config>
```

Una *ruta de subred* tiene una máscara más larga que la máscara de red correspondiente a la dirección IP de destino de la ruta. El siguiente mandato crea una ruta de subred estática:

```
IP config> add route 172.16.1.0
Address mask [255.255.0.0]? 255.255.255.0
Via gateway 1 at [ ]? 192.9.1.4
Cost [1]? 5
Via gateway 2 at [ ]?
IP config>
```

Una *ruta de sistema principal* es una ruta a una determinada dirección IP; tiene una máscara igual a 255.255.255.255. El siguiente mandato crea una ruta de sistema principal estática:

```
IP config> add route 172.16.1.2
Address mask [255.255.0.0]? 255.255.255.255
Via gateway 1 at [ ]? 192.9.1.4
Cost [1]? 5
Via gateway 2 at [ ]?
IP config>
```

## Interacción entre direccionamiento estático y direccionamiento dinámico

Las rutas que se aprenden de forma dinámica a través de los protocolos OSPF y RIP pueden alterar temporalmente las rutas estáticas. Para el protocolo RIP, puede desactivar este comportamiento. Consulte la sección sobre RIP de este capítulo que trata sobre los mandatos **enable/disable override static-routes**.

Puede configurar tanto OSPF como RIP para que anuncien rutas estáticas configuradas sobre interfaces en las que estos protocolos dinámicos están activados.

Para configurar RIP de modo que anuncie rutas estáticas, entre el siguiente mandato en el indicador `IP config>`:

```
IP config> enable sending static-routes dirección-interfaz-ip
```

Para configurar OSPF de modo que anuncie rutas estáticas, entre el siguiente mandato en el indicador `OSPF Config>`:

```
OSPF Config>enable as boundary
Use Route Policy [No]?
Import BGP routes [No]?
Import RIP routes [No]?
Import static routes [No]? yes
Import direct routes [No]?
Import subnet routes [Yes]?
```

## Nexthop Awareness

Nexthop Awareness (conocimiento del siguiente paso) permite al direccionador detectar si un direccionador contiguo está activo o inactivo. Cuando esta opción está activada, el direccionador determina de forma más precisa si una ruta estática que utiliza el direccionador contiguo como su siguiente salto funcionará o no. También permite al direccionador determinar sobre qué interfaz de red se puede alcanzar el siguiente salto de una ruta estática cuando el siguiente salto está en una subred IP que está definida en varias interfaces de red.

Para activar Nexthop Awareness en una determinada interfaz IP, entre el siguiente mandato en el indicador de configuración de IP:

```
IP config> enable nexthop-awareness dirección-interfaz-ip
```

Para desactivar Nexthop Awareness en una determinada interfaz IP, entre el siguiente mandato en el indicador de configuración de IP:

```
IP config> disable nexthop-awareness dirección-interfaz-ip
```

Nexthop Awareness sólo recibe soporte en redes Frame Relay en las que los direccionadores contiguos dan soporte a ARP inverso.

## Puesta a punto de la configuración ARP

El Protocolo de resolución de direcciones (ARP) sirve para correlacionar direcciones de protocolos con direcciones de hardware antes de que el direccionador reenvíe un paquete. ARP siempre está activo en el direccionador, así que no tiene que realizar ningún paso de configuración adicional para activarlo con sus características por omisión. Sin embargo, si tiene que modificar algún parámetro de configuración de ARP (como por ejemplo **enable auto-refresh** o **set refresh-timer**, que modifica el temporizador de renovación por omisión) o si tiene que añadir, modificar o suprimir correlaciones de direcciones permanentes, consulte el tema “Utilización de ARP” en la página 627.

Si la Emulación de LAN está configurada en una interfaz, se aplican los valores por omisión. Puede utilizar de forma efectiva el protocolo ARP sin cambios. Si se utiliza RFC 1577 (IP clásico y ARP sobre ATM), hay que realizar tareas adicionales de configuración para clientes ARP y servidores ARP para cada dirección IP configurada en esta interfaz ATM (tal como se describe en el tema “Mandatos de configuración de ARP sobre ATM” en la página 647).

## Activación del direccionamiento de subred ARP

Si hay sistemas principales en redes con subredes conectadas que no dan soporte a las subredes IP, utilice el direccionamiento de subred del Protocolo de resolución de direcciones (descrito en RFC 1027). Cuando el direccionador está configurado para el direccionamiento de subred ARP, responderá mediante proxy a las peticiones de ARP de destino (es decir, fuera de la LAN si el direccionador es la mejor ruta al destino y el destino está en la misma red natural que el origen). Para un funcionamiento correcto, todos los direccionadores conectados a una LAN que contiene sistemas principales que ignoran las subredes se deben configurar para el direccionamiento de subred ARP.

Para activar el direccionamiento de subred ARP, utilice el siguiente mandato:

```
IP config> enable arp-subnet-routing
```

### Activación del direccionamiento de red ARP

Algunos sistemas principales IP utilizan ARP para todos los destinos, tanto si el destino está en la misma red natural que el origen como si no es así. Para estos sistemas principales, el direccionamiento de subred ARP no resulta suficiente y el direccionador se puede configurar para que responda mediante proxy a las peticiones ARP, siempre que se pueda acceder al destino a través del direccionador y el destino no se encuentre en el mismo segmento de la red local que el origen.

Para activar el direccionamiento de red ARP, utilice el siguiente mandato:

```
IP config> enable arp-network-routing
```

## Función de filtro de IP

La función de filtro le permite especificar determinados criterios que debe utilizar el direccionador para controlar el reenvío de paquetes. Se ofrecen los siguientes tipos principales de funciones de filtro como ayuda para conseguir sus objetivos relacionados con seguridad y administración:

- Control de acceso
- La característica de políticas (consulte el tema Using the Policy Feature del manual *Utilización y configuración de las características*)
- Función de filtro de rutas

**Nota:** Para IPv4, ahora dispone de la opción de configurar reglas de control de acceso en una base de datos de políticas para designar control de acceso y determinar el modo en que se filtran los paquetes IP. Consulte el capítulo "Using Policy" del manual *Utilización y configuración de las características* para obtener más información.

## Control de acceso

El control de acceso permite al direccionador IP controlar el proceso de paquetes individuales en función de los siguientes parámetros:

- Dirección de origen IP
- Dirección de destino IP
- Número de protocolo IP
- Número de puerto de origen TCP o UDP
- Número de puerto de destino TCP o UDP
- Bits SYN y ACK de TCP
- Tipo y código ICMP
- Precedencia de función de filtro de Tipo de servicio (TOS)

El control de acceso puede limitar la capacidad de determinados grupos de servicios y sistemas principales IP de comunicarse entre sí.

Puede definir controles de acceso configurando listas de control de acceso. Se pueden especificar una lista global y dos listas por interfaz. La lista global se aplica al direccionador como conjunto. A las listas de interfaz, también denominadas filtros de paquetes, se les asignan nombres y se aplican únicamente a la interfaz designada. Para cada interfaz, se aplica una lista a los paquetes de entrada y la otra se aplica a los paquetes de salida. Las listas se aplican independientemente unas de otras. Un paquete puede *pasar* una lista de interfaz de entrada y puede *ser eliminado* por la lista global.

La Figura 31 en la página 252 ilustra las series de listas de control de acceso por las que debe pasar un paquetes antes de que se proceda a su reenvío.

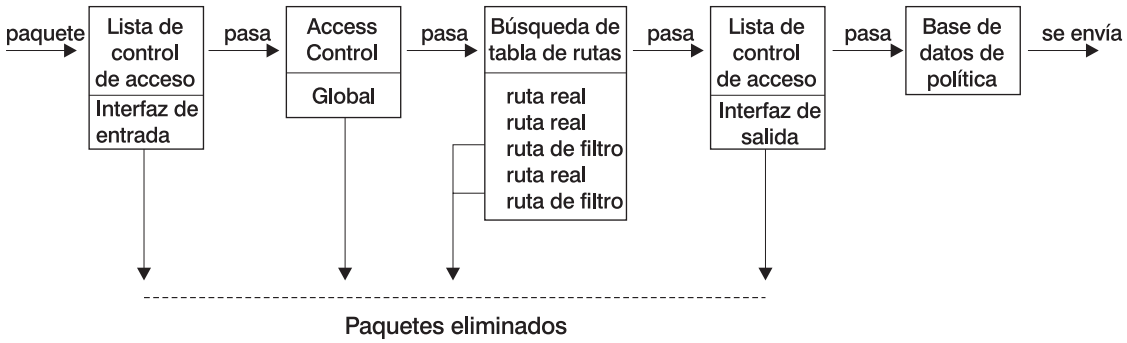



*Figura 31. Listas de control de acceso en la vía de acceso de reenvío de paquetes*

## Reglas de control de acceso

Cada lista de control de acceso consta de una o más reglas de control de acceso que definen los criterios de la función de filtro. Algunas reglas de control de acceso definen filtros globales que afectan a todas las interfaces del direccionador y otras definen las listas de control de acceso específicas de cada interfaz (también denominadas filtros de paquetes). Las reglas de control de acceso globales se configuran mediante el mandato **add access** desde el indicador `IP config>`. Los filtros de paquetes se definen mediante dos mandatos desde el indicador `IP config>`: el mandato **add packet-filter** para definir el filtro y el mandato **update packet-filter** para configurarlo.

A medida que los paquetes IP fluyen a través del direccionador, los campos de paquetes IP se comparan con las reglas de control de acceso. Un paquete coincide con una regla si cada campo especificado en la regla coincide con un campo correspondiente en el paquete. Si un paquete coincide con una regla y el tipo de filtro de la regla es inclusive, el paquete *pasa*. Si el tipo de filtro de la regla es exclusive, el paquete se *elimina* y el direccionador deja de procesarlo. Si después de examinar toda la lista no hay ninguna regla que coincida, el paquete también se elimina.

Al definir registros de listas de control de acceso, es importante recordar la siguiente información:

- El orden de los registros de una lista es importante. Se ofrecen mandatos de configuración que sirven para modificar el orden de los registros de una lista.
- Para cada lista que incluya al menos una regla de control de acceso, debe existir una regla inclusive para que pasen la lista los paquetes que no coinciden con ninguna de las reglas de control de acceso. Un método de permitir que pasen todos los paquetes que no coinciden con ninguna de las reglas especificadas consiste en incluir la siguiente regla comodín como la última regla de la lista:

```
IP config> add access-control
Enter type [E]? i
```

## Activación del control de acceso

El control de acceso IP (incluido el control de acceso global y de interfaz) se activa con el mandato **set access-control on** y se desactiva con el mandato **set access-control off**. Puede utilizar los mandatos **enable packet-filter** y **disable packet-filter** para activar y desactivar filtros específicos de paquetes cuando el control de acceso IP está activado.

Si el control de acceso IP está desactivado, debe tener cuidado con los paquetes que el direccionador origina y recibe. Asegúrese de no filtrar los paquetes RIP u OSPF que envía o recibe el direccionador. El modo más sencillo de hacerlo consiste en añadir una regla inclusive comodín como la última de la lista de control de acceso. También puede añadir reglas específicas para RIP y OSPF, quizás con direcciones y máscaras restrictivas. Tenga en cuenta que algunos paquetes OSPF se envían a las direcciones de difusión múltiple de Clase D 224.0.0.5 y 224.0.0.6, lo que es importante si se lleva a cabo comprobación de direcciones para los protocolos de direccionamiento. Consulte el mandato **add** para obtener más información sobre el control de acceso.

## Cómo definir la lista global de control de acceso

La lista global de control de acceso se define cuando se añaden reglas en el indicador `IP config>`:

```
IP config>  add access-control...
```

Las reglas de control de acceso global se pueden listar, mover o suprimir mediante los mandatos **list**, **move** o **delete**.  Consulte estos mandatos para obtener más información.

## Cómo definir filtros de paquetes

Para definir filtros de paquetes, que son específicos de cada interfaz, utilice el mandato **add packet-filter** en el indicador `IP config>`. El direccionador le solicitará el nombre del filtro, la dirección (entrada o salida) y el número de interfaz a la que se aplica.

```
IP config> add packet filter
Packet-filter name [ ]? test
Filter incoming or outgoing traffic? [IN]? in
Which interface is this filter for [0]? 1
```

Puede utilizar el mandato **list packet-filter** para listar todas las listas de control de acceso específicas de interfaz configuradas en el direccionador.

## Configuración de reglas de control de acceso para filtros de paquetes

Debe definir reglas de control de acceso para cada lista definida (filtro de paquetes). Si no lo hace, los filtros de paquetes definidos no tendrán ningún efecto sobre el tráfico de entrada o de salida. Utilice el mandato **update packet-filter** en el indicador `IP config>` para definir reglas de control de acceso. Primero el direccionador le solicitará el nombre del filtro de paquetes que desea actualizar. Luego el indicador `IP config>` pasa a ser `Packet-filter 'nombre' Config>` donde 'nombre' es el nombre de la lista especificada.

```
IP config>  update packet-filter
Packet-filter name [ ]?  test
Packet-filter 'test' Config>
```

Desde este indicador puede emitir los mandatos **add**, **list**, **move** y **delete**. Estos mandatos se parecen a los que se utilizan para modificar la lista global de control de acceso.

## Parámetros de las reglas de control de acceso

Las reglas de control de acceso constan de varios parámetros. Algunos parámetros se pueden especificar en todas las reglas de control de acceso, mientras que otras sólo se pueden especificar en las reglas correspondientes a filtros de paquetes. En todas las reglas de control de acceso se pueden especificar los siguientes parámetros:

- Tipo (inclusive, exclusive)
- Dirección y máscara de origen IP
- Dirección y máscara de destino IP
- Rango de números de protocolos IP
- Rango de números de puertos de destino TCP/UDP
- Rango de números de puertos de origen TCP/UDP
- Función de filtro SYN de TCP
- Tipo y código de mensajes ICMP
- Precedencia y soporte de función de filtro TOS
- Direccionamiento basado en políticas (selección de la pasarela del siguiente salto)
- Opción de recurso SysLog
- Opciones de registro cronológico de seguridad

Los siguientes parámetros corresponden sólo a los filtros de paquetes:

- Nombre de filtro de paquetes
- Verificación de la dirección de origen

Tipos adicionales:

- Conversión de dirección de red (NAT)

***Tipo:*** La designación de tipo de una regla de control de acceso determina el modo en que afecta a los paquetes que coinciden, del siguiente modo:

- Una regla *exclusive* (E) elimina paquetes.
- Una regla *inclusive* (I) permite que el direccionador siga procesando los paquetes.
- Una regla de *conversión de dirección de red*, o NAT (N), pasa los paquetes a NAT para que realice la conversión de direcciones.

Las reglas NAT sólo son válidas en filtros de paquetes y sólo si se especifican junto con inclusive (IN). Utilice el Configuration Program para especificar primero Inclusive y para especificar luego NAT.

***Direcciones y máscaras de origen y de destino IP:*** Cada regla tiene un par máscara y dirección IP para las direcciones tanto de origen como de destino IP. Cuando se compara un paquete IP con una regla de control de acceso, la dirección IP del paquete se suma (AND) a la máscara de la regla y el resultado se compara con la dirección de la regla. Por ejemplo, una dirección de origen igual a 26.0.0.0 con una máscara igual a 255.0.0.0 de una regla de control de acceso coincidirán con cualquier dirección de origen IP cuyo primer byte sea 26. Una dirección de destino igual a 192.67.67.20 y una máscara igual a 255.255.255.255 sólo coincidirán con una dirección de sistema principal de destino IP igual a

192.67.67.20. Una dirección igual a 0.0.0.0 con una máscara igual a 0.0.0.0 constituyen un comodín y coinciden con cualquier dirección IP.

***Rango de números de protocolos IP:*** Cada registro también puede tener un rango de número de protocolo IP. Este rango se compara con el byte de protocolo de la cabecera IP; un valor de protocolo dentro del rango especificado por la regla de control de acceso coincidirá (incluidos el primer y último números del rango). Si especifica un rango comprendido entre 0 y 255, cualquier protocolo coincidirá. Los números de protocolos que se suelen utilizar son 1 (ICMP), 6 (TCP), 17 (UDP) y 89 (OSPF).

***Rango de números de puertos de origen y de destino TCP/UDP:*** Si el rango de números de protocolos IP incluye 6 (TCP) o 17 (UDP), también se pueden especificar los rangos de números de puertos TCP/UDP en una regla de control de acceso, tanto para el puerto de origen como para el de destino. Estos rangos se comparan con el campo de número de puerto de la cabecera TCP o UDP del paquete IP; un valor de número de puerto que estén dentro del rango especificado (incluidos el primer y último números) coincidirá. Estos campos se pasan por alto para paquetes IP que no sean paquetes TCP o UDP. Si especifica un rango de 0 a 65535, cualquier número de puerto coincidirá. Los números de puertos que se suelen utilizar son 21 (FTP), 23 (Telnet), 25 (SMTP), 513 (rlogin) y 520 (RIP). Consulte RFC 1700 (Números asignados) para ver una lista de números de puertos y protocolos IP.

***Función de filtro de establecimiento de conexión TCP (SYN):*** Si el rango de números de protocolos incluye 6 (para TCP) y el tipo de filtro es exclusive, puede definir la función de filtro de establecimiento de conexión TCP. Cuando la función de filtro de establecimiento de conexión TCP está activada, la regla de control de acceso se aplica sólo a un paquete TCP si dicho paquetes establece una conexión TCP. (Son los paquetes en los que el bit SYN de TCP es 1 y el bit ACK es 0.)

***Tipo y código de mensajes ICMP:*** Si el rango de números de protocolos incluye 1 (para ICMP), puede especificar el tipo y código de mensajes ICMP. El valor por omisión consiste en aplicar la regla de control de acceso a todos los tipos y códigos de mensajes ICMP.

***Precedencia y soporte de función de filtro TOS:*** El direccionador que da soporte a TOS ha identificado determinadas reglas que ofrecen los niveles de servicio solicitados. El direccionador envía paquetes sobre las rutas en función del valor de sus bits TOS.

TOS en IP no constituye garantía alguna de ningún tipo particular de servicio, pero solicita al direccionador que proporcione servicio del tipo solicitado. Por ejemplo, un paquete con un campo TOS que solicite un rendimiento máximo se puede enviar sobre diversos saltos que tengan distintos anchos de banda. Se obtendrá un servicio normal (sin tratamiento especial) si pasa sobre un salto gestionado por un direccionador que no dé soporte a TOS. Consulte el mandato **add access-controls** en la página 276 para ver descripciones de estos parámetros.

También puede definir filtros a fin de ofrecer Calidad de servicio basado en los bits TOS mediante la característica Sistema de reserva de ancho de banda (BRS). BRS se utiliza con las interfaces PPP y Frame Relay. Consulte los temas “Using Bandwidth Reservation and Priority Queuing” y “Configuring and Monitoring

Bandwidth Reservation” del manual *Utilización y configuración de las características*.

*Parámetros para el soporte de direccionamiento basado en TOS:* Para activar el direccionador para que interprete los bits TOS y direccione los paquetes de acuerdo con estos bits, debe crear una regla de control de acceso a partir de la cual el direccionador recibirá paquetes TOS para la función de filtro y el direccionamiento de Tipo de servicio. Esta regla de control de acceso se aplica a todas las interfaces del direccionador. Se utilizan los siguientes parámetros par definir los bits TOS que el direccionador comparará:

- Valor Inicio-rango correspondiente a los bits del byte TOS
- Valor Fin-rango correspondiente a los bits del byte TOS
- Máscara de filtro para determinar qué bits del byte TOS se incluyen en el rango

*Modificación de los bits TOS:* Para activar el direccionador para que modifique los bits de los paquetes de entrada, debe crear una regla global de control de acceso a partir de la cual el direccionador recibirá los paquetes TOS que se deban modificar. Modificar el valor de los bits TOS constituye una actividad diferente de interpretarlos y direccionar el paquete. Si se ha configurado tanto la interpretación como la modificación, esta se llevará a cabo después que la interpretación. Se utilizan los siguientes parámetros para definir los bits TOS que se deben modificar:

- Un nuevo valor para los bits TOS
- Una máscara de modificación para determinar qué bits del byte TOS se deben modificar

***Direccionamiento basado en políticas (selección de la pasarela del siguiente salto):*** Puede filtrar paquetes de entrada para dirigirlos a la dirección de la pasarela del siguiente salto seleccionada de forma manual (lo que se denomina direccionamiento basado en políticas). Para hacerlo, cree una regla de control de acceso de entrada tipo inclusive de forma global, para el direccionador o para una determinada interfaz y especifique los siguientes parámetros:

- Si utilizar el direccionamiento basado en políticas
- La dirección IP de la pasarela del siguiente salto
- Si enviar o no el paquete utilizando la tabla de direccionamiento normal si el siguiente salto no está disponible

***Opción de recurso SysLog:*** SysLog es una opción de registro cronológico que genera un mensaje SysLog destinado a un servidor remoto de registro cronológico. Si SysLog está activado, la opción de recurso SysLog especifica el recurso SysLog que se utiliza para el registro cronológico remoto. Esta opción, cuyo valor por omisión es *Usuario*, define el archivo de registro cronológico remoto en el que se pueden guardar, y posteriormente analizar, los mensajes SysLog. La opción de recurso SysLog se visualiza tanto en el Configuration Program como en la interfaz de línea de mandatos.

***Opciones de registro cronológico de seguridad:*** Si activa el registro cronológico de seguridad, puede especificar cualquiera de las siguientes opciones de registro cronológico (o todas ellas):

- Mensajes ELS

- Rupturas SNMP
- SysLog

Si se especifica, los mensajes ELS y SysLog pueden utilizar el formato de mensajes *corto* o *largo*. Las rupturas SNMP se pueden *activar* o *desactivar*. Si no se especifica ninguna opción de registro cronológico, el registro cronológico de seguridad está desactivado.

El nivel de prioridad de SysLog también se puede configurar. Especifica el nivel de mensajes de error que se visualizará, como por ejemplo *Emergencia* o *Información*. El valor por omisión es el valor por omisión del sistema del direccionador. Los niveles de prioridad de SysLog se visualizan tanto en el Configuration Program como en la interfaz de línea de mandatos.

Los mensajes de SysLog se envían a un servidor remoto y se guardan en los archivos SysLog de la opción de recurso SysLog actual.

***Nombre de filtro de paquetes:*** Este parámetro específico de la interfaz puede consistir en cualquier nombre. Puede tener un máximo de 16 caracteres de longitud y puede incluir guiones (-) y símbolos de subrayado (_). Se puede configurar un máximo de dos listas de registros de control de acceso para cada nombre de filtro de paquetes, una para los paquetes de salida y una para los paquetes de entrada.

***Verificación de la dirección de origen:*** Esta opción de filtro de paquetes de entrada comprueba que la dirección IP de origen del paquete recibido es coherente, según la tabla de direccionamiento IP, con la interfaz de la que procede. Esta opción ayuda a evitar el reenvío de paquetes procedentes de un sistema principal IP cuyo comportamiento es erróneo que está utilizando una dirección IP de origen que no le pertenece; este comportamiento recibe el nombre de *simulación*.

***Ejemplos:*** El siguiente ejemplo permite que cualquier sistema principal envíe paquetes al zócalo TCP de SMTP en la dirección 192.67.67.20.

```
add access-control inclusive 0.0.0.0 0.0.0.0 192.67.67.20 255.255.255.255 6 6 25 25
```

El siguiente ejemplo evita que cualquier sistema principal de la subred 1 de la red de Clase B 150.150.0.0 envíe paquetes a los sistemas principales de la subred 2 de la red de Clase B 150.150.0.0 (suponiendo que hay una máscara de subred de 1 byte).

```
add access-control exclusive 150.150.1.0 255.255.255.0 150.150.2.0 255.255.255.0 0 255 0 65535
```

Este mandato permite al direccionador enviar y recibir todos los paquetes RIP.

```
add access-control inclusive 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 17 17 520 520
```

Este ejemplo muestra cómo crear una regla de control de acceso global. Se entran valores para activar la interpretación de bits TOS de paquetes que llegan de la dirección IP 9.1.2.3 y para modificar los valores de estos bits antes de enviar los paquetes. Consulte el mandato “Add” en la página 276 para ver una explicación del significado de los parámetros para crear una función de filtro de TOS y direccionamiento basado en políticas.

```
IP config> add access-control
Enter type [E]? i
Internet source [0.0.0.0]? 9.1.2.3
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]?
Destination mask [0.0.0.0]?
Enter starting protocol number ([0] for all protocols) [0]?
Enter starting DESTINATION port number ([0] for all ports) [0]?
Enter starting SOURCE port number ([0] for all ports) [0]?
Filter on ICMP Type ([-1] for all types) [-1]?
TOS/Precedence filter mask (00-FF - [0] for none) [0]? e0
TOS/Precedence start value (00-FF) [0]?
TOS/Precedence end value [0]?
TOS/Precedence modification mask (00-FF - [0] for none) [0]? 1f
New TOS/Precedence value (00-FF) [0]? 08
Use policy-based routing? [No]: y
Next hop gateway address [ ]? 9.2.160.1
Use default route if next hop gateway unreachable? [Yes]:
Enable Logging (Yes or [No]):
```

# Función de filtro de rutas sin políticas

La función de filtro de rutas influye sobre el reenvío de paquetes, al modificar el contenido de la tabla de direccionamiento. En general, la función de filtro de rutas es más eficaz pero menos flexible que el control de acceso. La función de filtro basada en campos de paquete que no sean la dirección IP de destino se puede llevar a cabo mediante el control de acceso, descrito anteriormente, o utilizando políticas de función de filtro de rutas, descrita en el tema “Función de filtro de rutas con políticas” en la página 259.

En este direccionador se utilizan los siguientes métodos para modificar el contenido de la tabla de direccionamiento.

- Rutas de filtro
- Filtros de entrada RIP
- Función de filtro de la tabla de rutas

## Definición de rutas de filtro

Puede designar un destino IP para que se inserte en la tabla de direccionamiento como una *ruta de filtro*. Los paquetes IP no se reenviarán a estos destinos y la información de direccionamiento asociada a los mismos no se anunciará. Las rutas de filtro ***no*** se recomiendan cuando se utiliza OSPF en la red; las rutas internas aprendidas por OSPF alterarán temporalmente las rutas filtradas en la tabla de direccionamiento.

Para configurar una ruta de filtro, entre el siguiente mandato en el indicador `IP config>`:

```
IP config> add filter dirección-IP-dest máscara-dirección
```

Las rutas de filtro se listarán como una entrada con el tipo *fltr* cuando se utilice el mandato **dump** para ver la tabla de direccionamiento IP.

**Nota:** Si se dispone de una ruta más específica, los paquetes se reenviarán. Por ejemplo, si se define una ruta de filtro para la red 9.0.0.0 (máscara 255.0.0.0), pero se aprende una ruta para una subred de la red (por ejemplo 9.1.0.0, máscara 255.255.0.0), los paquetes se reenviarán a la subred 9.1.0.0 pero no a las demás subredes de esta red.

### Cómo definir filtros de entrada RIP

Cuando se utiliza RIP como el protocolo de direccionamiento dinámico, puede configurar determinadas interfaces para que pasen por alto las rutas de actualizaciones RIP.

El mandato de reenvío da como resultado que se pasan por alto todas las actualizaciones RIP recibidas en una interfaz:

```
IP config>  disable receiving rip  dirección-interfaz-ip
```

Los siguientes mandatos dan como resultado que se pasen por alto determinados tipos de rutas recibidas en una interfaz:

```
IP config> disable receiving dynamic nets dirección-interfaz-ip
IP config> disable receiving dynamic subnets dirección-interfaz-ip
IP config> disable receiving dynamic host dirección-interfaz-ip
```

Si se necesita una función de filtro más granular de rutas RIP, se pueden utilizar las políticas de rutas que se describen en el siguiente mandato:

```
IP config> add accept-rip-route red-ip/subred/sistema principal
```

### Cómo definir una función de filtro de tabla de rutas

Cuando la función de filtro de tabla de ruta está activada y se han definido filtros de ruta, la comprobación se realiza antes de añadir rutas a la tabla de direccionamiento IP. Si la ruta a añadir coincide con un filtro de ruta tipo inclusive, se añadirá a la tabla de rutas IP. Si coincide con un filtro de ruta tipo exclusive, no se añadirá a la tabla de rutas IP. Las rutas directas y estáticas no se filtrarán nunca.

Se puede utilizar esta función para evitar que se añadan rutas a la tabla de rutas IP en situaciones en las que el administrador de la red no desea que estén disponibles todas las rutas anunciadas por los protocolos de direccionamiento. Esta función se puede utilizar en un entorno de proveedor de servicios para evitar que los clientes tengan acceso a las redes de los demás clientes.

## Función de filtro de rutas con políticas

Las políticas de filtro de rutas son definiciones que describen una ruta como un grupo de rutas. Una política de filtro de rutas consiste en el nombre de la política de filtro de rutas y al menos una entrada que define una dirección o un rango de direcciones para las rutas que se van a filtrar. Cada entrada incluye instrucciones para incluir las rutas definidas en dicha entrada en la tabla de direccionamiento o para excluirlas de la misma. Las políticas de filtro de rutas se pueden utilizar para filtrar las rutas que instalan RIP y OSPF en la tabla de reenvíos IP y avisar a la tabla de reenvíos IP.

Una política de filtro de rutas se identifica mediante una serie ASCII de 15 caracteres, por ejemplo, *ospf-import*. Una vez se ha especificado un nombre para la política de filtro de rutas, tiene que configurar al menos una entrada asociada a dicha política de filtro de rutas. Utilice el mandato **add route-policy** en el indicador `IP config>` para añadir la política, el mandato **change route-policy** para que aparezca el indicador `IP Route Policy Config>` y el mandato **add entry** en el indicador `IP Route Policy Config>` para definir cada entrada correspondiente a la política.

Tiene que asignar un número de índice a cada entrada al configurarla. Este número sirve para identificar la entrada para la búsqueda de coincidencias.

La búsqueda de coincidencias se realiza mediante una *coincidencia lineal* o una *búsqueda de la coincidencia más larga*. Debe seleccionar uno de estos métodos al utilizar el mandato **add route policy** para crear la política de filtro de rutas. Si selecciona la coincidencia lineal, la ruta que se filtra se compara con las entradas de la lista una tras otra, según el número de índice. Cuando se encuentra una coincidencia, se filtra la ruta. Si selecciona la búsqueda de la coincidencia más larga, la ruta que se filtra se compara con las entradas del filtro de acuerdo con la búsqueda de la coincidencia más larga. Si hay más de una entrada que especifiquen la misma dirección IP y máscara, la ruta que se filtra se compara en orden ascendente por número de índice.

Por ejemplo, supongamos que desea excluir las direcciones correspondientes a la red 9.8.0.0 con la máscara 255.255.0.0 pero desea incluir la dirección de sistema principal 9.8.1.8 con la máscara 255.255.255.255. De acuerdo con el método de función de filtro de búsqueda de coincidencia más larga, puede incluir 9.8.1.8 con la máscara 255.255.255.255 y excluir la dirección 9.8.0.0 con la máscara 255.255.0.0. De todas las direcciones de esta subred, sólo se incluirá 9.8.1.8.

Para obtener el mismo resultado utilizando una coincidencia lineal, tendría que asignar al filtro tipo inclusive un número de índice más bajo que al filtro de tipo exclusive. Por ejemplo, la dirección 9.8.1.8 con la máscara 255.255.255.255 necesita un número de índice más bajo que la dirección 9.8.0.0 con la máscara 255.255.0.0. De lo contrario, la regla que excluye 9.8.0.0 también excluiría la dirección 9.8.1.8.

El *tipo de coincidencia* es un parámetro que determina el modo en que se procesará la máscara de dirección correspondiente a la entrada. Si el valor de este parámetro es *exacto*, el software encontrará una coincidencia en la ruta únicamente en la dirección y máscara exactas especificadas por la entrada y no tratará la dirección como un rango. Si el tipo de coincidencia es *rango*, el direccionador leerá la dirección y la máscara como un rango y encontrará una coincidencia con la ruta si esta está dentro del rango.

Además de entradas, puede configurar acciones y condiciones de coincidencia asociadas a cada entrada. Las acciones son cambios que se efectúan en la ruta antes de que se anuncia, como por ejemplo la definición de un métrico en una ruta. Las condiciones de coincidencia cambiar las reglas de acuerdo a la ruta seleccionada. Una vez se ha encontrado una coincidencia en función de la dirección de destino, la condición de coincidencia define más restricciones para la coincidencia. Por ejemplo, si la condición de coincidencia es protocolo BGP, las rutas no coinciden a no ser que la dirección de entrada coincida y el paquete pertenezca al protocolo BGP. Estas son las condiciones de coincidencia:

- Protocolo, como RIP, OSPF o BGP
- Número AS (Sistema autónomo)
- Dirección de pasarela correspondiente al siguiente salto de la ruta
- Número de red correspondiente al siguiente salto de la ruta
- Rango métrico
- Pasarela de origen, que se aplica únicamente a la política de recepción de RIP

Las acciones y condiciones de coincidencia, que ajustan la función de filtro de la entrada, son opcionales.

### Políticas de filtro de direccionamiento límite AS para OSPF

Si se utiliza una política de filtro de rutas para controlar las tablas de direccionamiento OSPF, se configura durante la configuración de OSPF. Consulte el mandato **enable** en la página 387 para obtener más información.

### Políticas de filtro de envío y recepción para RIP

Puede utilizar políticas de filtro de rutas pare definir qué rutas va a enviar o recibir RIP. Estas políticas de filtro de rutas se pueden configurar de forma global, para todas las interfaces IP del direccionador, o para por interfaz IP. Si se activa una política de filtro de rutas de envío, todas las rutas que cumplan con la política se anuncian y los valores correspondientes a *rutas-omisión*, *rutas-sistema principal*, *rutas-red*, *rutas-subred* y *rutas-estáticas* se pasan por alto. Los valores correspondientes a *rutas-invertidas-prohibidas*, *rutas sólo-ripv1* y rutas *sólo-corte* no se ven afectados por la política de filtro de rutas de envío. Si se desactiva el envío a *todas las rutas*, no se anunciará a ninguna ruta, incluso aunque se haya especificado una política de envío global.

Si se ha configurado una política de filtro de rutas de recepción y la recepción de RIP está activada, la política configurada tomará el lugar de cualquier tipo de ruta dinámica activada o desactivada. Es decir, se aceptarán todas las rutas incluidas por la política de filtro de rutas y que cumplan con las restricciones del protocolo RIP.

## Configuración del proceso de reenvío BOOTP/DHCP

BOOTP (documentado en RFC 951 y en RFC 1542) es un protocolo de rutina de carga que utilizan las estaciones de trabajo sin disco para aprender su dirección IP, la ubicación de su archivo de arranque y el nombre del servidor de arranque. Se utiliza el Protocolo de configuración dinámica de sistema principal (DHCP), documentado en RFC 2131, para asignar direcciones de red reutilizables y parámetros de configuración específicos del sistema principal procedentes de un servidor.

Cuando se habla del proceso de reenvío BOOTP/DHCP se utilizan los siguientes términos:

- *Cliente* - la estación de trabajo que solicita servicios BOOTP/DHCP.
- *Servidores* - el sistema principal de arranque (con bootpd del daemon UNIX, versión de DOS disponible a través del software FTP u OS/2) u otro servidor DHCP/BOOTP que ofrece estos servicios. El direccionador puede suministrar la función de Servidor DHCP/BOOTP. Consulte el tema "Using DHCP Server" del manual *Utilización y configuración de las características*.
- *Agente de retransmisión BOOTP* o *Distribuidor BOOTP* - un dispositivo que reenvía las solicitudes/respuestas que intercambian el Cliente y el Servidor. Este direccionador puede ofrece la función Las de agente de retransmisión.

Los pasos siguientes ilustran un ejemplo de proceso de reenvío BOOTP. (los intercambios DHCP funcionan de forma parecida):

1. El Cliente copia su dirección Ethernet (o dirección MAC adecuada) en un paquete BOOTP y realiza una difusión general en la LAN local. BOOTP se está ejecutando sobre UDP.

2. El agente de retransmisión BOOTP local recibe el paquete y comprueba si está bien formateado y que el número máximo de saltos de aplicaciones no se ha excedido. También comprueba si el cliente lo ha intentado el tiempo suficiente.

   **Nota:** Si se necesitan varios saltos para alcanzar al agente BOOTP, el paquete se direcciona con normalidad a través de IP. Los demás direccionadores examinarían el paquete para determinar si se trata de un paquete BOOTP.

3. El agente BOOTP local reenvía una petición BOOTP a cada uno de sus servidores añadidos. La petición BOOTP es la misma que la que envió inicialmente el cliente excepto en que tiene una nueva cabecera IP con la dirección IP del agente de retransmisión copiada en la parte central de la petición BOOTP.
4. El servidor recibe la petición y busca la dirección del hardware del cliente (por ejemplo, Ethernet) en su base de datos. Si la encuentra, formatea una respuesta BOOTP que contiene la dirección IP del cliente, la ubicación de su archivo de arranque y el nombre del servidor de arranque. La respuesta se envía al agente de retransmisión BOOTP.
5. El agente de retransmisión BOOTP recibe la respuesta y efectúa una entrada en su tabla ARP correspondiente al cliente y luego reenvía la respuesta al cliente.
6. Luego el cliente continúa el arranque que utiliza TFTP usando la información del paquete de respuesta BOOTP.

## Activación/desactivación del reenvío BOOTP

Para activar o desactivar el reenvío BOOTP en el direccionador, entre el siguiente mandato en el indicador de configuración de IP. (Active el reenvío BOOTP para permitir que el direccionador reenvíe peticiones y respuestas BOOTP y/o DHCP entre Clientes y Servidores de distintos segmentos de la red.)

```
IP config> enable/disable bootp
```

**Nota:** La característica Servidor DHCP que se describe en el tema “Using DHCP Server” del manual *Utilización y configuración de las características* y este proceso de reenvío BOOTP no se deben activar en el mismo direccionador. Si ambos están activados, el Servidor DHCP tiene preferencia y no se producirá el reenvío BOOTP.

Cuando active BOOTP, se le solicitarán los siguientes valores:

- Número máximo de saltos de aplicación por los que desea que pase la solicitud BOOTP. Este es el número máximo de agentes de retransmisión BOOTP que pueden reenviar el paquete. ***No*** es el número máximo de saltos al Servidor. Un valor típico para este parámetro es 1.
- Número de segundos que desea que reintente el Cliente antes de que se reenvíe la solicitud BOOTP. *Este parámetro no se utiliza con frecuencia.* Un valor típico para este parámetro es 0.

Después de aceptar una solicitud BOOTP, el direccionador reenvía la solicitud BOOTP a cada servidor BOOTP. Si hay varios servidores configurados para BOOTP, el direccionador duplica el paquete.

## Cómo añadir un destino BOOTP/DHCP

Para añadir un servidor BOOTP o DHCP a la configuración del agente de retransmisión del direccionador, entre el siguiente mandato en el indicador de configuración de IP:

```
IP config> add bootp-server dirección-IP-servidor
```

Se pueden configurar varios servidores. Además, si sólo se conoce el número de red del servidor o si hay varios servidores que residen en el mismo segmento de red, se puede configurar una dirección de difusión general para el servidor.

## Integración de IP y SNA

Puede utilizar TN3270E para integrar IP y SNA. Consulte el capítulo titulado “Using APPN” del manual *Consulta de configuración y supervisión de protocolos Volumen 2* y el capítulo titulado “Configuración y supervisión de APPN” del manual *Consulta de configuración y supervisión de protocolos Volumen 2* para obtener más información sobre TN3270E.

## Configuración del reenvío UDP

El Protocolo de datagrama de usuario (UDP), documentado en RFC 768, es un protocolo de capa de transporte que ofrece servicio sin conexión a través del Protocolo Internet. Con el reenvío UDP, los paquetes UDP que se distribuyen de forma local (como una difusión general UDP en una LAN conectada a un IBM 2210) se pueden reenviar a un determinado destino IP o a una red de destino como una difusión general dirigida.

Por ejemplo, NetBIOS utiliza difusiones generales UDP en algunas aplicaciones cliente-servidor para efectuar una difusión general de paquetes Name-Query. A no ser que configure el reenvío UDP, el direccionador elimina estos paquetes; por lo tanto, el direccionador no reenviará paquetes de difusión general fuera de la red local.

Siga estos pasos para configurar el reenvío UDP:

1. Añada un número de puerto de destino UDP y una dirección IP. El direccionador correlaciona esta dirección IP con un puerto UDP.

   ```
   IP config> add udp-destination
   UDP port number [-1] 36
   Destination IP address [0.0.0.0] 20.1.2.2
   ```

2. Active el reenvío UDP.

   ```
   IP config>enable udp-forwarding
   For which UDP port number [-1] 36
   ```

En el ejemplo anterior, el direccionador reenvía los paquetes que recibe correspondientes al puerto UDP 36 a la dirección IP 20.1.2.2.

Entre **list udp-forwarding** para ver la configuración del reenvío UDP.

## Activación/desactivación del reenvío UDP

Para activar o desactivar el reenvío UDP en el direccionador, entre el siguiente mandato en el indicador de configuración de IP. (Active el reenvío UDP para permitir que el direccionador reenvíe paquetes de difusión general UDP a una determinada dirección por puerto UDP.)

```
IP config> enable/disable udp-forwarding número-puerto
```

## Cómo añadir un destino UDP

Puede añadir destinos de reenvío UDP especificando la dirección IP a la que se va a reenviar el paquete seguida del número de puerto. Para añadir un destino UDP, entre el siguiente mandato en el indicador de configuración de IP:

```
IP config> add udp-destination número-puerto dirección-ip-dest
```

---

## Configuración del Protocolo virtual de redundancia del direccionador (VRRP)

En muchas configuraciones IP de sistema principal se utiliza una ruta por omisión configurada de forma estática. Esto minimiza la actividad de configuración y de proceso y recibe soporte de prácticamente cualquier implantación IP. Esta modalidad de funcionamiento se suele emplear cuando se utilizan protocolos de configuración de sistemas principales dinámicos que suelen ofrecer configuración para una dirección IP de sistema principal final y una pasarela por omisión. Sin embargo, crea un solo punto de error. La pérdida del direccionador por omisión resulta un suceso catastrófico, que aísla todos los sistemas principales finales, los cuales no pueden detectar ninguna vía de acceso alternativa que pueda estar disponible.

El Protocolo virtual de redundancia del direccionador (VRRP) está diseñado para eliminar el único punto de error inherente del entorno de direccionamiento estático por omisión. VRRP especifica un protocolo seleccionado que permite que de forma dinámica un grupo de direccionadores actúen como direccionadores de reserva unos de otros. El direccionador VRRP que controla una o más direcciones IP recibe el nombre de Direccionador maestro, y reenvía paquetes enviados a estas direcciones IP. Este proceso de elección ofrece un sustituto dinámico en la responsabilidad de reenvío en el caso de que el maestro deje de estar disponible. Los sistemas principales finales pueden utilizar cualquiera de las direcciones IP de un direccionador virtual como direccionador por omisión del primer salto. La ventaja derivada de utilizar el VRRP es una vía de acceso por omisión de mayor disponibilidad sin necesidad de configurar protocolos de direccionamiento dinámico ni de descubrimiento de rutas en cada sistema principal final.

A fin de poder utilizar y configurar VRRP, antes debe definir un ID de direccionador virtual (VRID) en cada segmento de la LAN que ejecute VRRP. Para cada VRRP, un direccionador será el propietario de la dirección IP por omisión configurada para los sistemas principales del segmento de la LAN. El direccionador responderá a las solicitudes ARP de dicha dirección y reenviará paquetes mientras esté disponible. Se pueden configurar otros direccionadores del segmento de la LAN para que actúen como reserva del direccionador propietario de la dirección IP. El VRID implicará una dirección MAC de difusión individual o de difusión múltiple. Se necesita una dirección MAC común para minimizar las interrupciones cuando un direccionador de reserva pase a actuar como direccionador maestro. A continuación se muestra un ejemplo de una topología VRRP muy sencilla:

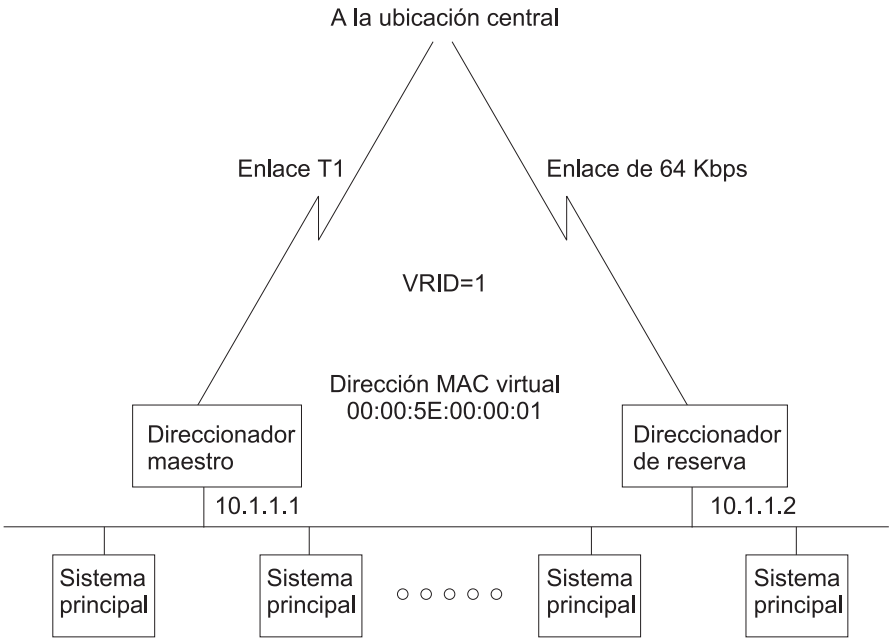



*Figura 32. LAN Ethernet con subred 10.1.1.0/255.255.255.0 Todos los sistemas principales configurados con pasarela por omisión 10.1.1.1*

1. Todos los sistemas principales se han configurado con una pasarela por omisión 10.1.1.1
2. El direccionador maestro responderá a todas las solicitudes ARP de 10.1.1.1 con la dirección MAC virtual 00:00:5E:00:00:01.
3. El direccionador maestro reenviará los paquetes destinados a la dirección MAC virtual.
4. Si el direccionador maestro no está disponible, el de reserva lo determina mediante la ausencia de anuncios VRRP y comenzará a recibir paquetes destinados a la dirección MAC virtual. El direccionador de reserva responderá a todas las solicitudes ARP de 10.1.1.1.

Una topología complicada sería una en la que hubiera varios direccionadores VRRP y se deseara equilibrar la carga entre los direccionadores, sin renunciar a la capacidad completa de reserva. En este caso se tendrían que definir 2 VRID y cada direccionador sería el maestro de uno y el direccionador de reserva del otro. A continuación se muestra esta ilustración:

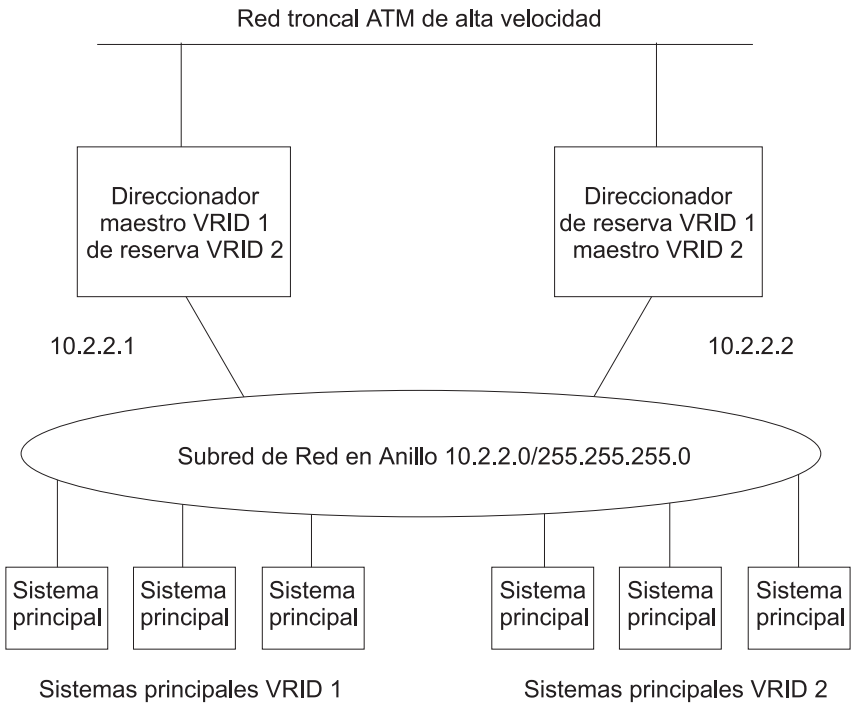



*Figura 33. Varios direccionadores VRRP*

1. Todos los sistemas principales VRID 1 se configurarán con una dirección de pasarela por omisión igual a 10.2.2.1.
2. Todos los sistemas principales VRID 2 se configurarán con una dirección de pasarela por omisión igual a 10.2.2.2.
3. El direccionador maestro VRID 1 responderá a las solicitudes ARP de la dirección 10.2.2.1 con la dirección MAC virtual C0:00:00:10:00:00. También recibirá y reenviará paquetes destinados a la dirección MAC virtual C0:00:00:10:00:00.
4. El direccionador maestro VRID 1 responderá a las solicitudes ARP de la dirección 10.2.2.2 con la dirección MAC virtual C0:00:00:20:00:00. También recibirá y reenviará paquetes destinados a la dirección MAC virtual C0:00:00:20:00:00.
5. Si alguno de los direccionadores deja de estar disponible, el otro retoma su actividad.
6. Si un direccionador no deja de estar disponible pero pierde su conectividad externa, redirigirá el tráfico a través del otro con redirecciones ICMP (se da por supuesto que los 2 direccionadores intercambian rutas mediante un protocolo de direccionamiento como RIP o OSPF).

VRRP recibe soporte en Ethernet, Fast Ethernet, y red en anillo.

VRRP de difusión múltiple no recibe soporte en la red de puente cuando las LAN direccionadas por origen forman parte de la red conectada por puente. La restricción sólo se aplica a topologías en las que se ha configurado IP en la red de puente.

## Configuración de la pasarela IP redundante por omisión

Esta sección describe los pasos a seguir para configurar pasarelas IP redundantes por omisión en ELAN. La configuración de una pasarela redundante permite a las estaciones finales con pasarelas por omisión configuradas de forma manual continuar pasando tráfico a las demás subredes después de que su pasarela principal deje de funcionar.

Para configurar un dispositivo con una pasarela principal o una pasarela de reserva:

1. Determine la dirección IP que utilizan las estaciones finales como pasarela por omisión.
2. Determine una dirección MAC que no utilice ninguna interfaz de la ELAN. Para determinar las direcciones MAC utilizadas, consulte el tema “Database List” en el capítulo “Monitoring LAN Emulation Services” del manual *Guía del usuario de software*.
3. Seleccione un dispositivo para que tenga la pasarela principal. Este dispositivo debe tener una interfaz LEC en la ELAN de la estación final.
4. Seleccione un dispositivo o grupo de dispositivos para que tengan la pasarela de reserva. Este dispositivo o grupo de dispositivos debe tener una interfaz LEC en la ELAN de la estación final.
5. Configure una pasarela redundante en cada dispositivo mediante la opción “Add” correspondiente a IP.

**Nota:** La pasarela principal y la pasarela de reserva deben tener la misma dirección MAC

## Soporte de difusión múltiple IP

La difusión múltiple IP es una extensión de la difusión múltiple de LAN a TCP/IP Internet. Es la posibilidad que tiene un sistema principal IP de enviar un solo datagrama (denominado datagrama de difusión general IP) que se distribuirá a varios destinos. Los datagramas de difusión múltiple IP se identifican como aquellos paquetes cuyos destinos son direcciones IP de clase D (es decir, cuyo primer byte se encuentra dentro del rango comprendido entre 224 y 239). Cada dirección de clase D define un grupo de difusión múltiple.

Las extensiones necesarias para que un sistema principal IP participe en la difusión múltiple IP se especifican en RFC 1112 (Extensiones de sistema principal para difusión múltiple IP.) Este documento define un protocolo, el Protocolo de gestión de grupos Internet (IGMP), que permite a los sistemas principales unirse y abandonar de forma dinámica grupos de difusión general. Este direccionador implanta las funciones del protocolo IGMP que le permiten llevar un seguimiento de los miembros de un grupo IP en sus LAN física local y emulada, enviando consultas de pertenencia a sistema principal IGMP y recibiendo informes de pertenencia a sistema principal IGMP.

Un direccionador también debe ser capaz de direccionar datagramas de difusión múltiple IP entre los sistemas principales de origen y de destino (varios). Este direccionador da soporte al protocolo Multicast Open Shortest Path First (MOSPF) definido en RFC 1584 (Extensiones de difusión múltiple a OSPF) y al Distance Vector Multicast Routing Protocol (DVMRP).

El direccionador MOSPF distribuye información de ubicación de grupos a través del dominio de direccionamiento enviando un nuevo tipo de anuncio de estado de enlace, el LSA-pertenencia-grupo (tipo 6). Este activa los direccionadores MOSPF para que reenvíen de forma más eficiente un datagrama de difusión múltiple a sus diversos destinos: cada direccionador calcula la vía de acceso del datagrama de difusión múltiple como un árbol cuya raíz es el origen del datagrama y cuyas ramas de terminal son LAN que contienen miembros del grupo. Para obtener más información, consulte el tema “OSPF de difusión múltiple” en la página 362.

DVMRP es un protocolo de direccionamiento de difusión múltiple obtenido del Protocolo de información de direccionamiento (RIP). Este direccionador ofrece soporte para DVMRP de modo que puede intercambiar información de direccionamiento de difusión general con otras entidades de direccionamiento que no dan soporte a MOSPF. La implantación DVMRP de este direccionador le permite conectar por túnel información DVMRP sobre una red con soporte de MOSPF y sobre una red IP sin soporte de difusión múltiple.

Este direccionador también le permite “inscribir” el direccionador como miembro de uno o más grupos de difusión múltiple. Como miembro de un grupo de difusión múltiple, el direccionador responderá a los “ping” y consultas SNMP destinados a la dirección de grupo (se puede utilizar un mandato para consultar varios direccionadores).

Además, se utiliza el soporte de difusión múltiple IP del dispositivo para establecer y gestionar grupos DLSw, lo que reduce la cantidad de configuración necesaria para DLSw. Para obtener más información, consulte el tema “Utilización de DLSw” en la página 525.

## Configuración del direccionador para difusión múltiple IP

Para permitir al direccionador efectuar un seguimiento de la pertenencia al grupo de difusión múltiple IP y reenviar datagramas de difusión múltiple, debe activar MOSPF, DVMRP o ambos (MOSPF y DVMRP).

### Cómo activar DVMRP

Para activar DVMRP:

1. Active DVMRP en el direccionador

   ```
   DVMRP config> dvmrp on
   ```

2. Establezca en qué interfaces de la LAN se va a ejecutar DVMRP

   ```
   DVMRP config> phyint
   interface-address metric threshold
   ```

El 2210 da soporte a IVMP versión 2 y DVMRP versión 3. IGMP se puede configurar para que funcione en la modalidad de la versión 1.

Consulte el tema sobre configuración de DVMRP en el manual *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener detalles sobre estos mandatos y otros mandatos de configuración que sirven para definir la interacción entre DVMRP y MOSPF cuando ambos están activos en el direccionador.

## Inscripción del direccionador en grupos de difusión múltiple IP

Si el direccionador se va a unir a uno o más grupos de difusión múltiple, se utilizarán los siguientes mandatos join/leave:

- **join multicast-group-address**
- **leave multicast-group-address**

Se puede acceder a estos mandatos **join** y **leave** desde el indicador `OSPF Config` y desde el indicador de supervisión `OSPF`. También están disponible en la consola de supervisión de DVMRP.

Tenga en cuenta que estos mandatos no son necesarios para que el direccionador realice sus funciones de reenvío de difusión múltiple IP o de seguimiento de grupos IGMP; sirven para añadir el direccionador a grupos para que pueda responder a mandatos “ping” y a consultas SNMP destinadas a estos grupos.

## Utilización del Acceso sencillo a Internet

Acceso sencillo a Internet es un método de configurar con rapidez muchas de las opciones necesarias para ofrecer acceso a Internet a un grupo de clientes del Protocolo de configuración dinámica del sistema principal (DHCP). Hay que activar esta opción y añadir una interfaz de LAN para configurar IP. Cuando se combina con una interfaz PPP configurada para acceder a una cuenta de un Proveedor de servicios de Internet (ISP), varios clientes DHCP pueden acceder a Internet a través de una sola dirección IP pública. Esto se consigue utilizando la característica Servidor DHCP y la característica Conversión de direcciones de red (NAT).

**Nota:** Esta opción sólo estará disponible en cargas de software del direccionador que incluyan la característica DHCP y la característica NAT. Si se necesita una conectividad parecida a Internet en cargas que no incluyen la característica Servidor DHCP pero incluyen la característica NAT, se debe utilizar una Dirección dinámica (consulte el tema “Utilización de Dirección dinámica” en la página 242) con una configuración parecida a la que se muestra en el ejemplo.

**Ejemplo:**

- Si PPP está configurado para solicitar una dirección IP en la interfaz 3, del siguiente modo:

```
PPP 3 Config>set ipcp
IP COMPRESSION [no]:
Request an IP address [no]: yes
Interface remote IP address to offer if requested (0.0.0.0 for none) [0.0.0.0]?
```

- Acceso sencillo a Internet se puede activar del siguiente modo:

```
IP config>enable simple-internet-access
Interface to Service Provider [0]? 3
SIMPLE-INTERNET-ACCESS enabled on interface 3

IP config>add address
Which net is this address for [0]? 0
New address []? 192.168.8.1
Address mask [255.255.255.0]?

IP config>list address
IP addresses for each interface:
intf  0   192.168.8.1      255.255.255.0    Local wire broadcast, fill 1
intf  1                                     IP disabled on this interface
intf  2                                     IP disabled on this interface
intf  3   0.0.0.3          255.255.255.255  Local wire broadcast, fill 1
                                            SIMPLE-INTERNET-ACCESS Enabled
```

- Se generarán de forma automática los siguientes filtros de paquetes de la configuración IP:

```
IP config>list packet-filter
List of packet-filter records:
Name              Direction   Interface   State  Src-Addr-Ver
simple-in         In          3           On     Off
simple-out        Out         3           On     N/A
Access Control is: enabled
```

- Se generarán de forma automática los siguientes controles de acceso en la configuración IP:

```
IP config> list packet-filter simple-in

Name              Direction      Interface      State     Src-Addr-Ver
simple-in         In             3              On        Off
Access Control is: enabled
Access Control facility: USER

List of access control records:
1   Type=IN   Source=0.0.0.0          Dest  =0.0.0.0          Prot=  0-255
              SMask =0.0.0.0          DMask =0.0.0.0
              SPorts=    0-65535      DPorts=    0-65535
                      T/C= **/**      Log=N

IP config>list packet-filter simple-out

Name              Direction      Interface      State     Src-Addr-Ver
simple-out        Out            3              On        N/A
Access Control is: enabled
Access Control facility: USER

List of access control records:

1   Type=IN   Source=0.0.0.0          Dest  =0.0.0.0          Prot=  0-255
              SMask =0.0.0.0          DMask =0.0.0.0
              SPorts=    0-65535      DPorts=    0-65535
                      T/C= **/**      Log=N
```

- Se generará de forma automática la siguiente Ruta estática en la configuración IP:

```
IP config>list routes

route to 0.0.0.0        ,0.0.0.0         via 0.0.0.3         cost 1
```

- Se generará de forma automática la siguiente configuración NAT:[3]

[3] Si ya se ha configurado el Servidor DHCP antes de activar el Acceso sencillo a Internet en IP, no se generará ni se modificará ninguna configuración DHCP. Se utilizarán las subredes DHCP existentes como rangos de conversión para la configuración NAT.

```
NAT config>list all

NAT Globals:
Current State    TCP Timeout    Non-TCP Timeout
ENABLED             24:00:00            0:01:00

NAT Reserve Pool(s):
Index   First Address       Reserve Mask     Size    NAPT Address  Pool Name
    1         Dynamic    255.255.255.255     1       FromNet:    3 simple-net

NAT Translate Range(s):
Index    Base Address      Range Mask  Associated Reserve Pool
    1     192.168.8.0   255.255.255.0  simple-net

NAT Static Mapping(s):
Index  Private Address//Port  Public Address//Port
None.
```

- Se generará de forma automática la siguiente configuración del Servidor DHCP:[3]

```
DHCP Server enabled: Yes

DHCP Server config>list subnet all
subnet      subnet           subnet           starting         ending
name        address          mask             IP Addr          IP Addr
-------------------------------------------------------------------------
simple-net  192.168.8.0      255.255.255.0    192.168.8.2      192.168.8.50

DHCP Server config>list option subnet
Enter the subnet name []? simple-net
option  option
code    data
-----------------------------------------------------------------
1       255.255.255.0
3       192.168.8.1
6       0.0.0.3
```

# Configuración y supervisión de IP

Este capítulo describe los mandatos de configuración y de supervisión de IP. Incluye las siguientes secciones:



## Cómo acceder al entorno de configuración de IP

Para acceder al entorno de configuración de IP, entre el siguiente mandato en el indicador `Config>`:

```
Config> Protocol IP
Internet protocol user configuration
IP config>
```

## Mandatos de configuración de IP

Esta sección describe los mandatos de configuración de IP. Estos mandatos le permiten modificar el comportamiento del protocolo IP para que se ajuste a sus necesidades. Algunas de las tareas de configuración son obligatorias para que el direccionador IP funcione por completo. Entre los mandatos de configuración de IP en el indicador `IP config>`.

*Tabla 18. Resumen de mandatos de configuración de IP*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Add | Añade a la información de configuración de IP. Se pueden añadir direcciones de interfaces, junto con controles de acceso, filtros y filtros de paquetes. |
| Change | Modifica información que se entró originalmente con el mandato **add**. |
| Delete | Suprime información de configuración de IP especificada con el mandato **add**. |
| Disable | Desactiva determinadas características de IP que se han activado mediante el mandato **enable**. |
| Enable | Activa determinadas características de IP, como direccionamiento de subredes ARP, reenvío UDP, generación de valor por omisión, difusiones generales dirigidas, BOOTP, los diversos distintivos RIP que controlan el envío y la recepción de información RIP diffserv y la función de filtro de tabla de rutas. |
| List | Muestra elementos de la configuración de IP. |
| Move | Cambia el orden de los registros de control de acceso. |
| Set | Establece modalidades de configuración de IP, como el uso de control de acceso y el formato de las direcciones de difusión general. También define parámetros de IP como TTL (tiempo de vida) de paquetes originados por el direccionador, el tamaño de la tabla de direccionamiento IP el tamaño de la antememoria y métricas de la interfaz RIP y define parámetros de configuración de IGMP. |
| Update | Sirve para asignar entradas de control de acceso a filtros de paquetes. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Respuesta a mandatos de configuración de IP

Este tema le permite determinar qué mandatos de configuración de IP (Talk 6) entran en vigor de forma inmediata y cuáles permanecen pendientes hasta que emite el mandato **reset ip** de Talk 5 a un direccionador. La Tabla 19 lista ambas categorías de mandatos. Los mandatos que no aparecen en la lista permanecen pendientes hasta que emite un mandato **reload** o **restart**.

*Tabla 19 (Página 1 de 3). Respuesta a mandatos de configuración de IP*

| Entran en vigor de forma inmediata | Entran en vigor tras un mandato reset |
|---|---|
| add route | add accept-rip-route ... |
| change route | add access-control ... |
| delete route | add address |
| disable icmp-redirect | add bootp-server |
| enable icmp-redirect | add packet-filter |
| set ttl | add udp-destination |
| | add vrid ... |
| | add vr-address |

*Tabla 19 (Página 2 de 3). Respuesta a mandatos de configuración de IP*

| Entran en vigor de forma inmediata | Entran en vigor tras un mandato reset |
|---|---|
| | change access-control ... |
| | change address ... |
| | delete accept-rip-route ... |
| | delete access-control ... |
| | delete address ... |
| | delete bootp-server |
| | delete packet-filter |
| | delete udp-destination |
| | delete vrid ... |
| | delete vr-address ... |
| | disable bootp-forwarding |
| | disable directed-broadcast |
| | disable echo-reply |
| | disable fragment-offset-check |
| | disable icmp-redirect |
| | disable nexthop-awareness ... |
| | disable override default/static-routes... |
| | disable packet-filter |
| | disable receiving ... |
| | disable record-route |
| | disable rip |
| | disable rip2 |
| | disable same-subnet |
| | disable sending ... |
| | disable source-addr-verification |
| | disable source-routing |
| | disable timestamp |
| | disable trace |
| | disable udp-forwarding |
| | disable vrrp ... |
| | enable bootp-forwarding |
| | enable directed-broadcast |
| | enable echo-reply |
| | enable fragment-offset-check ... |
| | enable icmp-redirect |
| | enable nexthop-awareness |
| | enable override ... |
| | enable packet-filter |
| | enable receiving ... |

*Tabla 19 (Página 3 de 3). Respuesta a mandatos de configuración de IP*

| Entran en vigor de forma inmediata | Entran en vigor tras un mandato reset |
|---|---|
| | enable record-route |
| | enable rip |
| | enable rip2 |
| | enable same-subnet |
| | enable sending ... |
| | enable source-address-verification |
| | enable source-routing |
| | enable timestamp |
| | enable trace |
| | enable udp-forwarding |
| | enable vrrp ... |
| | move access-control ... |
| | set access-control ... |
| | set access-control log-facility |
| | set broadcast-address ... |
| | set originate-rip-default |
| | set rip-in-metric |
| | set rip-out-metric |
| | set tag ... |
| | set ttl |
| | update packet-filter ... |

## Add

Utilice el mandato **add** para añadir información de IP a la configuración.

**Sintaxis:**

add
- accept-rip-route . . .
- access-control . . .
- address . . .
- bootp-server
- filter . . .
- packet-filter
- redundant-default-gateway
- route . . .
- route-policy . . .
- route-table-filter
- udp-destination . . .
- vrid . . .

vr-address . . .

**accept-rip-route** *red/subred-IP*

Permite que una interfaz acepte una ruta RIP cuando la función de filtro RIP está activada para una interfaz. Puede consultar la lista de redes y subredes que ya se han entrado mediante el mandato **list rip**. Puede activar la función de filtro de entrada de rutas RIP por interfaz IP. Esto se realiza de forma separada para rutas a nivel de red (por ejemplo, una ruta a 10.0.0.0), para rutas a nivel de subred (por ejemplo, una ruta a 128.185.0.0) y para rutas a nivel de sistema principal (por ejemplo, 128.185.123.28). Para activar la función de filtro de entrada de rutas en una interfaz IP, utilice el mandato **disable receiving dynamic nets**, el mandato **disable receiving dynamic subnets** o el mandato **disable receiving dynamic hosts**.

**red/subred-IP**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:**

```
add accept-rip-route

Network number [0.0.0.0]? 10.0.0.0
```

**access-control** *tipo origen-IP máscara-origen dest-IP máscara-dest primer-protocolo último-protocolo [primer-puerto-dest último-puerto-dest primer-puerto-origen último-puerto-origen] [tcp-syn] [tipo-icmp código-icmp] [máscara-tos rango-inf-tos rango-sup-tos máscara-mod-tos nuevo-valor-tos direccionamiento-basado-políticas pasarela-siguiente-salto utilizar-ruta-omisión] [reg els ruptura-snmp syslog nivel-syslog]*

Desde el indicador `IP config>`, utilice este mandato para añadir un registro de control de acceso al final de la lista global de control de acceso. Desde el indicador Packet-filter *nombre-filtro-paquetes* Config>, utilice este mandato para añadir una regla de control de acceso a final de la lista de control de acceso del filtro de paquetes. El control de acceso le permite definir categorías de paquetes a reenviar, eliminar o procesar con conversión de dirección de red, en función de los valores de paquete especificados en las reglas de control de acceso. La longitud y el orden de las listas de control de acceso pueden afectar al rendimiento de reenvío de paquetes IP.

**Nota:** El mandato **add access-control** configura reglas de control de acceso, pero no activa de forma automática el control de acceso; consulte el mandato **set access-control**.

**tipo** Indica lo que se hace con los paquetes que coinciden con los parámetros de las reglas de control de acceso.

- E Exclusive; los paquetes que coinciden se eliminan.
- I Inclusive; el direccionador sigue procesando los paquetes que coinciden.

N
: Conversión de dirección de red (NAT); los paquetes que coinciden se pasan a NAT para la conversión de dirección. Este tipo sólo es válido si se especifica junto con inclusive, por ejemplo, *IN*. Este parámetro sólo es válido en la consola de configuración de filtro de paquetes (a la que se accede mediante el mandato **update packet-filter**).

**origen-IP máscara-origen**
: Dirección IP de origen y máscara. La máscara-origen se suma (AND) por bits a la dirección IP de origen recibida para permitir que la regla coincida con un rango de direcciones IP de origen. Si los bits de la máscara de origen son 0, los bits correspondientes de la dirección de origen IP también deben ser 0.

  **Valores válidos**: 0.0.0.0 a 255.255.255.255

  **Valor por omisión**: 0.0.0.0 para la dirección IP de origen. El valor por omisión de la máscara de origen es la dirección de origen IP configurada.

**dest-IP máscara-dest**
: Dirección IP de destino y máscara. La máscara-dest se suma (AND) por bits a la dirección IP de destino recibida para permitir que la regla coincida con un rango de direcciones IP de destino. Si los bits de la máscara de destino son 0, los bits correspondientes de la dirección IP de destino IP también deben ser 0.

  **Valores válidos**: 0.0.0.0 a 255.255.255.255

  **Valor por omisión**: 0.0.0.0 para dirección IP de destino. El valor por omisión de la máscara de destino es la dirección de destino IP configurada.

**primer-protocolo último-protocolo**
: Un rango de números de protocolos IP.

  Algunos números de protocolos IP comunes son:

  1 para ICMP
  6 para TCP
  17 para UDP
  89 para OSPF

  **Valores válidos**: 0 a 255

  **Valores por omisión**: 0 para el primer protocolo y 255 para el último protocolo

**primer-puerto-dest último-puerto-dest**
: Un rango de números de puertos de destino TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolos IP incluye 6 (para TCP) o 17 (para UDP). Estos parámetros se pasan por alto para los paquetes cuyo número de protocolo IP no es 6 ni 17.

  Algunos números de puertos que se utilizan con frecuencia son los siguientes:

21 para FTP
23 para Telnet
25 para SMTP
513 para rlogin
520 para RIP

**Valores válidos**: 0 - 65535

**Valores por omisión**: 0 para el primer puerto de destino y 65535 para el último puerto de destino

**primer-puerto-origen último-puerto-origen**
Un rango de números de puertos de origen TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolos IP incluye 6 (para TCP) o 17 (para UDP). Estos parámetros se pasan por alto para los paquetes cuyo número de protocolo IP no es 6 ni 17. Consulte la descripción de *primer-puerto-dest último-puerto-dest* para ver una lista de los números de puertos TCP/UDP que se utilizan con más frecuencia.

**Valores válidos**: 0 - 65535

**Valores por omisión**: 0 para el primer puerto de origen y 65535 para el último puerto de origen

**tcp-syn** este parámetro coincide con los paquetes TCP que establecen conexiones TCP (es decir, los paquetes TCP cuyo bit SYN es 1 y cuyo bit ACK es 0). Este parámetro sólo es válido si el rango de números de protocolos IP incluye 6 (para TCP) y el tipo de regla es exclusive. Este parámetro no es válido para los tipos IPSec y NAT, que siempre son inclusive. Este parámetro se pasa por alto para los paquetes cuyo número de protocolo IP no es 6.

**Valores válidos**: Yes o No

**Valor por omisión**: No

**tipo-icmp** Este parámetro, que define el tipo ICMP, sólo es válido si el rango de números de protocolos IP incluye 1 (para ICMP). El valor de este parámetro define el tipo ICMP de la regla de acceso. Los paquetes ICMP sólo pueden coincidir con la regla de acceso si el tipo ICMP del paquete coincide con el tipo ICMP de la regla de acceso. Si se especifica el valor por omisión, -1, todos los valores de tipo ICMP se tratan como coincidentes con la regla de acceso. Este parámetro se pasa por alto para paquetes cuyo número de protocolo IP no es 1.

**Valores válidos**: -1 a 255

**Valor por omisión**: -1 (todos los tipos ICMP)

**código-icmp**
Este parámetro, que define el código ICMP, sólo es válido si el rango de números de protocolos IP incluye 1 (para ICMP). El valor de este parámetro define el código ICMP de la regla de acceso. Los paquetes ICMP sólo pueden coincidir con la regla de acceso si el código ICMP del paquete coincide con el código ICMP de la regla de acceso. Si se especifica el

valor por omisión, -1, todos los valores de código ICMP se tratan como coincidentes. Este parámetro se pasa por alto para paquetes cuyo número de protocolo IP no es 1.

**Valores válidos**: -1 a 255

**Valor por omisión**: -1 (todos los códigos ICMP)

**máscara-tos, rango-inf-tos, rango-sup-tos**

Si define para *máscara-tos* un valor distinto de cero, se activa la función de filtro en función de los bits del byte TOS. *Máscara-tos* identifica los bits del byte precedencia/TOS que no se filtran. Por ejemplo, si la *máscara-tos* es X'E0' (B'11100000'), la función de filtro sólo se aplica a los 3 bits de precedencia del byte TOS (los 3 bits más significativos del byte TOS).

el *rango-inf-tos* y el *rango-sup-tos* definen el rango de valores consecutivos dentro de los bits seleccionados. Si desea filtrar los 8 valores de los bits de precedencia (0 - 7 decimales), el *rango-inf-tos* es X'00' (B'00000000') y el *rango-sup-tos* es X'e0' (B'11100000', lo que define 7 decimales dentro de los 3 bits seleccionados para ser filtrados). Si desea filtrar los valores binarios B'000', B'001', B'010' y B'011' (0 - 3 decimales) de los 3 bits de precedencia, el *rango-inf-tos* es X'00' (B'00000000') y el *rango-sup-tos* es X'60' (B'01100000').

Si tiene que filtrar patrones de bits que no forman una secuencia consecutiva de valores, tiene que definir una regla de control de acceso para cada rango que desee. Por ejemplo, para filtrar los dos valores de bits de precedencia B'001' (1 decimal) y B'011' (3 decimal) sin filtrar B'010' (2 decimal), tiene que definir la primera regla de control de acceso con *máscara-tos* igual a X'e0' y *rango-inf-tos* y *rango-sup-tos* igual a X'20' (ambos). Luego tiene que definir la segunda regla de control de acceso con *máscara-tos* igual a X'e0' y *rango-inf-tos* y *rango-sup-tos* igual a X'60' (ambos).

**Valores válidos para** *máscara-tos*: X'00' - X'FF'

**Valor por omisión**: 0 para ninguno

**Valores válidos para** *rango-inf-tos*: X'00' - X'FF'

**Valor por omisión**: 0

**Valores válidos para** *rango-sup-tos*: X'00' - X'FF'

**Valor por omisión**: El *rango-inf-tos* configurado.

**nuevo-valor-tos, máscara-mod-tos**

Al definir estos parámetros, permite que el direccionador modifique los bits especificados en el byte TOS. La *máscara-mod-tos* identifica los bits dentro del byte TOS que se van a modificar. El *nuevo-valor-tos* define el nuevo valor para los bits seleccionados. Por ejemplo, si la *máscara-mod-tos* es X'1e' y el *nuevo-valor-tos* es X'00', los 4 bits del campo TOS (identificados dentro del byte mediante el valor de

*máscara-mod-tos* X'1e' [B'00011110']) se definen en B'0000'. Para definir para los bits TOS el valor correspondiente al rendimiento máximo (B'0100'), utilice el valor de *máscara-mod-tos* X'1e' y el *nuevo-valor-tos* X'08' (B'00001000').

**Valores válidos para** *máscara-mod-tos*: X'00' - X'FF'

**Valor por omisión**: 0 para ninguno

**Valores válidos para** *nuevo-valor-tos*: X'00' - X'FF'

**Valor por omisión**: 0

**direccionamiento-basado-políticas, pasarela-siguiente-salto, utilizar-ruta-omisión**
Estos parámetros activan el direccionamiento basado en políticas, que constituye la posibilidad de especificar la pasarela del siguiente salto a la que se envían los paquetes filtrados. Si define para *direccionamiento-basado-políticas* el valor Yes, significa que desea que los paquetes filtrados se envíen a la pasarela del siguiente salto definida. *Pasarela-siguiente-salto* es la dirección de la pasarela del siguiente salto a las que se van a enviar los paquetes.

Si define para *utilizar-ruta-omisión* es valor Yes, permite que el direccionador dirija el paquete utilizando la tabla de direccionamiento normal si la pasarela definida no está disponible. Si este parámetro tiene el valor No, el paquete se elimina si la pasarela definida no está disponible y se envía un mensaje de ICMP *no se puede alcanzar* a la dirección de origen del paquete eliminado.

**Valores válidos para** *direccionamiento-basado-políticas*: Yes or No

**Valor por omisión**: No

**Valor válido para** *pasarela-siguiente-salto*: una dirección IP válida

**Valor por omisión**: ninguno

**Valores válidos para** *utilizar-direccionamiento-omisión*: Yes o No

**Valor por omisión**: Yes

**reg** Activa el registro cronológico.

**Valores válidos**: Yes o No

**Valor por omisión**: No

**els** Si el registro cronológico está activado, activa los mensajes ELS para esta regla de control de acceso.

**Valores válidos**: No, short o long

**Valor por omisión**: No

**ruptura-snmp**
Si el registro cronológico está activado, activa el envío de rupturas SNMP para esta regla de control de acceso.

**Valores válidos**: Yes o No

**Valor por omisión**: No

**syslog** Si el registro cronológico está activado, activa SysLog para esta regla de control de acceso. SysLog envía mensajes del sistema a una estación de trabajo remota conectada.

**Valores válidos**: No, short o long

**Valor por omisión**: No

**nivel-syslog**
Si SysLog está activado, especifica el nivel de los mensajes SysLog.

**Valores válidos**: Sys Def, Emerg, Alert, Crit, Error, Warn, Notice, Info o Debug

**Valor por omisión**: Valor por omisión del sistema del direccionador

**Ejemplo**:

```
IP config> add access-control
Entre tipo [E] I
Origen Internet [0.0.0.0]?
Máscara de destino [0.0.0.0]?
Destino de Internet [0.0.0.0]?
Máscara de destino [0.0.0.0]?
Entre número de protocolo inicial ([CR] para todos) [-1]?
Entre número de puerto de destino inicial ([CR] para todos) [-1]?
Entre número de puerto de origen inicial ([CR] para todos) [-1]?
Entre tipo ICMP ([CR] para todos) [-1]? 3
Entre código ICMP ([CR] para todos) [-1]?
Máscara filtro TOS/Precedencia (00-FF - [0] para ninguno) [0]? CD
Valor inicial TOS/Precedencia (00-FF) [0]?
Valor final TOS/Precedencia [0]?
Máscara modificación TOS/Precedencia (00-FF - [0] para ninguno) [0]? FA
Nuevo valor TOS/Precedencia (00-FF) [0]?
Dirección pasarela siguiente salto [ ]? 8.8.8.2
Utilizar ruta omisión si no se puede alcanzar pasarela siguiente salto? [Yes]:
IP config>
```

**address** *número-interfaz dirección-IP máscara-dirección*
Asigna una dirección IP a una de las interfaces de red de hardware del direccionador. Una interfaz de red de hardware no recibirá ni transmitirá paquetes IP hasta que tenga al menos una dirección IP. Debe especificar una dirección IP junto con su máscara de subred. Por ejemplo, si la dirección está en una red de clase B, y se utiliza el tercer byte para subred, la máscara sería 255.255.255.0. Utilice el mandato **list devices** para obtener el número de interfaz adecuado para el mandato. Las líneas serie no necesitan direcciones. Estas líneas se denominan no numeradas. Sin embargo, tiene que activarlas para el tráfico IP mediante el mandato **add address**. La dirección que se utiliza es 0.0.0.*n*, donde *n* es el *número-interfaz*.

**Nota:** Para asignar una dirección IP a la red de puente del 2210, especifique **bridge** para el *número-interfaz*. Consulte el tema “Cómo asignar direcciones IP a la interfaz de red de puente” en la página 243 para obtener más información.

Debe especificar una dirección IP junto con su máscara de subred. Por ejemplo, si la dirección está en una red de clase B, y se utiliza el tercer byte para subred, la máscara sería 255.255.255.0. Utilice la opción **List Devices** para obtener el número de interfaz adecuado de la opción.

**número-interfaz**

**Valores válidos**: cualquier número de interfaz definido, o bien **bridge**

**Valor por omisión**: ninguno

**dirección-ip**

**Valores válidos**:

El rango de clase A es de 1.0.0.1 a 126.255.255.254
El rango de clase B es de 128.0.0.1 a 191.255.255.254
El rango de clase C es de 192.0.0.1 a 223.255.255.254
Para interfaces serie no numeradas, 0.0.0.n, donde *n* es el número de interfaz

**Valor por omisión**: ninguno

**máscara-subred**

**Valores válidos**: 0.0.0.0 - 255.255.255.255

**Valor por omisión**: ninguno

**Ejemplo:** `add address 0 128.185.123.22 255.255.255.0`

**bootp-server** *dirección-IP-servidor*

Añade un servidor BOOTP/DHCP a la lista de servidores a los que el direccionador reenviará peticiones BOOTP/DHCP. Consulte el tema "Configuración del proceso de reenvío BOOTP/DHCP" en la página 261 para obtener más información.

**dirección-IP-servidor**

**Valores válidos**: cualquier dirección IP válida de servidor Bootp

**Valor por omisión**: ninguno

**Ejemplo:** `add bootp-server 128.185.123.22`

**filter** *dirección-IP-destino máscara-dirección*

Designa un destino IP que se va a filtrar. Los paquetes IP no se reenviarán a los destinos filtrados ni se difundirá información de direccionamiento relacionada con estos destinos. Los paquetes destinados a los destinos filtrados simplemente se eliminan. Debe especificar un destino filtrado como una dirección IP con su máscara de subred. Por ejemplo, para filtrar una subred de una red de clase B, que utiliza el tercer byte para subred, la máscara debería ser 255.255.255.0. El mecanismo de filtro es más eficaz que los controles de acceso IP, aunque no resulta tan flexible. A diferencia de los controles de acceso, los filtros también afectan al funcionamiento de los protocolos de direccionamiento IP. Las redes/subredes filtradas se alteran temporalmente si se aprenden mediante el protocolo de direccionamiento OSPF.

Este mandato entra en vigor de inmediato; no tiene que volver a arrancar el direccionador para que entre en vigor.

**dirección-IP-dest**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**máscara-subred**

**Valores válidos**: 0.0.0.0 a 255.255.255.255

**Valor por omisión**: 0.0.0.0

**Ejemplo:** `add filter 127.0.0.0 255.0.0.0`

**packet-filter** *nombre-filtro tipo número-interfaz*

Define un registro de filtro de paquete dentro de la configuración del direccionador.

**nombre-filtro**

**Valores válidos**: cualquier nombre de 16 caracteres.

En el nombre puede incluir guiones (-) y símbolos de subrayado (_).

**Valor por omisión**: ninguno

**tipo** *IN* filtra el tráfico de entrada.

*OUT* filtra el tráfico de salida.

**número-interfaz**

**Valores válidos**: cualquier interfaz definida, o bien **bridge** para la Interfaz de red de puente

**Valor por omisión**: ninguno

**Ejemplo:** `add packet-filter`

```
Packet-filter name [ ]? filt-1-0
Filter incoming or outgoing traffic? [IN]?
Which interface is this filter for [0]? 1
```

**redundant-default-gateway** *número-interfaz dirección-IP-pasarela máscara-dirección dirección-MAC pasarela-principal*

Añade una dirección IP de pasarela redundante por omisión a la configuración.

**número-interfaz**

Especifica el número de red de las interfaces LEC de la ELAN.

**Valores válidos**: números de red de interfaces LEC

**Valor por omisión**: ninguno

**dirección-IP-pasarela**

Especifica la pasarela por omisión de la estación final.

**Valores válidos**: direcciones IP utilizadas como pasarelas por omisión

**Valor por omisión**: 0.0.0.0

**máscara-dirección**

Especifica la máscara de la dirección IP.

**Valores válidos**: cualquier máscara de red IP válida

**Valor por omisión**: 0.0.0.0

**dirección-MAC**

**Nota:** La pasarela principal y la pasarela de reserva deben tener la misma dirección MAC

**Valores válidos**: cualquier dirección MAC válida que no utilice ninguna otra interfaz de la ELAN

**Valor por omisión**: 00.00.00.00.00.00

**pasarela-principal**
Especifica si la pasarela se utiliza como pasarela principal o como pasarela de reserva.

Esta consulta pregunta si la pasarela de este dispositivo es la pasarela principal activa durante el funcionamiento normal de la red o la pasarela de reserva que se activa cuando la interfaz LEC que contiene la pasarela principal no está operativa. Si responde **Yes**, se configura una pasarela principal. Sólo debe haber una pasarela principal por ELAN.

**Valores válidos** Yes o No

**Valor por omisión**: No

**Ejemplo: `add redundant-default-gateway`**

```
Which net is this redundant gateway for [0]? 1
IP address of gateway [0.0.0.0]? 9.67.205.1
Address mask [255.255.0.0]? 255.255.240.0
MAC address [00.00.00.00.00.00.]? 00.00.00.00.00.BA
Is this the primary gateway [No]? Yes or No
```

**route** *dirección-dest máscara-dest siguiente-salto1 coste1 [siguiente-salto2 coste2 [siguiente-salto3 coste3 [siguiente-salto4 coste4]]]*
Añade entre 1 y 4 rutas estáticas a la configuración IP del dispositivo. Cuando la información sobre el direccionamiento dinámico no está disponible para un determinado destino, se utilizan las rutas estáticas.

El destino se especifica mediante una dirección IP (*dirección-dest*) junto con su máscara de dirección (*máscara-dest*). Si la dirección IP de destino es una dirección de red, la máscara-dest debe ser una máscara de red. Si la dirección IP de destino es una dirección de subred, la máscara-dest debe ser una máscara de subred. Finalmente, si la dirección IP de destino es una dirección de sistema principal, la máscara de destino debe se una máscara de sistema principal (lo que significa que el único valor válido es 255.255.255.255). La máscara de destino debe ser precisa; si no lo es, no se aceptará la ruta estática.

La ruta al destino se especifica mediante la dirección IP del siguiente salto *(siguiente-salto)* y el coste *(coste)* de direccionar el paquete al destino. El siguiente salto debe estar en la misma red o subred que una de las interfaces conectadas directamente del direccionador. Las rutas estáticas siempre se alteran temporalmente con rutas aprendidas a través de OSPF, pero, por omisión, las rutas aprendidas a través de RIP no alteran temporalmente las rutas estáticas. Sin embargo, puede activar o desactivar el hecho de que las rutas aprendidas a través de RIP alteren temporalmente las rutas estáticas mediante los mandatos **enable override static-routes** o **disable override static-routes**. Este mandato entra en vigor de forma inmediata; no tiene que volver a arrancar el direccionador.

**dirección-dest**
**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**máscara-dest**

**Valores válidos**: 0.0.0.0 a 255.255.255.255

**Valor por omisión**: ninguno

**siguiente-salto1, siguiente-salto2, siguiente-salto2, siguiente-salto4**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**coste1, coste2, coste3, coste4**

**Valores válidos**: un entero comprendido entre 0 y 255

**Valor por omisión**: 1

**Ejemplo:**

```
IP config> add route
IP destination []? 1.1.0.0
Address mask [255.0.0.0]? 255.255.0.0
Via gateway 1 at []? 10.1.1.1
Cost [1]? 1
Via gateway 2 at []?
IP config> add route 1.1.0.0 255.255.0.0
Via gateway 2 at []? 20.1.1.1
Cost [1]? 2
Via gateway 3 at []? 30.1.1.1
Cost [1]? 3
Via gateway 4 at []?
IP config> add route 2.2.0.0 255.255.0.0 10.2.2.2 1 20.2.2.2 2
IP config> list routes

route to 1.1.0.0        ,255.255.0.0     via 10.1.1.1        cost 1
                                         via 20.1.1.1        cost 2
                                         via 30.1.1.1        cost 3
route to 2.2.0.0        ,255.255.0.0     via 10.2.2.2        cost 1
                                         via 20.2.2.2        cost 2

IP config>
```

**route-policy** *identificador-política-rutas utilizar-política-estrictamente-lineal*

Añade una política de filtro de rutas. Una política de filtro de rutas consta de entradas que definen una serie de rutas que se pueden filtrar para ser incluidas o excluidas de la tabla de direccionamiento de un protocolo de direccionamiento externo, como OSPF o RIP.

**identificador-política-rutas**

Una serie de caracteres que identifica una política de filtro de rutas.

**Valores válidos:** cualquier serie ASCII que tenga entre 1 y 15 caracteres

**Valor por omisión:** ninguno

**utilizar-política-estrictamente-lineal**

*Yes* indica que la coincidencia se realizará estrictamente en función de la secuencia de números de índices de las entradas de la política de filtro de rutas. La entrada con el número de índice menor se procesará primero. *No* indica que la coincidencia se realizará utilizando la aplicación de la coincidencia más larga. La entrada con el número de índice menor se seleccionará únicamente cuando haya más de una entrada con la misma dirección y máscara.

**Valores válidos:** Yes o No

**Valor por omisión:** No

**route-table-filter** *máscara destino [both | exact | more-specific] [exclusive | inclusive]*

Añade un filtro de tabla de rutas correspondiente a las rutas especificadas. Cuando se activa **route-table-filtering**, el filtro de tabla de rutas se comparará con las rutas añadidas a la tabla de rutas IP. El orden de los filtros de la tabla de rutas no es importante. Se seleccionará el filtro de la tabla de rutas con la coincidencia más específica. Si no se encuentra ninguna coincidencia, la ruta se añade a la tabla de rutas. Si se especifica **exact**, el destino de la ruta y la máscara deben ser exactamente iguales que el destino del filtro de la tabla de rutas y su máscara para que se encuentre una coincidencia. Si se especifica **more-specific**, el destino de la ruta y la máscara deben encontrarse dentro del rango bajo el que está el filtro de la tabla de rutas y la máscara. Si se especifica **both**, se suman los efectos de los valores exact y more-specific (es decir, se producirá una coincidencia en el caso de una coincidencia exacta y en el caso de una coincidencia más específica). Si el filtro de la tabla de rutas especifica **include**, la ruta se añadirá a la tabla de rutas IP. Si el filtro de la tabla de rutas indica **exclude**, la ruta no se añadirá a la tabla de rutas IP. Las rutas estáticas y directas nunca se excluyen de la tabla de rutas IP.

**máscara destino**

**Valores válidos:** cualquier máscara IP válida

**Valor por omisión:** both exclude

**udp-destination** *número-puerto dirección*

Añade una dirección de destino de reenvío UDP. Los datagramas UDP recibidos con el número de puerto UDP de destino especificado se reenviarán a la dirección IP especificada.

Puede especificar una dirección IP de difusión general o de difusión individual.

Repita este mandato para añadir más de una dirección IP correspondiente al mismo puerto UDP. Esto hace que el direccionador reenvíe el datagrama UDP a cada una de las direcciones IP.

**número-puerto**

**Valores válidos**: 0 a 65535

**Valor por omisión**: ninguno

**dirección** **Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:**

```
add udp-destination 36 20.1.2.2
```

**vrid** *dirección-ip-interfaz vrid intervalo-anuncio direccionador-reserva dirección-ip-reserva prioridad modal-funcional/grupo tipo-autentificación clave-autentificación*

Añade una definición de ID de direccionador virtual correspondiente a un direccionador VRRP en un segmento de la LAN.

**dirección-ip-interfaz**

Indica la interfaz IP para la que se define este VRID.

**Valores válidos**: Cualquier interfaz IP configurada.

**Valor por omisión**: ninguno

**vrid** El identificador del Direccionador virtual. La combinación de *dirección-interfaz-ip* y *vrid* define de forma exclusiva el VRID. Se puede utilizar el mismo *vrid* en más de una interfaz física. Si el VRID ya existe, se modificará.

**Valores válidos**: 1-255

**Valor por omisión**: ninguno

**intervalo-anuncio**
El intervalo entre los anuncios VRRP.

**Valores válidos**: 1-255

**Valor por omisión**: 1

**direccionador-reserva**
Indica si este direccionador es el direccionador maestro o de reserva para este VRID.

**Valores válidos**: Yes o No

**Valor por omisión**: No

**dirección-ip-reserva**
Indica la primera dirección IP de reserva para este VRID. Se pueden añadir direcciones adicionales mediante el mandato *add vr-address* para segmentos de la LAN que dan soporte a más de una subred. No se aplica si se ha definido **No** para *direccionador-reserva*.

**Valores válidos**: Cualquier dirección IP válida.

**Valor por omisión**: ninguno

**prioridad** Indica la prioridad VRRP correspondiente a los direccionadores de reserva. Si un direccionador de reserva pasa a actuar como direccionador maestro, utilizará esta prioridad en sus anuncios VRRP. No se aplica si se ha definido **No** para *direccionador-reserva*. Un direccionador maestro siempre anunciará una prioridad de 255.

**Valores válidos**: 1-254

**Valor por omisión**: 100

**modalidad-funcional/grupo**
Indica si se utiliza o no una dirección MAC de difusión múltiple como dirección MAC virtual VRID. Para que VRRP funcione correctamente, todos los direccionadores configurados para este VRID deben tener el mismo valor para este parámetro.

**Valores válidos**: Yes o No

**Valor por omisión**: No

**tipo-autentificación**
Indica el tipo de autentificación utilizado para los anuncios VRRP. Las opciones para tipo de autentificación son 1, que indica una contraseña sencilla; o 0, que indica que no se utiliza autentificación.

**Valores válidos**: none, simple

**Valor por omisión**: none

**clave-autentificación**

El parámetro que define la contraseña para este VRID. Si se utiliza autentificación de contraseña, sólo se aceptan los paquetes con la clave de autentificación correcta. La *clave de autentificación* no se aplica cuando se especifica *none* o se adopta como valor por omisión para *tipo-autentificación*.

**Valores válidos**: Cualquier serie de entre 1 y 8 caracteres.

**Valor por omisión**: Una serie nula.

**Ejemplo:** `add vrid`

```
IP config> add vrid
IP Interface [ ]? 153.2.2.25
VRID (1-255) [0]? 1
Advertisement Interval (1-255) [1]?
Backup Virtual Router? [No]:
Use Functional/Group Address? [No]:
Authentication Type (0 - None, 1 - Simple) [0]?
VRID 153.2.2.25/1 added successfully
```

**vr-address** *dirección-ip-interfaz vrid dirección-ip*

Añade una dirección secundaria a una definición de ID de Dirección virtual (VRID) configurada. Las direcciones secundarias se incluyen en los anuncios VRRP correspondientes al VRID. Las direcciones secundarias son necesarias en LAN físicas que dan soporte a varias subredes IP. Cada dirección designa la dirección de pasarela por omisión correspondiente a dicha subred. Si el direccionador es un direccionador maestro, las direcciones añadidas con el mandato *add vr-address* se anunciarán además de la *dirección-interfaz-ip* correspondiente al VRID. Si el direccionador es un direccionador de reserva para el VRID, las direcciones añadidas con el mandato *add vr-address* se anunciarán además de la *dirección-ip-reserva*.

**dirección-ip-interfaz**

La interfaz IP correspondiente al VRID.

**Valores válidos**: Cualquier interfaz IP configurada.

**Valor por omisión**: ninguno

**vrid** El identificador del Direccionador virtual. La combinación de *dirección-interfaz-ip* y *vrid* define de forma exclusiva el VRID. El VRID debe estar configurado para las direcciones para que se pueda añadir a esta definición.

**Valores válidos**: 1-255

**Valor por omisión**: ninguno

**dirección-ip**

La dirección IP adicional que se va a incluir en los anuncios VRRP correspondientes al VRID.

**Valores válidos**: Cualquier dirección IP.

**Valor por omisión**: ninguno

**Ejemplo:** `add vr-address`

```
IP config>add vr-address
IP Interface [ ]? 153.2.2.25
Virtual Router ID (1-255) [0]? 1
Additional IP Address [ ]? 5.1.1.1
VRID 153.2.2.25/1 address 5.1.1.1 added successfully.
```

## Change

Utilice el mandato **change** para modificar un elemento de la configuración IP instalado anteriormente mediante el mandato **add**. En general, debe especificar el elemento que desea modificar del mismo modo que especificó el elemento con el mandato **add**.

**Sintaxis:**

**change** access-control . . .

address . . .

route . . .

route-policy

**access-control** *número-regla tipo origen-IP máscara-origen dest-IP máscara-dest primer-protocolo último-protocolo [primer-puerto-dest último-puerto-dest primer-puerto-origen último-puerto-origen] [tcp-syn] [tipo-icmp código-icmp] [máscara-tos rango-inf-tos rango-sup-tos máscara-mod-tos nuevo-valor-tos direccionamiento-basado-políticas pasarela-siguiente-salto utilizar-ruta-omisión] [reg els ruptura-snmp syslog nivel-syslog]*
Modifica un registro de control de acceso global existente. Utilice el mandato **list access-control** para ver todos los registros existentes y obtener el número de regla. Consulte el mandato **Add** de talk 6 para ver las definiciones de los parámetros.

**Ejemplo:**

```
IP config> change access-control 2
Enter type [E]? i
Internet source [9.1.2.3]?
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]?
Destination mask [0.0.0.0]?
Enter starting protocol number [0]?
Enter starting DESTINATION port number [0]?
Enter starting SOURCE port number [0]?
Filter on ICMP Type [-1]?
TOS/Precedence filter mask [e0]?
TOS/Precedence start value [0]?
TOS/Precedence end value [0]?
TOS/Precedence modification mask [1f]? 1e
New TOS/Precedence value[0]? 08
Use policy-based routing? [Yes]:
Next hop gateway address [9.2.160.1]?
Use default route if next hop gateway unreachable? [Yes]:
Enable Logging [No]:
```

**address** *dirección-antigua dirección-nueva máscara-nueva*
Modifica una de las direcciones de la interfaz IP del direccionador. Debe especificar cada nueva dirección junto con la nueva máscara de subred de la dirección. Este mandato también sirve para modificar una máscara de subred de la dirección existente.

Direcciones IP válidas:

- El rango de clase A es de 1.0.0.1 a 126.255.255.254
- El rango de clase B es de 128.0.0.1 a 191.255.255.254
- El rango de clase C es de 192.0.0.1 a 223.255.255.254

- Para interfaces serie no numeradas, 0.0.0.n, donde n es el número de la interfaz del hardware

Para las interfaces de línea serie:

- 0.0.0.n, donde n es el número de la interfaz de hardware.

**dirección-antigua**

**Valor válido**: una dirección de interfaz IP actualmente configurada

**Valor por omisión**: ninguno

**dirección-nueva**

**Valor válido**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**máscara-nueva**

**Valor válido**: 0.0.0.0 - 255.255.255.255

**Valor por omisión**: ninguno

**Ejemplo:** `change address 192.9.1.1 128.185.123.22  255.255.255.0`

**route** *dirección-dest máscara-dest nuevo-siguiente-salto1 nuevo-coste1 [nuevo-siguiente-salto2 nuevo-coste2[nuevo-siguiente-salto3 nuevo-coste3 [nuevo-siguiente-salto4 nuevo-coste4]]]*

Modifica los siguientes saltos o los costes asociados a las rutas estáticas configuradas para el destino especificado. Este mandato entra en vigor de inmediato; no tiene que volver a arrancar el direccionador para que entre en vigor.

**dirección-dest**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**máscara-dest**

**Valores válidos**: 0.0.0.0 a 255.255.255.255

**Valor por omisión**: ninguno

**nuevo-siguiente-salto1, nuevo-siguiente-salto2, nuevo-siguiente-salto3, nuevo-siguiente-salto4**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**nuevo-coste1, nuevo-coste2, nuevo-coste3, nuevo-coste4**

**Valores válidos**: un entero comprendido entre 0 y 255

**Valor por omisión**: 1

**Ejemplo:**

```
IP config>list routes

route to 1.1.0.0        ,255.255.0.0     via 10.1.1.1        cost 1
                                         via 20.1.1.1        cost 2
                                         via 30.1.1.1        cost 3
route to 2.2.0.0        ,255.255.0.0     via 10.2.2.2        cost 1
                                         via 20.2.2.2        cost 2

IP config>change route
IP destination []? 1.1.0.0
Address mask [255.0.0.0]? 255.255.0.0
Via gateway 1 at [.10.1.1.1]? 10.10.10.1
Cost [1]? 10
Via gateway 2 at [20.1.1.1]? 20.20.20.1
Cost [2]? 20
Via gateway 3 at [30.1.1.1]? 30.30.30.1
Cost [3]? 30
Via gateway 4 at []? 40.40.40.1
Cost [1]? 40
IP config>change route 2.2.0.0 255.255.0.0 10.10.10.2 10
IP config>list routes

route to 1.1.0.0        ,255.255.0.0     via 10.10.10.1      cost 10
                                         via 20.20.20.1      cost 20
                                         via 30.30.30.1      cost 30
                                         via 40.40.40.1      cost 40
route to 2.2.0.0        ,255.255.0.0     via 10.10.10.2      cost 10
```

**route-policy** *identificador-política-rutas*

Utilice este mandato para modificar una política existente de filtro de rutas, creada con el mandato **add route-policy**. El mandato **change route-policy** sirve para configurar las entradas, acciones y condiciones de coincidencia asociadas a la política de filtro de rutas. El mandato **change route-policy** le lleva al indicador `IP Route Policy Config>`.

**identificador-política-rutas**

**Valores válidos**: la serie ASCII de entre 1 y 15 caracteres que identifica una política existente de filtro de rutas

**Valor por omisión**: ninguno

## Delete

Utilice el mandato **delete** para suprimir un elemento de la configuración IP instalado anteriormente mediante el mandato **add**. En general, debe especificar el elemento que desea suprimir del mismo modo que especificó el elemento con el mandato **add**.

**Sintaxis:**

de**lete** accept-rip-route . . .
access-control . . .
address . . .
bootp-server
default network/subnet-gateway . . .
filter . . .
packet-filter
redundant-default-gateway
route . . .

route-policy . . .

route-table-filter

udp-destination . . .

vrid . . .

vr-address . . .

**accept-rip-route** *número-red*
Elimina una ruta de la lista de redes que el protocolo RIP acepta siempre.

**Valores válidos**: Cualquier dirección IP contenida en la lista de redes aceptadas.

**Valor por omisión**: ninguno

**Ejemplo:** `delete accept-rip-route 10.0.0.0`

**access-control** *número-regla*
Suprime una de las reglas de control de acceso de la lista global de control de acceso.

**Ejemplo:** `delete access-control 2`

**address** *dirección-interfaz-ip*
Suprime una de las direcciones de la interfaz IP del direccionador.

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `delete address 128.185.123.22`

**bootp-server** *dirección-IP-servidor*
Elimina un servidor BOOTP de una configuración IP.

**Valores válidos**: cualquier dirección IP configurada del servidor BOOTP

**Valor por omisión**: 0.0.0.0

**Ejemplo:** `delete bootp-server 128.185.123.22`

**default network/subnet-gateway** *[dirección-red-ip]*
Suprime la pasarela por omisión o la pasarela de subred por omisión correspondiente a la red con subredes especificada.

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: 0.0.0.0

**Ejemplo:** `delete default subnet-gateway 128.185.0.0`

**filter** *dirección-dest máscara-dest*
Suprime una de las redes filtradas del direccionador. Este mandato entra en vigor de inmediato; no tiene que volver a arrancar el direccionador para que entre en vigor.

**dirección-dest**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: 0.0.0.0

**máscara-dest**

**Valores válidos**: 0.0.0.0 - 255.255.255.255

**Valor por omisión**: ninguno

**Ejemplo:** **delete filter 127.0.0.0**

```
Address mask [0.0.0.0]? 255.0.0.0
```

**packet-filter** *nombre-filtro*

Suprime un filtro de paquete especificado de la configuración s del direccionador.

**Valores válidos**: cualquier nombre de 16 caracteres.

En el nombre puede incluir guiones (-) y símbolos de subrayado (_).

**Valor por omisión**: ninguno

**Ejemplo:**

```
IP config> delete packet-filter pf-in-0
All access controls defined for 'pf-in-0' will also be deleted.
Are you sure you want to delete (Yes or [No]): y
Deleted
IP config>
```

**redundant** *número-interfaz*

Suprime la pasarela IP redundante de una interfaz LEC.

**número-interfaz**

**Valores válidos**: Números de interfaz de LEC con una pasarela IP redundante por omisión.

**Valor por omisión**: ninguno

**Ejemplo:**

```
Enter the Net number of Redundant Gateway to delete:? 1
Gateway deleted.
```

**route** *dirección-dest máscara-dest [suprimir-siguiente-salto1 [suprimir-siguiente-salto2 [suprimir-siguiente-salto3 [suprimir-siguiente-salto4 ]]]]*

Suprime una de las rutas estáticas configuradas del dispositivo. Este mandato entra en vigor de inmediato; no tiene que volver a arrancar el direccionador para que entre en vigor.

**dirección-dest**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**máscara-dest**

**Valores válidos**: cualquier máscara IP válida

**Valor por omisión**: ninguno

**suprimir-siguiente-salto**

**Valores válidos**: Yes o No

**Valor por omisión**: No

**Ejemplo:**

```
IP config>list routes

route to 1.1.0.0        ,255.255.0.0     via 10.10.10.1      cost 10
                                         via 20.20.20.1      cost 20
                                         via 30.30.30.1      cost 30
                                         via 40.40.40.1      cost 40
route to 2.2.0.0        ,255.255.0.0     via 10.10.10.1      cost 10

IP config>delete route 1.1.0.0 255.255.0.0
Delete gateway 10.10.10.1? [No]:
Delete gateway 20.20.20.1? [No]: y
Delete gateway 30.30.30.1? [No]:
Delete gateway 40.40.40.1? [No]: y
IP config>delete route 2.2.0.0 255.255.0.0
IP config>delete route 1.1.0.0 255.255.0.0 n y
IP config>list routes

route to 1.1.0.0        ,255.255.0.0     via 10.10.10.1      cost 10

IP config>
```

**route-policy** *identificador-política-rutas suprimir-entradas-política-rutas*

Suprime una política existente de filtro de rutas de la configuración. Tiene la opción de suprimir todas las entradas de la política de filtro de rutas asociadas a la política de filtro de rutas. Si las entradas no se han suprimido, cuando vuelva a configurar la política de filtro de ruta suprimida se volverán a inicializar las entradas asociadas a dicha política de filtro de rutas. Utilice el mandato **add route-policy** para volver a configurar una política de filtro de rutas suprimida.

**identificador-política-rutas**

**Valores válidos**: la serie ASCII de entre 1 y 15 caracteres que identifica una política de filtro de rutas configurada

**Valor por omisión**: ninguno

**suprimir-entradas-política-rutas**

*Yes* suprime las entradas correspondientes de la política de rutas; *No*, las guarda.

**Valores válidos**: Yes o No

**Valor por omisión**: No

**route-table-filter** *destino máscara definición-máscara [both | exact | more specific]*

Suprime un filtro de rutas de los filtros de tabla de rutas añadidos mediante **add route-table-filter.** Consulte “route-table-filter” en la página 287 para ver definiciones de las extensiones del mandato.

**destino** **Valores válidos**: cualquier máscara IP válida

**Valor por omisión**: ninguno

**máscara** **Valores válidos**: cualquier máscara IP válida

**Valor por omisión**: ninguno

**definición-máscara**

**Valores válidos**: cualquier máscara IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `delete route-table-filter`

```
IP config>delete route-table-filter
Route Filter IP address []? 7.0.0.0
Route Filter IP mask []? 255.0.0.0
Enter Match type (B, E, or M) [B]?
Enter Definition type (I or E) [E]?
Route filter deleted
IP config>
```

**udp-destination** *número-puerto dirección*

Suprime una dirección de destino de reenvío UDP configurada mediante el mandato **add udp-destination**. Como resultado, los datagramas UDP distribuidos localmente que se reciban en el puerto especificado no se reenviarán a la dirección IP especificada.

**número-puerto**

**Valores válidos**: cualquier entero comprendido entre 0 y 65535

**Valor por omisión**: ninguno

**dirección** **Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplos:**

```
delete udp-destination 36 20.1.2.2
```

**vrid** *dirección-ip-interfaz vrid*

Suprime una definición configurada de ID de direccionador virtual correspondiente a un direccionador VRRP

**dirección-ip-interfaz**

Indica la interfaz IP para la que se suprime este VRID.

**Valores válidos**: Cualquier interfaz IP configurada.

**Valor por omisión**: ninguno

**vrid** El identificador del Direccionador virtual. La combinación de *dirección-interfaz-ip* y *vrid* define de forma exclusiva el VRID. Sirve para identificar el VRID que se va a suprimir.

**Valores válidos**: 1-255

**Valor por omisión**: ninguno

**Ejemplo:**

```
IP config>delete vrid
IP Interface [ ]? 153.2.2.25
Virtual Router ID (1-255) [0]? 1
VRID 153.2.2.25/1 deleted.
```

**vr-address** *dirección-ip-interfaz vrid dirección-ip*

Suprime una dirección secundaria de una definición de ID de Dirección virtual (VRID) configurada.

**dirección-ip-interfaz**

La interfaz IP correspondiente al VRID.

**Valores válidos**: Cualquier interfaz IP configurada.

**Valor por omisión**: ninguno

**vrid** El identificador del Direccionador virtual. La combinación de *dirección-interfaz-ip* y *vrid* define de forma exclusiva el VRID. El VRID debe estar configurado para las direcciones para que se pueda suprimir de esta definición.

**Valores válidos**: 1-255

**Valor por omisión**: ninguno

**dirección-ip**

La dirección IP adicional que se va a suprimir de la definición VRRP.

**Valores válidos**: Cualquier dirección IP.

**Valor por omisión**: ninguno

**Ejemplo:**

```
IP config>delete vr-address
IP Interface [ ]? 153.2.2.25
Virtual Router ID (1-255) [0]? 1
IP Address to delete [ ]? 5.1.1.1
VRID 153.2.2.25/1 addr 5.1.1.1 deleted.
```

## Disable

Utilice el mandato **disable** para desactivar características IP anteriormente activadas mediante el mandato **enable**.

**Sintaxis:**

**disable**

arp-net-routing

arp-subnet-routing

bootp-forwarding

classless

directed-broadcast

dynamic-address

echo-reply

fragment-offset-check

icmp-redirect . . .

nexthop-awareness . . .

override default/static-routes . . .

packet-filter

per-packet-multipath

receiving policy . . .

receiving rip . . .

receiving dynamic all/hosts/nets/subnets . . .

record-route

rip

rip2

route-table-filtering

same-subnet

sending all/default/net/subnet/poisoned/host/static/...

sending outage-only . . .

sending policy . . .

sending rip1-routes-only

simple-internet-access

source-addr-verification

source-routing

tftp-server

timestamp

trace

udp-forwarding . . .

vrrp . . .

**arp-net-routing**

Desactiva el direccionamiento de red ARP. Cuando está activado, el direccionador responde mediante proxy a todas las solicitudes ARP correspondientes a destinos remotos a los que se llega mejor a través del direccionador. Este es el valor por omisión y el valor generalmente recomendado.

**Ejemplo:** `disable arp-net-routing`

**arp-subnet-routing**

Desactiva la característica IP denominada direccionamiento de subred ARP o ARP de proxy, que, cuando está activada, actúa de interfaz con sistemas principales que no tienen soporte de subredes IP. Este es el valor por omisión y el valor generalmente recomendado.

**Ejemplo:** `disable arp-subnet-routing`

**bootp-forwarding**

Desactiva la función de retransmisión BOOTP/DHCP.

**Ejemplo:** `disable bootp-forwarding`

**classless** Desactiva la supresión de rutas de red naturales. Las rutas de red naturales (por ejemplo, las rutas de clase A, B o C) se generan de forma automática para anuncios en protocolos que no anuncian la máscara de subred (por ejemplo, RIPv1).

**directed-broadcast**

Desactiva el reenvío de paquetes IP cuyos destinos son una dirección de difusión general que no es local (por ejemplo, LAN remota). El sistema principal de origen origina el paquete como una difusión individual y a continuación se reenvía como una difusión individual a una subred de destino y se “divide” en una difusión general. Puede utilizar estos paquetes para localizar servidores de la red.

**Nota:** El reenvío y la división no se pueden desactivar por separado.

**Ejemplo:** `disable directed-broadcast`

**dynamic-address** *0.0.0.n*

En la interfaz de red PPP especificada, hace que el direccionador deje de aprender su dirección IP del nodo remoto de dicha interfaz de red. Por omisión, esta opción está desactivada.

Esta opción sólo es válida en una interfaz de red configurada como una interfaz de línea serie no numerada (la dirección IP asignada a la interfaz de red mediante el mandato **add address** es *0.0.0.n*, donde *n* es el número de interfaz de red).

**Ejemplo:**

```
IP config> disable dynamic-address
Interface address []? 0.0.0.1
IP config>
```

**echo-reply**

Desactiva la función de respuesta a ecos ICMP del direccionador. Esto hace que un mandato ping enviado a cualquiera de las interfaces del direccionador no genere ninguna respuesta. El valor por omisión del direccionador es que la respuesta a ecos esté activada.

**Ejemplo: `disable echo-reply`**

**fragment-offset-check**

Desactiva la comprobación del desplazamiento de fragmentos de los paquetes IP recibidos. Cuando esta comprobación está activada, el direccionador comprueba cada fragmento para asegurarse de que ningún fragmento secundario recubra los ocho primeros bytes de la carga del primer fragmento. Por omisión, esta comprobación está desactivada.

**icmp-redirect** *dirección-interfaz-ip*

Hace que el direccionador deje de enviar mensajes de redirección ICMP en la interfaz IP especificada. Si no entra ningún valor cuando se le solicite la dirección de la interfaz IP, el direccionador dejará de enviar mensajes de redirección ICMP en todas las interfaces IP.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:**

```
IP config> disable icmp-redirect
Interface address (NULL for all) []? 192.9.200.44
IP config>
```

**nexthop-awareness** *dirección-interfaz-ip*

Desactiva el aviso del siguiente salto en una interfaz IP.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:**

```
IP config>disable nexthop-awareness 1.1.1.1
IP config>disable nexthop-awareness
Interface address []? 2.2.2.2
IP config>
```

**override default/static-routes** *dirección-interfaz-ip*

Por omisión, las rutas recibidas por RIP no alteran temporalmente las rutas estáticas. Sin embargo, el mandato **enable override static-routes** permite que las rutas recibidas por RIP alteren temporalmente las rutas estáticas. Una vez se han activado las rutas RIP para que alteren temporalmente las rutas estáticas, puede utilizar el mandato **disable override default-route** o el mandato **disable override static-route**

para evitar de nuevo que las rutas recibidas por RIP alteren temporalmente las rutas estáticas. El mandato **disable override default-route** evita que una ruta por omisión recibida por RIP en la interfaz *dirección-interfaz-ip* sustituya a una ruta por omisión ya instalada en la tabla de direccionamiento IP. El mandato **disable override static-routes** evita que las rutas RIP recibidas en la interfaz *dirección-interfaz-ip* alteren temporalmente alguna de las rutas estáticas del direccionador.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `disable override default 128.185.123.22`

**packet-filter** *nombre-filtro*

Desactiva la lista de control de acceso (filtros de paquetes) específica de la interfaz especificada.

**nombre-filtro**

**Valores válidos**: cualquier nombre de 16 caracteres. En el nombre puede incluir guiones (-) y símbolos de subrayado (_).

**Valor por omisión**: Ninguno

**Ejemplo:** `disable packet-filter pf-in-0`

**per-packet-multipath**

Si per-packet-multipath está desactivado, las rutas multiacceso de igual coste equilibrarán la carga por destino cuando se coloque el destino en la antememoria IP. El valor por omisión es que esté desactivado.

**receiving policy global/interface** *dirección-interfaz-ip*

Desactiva el uso de la política para determinar las rutas que acepta el RIP. El mandato **disable receiving policy global** desactiva el uso de la política global de recepción de filtros de rutas para todas las interfaces RIP que cumplen estas dos condiciones:

- No tienen configuradas políticas de recepción de filtros de rutas RIP a nivel de interfaz. Si se ha configurado una política de recepción de filtros de rutas RIP a nivel de interfaz en una interfaz, la política continúa determinando qué rutas se aceptan.
- La recepción de rutas RIP no está desactivada.

Una vez desactivada la política global de recepción de filtros de rutas RIP, las interfaces RIP dejan de verse afectadas por dicha política.

El mandato **disable receiving policy interface** *nombre-interfaz-ip* desactiva el uso de la política de filtros de rutas para la interfaz especificada.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**receiving rip** *dirección-interfaz-ip*

Evita que RIP procese las actualizaciones RIP recibidas en la interfaz *dirección-interfaz-ip*

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `disable receiving rip 128.185.123.22`

**receiving dynamic all/hosts/nets/subnets** *dirección-interfaz-ip*

El mandato **disable receiving dynamic nets** asegura que, para las actualizaciones RIP recibidas en la interfaz *dirección-interfaz-ip*, el direccionador acepta únicamente las rutas a nivel de red entradas mediante el mandato **add accept-rip-route**. El mandato **disable receiving dynamic subnets** genera el comportamiento análogo para rutas de subred. El mandato **disable receiving dynamic host** genera el comportamiento análogo para rutas de sistema principal.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `disable receiving dynamic nets 128.185.123.22`

**record-route**

Hace que el direccionador deje de recibir y reenviar paquetes IP que contienen una opción IP de ruta de registro. Por omisión, el direccionador recibe y reenvía este tipo de paquetes.

**rip** Desactiva el protocolo RIP.

**Ejemplo:** `disable rip`

**rip2** Desactiva RIP2 en una interfaz IP en la que se había activado previamente.

**dirección-interfaz-ip**

Indica la interfaz IP en la que RIP2 está desactivado.

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `disable rip2 128.185.123.22`

**route-table-filtering**

Desactiva la aplicación de filtros de tabla de rutas cuando se añaden rutas a la tabla de direccionamiento.

**Ejemplo:** `disable route-table-filtering`

**same-subnet**

Desactiva la opción de misma subred. Cuando se vuelve a arrancar el direccionador, no permitirá que se instalen varias interfaces IP en la misma subred. Es el valor por omisión.

**Ejemplo:** `disable same-subnet`

**sending policy global/interface** *dirección-interfaz-ip*

Desactiva el uso de la política de filtro de rutas para determinar qué rutas va a anunciar RIP. El mandato **disable sending policy global** desactiva el uso de la política global de envío de filtro de rutas para todas las interfaces RIP que cumplen estas dos condiciones:

- No tienen configurada ninguna política de filtro de rutas de envío RIP a nivel de interfaz. Si se ha configurado una política de filtro de

rutas de envío RIP a nivel de interfaz, esta política continúa determinando qué rutas se anuncian.

- El envío de rutas RIP no está desactivado.

Una vez desactivada la política global de rutas de envío RIP, las interfaces RIP dejan de verse afectadas por dicha política.

El mandato **disable sending policy interface** *nombre-interfaz-ip* desactiva el uso de la política de filtros de rutas en la interfaz especificada.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**sending all/default/host/net/poisoned/static/subnet** *dirección-interfaz-ip*

Hace que el direccionador deje de anunciar el tipo especificado de ruta en actualizaciones RIP enviadas mediante la interfaz nombre-interfaz-ip. Los otros distintivos que controlan las rutas RIP enviadas por una interfaz son **host-routes**, **static-routes**, **net-routes** y **subnet-routes**. Puede desactivarlos de forma individual. Una ruta se anuncia si se ha especificado mediante uno de los distintivos activados.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `disable sending net-routes 128.185.123.22`

**sending rip-routes-only** *dirección-interfaz-ip*

Deja de anunciar únicamente rutas RIP en paquetes de difusión múltiple RIP2.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida de una interfaz que tenga activado RIP2.

**Valor por omisión**: ninguno

**Ejemplo:** `disable sending rip1-routes-only 128.185.123.22`

**sending outage-only** *dirección-ip-interfaz*

Desactiva el envío del contingente de actualizaciones RIP en presencia de la ruta especificada en el mandato de activación análogo. Cuando esta función está desactivada, los anuncios RIP se envían incondicionalmente.

**dirección-ip-interfaz**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `disable sending outage-only`

**simple-internet-access**

Esta opción desactiva el acceso sencillo a Internet en la interfaz especificada.

**source-addr-verification**

Esta opción de filtro de paquetes de entrada comprueba que la dirección IP de origen del paquete recibido es coherente, según la tabla de direccionamiento IP, con la interfaz de la que procede. Esta opción

ayuda a evitar el reenvío de paquetes procedentes de un sistema principal IP que está utilizando una dirección IP de origen que no le pertenece, una técnica denominada *simulación*. Este mandato sólo es válido en la consola de configuración de filtro de paquetes (a la que se accede mediante el mandato **update packet-filter**).

**source-routing**
Evita que el direccionador reenvíe paquetes direccionados de origen (es decir, paquetes IP que incluyen una opción de direccionamiento de origen). El valor por omisión es que el direccionamiento de origen esté activado.

**Ejemplo:** `disable source-routing`

**tftp-server**
Evita que el direccionador acepte solicitudes GET o PUT de TFTP procedentes de la red. Esto evita que se recubran por equivocación archivos de configuración o imágenes de carga procedentes de otro dispositivo. Puede realizar operaciones de cliente TFTP (GET y PUT) desde el direccionador a través de un terminal conectado directamente o de una sesión telnet.

**timestamp**
Hace que el direccionador deje de recibir o reenviar paquetes IP que contienen una opción IP de indicación horaria. Por omisión, el direccionador recibe y reenvía este tipo de paquetes.

**trace** *número-regla*
Desactiva el rastreo de paquetes IP que coinciden con el número de regla de control de acceso especificado. Por omisión, esta opción está desactivada. Para obtener más información sobre el rastreo de paquetes IP, consulte el mandato **enable trace**.

**Ejemplo:** `disable trace 1`

**udp-forwarding** *número-puerto*
Desactiva el reenvío UDP correspondiente a paquetes recibidos por el direccionador con el número de puerto de destino UDP especificado.

Valor por omisión: el reenvío UDP está desactivado para todos los números de puertos.

**número-puerto**
**Valores válidos**: un entero comprendido entre 0 y 65535

**Valor por omisión**: 0

**Ejemplo:** `disable udp-forwarding 36`

**vrrp** Desactiva el Protocolo virtual de redundancia del direccionador.

**Ejemplo:** `disable vrrp`

## Enable

Utilice el mandato **enable** para activar características, posibilidades e información de IP añadida a la configuración IP.

**Sintaxis:**

en**able** arp-net-routing

arp-subnet-routing

bootp-forwarding

classless

directed-broadcast

dynamic-address

echo-reply

fragment-offset-check

icmp-redirect

nexthop-awareness

override default ...

override static-routes ...

packet-filter

per-packet-multipath

receiving policy . . .

receiving rip ...

receiving dynamic all ...

receiving dynamic hosts...

receiving dynamic nets ...

receiving dynamic subnets ...

record-route

rip

rip2

route-table-filtering

same-subnet

sending all-routes ...

sending default-routes ...

sending host-routes ...

sending net-routes ...

sending outage-only . . .

sending poisoned-reverse-routes

sending policy . . .

sending rip1-routes-only

sending static-routes ...

sending subnet-routes ...

simple-internet-access

source-addr-verification

source-routing

tftp-server

timestamp

trace

udp-forwarding ...

vrrp ...

**arp-net-routing**

Activa el direccionamiento de red ARP. Cuando está activado, el direccionador responde mediante proxy a todas las solicitudes ARP correspondientes a destinos remotos a los que se llega mejor a través del direccionador. Utilice este mandato si hay sistemas principales en la LAN que envían solicitudes ARP a todos los destinos, en lugar de hacerlo únicamente (como es lo adecuado) a destinos locales.

**Ejemplo:** `enable arp-net-routing`

**arp-subnet-routing**

Activa la función de direccionamiento de subredes ARP (también denominada ARP proxy) del direccionador. Esta función se utiliza cuando hay sistemas principales que no conocen la existencia de subredes conectadas a subredes IP conectadas directamente. La subred conectada directamente que tiene sistemas principales que no reconocen las subredes debe utilizar ARP para que esta característica sea útil.

El direccionamiento de subred ARP funciona del siguiente modo. Cuando un sistema principal que no reconoce subredes desea enviar un paquete IP a un destino de una subred remota, no se da cuenta que debería enviar el paquete a un direccionador. Por lo tanto, el sistema principal que no reconoce subredes sencillamente realiza una difusión general de una petición ARP. El direccionador recibe esta petición ARP. El direccionador responde como destino (es decir, proxy de nombres) si el direccionamiento de subredes ARP está activado y el siguiente salto al destino se realiza sobre una interfaz distinta de la interfaz que recibe la petición ARP.

Si en la LAN no hay ningún sistema principal que “no dé soporte a subredes,” no active el direccionamiento de subredes ARP. Si se necesita el direccionamiento de subredes ARP en una LAN, se debe activar en todos los direccionadores de dicha LAN.

**Ejemplo:** `enable arp-subnet-routing`

**bootp-forwarding**

Activa el reenvío de paquetes BOOTP/DHCP. Para poder utilizar el reenvío BOOTP, también debe añadir uno o más servidores BOOTP con el mandato **add bootp-server**.

**Ejemplo:** `enable bootp-forwarding`

```
Maximum number of forwarding hops [4]?
Minimum seconds before forwarding [0]?
```

**Maximum number of forwarding hops**

Número máximo de agentes BOOTP que pueden reenviar una petición BOOTP del cliente al servidor (no es el número máximo de saltos IP al servidor).

**Valor por omisión: 4**

**Minimum seconds before forwarding**

Generalmente este parámetro no se utiliza. Utilice este parámetro cuando exista una vía de acceso redundante entre el cliente y el servidor y desee utilizar la vía o vías de acceso secundarias como vías de acceso en espera.

**Valor por omisión**: 0

**classless** Indica que el direccionador va a funcionar en un entorno de direccionamiento IP sin clases. El IBM 2210 da soporte completo al direccionamiento CIDR, tal como se describe en RFC 1817, sin que esta opción esté activada. Al activar esta opción, evita la generación automática de rutas de red naturales (por ejemplo, rutas de red de Clase A, B o C ) correspondientes a rutas añadidas a la tabla de rutas IP. Si no ejecuta RIPv1 no necesita la ruta de red natural.

**Ejemplo:** `enable classless`

**directed-broadcast**

Activa el reenvío de paquetes IP cuyos destinos son una dirección dirigida por red o una dirección de difusión general dirigida por subred. El sistema principal de origen origina el paquete como una difusión individual y a continuación se reenvía como una difusión individual a una subred de destino y se “divide” en una difusión general. Estos paquetes sirven para localizar servidores de la red. Este mandato activa el reenvío y la división de difusiones generales dirigidas. El distribuidor de paquetes IP nunca reenvía difusiones generales/difusiones múltiples a nivel de enlace, a no ser que correspondan a direcciones IP de Clase D. (Consulte el mandato **enable multicast-routing** de OSPF.) El valor por omisión es que esta característica esté activada.

**Nota:** El reenvío y la división no se pueden implantar por separado. Además, el direccionador no reenviará difusiones generales IP a todas las subredes.

**Ejemplo:** `enable directed-broadcast`

**dynamic-address** *0.0.0.n*

En la interfaz de red PPP especificada, hace que el direccionador aprenda su dirección IP del nodo remoto de dicha interfaz de red. Por omisión, esta opción está desactivada.

Esta opción sólo es válida en una interfaz de red configurada como una interfaz de línea serie no numerada (la dirección IP asignada a la interfaz de red mediante el mandato **add address** es *0.0.0.n*, donde *n* es el número de interfaz de red).

**Nota:** Para que el direccionador aprenda su dirección IP del nodo remoto, además de activar este opción tiene que configurar IPCP en la red PPP para que solicite una dirección IP del nodo remoto.

**Ejemplo:**

```
Config>network 1
Point-to-Point user configuration
PPP 1 Config>set ipcp
IP COMPRESSION [no]:
Request an IP address [no]: yes
Interface remote IP address to offer if requested (0.0.0.0 for none) [0.0.0.0]?
PPP 1 Config>exit
Config>protocol ip
Internet protocol user configuration
IP config>add address
Which net is this address for? [0]? 1
New address []? 0.0.0.1
Address mask [0.0.0.0]?
IP config>enable dynamic-address
Interface address []? 0.0.0.1
IP config>
```

**echo-reply**

Activa la creación y envío de una respuesta a ecos ICMP como respuesta a una petición de eco ICMP.

**Ejemplo: `enable echo-reply`**

**fragment-offset-check**

Activa la comprobación del desplazamiento de fragmentos de los paquetes IP recibidos cuyo número de protocolo IP es 6 (es decir, TCP). Los paquetes con un desplazamiento de fragmento igual a 1 se eliminan. Por omisión, esta comprobación está desactivada.

**Nota:** Una vez activada, esta función se puede utilizar sin que afecte a ninguna otra función de IP. Consulte el mandato **reset IP** de talk 5 para obtener más información.

**icmp-redirect** *dirección-interfaz-ip*

Hace que el direccionador envíe mensajes de redirección ICMP en la interfaz IP especificada. Si no entra ningún valor cuando se le solicite la dirección de la interfaz IP, el direccionador enviará mensajes de redirección ICMP en todas las interfaces IP.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida, o nada para todas las interfaces

**Valor por omisión**: ninguno

**Ejemplo:**

```
IP config> enable icmp-redirect
Interface address (NULL for all) []? 192.9.200.44
IP config>
```

**nexthop-awareness** *dirección-interfaz-ip*

Activa el aviso del siguiente salto en una interfaz IP.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: desactivado

**Ejemplo:**

```
IP config>enable nexthop-awareness 1.1.1.1
IP config>enable nexthop-awareness
Interface address []? 2.2.2.2
IP config>
```

**override default** *dirección-interfaz-ip*

Activa el hecho de que la información RIP recibida altere temporalmente cualquier ruta por omisión instalada en la tabla de direccionamiento IP. Este mandato se invoca por interfaz IP. Cuando se invoca el mandato **enable override default**, las rutas RIP por omisión recibidas en la dirección-interfaz-ip de la interfaz alteran temporalmente la ruta actual por omisión del direccionador, suponiendo que el coste del nuevo valor por omisión sea menor.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `enable override default 128.185.123.22`

**override static-routes** *dirección-interfaz-ip*

Activa el hecho de que la información RIP recibida altere temporalmente parte de la información de direccionamiento configurada de forma estática del direccionador. Este mandato se invoca por interfaz IP. Cuando se invoca el mandato **enable override static-routes**, la información de direccionamiento RIP recibida en la dirección-interfaz-ip de la interfaz se graba sobre las rutas de red/subred configuradas de forma estática, suponiendo que el coste de la información RIP sea menor.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `enable override static-routes 128.185.123.22`

**packet-filter** *nombre-filtro*

Activa la lista de control de acceso (filtros de paquetes) específica de la interfaz especificada.

**nombre-filtro**

**Valores válidos**: cualquier nombre de 16 caracteres. En el nombre puede incluir guiones (-) y símbolos de subrayado (_).

**Valor por omisión**: ninguno

**Ejemplo:** `enable packet-filter pf-in-0`

**per-packet-multipath**

Si per-packet-multipath está activado y hay varias vías de acceso al destino con el mismo coste, el direccionador equilibra la carga entre vías de acceso de igual coste para cada paquete de forma rotatoria. El valor por omisión es que esta característica esté desactivada.

**Ejemplo:** `enable per-packet-multipath`

**receiving policy global/interface** *dirección-interfaz-ip identificador-política-rutas*

Activa el uso de la política de filtro de rutas para determinar las rutas que acepta el RIP. El mandato **enable receiving policy global** *identificador-política-rutas* activa el uso de la política de recepción global de filtro de rutas para las interfaces RIP que cumplen estas dos condiciones:

- No tienen configurada ninguna política de filtro de rutas de recepción RIP a nivel de interfaz. Si se ha configurado una política de

filtro de rutas de recepción RIP a nivel de interfaz, esta política continúa determinando qué rutas se aceptan.

- La recepción de rutas RIP no está desactivada.

Una vez activada la política global de recepción de filtro de rutas, las interfaces RIP que cumplen estas condiciones aceptarán rutas según define la política.

El mandato **enable receiving policy interface** *dirección-interfaz-ip identificador-política-rutas* activa el uso de la política de filtro de rutas para determinar qué rutas se aceptan en una interfaz RIP especificada. Tenga en cuenta que las redes, subredes y sistemas principales dinámicos no se aplican si se ha activado la política de recepción global o de interfaz.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**identificador-política-rutas**

**Valores válidos**: un identificador de política de rutas válido que conste de una serie de entre 1 y 15 caracteres ASCII

**Valor por omisión**: ninguno

**receiving rip** *dirección-interfaz-ip*

Activa el proceso de actualizaciones RIP que se reciben en una determinada interfaz. Este mandato tiene un mandato análogo de desactivación. (Consulte el mandato **disable receiving**.) Por omisión, este mandato está activado.

Si invoca el mandato **disable receiving rip**, no se aceptará ninguna actualización RIP en la dirección de interfaz *dirección-interfaz-ip*.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `enable receiving rip 128.185.123.22`

**receiving dynamic nets** *dirección-interfaz-ip*

Modifica el proceso de actualizaciones RIP que se reciben en una determinada interfaz. Este mandato tiene un mandato análogo de desactivación. (Consulte el mandato **disable receiving**.) Por omisión, este mandato está activado.

Si invoca el mandato **disable receiving dynamic nets**, para las actualizaciones RIP recibidas en la interfaz *dirección-interfaz-ip*, el direccionador no aceptará ninguna ruta a nivel de red a no ser que se hayan especificado en un mandato **add accept-rip-route**.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `enable receiving dynamic nets 128.185.123.22`

**receiving dynamic subnets** *dirección-interfaz-ip*

Modifica el proceso de actualizaciones RIP que se reciben en una determinada interfaz. Este mandato tiene un mandato análogo de des-

activación. (Consulte el mandato **disable receiving**.) Por omisión, este mandato está activado.

Si invoca el mandato **disable receiving dynamic subnets**, para las actualizaciones RIP recibidas en la interfaz *dirección-interfaz-ip*, el direccionador no aceptará ninguna ruta a nivel de subred a no ser que se hayan especificado en un mandato **add accept-rip-route**.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `enable receiving dynamic subnets 128.185.123.22`

**record-route**

Permite al direccionador recibir y reenviar paquetes IP que contienen una opción IP de ruta de registro. Es el valor por omisión.

**Nota:** Una vez activada, esta función se puede utilizar sin que afecte a ninguna otra función de IP. Consulte el mandato **reset IP** de talk 5 para obtener más información.

**rip** Activa el proceso de protocolos RIP del direccionador.

Cuando RIP está activado, se establece el siguiente comportamiento por omisión:

- El direccionador incluye todas las rutas de red y subred en actualizaciones de RIP que se envían a cada una de sus interfaces IP configuradas.
- El direccionador procesa todas las actualizaciones RIP recibidas en cada una de sus interfaces IP configuradas.

Para cambiar alguno de los comportamientos de envío o recepción por omisión, utilice los mandatos de configuración de IP, que se definen por interfaz IP.

**Ejemplo:** `enable rip`

**rip2** *dirección-interfaz-ip autentificación-RIP2 claves-autentificación*

Activa RIP2 en una interfaz IP. Los anuncios RIP2 se envían a la dirección de difusión múltiple 224.0.0.9. RIP2 se describe en RFC 1723.

**dirección-interfaz-ip**

Indica la interfaz IP en la que está activado RIP2.**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**autentificación-RIP2**

Indica se se utilizará o no una sola clave de borrar texto para la autentificación RIP2. La autentificación no es obligatoria.**Valores válidos**: yes o no

**Valor por omisión**: yes

**clave-autentificación**

Define una contraseña de borrar texto que se utilizará para la autentificación RIP2. Sólo se le solicitará esta serie cuando responda **yes** a la pregunta “Definir autentificación RIP-2?” Cuando se utiliza la autentificación RIP2, sólo se aceptan los paquetes RIP2 con una contraseña que coincida.**Valores válidos**: una serie ASCII para borrar texto

**Valor por omisión**: una serie nula

**Ejemplo:**

```
IP config>enable rip2
Set for which interface address [0.0.0.0]? 153.2.2.25
RIP2 is enabled on this interface.
Set RIP-2 Authentication? [Yes]: yes
Authentication Key []? C1C3C5C5
Retype Auth. Key []? C1C3C5C5
RIP2 Authentication is enabled on this interface.
```

**route-table-filtering**

Aplica filtros de tabla de rutas a cualquier ruta añadida a la tabla de direccionamiento. Los filtros de tabla de rutas se aplican en función de una coincidencia más específica del destino y la nueva máscara. Los filtros de tabla de rutas nunca se aplican a rutas directas o rutas estáticas.

**Ejemplo:** `enable route-table-filtering`

**same-subnet**

Activa la opción de misma subred. Cuando se vuelve a arrancar el dispositivo, permitirá que se instalen varias interfaces IP en la misma subred. Tener varias interfaces IP en la misma subred sólo resulta útil bajo las siguientes condiciones:

- Se ha configurado OSPF punto a multipunto en las interfaces IP.
- Nexthop Awareness está activado en las interfaces IP y se han definido rutas estáticas para los direccionadores que van a través de las interfaces IP.

Por omisión, esta opción está desactivada.

**Ejemplo:** `enable same-subnet`

**sending default-routes** *dirección-interfaz-ip*

Determina el contenido de actualizaciones RIP que se envían a una determinada interfaz. Este mandato tiene un mandato análogo de desactivación. (Consulte el mandato **disable sending**.) El efecto del mandato **enable sending** es acumulativo. Cada mandato enable sending especifica que se deben anunciar ciertas rutas procedentes de una determinada interfaz. Una ruta se incluye en una actualización RIP únicamente si la ha incluido al menos uno de los mandatos enable sending. El mandato **enable sending default-routes** especifica que se debe incluir la ruta por omisión (si existe) en las actualizaciones RIP enviadas a la interfaz dirección-interfaz-ip.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `enable sending default-routes 128.185.123.22`

**Nota:** Por omisión, RIP envía rutas de red, de subred y estáticas.

**sending net-routes** *dirección-interfaz-ip*

Determina el contenido de actualizaciones RIP que se envían a una determinada interfaz. Este mandato tiene un mandato análogo de desactivación. (Consulte el mandato **disable sending**.)

El efecto del mandato **enable sending** es acumulativo. Cada mandato **enable sending** especifica que se deben anunciar ciertas rutas procedentes de una interfaz determinada. Una ruta se incluye en una actualización RIP únicamente si la ha incluido al menos uno de los mandatos **enable sending**. El mandato **enable sending network-routes** especifica que todas las rutas a nivel de red se deben incluir en actualizaciones RIP enviadas a la interfaz *dirección-interfaz-ip*. Una ruta a nivel de red es una ruta a una sola red IP de clase A, B o C.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `enable sending net-routes 128.185.123.22`

**sending outage-only** *dirección-ip-interfaz red-corte máscara-red-corte*

Activa el envío de paquetes de actualización RIP en la interfaz especificada por el contingente *dirección-ip-interfaz* en presencia de la ruta IP especificada por *red-corte* y *máscara-red-corte*. Normalmente, las actualizaciones se envían incondicionalmente a las interfaces configuradas para anunciar rutas RIP. Además, las actualizaciones RIP se pasan por alto en una interfaz sólo de corte cuando está presente la ruta especificada. Esta función resulta útil en escenarios de reserva en los que el circuito de marcación de reserva está configurado como un circuito de Marcación bajo demanda.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**red-corte** **Valores válidos:** cualquier dirección IP válida

**Valor por omisión:** ninguno

**máscara-red-corte**

**Valores válidos:** cualquier máscara IP válida

**Valor por omisión:** ninguno

**Ejemplo:** `enable sending outage-only`

```
IP config>enable sending outage-only
Set for which interface address [0.0.0.0]? 0.0.0.2
Outage network []? 10.50.0.0
Outage network mask []? 255.255.0.0
```

En este ejemplo, los anuncios RIP no se enviarán a la interfaz no numerada cuando no aparezca la ruta 10.50.0.0/255.255.0.0 en la tabla de direccionamiento.

**sending poisoned-reverse-routes** *dirección-interfaz-ip*

Una técnica que utiliza RIP para mejorar el tiempo de convergencia cuando cambian las rutas (para obtener más información sobre esta

técnica, consulte RFC 1058). La utilización de esta técnica aumenta el tamaño de los mensajes de actualización RIP. Puede que le convenga más minimizar la actividad general de direccionamiento aceptando una convergencia más lenta. El mandato **disable sending poisoned-reverse-routes** especifica que las rutas inversas prohibidas no se deben incluir en las actualizaciones RIP enviadas a una interfaz especificada en el mandato **enable ip-interface-address**.

Valor por omisión: activado

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**sending policy global/interface** *dirección-interfaz-ip identificador-política-rutas*

Activa el uso de la política de filtro de rutas para determinar las rutas que anuncia el RIP. El mandato **enable sending policy global** *identificador-política-rutas* activa el uso de la política global de envío de filtro de rutas para las interfaces RIP que cumplen estas dos condiciones:

- No tienen configurada ninguna política de envío de RIP a nivel de interfaz. Si se ha configurado una política de envío de RIP a nivel de interfaz, continúa determinando qué rutas se anuncian.
- El envío de rutas RIP no está desactivado.

Una vez activada la política global de envío de filtro de rutas, las interfaces RIP que cumplen estas dos condiciones anunciarán rutas según lo determinado en la política global de envío de filtro de rutas.

El mandato **enable sending policy interface** *dirección-interfaz-ip identificador-política-rutas* activa el uso de la política de filtro de rutas para determinar qué rutas se anuncian en la interfaz RIP especificada.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**identificador-política-rutas**

**Valores válidos**: un identificador de política de rutas válido que conste de una serie de entre 1 y 15 caracteres ASCII

**Valor por omisión**: ninguno

**sending rip-routes-only** *dirección-interfaz-ip*

Para anunciar únicamente rutas RIP en paquetes de difusión múltiple RIP2.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida de una interfaz que tenga activado RIP2.

**Valor por omisión**: ninguno

**Ejemplo:** `enable sending rip-routes-only 128.185.123.22`

**sending subnet-routes** *dirección-interfaz-ip*

Determina el contenido de actualizaciones RIP que se envían a una determinada interfaz. Este mandato tiene un mandato análogo de desactivación. (Consulte el mandato **disable sending**.) El efecto del

mandato **enable sending** es acumulativo. Cada mandato **enable sending** especifica que se deben anunciar ciertas rutas procedentes de una determinada interfaz. Una ruta se incluye en una actualización RIP únicamente si la ha incluido al menos uno de los mandatos enable sending. El mandato **enable sending subnet-routes** especifica que todas las rutas a nivel de subred se deben incluir en actualizaciones RIP enviadas a la interfaz dirección-interfaz-ip. Sin embargo, una ruta de subred se incluye únicamente si la dirección-interfaz-ip está directamente conectada a una subred de la misma red con subredes IP.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `enable sending subnet-routes 128.185.123.22`

**sending static-routes** *dirección-interfaz-ip*

Determina el contenido de actualizaciones RIP que se envían a una determinada interfaz. Este mandato tiene un mandato análogo de desactivación. (Consulte el mandato **disable sending**.) El efecto del mandato **enable sending** es acumulativo. Cada mandato **enable sending** especifica que se deben anunciar ciertas rutas que cumplen otros criterios de envío a una determinada interfaz. Una ruta se incluye en una actualización RIP únicamente si la ha incluido al menos uno de los mandatos **enable sending**. El mandato **enable sending static-routes** especifica que todas las rutas configuradas de forma estática y conectadas directamente se deben incluir en actualizaciones RIP enviadas a la interfaz *dirección-interfaz-ip*.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `enable sending static-routes 128.185.123.22`

**sending host-routes** *dirección-interfaz-ip*

Determina el contenido de actualizaciones RIP que se envían a una determinada interfaz. Este mandato tiene un mandato **disable ...** análogo. (Consulte el mandato **disable sending**.) El efecto del mandato **enable sending** es acumulativo. Cada mandato **enable sending** especifica que se deben anunciar ciertas rutas procedentes de una determinada interfaz. Una ruta se incluye en una actualización RIP únicamente si la ha incluido al menos uno de los mandatos **enable sending**. El mandato **enable sending host-routes** especifica que todas las rutas de sistema principal se deben incluir en actualizaciones RIP enviadas a la interfaz dirección-interfaz-ip.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**simple-internet-access**

Esta opción activa el acceso sencillo a Internet en la interfaz especificada. Utilice el Acceso sencillo a Internet para crear una configuración integrada que incluya una línea serie no numerada con la opción Dirección dinámica activada, Filtros de paquetes IP (de entrada y de salida), Controles de acceso IP (de entrada y de salida), una Ruta por omisión,

una agrupación de reserva NAT/NAPT dinámica y una subred de direcciones privadas en la característica DHCP. Los usuarios con requisitos adicionales para la configuración integrada listada deben tener en cuenta la posibilidad de llevar a cabo una configuración manual.

**Nota:** Esta opción sólo está disponible en imágenes que incluyan la DHCP y la característica NAT.

**source-addr-verification**

Esta opción de filtro de paquetes de entrada comprueba que la dirección IP de origen del paquete recibido es coherente, según la tabla de direccionamiento IP, con la interfaz de la que procede. Esta opción ayuda a evitar el reenvío de paquetes procedentes de un sistema principal IP que está utilizando una dirección IP de origen que no le pertenece, una técnica denominada *simulación*. Este mandato sólo es válido en la consola de configuración de filtro de paquetes (a la que se accede mediante el mandato **update packet-filter**).

**source-routing**

Permite al direccionador reenviar paquetes IP que contienen una opción de direccionamiento de origen IP.

**Ejemplo:** `enable source-routing`

**tftp-server**

Permite al direccionador aceptar peticiones GET o PUT de TFTP procedentes de la red para archivos de configuración o cargas de imágenes.

**Ejemplo:** `enable tftp-server`

**timestamp**

Permite al direccionador recibir y reenviar paquetes IP que contienen una opción IP de indicación horaria. Es el valor por omisión.

**Nota:** Una vez activada, esta función se puede utilizar sin que afecte a ninguna otra función de IP. Consulte el mandato **reset IP** de talk 5 para obtener más información.

**trace** *número-regla*

Activa el rastreo de paquetes IP que coinciden con el número de regla de control de acceso especificado. Por omisión, esta opción está desactivada.

El rastreo de paquetes IP utiliza la función de rastreo de paquetes del Sistema de registro cronológico de sucesos. Consulte los mandatos **set trace** y **view** en el capítulo Configuring and Monitoring the Event Logging System (ELS) del manual *Guía del usuario de software* para obtener más información sobre estos mandatos. Sólo se lleva a cabo un rastreo de los paquetes IP que coinciden con una regla de control de acceso para la que está activado el rastreo. La regla de control de acceso puede estar en la lista global de control de acceso o en una lista de control de acceso de filtro de paquetes. Utilice el mandato **list access-control** para ver las reglas para las que está activado el rastreo.

**Ejemplo: Tracing all IP Packets**

```
IP config>set access-control on
IP config>add access-control
Access Control type [E]? i
Internet source [0.0.0.0]?
Source mask [0.0.0.0]?
Internet destination [0.0.0.0]?
Destination mask [0.0.0.0]?
Starting protocol number ([0] for all protocols) [0]?
Starting DESTINATION port number ([0] for all ports) [0]?
Starting SOURCE port number ([0] for all ports) [0]?
Filter on ICMP Type ([-1] for all types) [-1]?
TOS/Precedence filter mask (00-FF - [0] for none) [0]?
TOS/Precedence modification mask (00-FF - [0] for none) [0]?
Use policy-based routing? [No]:
Enable logging? [No]:
IP config>list access-control
Access Control is: enabled
Access Control facility: USER

List of access control records:

1   Type=I    Source=0.0.0.0          Dest  =0.0.0.0          Prot=  0-255
              SMask =0.0.0.0          DMask =0.0.0.0
              SPorts=    0-65535      DPorts=    0-65535
                     T/C= **/**      Log=N
IP config>enable trace
Index of access control to be traced [1]?
IP config> Ctrl-P
*talk 5
+protocol ip
IP>reset ip
IP>exit
+event
Event Logging System user console
ELS>set trace memory-trace-buffer-size
Amount of memory (in bytes) reserved for tracing [0]? 10000
ELS>set trace on
ELS>set trace decode on
ELS>view first
#1 Dir:INCOMING  Time:0.5.47.53  Trap:450
Comp:IPV4  Type:UNKNOWN  Port:65535  Circuit:0x000000  Size:64

** IPv4 Packet **
Ver/Hdr Len/TOS:           4 20 0x00
Packet Length/ID:          64 0x9E4E
Fragment Offset:           0x0000
TTL/Protocol/Hdr Chksum:   1 OSPF  0xA89D
Source Addr/Dest Addr:     10.0.10.106 224.0.0.5

** OSPF Header **
Version:                   2
Packet type:               Hello
Packet length:             44
Router ID:                 10.0.0.106
Area ID:                   0.0.0.0
Checksum:                  0xDDB5
Authentication type:       0
Authentication:            0x00000000
Authentication:            0x00000000
Network mask:              255.255.255.0
Hello interval:            10
Options:                   E-bit
Options:                   MC-bit
Router priority:           1
Router dead interval:      40
Designated router:         10.0.10.106
Backup Designated router:  0.0.0.0
ELS>
```

**udp-forwarding** *número-puerto*

Activa el reenvío UDP correspondiente a paquetes recibidos por el direccionador con el número de puerto de destino UDP especificado.

Valor por omisión: el reenvío UDP está desactivado para todos los números de puertos.

**número-puerto**

**Valores válidos**: un entero comprendido entre 0 y 65535

**Valor por omisión**: 0

**Ejemplo:** `enable udp-forwarding 36`

**vrrp** Activa el Protocolo virtual de redundancia del direccionador

**Ejemplo:** `enable vrrp`

## List

Utilice el mandato **list** para visualizar distintas partes de los datos de configuración de IP, según el submandato que invoque.

**Sintaxis:**

**list**

all
access-control
addresses
bootp
filters
icmp-redirect
igmp
mtu
nexthop-awareness
packet-filter
parameters
protocols
redundant-default-gateway
rip
route-policy
route-table-filtering
routes
simple-internet-access
sizes
tags
udp-forwarding
vrid

**all** Muestra toda la configuración de IP.

**Ejemplo:** `list all`

**access-control**

Muestra la modalidad configurada de control de acceso (activada o desactivada) y la lista de registros configurados de control de acceso global. Cada registro aparece listado con su número de registro. Este número de registro sirve para volver a ordenar la lista con el mandato **move access-control** de IP.

**Ejemplo: `list access-control`**

**addresses**

Muestra las direcciones de interfaces IP que se han asignado al direccionador, junto con sus formatos configurados de difusión general. La interfaz identificada mediante *BDG/0* es la interfaz de la conexión por puente.

**Ejemplo: `list addresses`**

**bootp** Indica si el reenvío BOOTP está activado o desactivado, así como la lista configurada de servidores BOOTP.

**Ejemplo: `list bootp`**

**filters** Lista las redes filtradas configuradas del direccionador.

**icmp-redirect**

Lista si el envío de mensajes de redireccionamiento ICMP está activado o desactivado en cada interfaz IP.

**igmp** Muestra la configuración de IGMP.

**Ejemplo:**

```
IP config>list igmp

Net          IGMP          Query          Response          Leave Query
            Version       Interval        Interval           Interval
                            (secs)          (secs)             (secs)
---         -------       --------        --------          -----------
   0            2             250             10                 1
   1            1             125             10                 1
   4            2             125             10                 2
   5            2             125             20                 1

IP config>
```

**mtu** Lista los valores MTU configurados.

**nexthop-awareness**

Lista el valor de aviso de siguiente salto en todas las interfaces IP.

**Ejemplo:**

```
IP config>list nexthop-awareness
Nexthop awareness for each IP interface address:
   intf  0   1.1.1.1          255.0.0.0        nexthop awareness enabled
   intf  1   2.2.2.2          255.0.0.0        nexthop awareness disabled
IP config>
```

**packet-filter** *nombre-filtro*

Lista información sobre filtros de paquetes. Si especifica un nombre, el mandato lista la información de control de acceso configurada para el filtro. Si no especifica ningún nombre de filtro, el mandato lista los filtros de paquetes configurados. Si tiene un filtro de paquete configurado en la interfaz de puente, la interfaz aparece identificada mediante *BDG/0*.

**Ejemplo: `list packet-filter pf-in-0`**

```
Name              Direction     Interface
pf-in-0           In            0

Access Control is: enabled

List of access control records:

1  Type=E    Source=128.185.0.0   Dest=0.0.0.0           Prot=0-255
             Mask=255.255.0.0     Mask=0.0.0.0
             Sports=  0-65535     Dports=  1-65535
             ACK0=N  T/C= **/**   Log=No

2  Type=IN   Source=10.1.1.1      Dest=10.1.1.2          Prot=0-255
             Mask=255.255.255.255 Mask=255.255.255.254
             Sports=  N/A         Dports=  N/A
                                  Log=Yes ELS=N SNMP=Y SLOG=L(Emergency)

3  Type=I    Source=0.0.0.0       Dest=0.0.0.0          Prot=0-255
             Mask=0.0.0.0         Mask=0.0.0.0
             Sports= 1-65535      Dports=  1-68835
                                  Log=No
             Trace=Enabled
```

**parameters**

Lista los distintos parámetros globales de IP.

**Ejemplo: `list parameters`**

```
IP config>list parameters
ARP-SUBNET-ROUTING    : enabled
ARP-NET-ROUTING       : enabled
CLASSLESS             : disabled
DIRECTED-BROADCAST    : enabled
DSCACHE-SIZE          : 1024 entries
 ECHO-REPLY            : enabled
FRAGMENT-OFFSET-CHECK : enabled
PER-PACKET-MULTIPATH  : disabled
REASSEMBLY-SIZE       : 12000 bytes
RECORD-ROUTE          : enabled
ROUTING TABLE-SIZE    : 768 entries (52224 bytes)
(Routing) CACHE-SIZE  : 64 entries
SAME-SUBNET           : disabled
SOURCE-ROUTING        : enabled
TIMESTAMP             : enabled
TTL                   : 64
```

**protocols**

Muestra el estado configurado de los protocolos de direccionamiento IP (OSPF, RIP, BGP) junto con otros valores generales de configuración.

**Ejemplo: `list protocols`**

**redundant-default-gateway**

Muestra la pasarela IP redundante por omisión para cada interfaz configurada.

**Ejemplo: `list redundant`**

```
Redundant Default IP Gateways for each interface:
   inf 4  11.1.1.6     255.0.0.0     00.00.00.00.00.BA  primary
   inf 8  33.3.3.6     255.0.0.0     00.00.00.00.00.AB  backup
```

**rip** Muestra todos los parámetros de configuración RIP. RIP se puede configurar para que reciba y envíe rutas dinámicas o se pueden definir rutas mediante una política de filtro de rutas. Consulte los mandatos de configuración de IP **enable receiving dynamic nets/subnets/hosts** para obtener más información sobre el direccionamiento dinámico. Consulte “Configuración de políticas de filtros de rutas” en la página 332 para obtener más información sobre las políticas de filtro de rutas.

**Ejemplo:**

```
IP config>list rip

RIP: enabled
RIP default origination: disabled
RIP global receive policy: rip-in

  Per-interface address flags:
  Net:     0  153.2.2.25       RIP Version 1
                               Send net, subnet and static routes
                               Receive routes based on global receive
                                    policy: rip-in
                               RIP interface input metric: 1
                               RIP interface output metric: 0
  Net:     1  153.2.1.1        RIP Version 1
                               Send net, subnet and static routes
                               Receive routes based on global receive
                                    policy: rip-in
                               RIP interface input metric: 1
                               RIP interface output metric: 0
  Net:     2  0.0.0.2          RIP Version 1
                               Send routes based on interface send
                                    policy: rip-import
                               Receive routes based on global receive
                                    policy: rip-in
                               RIP interface input metric: 1
                               RIP interface output metric: 0

Accept RIP updates always for:
[NONE]
```

**route-policy** *identificador-política-rutas*

Muestra información sobre las políticas de rutas configuradas. Si especifica una determinada política de rutas, aparecerá un listado detallado de dicha política de rutas. Si no especifica ninguna política de rutas, aparecerá un resumen de todas las políticas.

**Ejemplo:**

```
IP config>list route-policy
Route Policy Identifier [1-15 characters] [ ]?

 Route Policy        Checksum  Policy-Application
   ---------------------------------------------
 rip-send            0x8637      Longest-match
 rip-receive         0x5049      Longest-match
 rip-global-send     0xC9EA      Longest-match
```

**route-table-filtering**

Muestra la lista de los filtros de rutas añadidos al filtro de direccionamiento.

**Ejemplo: `list route-table-filtering`**

```
IP config>list route-table-filtering

Route Filtering Disabled

Destination     Mask           Match Type
10.1.1.0        255.255.255.0   BOTH  E
50.50.0.0       255.255.0.0     BOTH  I
10.1.1.1        255.255.255.255 EXACT I
50.0.0.0        255.0.0.0       BOTH  E

MORE-Match more-specific routes   EXACT-Match route exactly
BOTH-Match exact and more-specific routes  E-Exclude  I-Include
IP config>
```

**routes** Muestra la lista de las rutas estáticas configuradas.

**Ejemplo: `list routes`**

```
IP config>list routes

route to 1.1.0.0        ,255.255.0.0     via 10.1.1.1        cost 1
                                         via 20.1.1.1        cost 2
                                         via 30.1.1.1        cost 3
route to 2.2.0.0        ,255.255.0.0     via 10.2.2.2        cost 10
route to 3.3.0.0        ,255.255.0.0     via 10.3.3.3        cost 100
                                         via 20.3.3.3        cost 200
```

**simple-internet-access**
Muestra el número de interfaz de Acceso sencillo a Internet.

**sizes** Muestra el tamaño de la tabla de direccionamiento, el tamaño del almacenamiento intermedio de ensamblaje y el tamaño de la antememoria de rutas.

**Ejemplo: `list sizes`**

**tags** Muestra los distintivos por interfaz que se asociarán a la información RIP recibida. Estos distintivos sirven para agrupar rutas, para anunciarlas posteriormente mediante BGP, donde el distintivo se tratará como si fuera un sistema autónomo (AS) de origen del direccionador. Los distintivos también se propagan mediante el protocolo de direccionamiento OSPF.

**Ejemplo: `list tags`**

**udp-forwarding**
Muestra toda la información configurada correspondiente a la función de reenvío UDP, incluidos todos los puertos y todas las direcciones IP.

**Ejemplo: `list udp-forwarding`**

**vrid** Muestra el estado VRRP configurado, los VRID y las direcciones VRID.

**Ejemplo:**

```
IP config>list vrid

VRRP Enabled

                            --VRID Definitions--

IP address      VRID  Priority Interval Auth   Auth-key Flags Address(es)
153.2.2.25         1       255        1 None   N/A      P     5.1.1.1
```

## Move

Utilice el mandato **move** para cambiar el orden de los registros en la lista global de control de acceso. Este mandato coloca el registro número *de núm.* inmediatamente después del registro número *a núm.*. Después de mover los registros, se cambia automáticamente su número para reflejar el nuevo orden.

El direccionador aplica los registros de control de acceso de una lista en el orden en el que se han creado. Para cada paquete recibido en una interfaz, el direccionador aplica cada registro de control de acceso en su orden hasta que encuentra una coincidencia. El primer registro que coincide con el paquete determina si si eliminará o se reenviará a su destino.

Esto hace que el orden de los registros de control de acceso sea muy importante. Si están en el orden incorrecta, algunos paquetes pueden colarse o pueden bloquearse contrariamente a sus intenciones.

Supongamos, por ejemplo, que el registro 1 de control de acceso hace cumplir la regla: *todos los paquetes procedentes de la red 10.0.0.0 se deben bloquear en*

*esta interfaz.* Por el contrario, el registro 2 de control de acceso indica que: *Se debe dejar pasar a los paquetes procedentes de la subred 10.5.5.0 de la red 10.0.0.0, destinados a la dirección 1.2.3.4.* Asignados en este orden, estos registros bloquearán el tráfico procedente de 10.0.0.0, aunque el registro 2 permite de forma explícita que pasen determinados tipos de paquetes.

En este ejemplo, el registro 1 hace que el registro 2 sea discutible. El registro 1 garantiza que el direccionador eliminará todos los paquetes procedentes de 10.0.0.0, a pesar del objetivo del registro 2, que consiste en que ciertos paquetes se reenvíen. La clave para corregir este tipo de problema está en el orden de los registros de control de acceso. De este modo, los paquetes de la subred 10.5.5.0 y destinados a la dirección 1.2.3.4 pasarán a través de la interfaz; el direccionador elimina los demás paquetes procedentes de 10.0.0.0, lo cual constituye el objetivo.

**Sintaxis:**

m**ove** a**ccess-control** *de núm. a núm.*

**Ejemplo:** `move 5 2`

## Set

Utilice el mandato **set** para definir determinados valores, rutas y formatos dentro de la configuración de IP.

**Sintaxis:**

| | |
|---|---|
| s**et** | access-control... |
| | access-control log-facility |
| | broadcast-address... |
| | cache-size |
| | default network-gateway... |
| | default subnet-gateway... |
| | dscache-size |
| | igmp ... |
| | internal-ip-address |
| | mtu |
| | originate-rip-default |
| | reassembly-size |
| | rip-in-metric |
| | rip-out-metric |
| | router-id |
| | routing table-size |
| | tag . . . |
| | ttl |

**access-control** *on* **u** *off*

Le permite configurar el direccionador para que active o desactive el control de acceso IP. Si define para el control de acceso el valor *on*, se

activa la lista global de control de acceso así como las listas específicas de la interfaz. Si define el valor *off*, desactiva todas las listas pero no las suprime.

**Ejemplo:** `set access-control on`

**access-control log-facility** *recurso-registro*

Define el recurso SysLog para el control de acceso. La opción recurso SysLog define el sistema en el que se visualizarán los mensajes SysLog.

**Nota:** Una vez activada, esta función se puede utilizar sin que afecte a ninguna otra función de IP. Consulte el mandato **reset IP** de talk 5 para obtener más información.

**recurso-registro**

**Valores válidos**: KERN, USER, MAIL, DAEMON, AUTH, SYSLOG, LPR, NEWS, UUCP, CRON, AUTHPRIV, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7, USER

**Valor por omisión**: USER

**Ejemplo:**

```
IP config> set access-control log-facility
SYSLOG facility? (KERN, USER, MAIL, DAEMON, AUTH, SYSLOG, LPR,
NEWS, UUCP, CRON, AUTHPRIV, LOCAL0, LOCAL1, LOCAL2,
LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7) [USER]?
```

**broadcast-address** *dirección-interfaz-ip estilo patrón-relleno*

Especifica el formato de difusión general IP que utiliza el direccionador al realizar una difusión general de paquetes en una determinada interfaz. El direccionador utiliza con más frecuencia las difusiones generales IP al enviar paquetes de actualización RIP.

El parámetro estilo puede tener el valor local wire o el valor network. Las direcciones de difusión general de estilo local-wire son todo unos (255.255.255.255) o todo ceros (0.0.0.0). Las difusiones generales de estilo network comienzan on la parte de red y subred de la dirección-interfaz-ip.

Puede definir para el parámetro patrón-relleno los valores 1 ó 0. Esto indica si el valor del resto de la dirección de difusión general (es decir, la parte que queda sin contar las partes de red y subred, si la hay) debe ser todo unos o todo ceros.

En el momento de la recepción, el direccionador reconoce todos los formatos de la dirección de difusión general IP.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**estilo** **Valores válidos**: *local-wire* o *network*

**Valor por omisión**: local-wire

**patrón-relleno**

**Valores válidos**: *0* o *1*

**Valor por omisión**: 1

El ejemplo siguiente configura una dirección de difusión general de 255.255.255.255. El segundo ejemplo genera una dirección de difusión general de 192.9.1.0, suponiendo que la red 192.9.1.0 no tiene subredes.

**Ejemplo:** `set broadcast-address 192.9.1.11 local-wire 1 set broadcast-address 192.9.1.11 network 0`

**cache-size** *entradas*

Configura el número máximo de entradas para la antememoria de direccionamiento IP. Esta antememoria guarda información sobre las direcciones IP específicas a las que el direccionador ha reenviado paquetes. La antememoria reduce el tiempo de proceso necesario para reenviar varios paquetes al mismo destino.

Por el contrario, la *tabla* de direccionamiento IP guarda información sobre todas las redes a las que se puede acceder, pero no contiene direcciones específicas de destino IP. Utilice el mandato **set routing table-size** para configurar el tamaño de la tabla de direccionamiento IP.

**Valores válidos**: 64 a 10000

**Valor por omisión**: 64

**Ejemplo:** `set cache-size 64`

**default network-gateway** *siguiente-salto coste*

Configura una ruta al direccionador con autorización (pasarela por omisión). Debe dar por supuesto que la pasarela por omisión del direccionador tiene más información sobre direccionamiento que el propio direccionador.

La ruta se especifica mediante la dirección IP del siguiente salto (siguiente-salto) y la distancia (coste) a la pasarela por omisión.

Todos los paquetes que tienen destinos desconocidos se reenvían al direccionador con autorización (pasarela por omisión).

*siguiente-salto* **Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: 0.0.0.0 con un coste de pasarela de 1.

*coste* **Valores válidos**: un entero comprendido entre 0 y 255

**Valor por omisión**: 1

**Ejemplo:** `set default network-gateway 192.9.1.10 10`

**default subnet-gateway** *red-subredes siguiente-salto coste*

Configura una ruta a un direccionador con autorización de la red con subredes (pasarela de subred por omisión). Puede configurar una pasarela de subred por omisión para cada red con subredes.

La dirección IP del siguiente salto (siguiente-salto) y la distancia (coste) a la pasarela de subred por omisión especifican la ruta.

Todos los paquetes destinados a subredes desconocidas de una red con subredes conocida se reenvían al direccionador con autorización de la red con subredes (pasarela de subred por omisión).

*red-subredes*

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: 0.0.0.0

*siguiente-salto*

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: 0.0.0.0

*coste*

**Valores válidos**: un entero comprendido entre 0 y 255

**Valor por omisión**: 1

**Ejemplo:** `set default subnet-gateway 128.185.0.0 128.185.123.22 6`

**dscache-size** *entradas*
Configura el número de entradas a asignar para la antememoria de flujo DiffServ. La antememoria de flujo DiffServ se asigna si se cumple alguna de estas condiciones:

- La característica Differentiated Services (DiffServ o DS) está activada (consulte el tema Configuring and Monitoring the Differentiated Services Feature del manual *Utilización y configuración de las características* para obtener más información).
- La característica IP Security (IPSec) está activada (consulte el tema Configuring and Monitoring IP Security del manual *Utilización y configuración de las características* para obtener más información).
- La característica Policy está activada (consulte el tema Configuring and Monitoring the Policy Feature del manual *Utilización y configuración de las características* para obtener más información).

**Valores válidos**: 64 a 8192

**Valor por omisión**: 1024

**igmp...** Configura parámetros de Gestión de grupos de Internet (IGMP). Puede especificar valores para los siguientes parámetros:

qu**ery interval** *red intervalo*
Modifica el intervalo entre consultas generales IGMP.

**red** Especifica el número de red correspondiente a la interfaz que se está configurando.

**Valores válidos:** Cualquier número válido de red

**Valor por omisión:** Ninguno

**intervalo** Especifica el número de segundos entre las transmisiones de consultas generales.

**Valores válidos:** 1 - 3600

**Valor por omisión:** 125

re**sponse-interval** *red intervalo*
Modifica el tiempo máximo de respuesta insertado en las consultas generales IGMP.

**red** Especifica el número de red correspondiente a la interfaz que se está configurando.

**Valores válidos:** Cualquier número válido de red

**Valor por omisión:** Ninguno

**intervalo** Especifica el número de segundos entre las transmisiones entre una consulta y un envío de sistema principal de un Informe IGMP como respuesta.

**Valores válidos:** 1 - 60

**Valor por omisión:** 10

ro**bustness-variable** *red variable*

Modifica la variable de potencia correspondiente a una red.

**red** Especifica el número de red correspondiente a la interfaz que se está configurando.

**Valores válidos:** Cualquier número válido de red

**Valor por omisión:** Ninguno

**variable** Especifica el número de paquetes IGMP enviados para combatir la pérdida de paquetes en una red.

**Valores válidos:** 2 - 10

**Valor por omisión:** 2

le**ave-interval** *red intervalo*

Modifica el tiempo máximo de respuesta insertado en consultas específicas IGMP.

**red** Especifica el número de red correspondiente a la interfaz que se está configurando.

**Valores válidos:** Cualquier número válido de red

**Valor por omisión:** Ninguno

**intervalo** Especifica el número de segundos permitidos entre las transmisiones de consultas específicas y un envío del sistema principal de un Informe IGMP como respuesta.

**Valores válidos:** 1 - 60

**Valor por omisión:** 1

ve**rsion** *red númver*

Modifica la versión de IGMP que se ejecuta en una red.

**red** Especifica el número de red correspondiente a la interfaz que se está configurando.

**Valores válidos:** Cualquier número válido de red

**Valor por omisión:** Ninguno

**númver** Especifica el número de versión a ejecutar en la red.

**Valores válidos:** 1 ó 2

**Valor por omisión:** 2

**internal-ip-address** *dirección-ip*

Configura una dirección IP que no depende del estado de ninguna interfaz. La dirección interna siempre se considera activa. La principal razón para definir una dirección interna consiste en ofrecer una dirección para una conexión TCP que pasará a estar inactiva cuando una

interfaz pase a estar inactiva. Esta dirección se utiliza para la conmutación de enlace de datos (DLSw), permitiendo utilizar vías de acceso alternativas para evitar que se interrumpan las conexiones DLSw cuando una interfaz pase a estar inactiva. Puesto que la dirección interna permanece activa y puesto que OSPF mantiene rutas IP activas a este destino, el direccionamiento IP puede conmutar tráfico DLSw a la vía de acceso alternativa sin interrumpir la conexión TCP ni las sesiones SNA que se ejecutan sobre DLSw.

La dirección IP interna también ofrece algún valor cuando se utilizan interfaces sin numerar. Es la primera opción como dirección de origen para los paquetes originados por este direccionador y transmitidos sobre una interfaz sin numerar. La estabilidad de esta dirección facilita el seguimiento de este tipo de paquetes. Se reducen las posibilidades de confusión cuando se utiliza la misma dirección IP para el ID de direccionador y para la dirección interna. Por lo tanto, el valor por omisión del ID del direccionador será la dirección interna.

Cuando se define una dirección interna, OSPF la anunciará como ruta del sistema principal en todas las áreas conectadas directamente al direccionador. También aparecerá como una ruta del sistema principal y se anunciará en RIP si así lo permite la configuración de envío de RIP de la interfaz.

**Valores válidos**: cualquier dirección IP válida.

**Valor por omisión**: ninguno

**Ejemplo:** `set internal-ip-address 142.82.10.1`

**mtu** Define el valor MTU correspondiente al protocolo IP en esta interfaz.

**Valores válidos**: 0, 68 - 65535

**Valor por omisión**: Un mínimo de todas las MTU distintas de cero de la red

**originate-rip-default**

Hace que RIP anuncie este direccionador como la pasarela por omisión. Utilice este mandato en el siguiente entorno:

- Las rutas IP de la tabla de direccionamiento de este direccionador se determinan mediante diversos protocolos.
- RIP es uno de estos protocolos.
- Se importa información de direccionamiento más parcial de otros protocolos, y se anuncian mediante RIP.

El tráfico de la red RIP dirigido a destinos desconocidos para RIP puede ir detrás de la vía de acceso por omisión a este direccionador. Se puede utilizar la información de direccionamiento más completa de la tabla de rutas de este nodo para reenviar el tráfico por una vía de acceso adecuada hasta su destino. Puede configurar el direccionador para que sólo origine el valor por omisión cuando las rutas son conocidas para este direccionador, que no recibirá anuncios en la red RIP.

Cuando emita este mandato, se le solicitará que indique si el direccionador debe originar siempre un valor por omisión de RIP o debe originar dicho valor sólo cuando esté disponible la ruta de otros protocolos.

Esta ruta por omisión dirigirá el tráfico enlazado dirigido a una red no RIP a un direccionador de límite. El originar una sola ruta por omisión significa que el direccionador de límite no tiene que distribuir la información de direccionamiento de la otra red a los demás nodos de su red.

**de número AS**

**Valores válidos**: un entero comprendido entre 0 y 65535

**Valor por omisión**: ninguno

**a número red**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**coste por omisión**

**Valores válidos**: un entero comprendido entre 0 y 255

**Valor por omisión**: 1

**Ejemplo: `set originate-rip-default`**

```
IP config> set originate rip-default
Always originate default route? [No]:?
Originate default if BGP routes available? [No] yes
  From AS number [6]?
  To network number [0.0.0.0]?
Originate default if OSPF routes available? [No]
Originate default cost [1]?
```

- Si responde “Yes” a la pregunta “Always originate” significa que siempre se origina una ruta por omisión.
- Si responde “Yes” a la pregunta “BGP” se origina un valor por omisión cuando hay rutas BGP en la tabla de direccionamiento.
- Si responde “Yes” a la pregunta “if OSPF routes available”, el valor por omisión de RIP se anunciará cuando la tabla de direccionamiento contenga rutas OSPF.
- Cuando el direccionador decide originar una valor por omisión de RIP, utiliza el número “coste por omisión original”.
- Cuando se especifica 0 para el número AS (Sistema autónomo) de ruta BGP, una ruta que cumpla con los criterios de red procedente de cualquier AS hará que se origine un valor por omisión de RIP.
- Cuando se especifique 0.0.0.0 para los criterios de red BGP, cualquier BGP que cumpla con los criterios AS hará que se origine un valor por omisión de RIP.

**reassembly-size** *bytes*

Configura el tamaño de los almacenamientos intermedios que se utilizan para volver a ensamblar los paquetes IP fragmentados.

**Valores válidos:** 2048-65535

**Valor por omisión:** 12000

**Ejemplo: `set reassembly-size 12000`**

**rip-in-metric** *dirección-interfaz-ip métrica*

Permite configurar la métrica a añadir a las rutas RIP de una interfaz antes de su instalación en la tabla de direccionamiento.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**métrica** **Valores válidos**: un entero comprendido entre 1 y 15

**Valor por omisión**: 1

**Ejemplo:** `set rip-in-metric 128.185.120.209 1`

**rip-out-metric** *dirección-interfaz-ip métrica*

Permite configurar la métrica a añadir a las rutas RIP anunciadas en una interfaz configurada para anunciar rutas RIP o RIP2.

**dirección-interfaz-ip**

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**métrica** **Valores válidos**: un entero comprendido entre 0 y 15

**Valor por omisión**: 0

**Ejemplo:** `set rip-out-metric 128.185.120.209 0`

**router-id** *dirección-ip*

Define la dirección IP por omisión que utiliza el direccionador al direccionar por origen varios paquetes IP. Esta dirección resulta de particular importancia en difusiones múltiples y OSPF.

El ID del direccionador debe coincidir con una de las direcciones de interfaz IP configuradas del direccionador o con la dirección IP interna configurada. Si no es así, se pasa por alto. Si se pasa por alto, o no se configura, se adopta como dirección IP por omisión del direccionador (y su ID de direccionador de OSPF) la dirección IP interna (si está configurada) o la primera dirección IP de la configuración del direccionador.

**Valores válidos**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**Ejemplo:** `set router-id 128.185.120.209`

**routing table-size** *número-de-entradas*

Define el tamaño de la tabla de direccionamiento IP del direccionador. El tamaño por omisión es 768 entradas. Si define un tamaño de tabla de direccionamiento insuficiente, se eliminará información sobre direccionamiento dinámico. Si define un tamaño de tabla de direccionamiento excesivo, se malgastan recursos de memoria del direccionador. Consulte el tema “Sizes” en la página 354 para obtener más información sobre tamaños de tablas.

**Valores válidos**: un número entero de entradas comprendido entre 64 y 65535

**Valor por omisión**: 768 entradas

**Ejemplo:** `set routing table-size 1000`

**tag** Configura los distintivos por interfaz asociados a la información RIP recibida. Estos distintivos sirven para agrupar rutas, para anunciarlas posteriormente mediante BGP, donde el distintivo se tratará como si fuera un número de sistema autónomo (AS) de origen del direccionador. (Consulte la información sobre cómo originar, enviar y recibir políticas del

capítulo “Utilización y configuración de BGP” del manual *Consulta de configuración y supervisión de protocolos Volumen 1*.) Los distintivos también se propagan mediante el protocolo de direccionamiento OSPF.

**Valores válidos**: un entero comprendido entre 0 y 65535

**Valor por omisión**: 0

**Ejemplo: `set tag`**

```
Interface address [0.0.0.0]? 1.1.1.1
Interface tag (AS number) [0]? 1
```

**ttl** Especifica el tiempo de vida de los paquetes originados por el direccionador.

**Valores válidos**: un valor numérico comprendido entre 1 y 255

**Valor por omisión**: 64

**Ejemplo: `set ttl 255`**

## Update

Utilice el mandato **update packet-filter** para configurar filtros de paquetes. Este es un ejemplo del mandato:

```
IP config> update packet-filter
Packet-filter name [ ]? pf-1-in
Packet-filter 'pf-1-in' Config>
```

*Nombre-filtro-paquete* es cualquier nombre de filtro de paquete creado mediante el mandato **add packet-filter** *nombre-filtro-paquete* desde el indicador `IP config>`. Para activar el filtro de paquete, utilice el mandato **set access-control on**. Desde el indicador `Packet-filter '`*`nombre-filtro-paquete`*`' Config>`, puede entrar los siguientes mandatos:

**Sintaxis:**

add access-control

change access-control

delete access-control

disable

enable

list access-control

move access-control

Para los mandatos **add access-control**, **change access-control**, **delete access-control**,**list access-control** y **move access-control** correspondientes al indicador `Packet-filter '`*`nombre-filtro`*`' Config>`, consulte las descripciones de los parámetros que hay bajo el parámetro **access-control** que se visualiza en el indicador `IP config>`. Por ejemplo, consulte **add access-control** para ver una descripción de los parámetros correspondientes al mandato **update packet-filter add access-control**.

Para los parámetros **disable** y **enable**, la palabra clave **source-addr-verification** sólo se puede configurar desde el indicador `Packet-filter '`*`nombre-filtro`*`' Config>`.

Las siguientes secciones listan los parámetros que son exclusivos del mandato **update packet-filter**. Hay parámetros que se aplican a filtros de paquetes, pero no a filtros a nivel de direccionador, y se entran únicamente en el indicador `Packet-filter 'nombre-filtro' Config>`.

**add/change access-control** *tipo*

**Conversión de dirección de red (NAT)**

Este tipo de regla de control de acceso de filtro de paquete pasa los paquetes a NAT para que realice la conversión de dirección. Este tipo sólo es válido en filtros de paquetes y sólo si se especifica junto con inclusive, por ejemplo, ***IN***. Consulte la descripción de la característica NAT en el manual *Guía del usuario de software*para obtener más información. Encontrará un ejemplo de reglas de control de acceso para NAT en el capítulo Using Network Address Translation del manual *Utilización y configuración de las características*.

**Valor válido**: N

**Valor por omisión**: ninguno

**disable/enable source-addr-verification**

Esta opción de filtro de paquetes de entrada comprueba que la dirección IP de origen del paquete recibido es coherente, según la tabla de direccionamiento IP, con la interfaz de la que procede. Esta opción ayuda a evitar el reenvío de paquetes procedentes de un sistema principal IP que está utilizando una dirección IP de origen que no le pertenece, una técnica denominada *simulación*.

**Ejemplo:**

```
Packet-filter 'nombre-filtro' Config> enable source-addr-verification
```

**disable/enable trace** *número-índice-control-acceso*

Esta opción desactiva o activa el rastreo de paquetes correspondiente a una determinada regla de control de acceso. Para ver los paquetes de los que se ha efectuado un rastreo, utilice el mandato **event** de Talk 5 GWCON y utilice el mandato **view** de Talk 5 ELS con las opciones adecuadas para visualizar los registros de rastreo.

**Nota:** Para activar el valor de rastreo, entre el mandato **reset IP** de Talk 5.

**Ejemplo:**

```
Packet-filter 'nombre-filtro' Config> enable trace 1
```

## Ejemplos:

Los siguientes ejemplo muestran cómo configurar diversas reglas de control de acceso para filtros de paquetes. Consulte el capítulo “Using Network Address Translation” del manual Utilización y configuración de las características para ver un ejemplo de reglas de control de acceso para NAT.

**Ejemplo 1—Regla de control de acceso tipo exclusive**

Este ejemplo muestra cómo excluir todos los paquetes de entrada originados en la red 128.185.0.0 y recibidos en la interfaz 0.

```
    Packet-filter 'pf-in-0' Config> add access-control
    Enter type [E]?
    Internet source [0.0.0.0]? 128.185.0.0
    Source mask [255.255.255.255]? 255.255.0.0
    Internet destination [0.0.0.0]?
    Destination mask [255.255.255.255]? 0.0.0.0
    Enter starting protocol number ([CR] for all) [-1]?
Enable Logging? (Yes or [No]):
```

**Ejemplo 2—Supresión de una regla de control de acceso**

Utilice el mandato **list access-control** para buscar el número de índice de control de acceso.

```
    Packet-filter 'test' Config> delete access-control
    Enter index of access control to be deleted [1]? 4
```

El direccionador responde mostrando el registro de control de acceso especificado.

```
4  Type=I    Source=1.2.9.9       Dest=0.0.0.0          Prot=0-255
             Mask=255.0.0.255     Mask=0.0.0.0
             Sports=  0-65535     Dports=  1-65535
                                  Log=No
Are you sure this is the record you want to delete (Yes or [No]): y
    Deleted
    Packet-filter 'test' Config>
```

*Dports* son puertos de destino y *Sports* son puertos de origen.

**Ejemplo 3— Mandato list access-control**

Puede utilizar el mandato **list access-control** para ver los controles de acceso configurados para cada filtro de paquete.

```
Packet-filter 'pf-in-0' Config> list access-control
Access Control is: enabled
Access Control facility: USER

List of access control records:

1  Type=E    Source=128.185.0.0   Dest=0.0.0.0           Prot=0-255
             Mask=255.255.0.0     Mask=0.0.0.0
             Sports=  0-65535     Dports=  1-65535
             ACK0=N  T/C= **/**   Log=No
             Trace=Enabled

2  Type=I    Source=9.67.8.3      Dest=128.54.67.8     Prot=0-255
             Mask=255.255.255.255 Mask=255.255.255.254
             Sports=  N/A         Dports=  N/A
                                  Log=Yes ELS=N SNMP=Y SLOG=L(Emergency)

3  Type=I    Source=0.0.0.0       Dest=0.0.0.0           Prot=0-255
             Mask=0.0.0.0         Mask=0.0.0.0
             Sports= 1-65535      Dports=  1-68835
                                  Log=No
```

## Configuración de políticas de filtros de rutas

Esta sección describe el subconjunto de mandatos que sirven para configurar políticas de filtros de rutas. Para acceder a este subconjunto de mandatos de configuración de IP, siga los pasos siguientes:

1. Cree una política de filtro de rutas. Consulte el mandato **add route-policy** en la página 286.
2. Utilice el mandato **change route-policy** para que aparezca el indicador `IP Route Policy Config>`. El indicador `IP Route Policy Config>` se aplica sólo a una determinada política de rutas, identificada mediante el mandato **change route-policy**.

   **Ejemplo:**

```
IP config>change route-policy ospf-import
ospf-import IP Route Policy Configuration
IP Route Policy Config>
```

**Nota:** Las políticas de filtros de rutas pueden servir para determinar qué rutas se importan en OSPF y los detalles específicos de su anuncio, incluido el tipo externo de OSPF, su métrica y el valor del distintivo. Consulte el mandato **enable as boundary routing** en la página 387 para obtener información sobre cómo utilizar políticas de filtros de rutas para configurar OSPF.

Las políticas de filtros de rutas también sirven para controlar las rutas que se anuncian o se aceptan cuando se utiliza RIP. Consulte los mandatos anteriormente descritos **enable receiving**, **enable sending**, **disable receiving** y **disable sending**.

*Tabla 20. Resumen de mandatos de configuración de políticas de rutas IP*

| Mandato | Función |
|---|---|
| Add | Añade una acción, una entrada o una condición de coincidencia a una política de filtro de rutas. |
| Delete | Suprime una acción, una entrada o una condición de coincidencia de una política de filtro de rutas. |
| List | Lista las entradas, acciones y condiciones de coincidencia de política de rutas correspondientes a la política de rutas que se está modificando. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Add

Utilice el mandato **add** para añadir entradas de políticas de filtros de rutas a la política de filtros de rutas, para añadir condiciones de coincidencia a entradas existentes o para añadir acciones a entradas existentes.

**Sintaxis:**

**add** action . . .
entry . . .
match-condition . . .

**action . . .**

Añade una acción a una entrada existente de política de filtro de rutas. El añadir una acción a una política de filtro de rutas es opcional. Se puede añadir una acción a cada entrada. Si desea aplicar más de una acción a una dirección o rango de direcciones, especifique una segunda entrada para dicha dirección o rango. Luego, defina la segunda acción para la segunda entrada. Estas son las acciones que se pueden especificar:

**Sintaxis:**

auto-tag
set manual-tag
set metric
set route-type

**auto-tag** *índice-política-rutas*

Define de forma automática el distintivo para la ruta, utilizando una heurística específica del protocolo de direccionamiento. Esta opción se describe en RFC 1745.

**índice-política-rutas**

Identifica la entrada a la que se debe aplicar la acción.

**Valor válido**: 1 a 65535

**Valor por omisión**: ninguno

**set manual-tag** *índice-política-rutas distintivo-manual*

Define para el distintivo manual correspondiente a la ruta el valor especificado. Este distintivo suele ser el número de AS cuando el protocolo es OSPF.

**índice-política-rutas**

Identifica la entrada a la que se debe aplicar la acción.

**Valor válido**: 1 a 65535

**Valor por omisión**: ninguno

**distintivo-manual**

**Valor válido**: X'0' a X'FFFFFFFF'

**Valor por omisión**: ninguno

**set metric** *índice-política-rutas métrica*

Define para la métrica correspondiente a la ruta el valor especificado.

**índice-política-rutas**

Identifica la entrada a la que se debe aplicar la acción.

**Valor válido**: 1 a 65535

**Valor por omisión**: ninguno

**métrica**

**Valor válido**: 1 a 255

**Valor por omisión**: ninguno

**set route-type** *índice-política-rutas tipo-ruta*

Define el tipo de ruta externa OSPF. Esta acción se pasa por alto para las aplicaciones que no sean la importación de rutas límite AS de OSPF.

**índice-política-rutas**

Identifica la entrada a la que se debe aplicar la acción.

**Valor válido**: 1 a 65535

**Valor por omisión**: ninguno

**tipo-ruta**

**Valor válido**: 1 ó 2

**Valor por omisión**: ninguno

**entry** *índice-política-rutas dirección-ip máscara-ip coincidencia-dirección tipo-política*

Añade una entrada de política de filtro de rutas a la política de filtro de rutas que se está modificando. Cada entrada de una política de filtro de rutas se identifica mediante un número de índice exclusivo, que se configura de forma manual. Si la entrada con el número de índice especificado ya existe, dicha entrada se modifica de acuerdo con los nuevos parámetros configurados.

Cuando añade una política de filtro de rutas, define el proceso de entradas como estrictamente lineal o de la longitud más larga. Si el proceso de política de filtro de rutas es estrictamente lineal, las entradas de la política de filtro de rutas se procesan según el orden ascendente de sus números de índice. Si el proceso de política de filtro de rutas es según la coincidencia más larga, las entradas de la política de filtro de rutas se procesan según la dirección y la máscara IP que tiene la coincidencia más larga. Si hay varias entradas de la política de filtro de rutas con la misma dirección y máscara IP cuando se utiliza la coincidencia más larga, la coincidencia estará en orden de número de índice ascendente entre las entradas con la misma dirección y máscara IP.

**índice-política-rutas**

Identifica la entrada.

**Valor válido**: 1 a 65535

**Valor por omisión**: ninguno

**dirección-ip**

**Valor válido**: cualquier dirección IP válida

**Valor por omisión**: ninguno

**máscara-ip**

**Valor válido**: cualquier máscara IP válida

**Valor por omisión**: ninguno

**coincidencia-dirección exacta/rango**

Si este valor es *exact*, la entrada de la política de filtro de rutas sólo coincidirá con una ruta que tenga exactamente la misma dirección y máscara. Si este valor es *range*, la entrada de la política de filtro de rutas coincidirá con cualquier ruta que se encuentre dentro del rango comprendido en la dirección y máscara, incluida la ruta exacta.

**Valor válido**: exact o range

**Valor por omisión**: range

**tipo-política inclusive/exclusive**

Si este valor es *inclusive*, las rutas que coincidan con esta entrada de política de filtro de rutas se incluyen en la tabla

de direccionamiento. Si este valor es *exclusive*, las rutas que coincidan con esta entrada de política de filtro de rutas se excluyen, es decir, no se entran en la tabla de direccionamiento. Aunque se configuren acciones para una entrada de política de filtro de rutas exclusive, estas acciones no se aplican.

**Valor válido**: inclusive o exclusive

**Valor por omisión**: inclusive

**match-condition . . .**

Añade una condición de coincidencia a una entrada existente de política de filtro de rutas. Una condición de coincidencia, que es un parámetro o serie de parámetros opcionales, se aplica a una ruta con la que coincida la definición de esta entrada. La condición de coincidencia filtra el paquete según determinadas condiciones, además de la dirección IP y la máscara IP. Sólo se puede configurar una condición de coincidencia por entrada. Para poder utilizar dos condiciones de coincidencia para la misma dirección o rango de direcciones puede añadir una segunda entrada a la política de filtro de rutas y especificar la segunda condición de coincidencia para dicha entrada. Estas son las condiciones de coincidencia:

**Sintaxis:**

as

gateway

metric

net

protocol

source-gateway

**as** *índice-política-rutas número-as*

Compara la ruta según su número AS. Este valor sólo se interpreta cuando la política de filtro de rutas se aplica a direccionamiento límite AS.

**índice-política-rutas**

Un entero que identifica la entrada con la que se debe realizar la comparación.

**Valor válido**: 1 a 65535

**Valor por omisión**: ninguno

**número-as**

**Valor válido**: 1 a 65535

**Valor por omisión**: ninguno

**gateway** *índice-política-rutas dirección-y-máscara-pasarela*

Compara la ruta con una pasarela del siguiente salto del rango especificado.

**índice-política-rutas**
Identifica la entrada con la que se debe realizar la comparación.

**Valor válido**: 1 a 65535

**Valor por omisión**: ninguno

**dirección-y-máscara-pasarela**

**Valor válido**: una dirección y máscara IP válidas

**Valor por omisión**: ninguno

**metric** *índice-política-rutas número-métrica-inferior número-métrica-superior*
Compara la métrica de la ruta con uno de los números de un rango de números de métrica. Se le solicitarán dos números para identificar el rango de números de métrica: uno para el límite inferior del rango y uno para el límite superior. Si desea un solo número de métrica, especifique dos veces el mismo número.

**índice-política-rutas**

**Valor válido**: 1 a 65535

**Valor por omisión**: ninguno

**número-métrica-inferior**

**Valor válido**: 1 a 65535

**Valor por omisión**: ninguno

**número-métrica-superior**

**Valor válido**: 1 a 65535

**Valor por omisión**: ninguno

**net** *índice-política-rutas número-red-inferior número-red-superior*
Compara las rutas que tienen un salto siguiente con un número de red de salida comprendido en el rango identificado por los números de red inferior y superior. Se le solicitarán dos números para identificar el rango de números de red de salida: uno para el límite inferior del rango y uno para el límite superior. Si desea un solo número de red, especifique dos veces el mismo número.

**índice-política-rutas**
Identifica la entrada con la que se debe realizar la comparación.

**Valor válido**: 1 a 65535

**Valor por omisión**: ninguno

**número-red-inferior**
El límite inferior del rango de números de red para la comparación de redes de salida del

siguiente salto. Se pueden ver mediante el mandato **list devices** desde el indicador `Config>`.

**Valor válido**: 1 a 65536

**Valor por omisión**: ninguno

**número-red-superior**
El límite superior del rango de números de red para la comparación de redes de salida del siguiente salto.

**Valor válido**: 1 a 65536

**Valor por omisión**: ninguno

**protocol** *protocolo índice-política-rutas*
Compara la ruta con un protocolo.

**protocolo**

**Valores válidos**:

**Sintaxis:**

bgp

direct

natural-nets

ospf-intra

ospf-inter

ospf

ospf-all

ospf-ext

ospf-e1

ospf-e2

rip

static

**Valor por omisión**: ninguno

**índice-política-rutas**
Un entero que identifica la entrada con la que se debe realizar la comparación.

**Valor válido**: 1 a 65535

**Valor por omisión**: ninguno

**source-gateway** *índice-política-rutas dirección-y-máscara-ip*
Compara las rutas procedentes de una determinada pasarela de origen o rango de pasarelas de origen.

**índice-política-rutas**
Un entero que identifica la entrada con la que se debe realizar la comparación.

**Valor válido**: 1 a 65535

**Valor por omisión**: ninguno

**dirección-y-máscara-ip**

**Valores válidos**: cualquier combinación de dirección y máscara IP válidas

**Valor por omisión**: ninguno

## Delete

Utilice el mandato **delete** para suprimir entradas de la política de filtro de rutas, condiciones de coincidencia de las entradas existentes de la política de filtro de rutas o acciones de las entradas existentes de la política de filtro de rutas. Consulte el mandato **add** de esta sección para ver una descripción de los parámetros que se pueden suprimir.

## List

Utilice el mandato **list** para listar las entradas de política de filtro de rutas, condiciones de coincidencia y acciones existentes correspondientes a la política de filtro de rutas que se está modificando.

**Sintaxis: list**

**Ejemplo:**

```
IP Route Policy Config>list

     IP Address      IP Mask           Match  Index  Type
     ---------------------------------------------------
     9.0.0.0         255.0.0.0         Range  1      Include
     10.0.0.0        255.0.0.0         Range  2      Exclude
         Match Conditions:  Protocol: BGP
     0.0.0.0         0.0.0.0           Range  3      Include
         Match Conditions:  Protocol: Static
                            Gateway IP Address Range: 153.2.2.20/255.255.255.255
     10.1.1.0        255.255.255.0     Range  4      Include
     0.0.0.0         0.0.0.0           Range  7      Include
         Policy Actions:    Set Manual Tag: 0xACEEACEE
     0.0.0.0         0.0.0.0           Range  8      Include
         Match Conditions:  Protocol: RIP
```

# Cómo acceder al entorno de supervisión IP

Utilice el siguiente procedimiento para acceder a los mandatos de supervisión de IP. Este proceso le ofrece acceso al proceso de *supervisión* de IP.

1. En el indicador OPCON, entre **talk 5**. (Para obtener más información sobre este mandato, consulte el tema “The OPCON Process and Commands” del manual *Guía del usuario de software*.)Por ejemplo:

   ```
   * talk 5
   +
   ```

   Una vez haya especificado el mandato **talk 5**, aparece el indicador GWCON (+) en el terminal. Si no aparece este indicador la primera vez que entre en la configuración, vuelva a pulsar **Intro**.

2. En el indicador +, entre el mandato **protocol ip** para que aparezca el indicador IP>.

   **Ejemplo:**

```
+ prot ip
IP>
```

## Mandatos de supervisión de IP

Esta sección describe los mandatos de supervisión de IP. La Tabla 21 lista los mandatos de supervisión de IP. Los mandatos le permiten supervisar el proceso de reenvíos IP del direccionador. Las funciones de supervisión incluyen las siguientes: los parámetros configurados, como dirección de interfaz y rutas estáticas, se pueden consultar, el estado actual de la tabla de direccionamiento IP se puede visualizar y se puede listar el número de errores de direccionamiento IP.

*Tabla 21 (Página 1 de 2). Resumen de mandatos de supervisión de IP*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Access controls | Lista la modalidad actual de control de acceso IP, junto con los registros configurados de control de acceso. |
| Cache | Muestra una tabla de todos los destinos de direccionamiento recientes. |
| Counters | Lista diversas estadísticas de IP, incluidos el número de errores de direccionamiento y de paquetes eliminados. |
| Dscache | Lista las acciones, estadísticas y orden de la antememoria de flujo de DiffServ. |
| Dump routing tables | Lista el contenido de la tabla de direccionamiento IP. |
| IGMP | Muestra contadores y parámetros de IGMP. |
| Interface addresses | Lista las direcciones de interfaces IP del direccionador. |
| Packet-filter | Muestra la información de control de acceso definida para el filtro de paquetes especificado o para todos los filtros. |
| Parameters | Lista valores de diversos parámetros. |
| Ping | Envía solicitudes de eco ICMP a otro sistema principal y espera una respuesta. Este mandato se puede utilizar para identificar un problema en un entorno de interredes. |
| Redundant Default Gateway | Muestra si existe o no una pasarela por omisión redundante y si está activa o inactiva. |
| Reset | Le permite restablecer de forma dinámica la configuración IP/RIP. |
| RIP | Muestra el estado del protocolo RIP. |
| RIP-Policy | Muestra la política de filtro de rutas que se aplica a la interfaz especificada. |
| Route | Muestra si existe o no una ruta a un destino IP específico y, si es así, la entrada de la tabla de direccionamiento que corresponde a la ruta. |
| Route-table-filtering | Lista los filtros de rutas definidos e indica si la función de filtro de rutas está activada o desactivada. |
| Sizes | Muestra el tamaño de determinados parámetros IP. |

*Tabla 21 (Página 2 de 2). Resumen de mandatos de supervisión de IP*

| Mandato | Función |
|---|---|
| Static routes | Muestra las rutas estáticas que se han configurado. Esto incluye la pasarela por omisión. |
| Traceroute | Muestra la vía de acceso completa (salto por salto) a un determinado destino. |
| UDP-Forwarding | Muestra los números de puertos UDP y las direcciones IP de destino que ha añadido mediante el mandato **add** o el mandato **enable**. |
| VRID | Muestra información detallada sobre un determinado VRID |
| VRRP | Lista el estado de resumen correspondiente al protocolo VRRP. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Access Controls

Utilice el mandato **access controls** para imprimir la modalidad global de control de acceso que se utiliza junto con una lista de las reglas configuradas de control de acceso global.

El control de acceso está desactivado (lo que significa que no se realiza ningún control de acceso y que las reglas de control de acceso se pasan por alto) o activado (lo que significa que se realiza un control de acceso y que se reconocen las reglas de control de acceso). El mandato de talk 6 **set access on** activa el control de acceso.

**Sintaxis:**

**access**

**Ejemplo:** `access`

```
            Access Control currently enabled
            Access Control facility: USER
            Access Control run 702469 times, 657159 cache hits

            List of access control records:

1  Type=I    Source=2.2.2.2          Dest=2.2.2.128         Prot= 0-255
             SMask =255.255.255.254  DMask=255.255.255.128  Use=271
             Sports=  2-200          Dports=  1-100
                    T/C= 1/4         Log=Yes  ELS=L SNMP=Y  SLOG=S(Information)
             Trace=Enabled

2  Type=E    Source=0.0.0.0          Dest=0.0.0.0           Prot= 1
             SMask =255.255.255.255  DMask=255.255.255.255  Use=18962
             Sports=  N/A            Dports=  N/A
                      T/C= 1/**      Log=Yes ELS=N SNMP=N   SLOG=L(Alert)

3  Type=I    Source=1.1.1.1          Dest=1.1.1.2           Prot= 6
             SMask =255.255.255.255  DMask=255.255.255.254  Use=42
             Sports=  2-200          Dports=  1-100
                                     Log=No

4  Type=I    Source=9.1.2.3          Dest=0.0.0.0       Prot=  0-255
             SMask =255.255.255.255  DMask=0.0.0.0      Use=0
             SPorts=  0-65535        DPorts=  0-65535
                      T/C= **/**     Log=N
             Tos=xE0/x00-x00         ModifyTos=x1F/x08
             PbrGw=9.2.160.1         UseDefRte=Y

5  Type=I    Source=0.0.0.0        Dest=0.0.0.0         Prot= 0-255
             Mask=0.0.0.0          Mask=0.0.0.0         Use=683194
             Sports=  1-65535      Dports=  1-65535
                                   Log=No
```

Exclusive (E) significa que los paquetes que coinciden con la regla de control de acceso se eliminan. Inclusive (I) significa que los paquetes que coinciden con la regla de control de acceso se reenvían. Cuando el control de acceso está activado, los paquetes que no coinciden con ningún registro de control de acceso se eliminan. *Prot* (protocolo) indica el número de protocolo IP. *Sports* indica el rango de números de puertos de origen TCP/UDP; *Dports* indica el rango de números de puertos de destino TCP/UDP.*SYN* indica la función de filtro de establecimiento de conexión TCP. *T/C* indica el tipo y código ICMP; *SLOG* significa SysLog.

El campo Use especifica el número de veces que el sistema de control de acceso ha encontrado una coincidencia entre un registro determinado y un paquete de entrada, por ejemplo, el número de veces que un determinado registro del sistema de control de acceso IP ha sido invocado por las características de un paquete de entrada o de salida.

En este ejemplo, la regla de control de acceso número 4 ha activado el filtro TOS. Se muestran los parámetros de TOS. Consulte el mandato **add access-control** de talk 6 para ver una descripción de estos parámetros.

## Cache

Utilice el mandato **cache** para visualizar la antememoria de direccionamiento IP, que contiene los destinos a los que se ha direccionado recientemente. Si un destino no se encuentra en la antememoria, el direccionador busca el destino en la tabla de información de direccionamiento a fin de tomar una decisión sobre el reenvío.

**Sintaxis:**

**cache**

**Ejemplo:** **cache**

```
Destination     Usage           Next hop
128.185.128.225 1               128.185.138.180 (Eth/0)
192.26.100.42   1               128.185.138.180 (Eth/0)
128.185.121.1   18              128.185.123.18  (PPP/0)
128.185.129.219 76              128.185.125.25  (PPP/1)
128.185.129.41  130             128.185.125.25  (PPP/1)
128.185.129.134 546             128.185.125.40  (PPP/1)
128.185.129.221 1895            128.185.125.40  (PPP/1)
128.185.129.193 96              128.185.125.40  (PPP/1)
128.197.3.4     4               128.185.123.18  (PPP/0)
128.185.128.25  98              128.185.125.41  (PPP/1)
128.185.124.121 4               128.185.124.121 (Eth/0)
128.185.136.203 95              128.185.125.39  (PPP/1)
128.185.194.4   581             128.185.125.39  (PPP/1)
128.185.123.17  2               128.185.123.17  (PPP/0)
192.26.100.42   1               128.185.125.38  (PPP/1)
128.52.22.6     2               128.185.123.18  (PPP/0)
128.197.3.2     1               128.185.123.18  (PPP/0)
128.185.126.24  61              128.185.125.25  (PPP/1)
128.185.138.150 482             128.185.125.39  (PPP/1)
128.185.123.18  152             128.185.123.18  (PPP/0)
```

**Destination**
Sistema principal de destino IP.

**Usage** Número de paquetes recientemente enviados al sistema principal de destino.

**Next hop** Dirección IP del siguiente direccionador de la vía de acceso hacia el sistema principal de destino. También se muestra el nombre de red de la interfaz utilizada por el direccionador de envío para reenviar el paquete.

## Counters

Utilice el mandato **counters** para visualizar estadísticas relacionadas con el proceso de reenvío IP. Esto incluye el número de errores de direccionamiento, junto con el número de paquetes que se han eliminado debido a la congestión.

**Sintaxis:**

**counters**

**Ejemplo:** **counters**

```
Routing errors
Count   Type
    0   Routing table overflow
 2539   Net unreachable
    0   Bad subnet number
    0   Bad net number
    0   Unhandled broadcast
58186   Unhandled multicast
     0   Unhandled directed broadcast
 4048   Attempted forward of LL broadcast

Packets discarded through filter  0
IP multicasts accepted:           60592
 IP input packet overflows
    Net   Count
   TKR/0  0
    FR/0  0
```

**Routing table overflow**
Lista el número de rutas que se han eliminado porque la tabla de direccionamiento estaba llena.

**Net unreachable**
Indica el número de paquetes que no se han podido reenviar porque el destino era desconocido. Esto no cuenta el número de paquetes que se han reenviado al direccionador con autorización (pasarela por omisión).

**Bad subnet number**
Cuenta el número de paquetes o rutas que se han recibido para subredes no permitidas (todo unos o todo ceros).

**Bad net number**
Cuenta el número de paquetes o rutas que se han recibido para destinos IP no válidos (por ejemplo, direcciones de clase E).

**Unhandled broadcasts**
Cuenta el número de difusiones generales IP (no locales) recibidas (no se reenvían).

**Unhandled multicasts**
Cuenta el número de difusiones múltiples IP que se han recibido, pero cuyas direcciones no ha reconocido el direccionador (se eliminan).

**Unhandled directed broadcasts**
Cuenta el número de difusiones generales IP directas (no locales) recibidas cuando el reenvío de estos paquetes estaba desactivado.

**Attempted forward of LL broadcast**
Cuenta el número de paquetes recibidos que tenían direcciones IP no locales pero que se enviaron a una dirección de difusión general a nivel de enlace. Estos paquetes se eliminan.

**Packets discarded through filter**
Cuenta el número de paquetes recibidos dirigidos a redes/subredes filtradas. Estos paquetes se eliminan de forma silenciosa.

**IP multicasts accepted**
Cuenta el número de difusiones múltiples IP que se han recibido y que el direccionador ha procesado satisfactoriamente.

**IP packet overflows**
Cuenta el número de paquetes que se han eliminado debido a una congestión en la cola de entrada del distribuidor. La interfaz receptora clasifica estos números.

## Dscache

Utilice el mandato **dscache** para listar las acciones, estadísticas y orden de la antememoria de flujo DiffServ.

**Ejemplo:** dscache actions

```
IP>dscache actions
Source          Destination     Pro ProtocolInf Net TosIn/Out Action
10.1.100.1      9.1.140.1         1 T:x08 C:x00   0 x05->x05   DROP
9.1.140.1       10.1.100.1        1 FrgId:x0008  -1 x00->x15   PASS
10.1.100.1      9.1.140.1         1 FrgId:x0008  -1 x03->x15   PASS
10.1.100.1      9.1.140.1         6  1024>   23   0 xFE->x15   PASS
9.1.140.1       10.1.100.1        1 T:x03 C:x03   1 x00->x15   PASS
10.1.100.1      9.1.140.1        17 12585>33437   0 x00->x15   PASS
10.1.100.1      9.1.140.1         1 FrgId:x0010  -1 x05->x05   DROP
9.1.140.1       10.1.100.1        6    23> 1024   1 x00->x15   PASS
9.1.140.1       10.1.100.1        1 T:x00 C:x00   1 x00->x15   PASS
10.1.100.1      9.1.140.1         1 FrgId:x0009  -1 x05->x05   DROP
```

**Ejemplo:** dscache stats

```
IP>dscache stats
Source          Destination     Pro ProtocolInf Net Tos     RxPkts    RxBytes
10.1.100.1      9.1.140.1         1 T:x08 C:x00   0 x05          2       4088
9.1.140.1       10.1.100.1        1 FrgId:x0008  -1 x00          1         26
10.1.100.1      9.1.140.1         1 FrgId:x0008  -1 x03          1         26
10.1.100.1      9.1.140.1         6  1024>   23   0 xFE          9        383
9.1.140.1       10.1.100.1        1 T:x03 C:x03   1 x00          1         56
10.1.100.1      9.1.140.1        17 12585>33437   0 x00          1         84
10.1.100.1      9.1.140.1         1 FrgId:x0010  -1 x05          1         26
9.1.140.1       10.1.100.1        6    23> 1024   1 x00          8        879
9.1.140.1       10.1.100.1        1 T:x00 C:x00   1 x00          8       6552
10.1.100.1      9.1.140.1         1 FrgId:x0009  -1 x05          1         26
```

**Ejemplo:** dscache order

```
IP>dscache order
Source          Destination     Pro ProtocolInf Net Tos
10.1.100.1      9.1.140.1         6  1024>   23   0 xFE
9.1.140.1       10.1.100.1        6    23> 1024   1 x00
9.1.140.1       10.1.100.1        1 T:x03 C:x03   1 x00
10.1.100.1      9.1.140.1        17 12585>33437   0 x00
10.1.100.1      9.1.140.1         1 FrgId:x0010  -1 x05
10.1.100.1      9.1.140.1         1 T:x08 C:x00   0 x05
10.1.100.1      9.1.140.1         1 FrgId:x0009  -1 x05
9.1.140.1       10.1.100.1        1 FrgId:x0008  -1 x00
9.1.140.1       10.1.100.1        1 T:x00 C:x00   1 x00
10.1.100.1      9.1.140.1         1 FrgId:x0008  -1 x03
```

## Tabla de direccionamiento de vuelcos

Utilice el mandato **dump** para visualizar la tabla de direccionamiento IP. Se muestra una entrada para cada red/subred IP que se puede alcanzar. La pasarela por omisión IP que se utiliza (si la hay) aparece en la parte inferior de la pantalla.

**Sintaxis:**

**dump**

**Ejemplo:** `dump`

```
Type   Dest net         Mask     Cost Age   Next hop(s)
SPE1   0.0.0.0          00000000  4    3    128.185.138.39  (2)
SPF*   128.185.138.0    FFFFFF00  1    1    Eth/0
Sbnt   128.185.0.0      FFFF0000  1    0    None
SPF    128.185.123.0    FFFFFF00  3    3    128.185.138.39  (2)
SPF    128.185.124.0    FFFFFF00  3    3    128.185.138.39  (2)
SPF    192.26.100.0     FFFFFF00  3    3    128.185.131.10  (2)
RIP    197.3.2.0        FFFFFF00  10   30   128.185.131.10
RIP    192.9.3.0        FFFFFF00  4    30   128.185.138.21
Del    128.185.195.0    FFFFFF00  16   270  None


Default gateway in use.

Type Cost Age  Next hop
SPE1 4    3    128.185.138.39

Routing table size: 768 nets (36864 bytes), 36 nets known
```

**Type** Indica el modo en que se ha obtenido la ruta.

Sbnt - Indica que la red tiene subredes; esta entrada es únicamente un área de retención de posición.

Dir - Indica una red o subred directamente conectada.

RIP - Indica que la ruta se ha aprendido a través del protocolo RIP.

Del - Indica que la ruta se ha eliminado.

Stat - Indica una ruta configurada de forma estática.

BGP - Indica rutas aprendidas a través del protocolo BGP.

BGPR - Indica rutas aprendidas a través del protocolo BGP que OSPF y RIP han vuelto a anunciar.

Fltr - Indica un filtro de direccionamiento.

SPF - Indica que la ruta es una ruta interna del área OSPF.

SPIA - Indica que es una ruta entre áreas OSPF.

SPE1, SPE2 - Indica rutas externas OSPF (de tipo 1 y de tipo 2 respectivamente)

Rnge - Indica un tipo de ruta que es un rango de direcciones de área OSPF y que no se utiliza en el reenvío de paquetes.

**Dest net** Red/subred de destino IP.

**Mask** Máscara de dirección IP.

**Cost** Coste de la ruta.

**Age** Para rutas RIP y BGP, el tiempo transcurrido desde la última vez que se renovó la entrada de la tabla de direccionamiento.

**Next Hop** Dirección IP del siguiente direccionador de la vía de acceso hacia el sistema principal de destino. También se muestra el tipo de interfaz utilizada por el direccionador emisor para reenviar el paquete.

Un asterisco (*) tras el tipo de ruta indica que la ruta tiene una reserva conectada de forma estática o directa. Un símbolo de porcentaje (%) tras el tipo de ruta indica que las actualizaciones RIP se aceptarán siempre para esta red/subred.

Un número entre paréntesis al final de la columna indica el número de rutas de igual coste hasta el destino. Los primeros saltos pertenecientes a estas rutas se pueden visualizar con el mandato de IP **route**.

## IGMP

Utilice el mandato **igmp** para visualizar contadores de IGMP y parámetros operativos correspondientes a IGMP.

**Sintaxis:**

**igmp** counters

parameters

**counters** Muestra el número de mensajes IGMP enviados y recibidos.

**Ejemplo:**

```
IP+ igmp counters
     Net      Querier      Polls Sent      Polls Rcvd      Reports Rcvd
     ---      -------      ----------      ----------      ------------
      0         Y            4973             0              0
      2         N               1           4921              0
      5         Y            4972             0              0
```

**Net** Especifica el número de red.

**Querier** Especifica si el dispositivo es el consultor de la red especificada.

**Polls Sent**
Número de consultas IGMP enviadas.

**Polls Rcvd**
Número de consultas IGMP recibidas.

**Reports Rcvd**
Número de informes IGMP recibidos.

**parameters**
Muestra los parámetros operativos de IGMP de las interfaces conectadas al dispositivo.

**Ejemplo:**

```
IP+ igmp parameters

        Net      Robustness      Query       Response     Leave Query
                  Variable      Interval     Interval      Interval
                                 (secs)       (secs)        (secs)
        ---      ----------     --------     --------     -----------
          0          2            125          10             1
          2          2            125          10             1
          5          2            125          10             1
```

**Net** El número de red de la interfaz IGMP.

**Robustness variable**
La variable de potencia de la interfaz especificada.

**Query interval**
El número de segundos entre consultas IGMP generales en esta red si este dispositivo es el consultor IGMP designado.

**Response interval**
El tiempo máximo de respuesta insertado en consultas generales IGMP en esta red si este dispositivo es el consultor IGMP designado.

**Leave query interval**
El tiempo máximo de respuesta insertado en consultas específicas IGMP en esta red si este dispositivo es el consultor IGMP designado.

## Interface Addresses

Utilice el mandato **interface addresses** para visualizar las direcciones de interfaces IP del direccionador. Cada interfaz se muestra junto con su interfaz de hardware correspondiente y su máscara de dirección IP. Si a la interfaz de puente utilizada para la conexión por puente y para el direccionamiento se le ha asignado una dirección IP, esta también se mostrará. La interfaz de puente se identifica mediante *BDG/0*.

Las interfaces de hardware que no tienen direcciones de interfaces IP configuradas no se utilizarán en el proceso de reenvío de IP; esto se indica mediante Not an IN net. Hay una excepción. A las líneas serie no se les asignar direcciones de interfaces IP a fin de poder reenviar tráfico IP. Estas líneas serie se denominan no numeradas. Para estas, se muestra la dirección .0.0.0.

**Sintaxis:**

**interface**

**Ejemplo:** **`interface`**

```
Interface  IP Address(es)   Mask(s)          MTU
   TKR/0   133.1.169.2      255.255.252.0
    FR/0   133.1.167.2       255.255.254.0
```

**Interface** Indica el tipo de hardware de la interfaz.

**IP addresses**
Indica la dirección IP de la interfaz.

**Mask** Indica la máscara de subred de la interfaz.

## Packet-filter

Utilice el mandato **packet-filter** para visualizar información definida para un determinado filtro de paquetes o para todos los filtros de paquetes. Los filtros de paquetes son listas, específicas de cada interfaz, de registros de control de acceso. Las interfaces se identifican mediante números de interfaz, excepto para la interfaz de puente utilizada para direccionar y conectar por puente en la misma interfaz. Esta se identifica mediante *BDG/0*.

**Sintaxis:**

**packet-filter** [*nombre*]

**Ejemplo de IPv4:** **`packet-filter pf-in-0`**

```
Name              Direction     Interface  State  SRC-Addr-Check #Access-Controls
pf-in-0           Out           0          On     N/A            3

Access Control is: enabled
Access Control run 563 times, 271 cache hits

List of access control records:

0  Type=IN   Source=10.1.1.1      Dest=10.1.1.2          Prot=0-255
             Mask=255.255.255.255 Mask=255.255.255.254   Use=71
             Sports=  N/A         Dports=  N/A
                                  Log=Yes ELS=N SNMP=Y SLOG=L(Emergency)
             Trace=Enabled

1  Type=I    Source=9.67.1.5      Dest=9.37.192.1        Prot=6-255
             Mask=255.255.255.255 Mask=255.255.255.255   Use=15
             Sports=  N/A         Dports=  N/A
                                  Log=Yes ELS=L SNMP=N SLOG=L(Debug)

2  Type=I    Source=0.0.0.0       Dest=0.0.0.0           Prot=0-255
             Mask=255.255.255.255 Mask=255.255.255.255   Use=477
             Sports=  0-65535     Dports=  1-65535
                                  Log=N
```

### Ejemplo de IPv6: `packet-filter pf-in-0`

```
Name              Direction     Interface   #Access-Controls
pf-in-0           In            0           2

Access Control currently enabled
Access Control run 8 times, 7 cache hits

List of access control records:

                                                        Beg End  Beg  End
  Ty  Source       Mask     Destination  Mask      PPP PPP  Port Port  Use
0 I   0.0.0.0      00000000 192.67.67.20 00000000  6   6    25   25    0
1 E   150.150.1.0  FFFFFF00 150.150.2.0  00000000  0   255  0    655   0
2 I   0.0.0.0      00000000 0.0.0.0      00000000  89  89   0    655   27
  Trace=Enabled
```

## Parameters

Utilice el mandato **parameters** para listar los valores de diversos parámetros.

### Ejemplo:

```
IP> parameters
ARP-SUBNET-ROUTING     : disabled
ARP-NET-ROUTING        : disabled
CLASSLESS              : disabled
DIRECTED-BROADCAST     : enabled
DSCACHE-SIZE           : 64 entries
 ECHO-REPLY             : enabled
FRAGMENT-OFFSET-CHECK  : disabled
PER-PACKET-MULTIPATH   : disabled
REASSEMBLY-SIZE        : 12000 bytes
RECORD-ROUTE           : enabled
ROUTING TABLE-SIZE     : 768 entries (52224 bytes)
(Routing) CACHE-SIZE   : 64 entries
SAME-SUBNET            : disabled
SOURCE-ROUTING         : enabled
TIMESTAMP              : enabled
TTL                    : 64

IP>
```

## Ping

Utilice el mandato **ping** para que el direccionador envíe mensajes de eco de ICMP a un determinado destino y espere una respuesta. Este mandato puede servir para identificar un problema en la interred.

**Sintaxis:**

| | |
|---|---|
| p**ing** | *dirección-dest [dirección-origen tamaño-datos ttl velocidad tos valor-data]* |

El proceso ping se realiza continuamente, aumentando el número de secuencia de ICMP con cada paquete adicional. Cada respuesta de eco de ICMP de coincidencia recibida se notifica con su número de secuencia y el tiempo de envío y respuesta. La granularidad (resolución de tiempo) del cálculo de tiempo de envío y respuesta suele ser de unos 20 milisegundos, en función de la plataforma.

Para detener el proceso de ping, escriba cualquier carácter en la consola. En ese momento aparecerá un resumen de paquetes perdidos, periodos de tiempo de envío y respuesta y número de destinos ICMP que no se han podido alcanzar.

Cuando se especifica una dirección de difusión general o de difusión múltiple como destino, pueden aparecer varias respuestas por cada paquete enviado, una por cada miembro del grupo. Cada respuesta recibida se muestra junto con la dirección de origen del emisor de la respuesta.

Puede especificar el tamaño de ping (número de bytes de datos del mensaje ICMP, excluida la cabecera ICMP), el valor de los datos, el valor de tiempo de vida (TTL), la velocidad de emisión de mandatos ping y los bits TOS a definir. También puede especificar la dirección IP de origen. Si no especifica la dirección IP de origen, el direccionador utiliza su dirección local en la interfaz de salida al destino especificado. Si está comprobando la conectividad desde cualquiera de las otras interfaces del direccionador hacia el destino, entre la dirección IP correspondiente a dicha interfaz como dirección de origen.

Sólo el parámetro de destino es obligatorio; los demás son opcionales. Por omisión es tamaño es 56 bytes, el TTL es 64, la velocidad es 1 ping por segundo, y el valor de TOS es 0. Los 4 primeros bytes de los datos ICMP se utilizan como indicador horario. Por omisión, los demás datos son una serie de bytes con valores que se incrementan en 1, comenzando por X'04', y pasando de X'FF' a X'00' (por ejemplo, X'04 05 06 07 . . . FC FD FE FF 00 01 02 03 . . .'). Estos valores sólo se incrementan cuando se utiliza el valor por omisión; si se especifica el valor de bytes de datos, todos los datos ICMP (excepto los 4 primeros bytes) adoptan dicho valor, el cual no se incrementa. Por ejemplo, si define como valor de byte de datos el valor X'FF', los datos ICMP son una serie de bytes con el valor X'FF FF FF . . .'.

**Ejemplo:**

```
   IP> ping
   Destination IP address [0.0.0.0]? 192.9.200.1
   Source IP address [192.9.200.77]?
   Ping data size in bytes [56]?
   Ping TTL [64]?
   Ping rate in seconds [1]?
   Ping TOS (00-FF) [0]? e0
   Ping data byte value (00-FF) [ ]?
   PING 192.9.200.77-> 192.9.200.1:56 data bytes,ttl=64,every 1 sec.
   56 data bytes from 192.9.200.1:icmp_seq=0.ttl=255.time=0.ms
   56 data bytes from 192.9.200.1:icmp_seq=1.ttl=255.time=0.ms
   56 data bytes from 192.9.200.1:icmp_seq=2.ttl=255.time=0.ms


   ----192.9.200.1 PING Statistics----
   3 packets transmitted, 3 packets received, 0% packet loss
   round-trip min/avg/max=0/0/0 ms
   IP>
IP>ping
```

## Redundant Default Gateway

Utilice el mandato **redundant default gateway** para visualizar las pasarelas IP por omisión redundantes configuradas para cada interfaz.

**Sintaxis:**

red**undant default gateway**

**Ejemplo:**

```
Redundant Default IP Gateways for each interface:
   inf  3   22.2.2.6   255.0.0.0   00.00.00.00.00.AB   backup standby
   inf  4   11.1.1.6   255.0.0.0   00.00.00.00.00.BA   primary active
```

**Nota:** El tipo puede ser “Primary” o “Backup”. El estado puede ser “Active” o “Standby”.

## Reset IP

Utilice el mandato **reset IP** para que entren en vigor determinados cambios en la configuración de IP y RIP. Consulte el tema “Respuesta a mandatos de configuración de IP” en la página 274 para ver una lista de cambios de configuración que entran en vigor con este mandato.

**Sintaxis:**

**reset ip**

**Ejemplo:**

```
IP>interface
Interface  IP Address(es)   Mask(s)
  Eth/0    30.1.1.2         255.255.255.0
           30.1.1.1         255.255.255.0
           153.2.2.25       255.255.255.240
   FR/0    10.69.1.1        255.255.255.0
  PPP/0    0.0.0.0          255.255.0.0
IP>
*talk 6

IP config>add address 0 5.1.1.1 255.255.0.0
IP config>
*talk 5

IP>reset ip

IP>interface
Interface  IP Address(es)   Mask(s)
  Eth/0    5.1.1.1          255.255.0.0
           30.1.1.2         255.255.255.0
           30.1.1.1         255.255.255.0
           153.2.2.25       255.255.255.240
   FR/0    10.69.1.1        255.255.255.0
  PPP/0    0.0.0.0          255.255.0.0

IP>
```

## RIP

Utilice el mandato **rip** para visualizar detalles sobre el estado del protocolo RIP.

**Sintaxis:**

**rip**

**Ejemplo:**

```
IP>rip

                                RIP Interfaces

Interface-Addr  Interface-Mask  Version  In Out  Send-Flags      Receive-Flags
10.69.1.2       255.255.255.0      1      1   0  D,P
200.1.1.2       255.255.255.0      2      1   0  Policy,P        Policy
Send Flags: N=Network S=Subnet H=Host St=Static D=Default O=Outage-Only
            P=PoisonReverse Policy=Send-Policy
Recv Flags: N=Network S=Subnet H=Host OSt=Override-Static OD=Override-Default
            Policy=Receive-Policy

        RIP Policy

Interface-Address  Send Policy        Receive-Policy
10.69.1.2          rip-global-send    rip-global-recv
200.1.1.2          rip-send           rip-receive
RIP global receive policy: rip-global-recv
RIP global send policy: rip-global-send

RIP never originates a default route
```

## RIP-Policy

Utilice el mandato **rip-policy** para visualizar la política RIP que se aplica actualmente a la interfaz especificada.

**Sintaxis:**

**rip-policy**

**Ejemplo:**

```
IP>rip-policy
For which interface [0.0.0.0]? 200.1.1.2

Interface Send Policy: rip-send for 200.1.1.2
Checksum 0x8637  Longest-Match Application

IP Address      IP Mask          Match  Index  Type
-------------------------------------------------------
0.0.0.0         0.0.0.0          Range  1      Include
    Match Conditions:  Protocol: BGP
    Policy Actions:    Set Manual Tag: 0xACEEACEE
                       Set Metric: 3

Interface Receive Policy: rip-receive for 200.1.1.2
Checksum 0x5049  Longest-Match Application

IP Address      IP Mask          Match  Index  Type
-------------------------------------------------------
0.0.0.0         0.0.0.0          Range  1      Include
    Match Conditions:  Source Gateway IP Address Range: 200.1.1.1/255.255.255.255
```

## Route

Utilice el mandato **route** para visualizar la ruta (si existe alguna) a un determinado destino IP. Si existe una ruta, se muestran las direcciones IP de los saltos siguientes junto con información detallada sobre la entrada coincidente de la tabla de direccionamiento.(Consulte el mandato de IP **dump**.)

**Sintaxis:**

**route** *destino-ip*

**Ejemplo: route 133.1.167.2**

```
Destination:    133.1.166.0
Mask:           255.255.254.0
Route type:     SPF
Distance:       1
Age:            1
Tag:            0
Next hop(s):    133.1.167.2       (FR/0)
```

**Ejemplo: route 128.185.230.0**

```
Destination:   128.185.230.0
Mask:          255.255.255.0
Route type:    SPF
Distance:      1
Age:           1
Next hop(s):   128.185.230.0    (TKR/0)
```

**Ejemplo: route 128.185.232.0**

```
Destination:   128.185.232.0
Mask:          255.255.255.0
Route type:    RIP
Distance:      3
Age:           0
Next hop(s):   128.185.146.4   (Eth/0)
```

## Route-table-filtering

Utilice el mandato **route-table-filtering** para visualizar si la función de filtro de tabla de rutas está o no activada y listar los filtros de tabla de rutas definidos.

**Sintaxis:**

**route-table-filtering**

**Ejemplo:** route-table-filtering

```
IP>route-table-filtering
Route Filters

Destination     Mask            Match Type
10.1.1.0        255.255.255.0   BOTH  E
10.1.1.1        255.255.255.255 EXACT I
50.0.0.0        255.0.0.0       BOTH  E
50.50.0.0       255.255.0.0     BOTH  I

IP>
```

## Sizes

Utilice el mandato **sizes** para visualizar los tamaños configurados de determinados parámetros de IP.

**Sintaxis:**

**sizes**

**Ejemplo:** **sizes**

```
Routing table size:         768
Table entries used:         3
Reassembly size:            12000
Largest reassembled pkt:    0
Size of routing cache:      64
# of cache entries in use:  0
```

**Routing table size**
El número configurado de entradas que mantendrá la tabla de direccionamiento.

**Table entries used**
El número de entradas utilizadas procedentes de la tabla de direccionamiento. Este número incluye entradas tanto activas como inactivas. El valor que se muestra con el mandato “dump” como “xx nets known” es el número de entradas activas de la tabla de direccionamiento. El tamaño configurado de la tabla de direccionamiento debe ser suficiente para mantener entradas activas así como otras entradas de direccionamiento anticipadas.

**Reassembly buffer size**
El tamaño configurado del almacenamiento intermedio de reensamblaje que se utiliza para volver a ensamblar paquetes IP fragmentados.

**Largest reassembled pkt**
El paquete IP de mayor tamaño que tiene que volver a ensamblar este direccionador.

**Size of routing cache**
El tamaño configurado de la antememoria de direccionamiento.

**# of cache entries in use**

El número de entradas que se utilizan actualmente procedentes de la antememoria.

## Static Routes

Utilice el mandato **static routes** para visualizar la lista de rutas estáticas configuradas. También se muestran las pasarelas por omisión configuradas y las pasarelas de subred por omisión.

Cada destino de ruta estática se especifica mediante un par dirección-máscara. Las pasarelas por omisión aparecen como rutas estáticas al destino 0.0.0.0 con máscara 0.0.0.0. Las pasarelas de subred por omisión también aparecen como rutas estáticas ante la red completa con subredes IP.

El siguiente ejemplo muestra una pasarela por omisión configurada, una pasarela de subred por omisión configurada (suponiendo que 128.185.0.0 tiene subredes) y una ruta estática a la red 192.9.10.0.

**Sintaxis:**

**static**

```
IP>static routes
Net             Mask            Cost  Next hop
1.1.0.0         255.255.0.0     1     10.1.1.1        TKR/0
                                2     20.1.1.1        TKR/1
                                3     30.1.1.1        TKR/2
2.2.0.0         255.255.0.0     10    10.2.2.2        TKR/0
3.3.0.0         255.255.0.0     100   10.3.3.3        TKR/0
                                200   20.3.3.3        TKR/1

IP>
```

**Net** La dirección de destino de la ruta.

**Mask** La máscara de destino de la ruta.

**Cost** El coste de utilizar esta ruta.

**Next Hop** El siguiente salto por el que pasará un paquete que siga esta ruta.

## Traceroute

Utilice el mandato **traceroute** para visualizar la vía de acceso completa a un determinado destino, salto a salto. Para cada salto sucesivo, **traceroute** envía por omisión tres puntas de prueba y muestra la dirección IP del emisor de la respuesta, junto con el tiempo de envío y respuesta asociado a la respuesta. Si una determinada punta de prueba no recibe respuesta, se muestra un asterisco. Cada línea de la pantalla está relacionada con esta serie de tres puntas de prueba; el número que hay más a la izquierda indica la distancia desde el direccionador que ejecuta el mandato (en saltos de direccionador).

El mandato traceroute termina cuando se alcanza el destino, se recibe un mensaje que indica que no se puede alcanzar el destino ICMP o la longitud de la vía de acceso alcanza un valor máximo por omisión igual a 32 saltos de direccionador.

Cuando una punta de prueba recibe un resultado inesperado, pueden aparecer diversas indicaciones. “!N” significa que se ha recibido un mensaje que indica que no se puede alcanzar el destino ICMP (no se puede alcanzar la red). “!H” significa que se ha recibido un mensaje que indica que no se puede alcanzar el destino

ICMP (no se puede alcanzar el sistema principal). “!P” indica que se ha recibido un mensaje que indica que no se puede alcanzar el destino ICMP (no se puede alcanzar el protocolo); puesto que una punta de prueba es un paquete UDP enviado a un puerto extraño, se espera un mensaje que indique que no se puede alcanzar el puerto. “!” indica que se ha alcanzado el destino, pero la respuesta enviada por el destino se ha recibido con un valor de TTL igual a 1. Esto suele indicar un error en el destino, especialmente en algunas versiones de UNIX, por el que el destino inserta el TTL de la punta de prueba en sus respuestas. Esto genera una serie de líneas que solo contienen asteriscos antes de alcanzar finalmente el destino.

**Sintaxis:**

tr**aceroute** *dirección-dest [dirección-origen tamaño-datos puntas-prueba espera tos ttl-máx]*

**dirección-dest**
La dirección más alejada de la ruta.

**dirección-origen**
La dirección de origen desde la que se origina el rastreo.

**tamaño-datos**
El tamaño en bytes del campo de datos del mensaje traceroute. El campo de datos no incluye la cabecera UDP.

**puntas-prueba**
número de mensajes traceroute de UDP enviados desde cada salto.

**espera** tiempo en segundos entre reintentos.

**tos** >El valor de los bits TOS en los mensajes UDP. Por ejemplo, un valor de X'10' (B'00010000') define para los bits TOS el valor B'1000'. El valor por omisión es 0, que define para los bits TOS el valor B'1000'.

**ttl-máx** Tiempo de vida máximo en segundos para cada mensaje.

**Ejemplo:**

```
IP> traceroute Destination IP address [0.0.0.0]? 128.185.142.239
Source IP address [128.185.142.1]?
Data size in bytes [56]?
Number of probes per hop [3]?
Wait time between retries in seconds [3]?
Maximum TTL [32]?
Traceroute TOS (00-FF) [0]? 10

TRACEROUTE 128.185.142.1 -> 128.185.142.239: 56 data bytes
1 128.185.142.7 16 ms 0 ms 0 ms
2 128.185.123.22 16 ms 0 ms 16 ms
3 * * *
4 * * *
5 128.185.124.110 16 ms ! 0 ms ! 0 ms !
```

**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 tardado el paquete en llegar a su destino. Se efectúan tres rastreos del paquete.

**Destination unreachable**
Indica que no hay ninguna ruta al destino disponible.

**3 * * *** Indica que el direccionador espera algún tipo de respuesta del destino, pero dicho destino no responde.

## UDP-Forwarding

Utilice el mandato **UDP-forwarding** para visualizar las direcciones y el puerto UDP añadidos mediante el mandato **add udp-destination** o el mandato **enable udp-forwarding**.

**Sintaxis:**

u**dp-forwarding**

**Ejemplo: udp-forwarding**

```
UDP Port   IP Address
    35      20.2.1.1
    20      22.2.1.2
```

## VRID

Utilice el mandato **VRID** para visualizar el estado detallado correspondiente a un determinado direccionador virtual identificado mediante una dirección de interfaz y un VRID.

**Sintaxis:**

vrid

**Ejemplo:**

```
IP>vrid 153.2.2.25 1

             --- Detailed VRID Information ----

            Interface address:      153.2.2.25
            Interface mask:         255.255.255.240
            VRID:                   1
            VRID State:             MASTER
            Virtual MAC Address:    00:00:5E:00:00:01
            Source MAC Address:     00:00:5E:00:00:01
            Ethernet V2 Interface:  UP

  Priority:             255       Advertise interval:   1
  Advertise Timer:      1         Skew (in ticks):      0
  Authentication Type:  NONE      Authentication Key:
  State transitions:    1         Advertisements out:   9019
  Advertisements in:    0         Advertisements error: 0
  ARPs Modified:        22        Gratuitous ARPs:      2

                  VRID Addresses
153.2.2.25        5.1.1.1
```

# VRRP

Utilice el mandato **VRRP** para visualizar información de resumen

**Sintaxis:**

vrrp

**Ejemplo:**

```
                                --VRID Summary--
IP address       VRID  State  Advertise Master-Dead  Address(es)
153.2.2.25          1  MASTER         1         N/A  153.2.2.25
                                                     5.1.1.1
```

# Utilización de OSPF

Este capítulo describe cómo utilizar el protocolo Open Shortest Path First (OSPF), que es un Protocolo de pasarela interior (IGP). El direccionador da soporte a los siguientes IGP para crear la tabla de direccionamiento IP: protocolo Open Shortest Path First (OSPF) y protocolo RIP. OSPF se basa en la tecnología de estado de enlace o algoritmo vía de acceso más corta primero (SPF). RIP se basa en el algoritmo Bellman-Ford o algoritmo de vector de distancia.

Este capítulo incluye las siguientes secciones:



Los direccionadores que utilizan un protocolo de direccionamiento común forman un *sistema autónomo* (AS). Este protocolo de direccionamiento común se denomina Protocolo de pasarela interior (IGP). Los IGP detectan de forma dinámica información sobre el nivel de alcance de la red y sobre direccionamiento de un AS y utilizan esta información para crear la tabla de direccionamiento IP. Los IGP también pueden importar información de direccionamiento externa en el AS. El direccionador puede ejecutar simultáneamente OSPF y RIP. Cuando lo hace, son más recomendable las rutas OSPF. En general, se recomienda el uso del protocolo OSPF debido a su potencia, nivel de respuesta y menor requisito de ancho de banda.

## El protocolo de direccionamiento OSPF

El direccionador da soporte a una implantación completa del protocolo de direccionamiento OSPF, tal como se especifica en RFC 1583 (Versión 2). OSPF es un protocolo de direccionamiento dinámico de estado de enlace que detecta y aprende las mejoras rutas a los destinos que se pueden alcanzar. OSPF puede detectar con rapidez cambios en la topología de un AS y, tras un breve periodo de convergencia, calcula nuevas rutas. El protocolo OSPF no encapsula paquetes IP, sino que los reenvía en función únicamente de la dirección de destino.

## Resumen del direccionamiento OSPF

Cuando se inicializa un direccionador, utiliza el protocolo Hello para enviar paquetes Hello a sus direccionadores contiguos, los cuales envían por turnos paquetes al direccionador. En redes de difusión general y punto a punto, el direccionador detecta de forma dinámica sus direccionadores contiguos enviando paquetes Hello a la dirección de difusión múltiple *ALLSPFRouters (224.0.0.5);* en redes que no son de difusión general, el usuario debe configurar información que ayude al direccionador a descubrir a sus direccionadores *contiguos*. En todas las redes multiacceso (de difusión general y no de difusión general), el protocolo Hello elige también un *direccionador designado* para la red.

**Nota:** Para las redes ATM, RFC 1577 permitirá a IP utilizar la red como una red de acceso múltiple no de difusión general. Por lo tanto, se debe configurar OSPF dando por supuesto que se trata de una red que no es de difusión general. Si utiliza Emulación de LAN, la red se trata como una red de difu-

sión general, y debe configurar OSPF en consecuencia. Si utiliza tanto RFC 1577 como Emulación de LAN en una sola interfaz física, configure OSPF como no de difusión general en las interfaces RFC 1577 (se asignan direcciones IP a la interfaz real, por ejemplo ATM/0), y configure OSPF como de difusión general en interfaces virtuales o emuladas (se asignan direcciones IP a interfaces virtuales o emuladas, por ejemplo TKR/0).

Luego el direccionador intenta formar adyacencias con sus direccionadores contiguos a fin de sincronizar sus bases de datos topológicas. Las adyacencias controlan la distribución (envío y recepción) de paquetes del protocolo de direccionamiento, así como la distribución de las actualizaciones de bases de datos topológicas. En una red multiacceso, el direccionador designado determina qué direccionadores son adyacentes.

Un direccionador anuncia periódicamente su estado o estado de enlace a sus adyacencias. Los *anuncios de estado de enlace* (LSA) fluyen por un área, asegurando que todos los direccionadores tienen exactamente la misma base de datos topológica. Esta base de datos es una recopilación de los anuncios de estado de enlace recibidos de cada direccionador perteneciente a un área. A partir de la información de esta base de datos, cada direccionador puede calcular el árbol de vía de acceso más corta, designándose a sí mismo como raíz. Luego el árbol de vía de acceso más corta genera la tabla de direccionamiento.

OSPF ofrece servicios que no están disponibles con RIP. OSPF incluye las siguientes características:

- *Direccionamiento de menor coste.* Le permite configurar costes de vías de accesos en función de cualquier combinación de parámetros de la red. Por ejemplo, ancho de banda, retraso y coste en dólares.
- *No hay limitaciones en la métrica de direccionamiento.* Mientras que RIP restringe la métrica de direccionamiento a 16 saltos, OSPF no impone ninguna restricción.
- *Direccionamiento de varias vías de acceso.* Le permite utilizar varias vías de acceso de igual coste que conectan los mismos puntos. Luego puede utilizar estas vías de acceso para la distribución de cargas, lo que le permite utilizar de forma más eficiente el ancho de banda.
- *Direccionamiento de áreas.* Reduce los recursos (memoria y ancho de banda de la red) que consume el protocolo y ofrece un nivel adicional de protección de direccionamiento.
- *Máscaras de subred de longitud variable.* Le permite dividir una dirección IP en subredes de tamaño variable, conservando el espacio de direcciones IP.
- *Autentificación de direccionamiento.* Ofrece seguridad de direccionamiento adicional.

OSPF da soporte a los siguientes tipos de redes físicas:

- *Punto a punto.* Redes que utilizan una línea de comunicación para unir un par de direccionadores. Una línea serie de 56 Kbps que conecta dos direccionadores es un ejemplo de una red punto a punto.
- *Difusión general.* Redes que dan soporte a más de dos direccionadores conectados que pueden enviar un solo mensaje físico a todos los direccionadores conectados. Una red en anillo es un ejemplo de red de difusión general. Las LAN emuladas sobre ATM tratan la red ATM como una red de difusión general.

- *Multiacceso no de difusión general (NBMA).* Redes que dan soporte a más de dos direccionadores conectados, pero no disponen de la función de difusión general. Una red de datos pública X.25 es un ejemplo de una red que no es de difusión general. Para que OSPF funcione correctamente, esta red necesita información de configuración adicional sobre los otros direccionadores OSPF conectados a la red que no es de difusión general. IP clásico sobre ATM (RFC 1577) trata la interfaz ATM como una interfaz de acceso múltiple no de difusión general (NBMA).
- *Punto a multipunto.* Redes que dan soporte a más de dos direccionadores conectados, no disponen de la función de difusión general y no forman una malla completa. Una red Frame Relay sin PVC entre todos los direccionadores conectados es un ejemplo de red punto a multipunto. Al igual que las redes que no son de difusión general, se necesita información de configuración adicional sobre los demás direccionadores OSPF conectados a la red.

## Direccionador designado

Cada red de difusión general o multiacceso no de difusión general tiene un direccionador designado que lleva a cabo dos funciones principales correspondientes al protocolo de direccionamiento: origina anuncios de enlace de red y pasa a ser adyacente a los demás direccionadores de la red.

Cuando un direccionador designado origina anuncios de enlace de red, lista todos los direccionadores, incluido él mismo, actualmente conectados a la red. El ID de enlace correspondiente a esta nuncio es la dirección de interfaz IP del direccionador designado. Al utilizar la máscara de subred/red, el direccionador obtiene el número de red IP.

El direccionador designado pasa a ser adyacente a los demás direccionadores y se convierte en el encargado de sincronizar las bases de datos de estado de enlace de la red de difusión general.

El protocolo Hello de OSPF elige el direccionador designado después de determinar la prioridad del direccionador a partir del campo *Rtr Pri* del paquete Hello. La primera vez que la interfaz del direccionador pasa a estar operativa, comprueba si la red tiene actualmente un direccionador designado. Si es así, acepta dicho direccionador designado, independientemente de la prioridad de este direccionador; de lo contrario, se declara a sí mismo direccionador designado. Si el direccionador se declara a sí mismo direccionador designado al mismo tiempo que lo hace otro direccionador, el direccionador con la prioridad de direccionador más alta (*Rtr Pri*) se convierte en el direccionador designado. Si los campos *Rtr Pri* de ambos son iguales, se elige el que tiene el ID de direccionador más alto.

Una vez se ha elegido un direccionador designado, este se convierte en el punto final de muchas adyacencias. En una red de difusión general, esto optimiza el procedimiento de flujo al permitir a la ruta designada realizar una difusión múltiple de sus paquetes de actualización de estado de enlace a la dirección ALLSPFRouters (224.0.0.5), en lugar de tener que enviar distintos paquetes sobre cada adyacencia.

## OSPF de difusión múltiple

El envío de difusiones múltiples es una técnica de LAN que permite pasar copias de un solo paquete a un subconjunto seleccionado de todos los destinos posibles. Algunos elementos de hardware (Ethernet, por ejemplo) dan soporte a la difusión múltiple, permitiendo que una interfaz de red pertenezca a uno o varios grupos de difusión múltiple. Consulte el tema “Soporte de difusión múltiple IP” en la página 267 para obtener más información sobre el soporte del direccionador de difusión múltiple IP.

El protocolo OSPF da soporte al direccionamiento de difusión múltiple IP a través de extensiones de difusión múltiple de OSPF (MOSPF).

Un direccionador MOSPF distribuye información sobre la ubicación de grupos a través del dominio de direccionamiento, enviando un nuevo tipo (tipo 6) de anuncio de estado de enlace, el LSA de pertenencia a grupo. Esto permite a los direccionadores MOSPF reenviar de forma eficiente un datagrama de difusión múltiple a sus diversos destinos. Cada direccionador lo hace calculando la vía de acceso del datagrama de difusión múltiple como un árbol cuya raíz es el origen del datagrama y cuyas ramas de terminal son LAN que contienen miembros del grupo.

Al ejecutar MOSPF, el reenvío de datagramas de difusión múltiple funciona de las siguientes formas:

- Aunque el reenvío de difusiones múltiples IP no es fiable, los datagramas de difusión múltiple IP se distribuyen de la misma manera que los envíos de difusión individual IP.
- Los datagramas de difusión múltiple viajan por la vía de acceso más corta entre el origen del datagrama y cualquier destino determinado (coste de estado de enlace OSPF). Esto sucede porque se crea un árbol para cada par de origen del datagrama y grupo de destino.
- Un datagrama de difusión múltiple se reenvía como una difusión múltiple de enlace de datos en cada salto. No se utiliza el protocolo ARP. Para algunas tecnologías de red, se produce una correlación entre las direcciones IP de clase D y la difusión múltiple de enlace de datos, mientras que para otras, las direcciones IP de clase D se correlacionan con direcciones de difusión general de enlace de datos.
- Cuando vías de acceso entre el origen del datagrama y dos miembros del grupo comparten un segmento inicial común, sólo se reenvía un datagrama hasta que la vía de acceso se bifurca en distintas direcciones. La vía de acceso se puede dividir en un direccionador o en una red. Si la vía de acceso se divide en un direccionador, este duplica el paquete antes de que se envíe. Si la vía de acceso se divide en una red, esta duplica a través de una difusión múltiple de enlace de datos.
- Una configuración de red puede incluir direccionadores MOSPF y direccionadores sin extensiones de difusión múltiple. En esta configuración, todos los direccionadores interoperan en el direccionamiento de difusiones individuales. Esto le permite incorporar paulatinamente en una interred la función de difusión múltiple.

  Algunas configuraciones de direccionadores MOSPF y no MOSPF puede generar errores inesperados en el direccionamiento de difusión múltiple.

- El direccionador se puede configurar para enviar rupturas SNMP a una dirección de grupo de difusión múltiple añadiendo una dirección de grupo a un determinado nombre de comunicad SNMP.

## Configuración de OSPF

Las siguientes secciones contienen información sobre cómo configurar inicialmente el protocolo OSPF. Esta información describe las tareas necesarias para configurar y poner a punto el protocolo OSPF. Encontrará información sobre cómo efectuar cambios en la configuración en el tema “Mandatos de configuración de OSPF” en la página 381.

Los pasos siguientes describen las tareas necesarias para configurar y poner a punto el protocolo OSPF. Las siguientes secciones explican en detalle cada paso e incluyen ejemplos.

Antes de que el direccionador pueda ejecutar el protocolo OSPF, debe:

1. Activar el protocolo OSPF. Para hacerlo, debe estimar el tamaño final del dominio de direccionamiento OSPF. (Consulte el tema “Activación del protocolo OSPF” en la página 364.)
2. Definir el ID de direccionador OSPF. Para tecnologías de red que no dan soporte a la difusión general o a la difusión múltiple de enlace de datos (como por ejemplo Frame Relay), el direccionador debe duplicar el datagrama de difusión múltiple y lo debe reenviar como una difusión individual de enlace de datos. (Consulte el tema “Definición de ID de direccionadores OSPF” en la página 364.)
3. Definir áreas OSPF conectadas al direccionador. Si no hay áreas OSPF definidas, se da por supuesto que se trata de una sola área de red troncal. (Consulte el tema “Definición de áreas OSPF conectadas y de la red troncal” en la página 365.)
4. Definir las interfaces de red OSPF del direccionador. Defina el coste de enviar un paquete a cada interfaz, junto con una serie de parámetros operativos de OSPF. (Consulte el tema “Definición de interfaces OSPF” en la página 368.)
5. Si desea reenviar difusiones múltiples IP (direcciones IP de Clase D), debe activar la función de direccionamiento de difusión múltiple IP. (Consulte el tema “Reenvío de difusiones múltiples” en la página 371.)
6. Si las interfaces del direccionador a redes que no son de difusión general (X.25, IP clásico sobre ATM o Frame-Relay), debe definir parámetros de interfaz adicionales. (Consulte los temas “Definición de parámetros de interfaz de red que no es de difusión general” en la página 371 y “Configuración de subredes de área amplia” en la página 372.)
7. Si desea que el direccionador importe rutas aprendidas de otros protocolos de direccionamiento que se ejecutan en este direccionador (BGP, RIP o rutas configuradas de forma estática), debe activar el direccionamiento límite AS. Además, debe definir qué rutas se importan como externas de Tipo 2 o de Tipo 1. (Consulte el tema “Activación del direccionamiento límite AS” en la página 373.)
8. Si desea arrancar mediante un direccionador contiguo sobre una interfaz conectada punto a punto o punto a multipunto, debe configurar la dirección IP

del direccionador contiguo. Para eso, añada un direccionador contiguo OSPF correspondiente al destino de la interfaz punto a punto.

## Activación del protocolo OSPF

Al activar el protocolo de direccionamiento OSPF, debe especificar los dos valores siguientes para estimar el tamaño final del dominio de direccionamiento OSPF:

- Número total de rutas externas AS que se importarán en el dominio de direccionamiento OSPF. Un solo destino puede dar lugar a varias rutas externas si lo importan distintos direccionadores límite AS. Por ejemplo, si el dominio de direccionamiento OSPF tiene dos direccionadores límite AS, y ambos importan rutas a los mismos 100 destinos, defina como número de rutas externas AS el valor 200.
- Número total de direccionadores OSPF del dominio de direccionamiento.

Configure estos dos valores de forma idéntica en todos los direccionadores OSPF. Cada direccionador que ejecuta el protocolo OSPF tiene una base de datos que describe un mapa del dominio de direccionamiento. Esta base de datos es idéntica en todos los direccionadores participantes. A partir de esta base de datos se crea la tabla de direccionamiento IP mediante la construcción del árbol de la vía de acceso más corta, siendo el direccionador la raíz. El dominio de direccionamiento hace referencia a un AS que ejecuta el protocolo OSPF.

Para activar el protocolo de direccionamiento OSPF, consulte el mandato **enable** que se muestra en el siguiente ejemplo.

```
OSPF Config> enable ospf
Estimated # external routes[100]? 200
Estimated # OSPF routers [50]? 60
Maximum Size LSA [0]? 2048
```

Normalmente, 2048 bytes es suficiente para cualquier Anuncio de estado de enlace (LSA) generado por el direccionador. Sin embargo, puede que los direccionadores que tienen muchos enlaces de marcación OSPF (como los enlaces de marcación ISDN) necesiten un LSA mayor. Además, en estas situaciones puede que se necesite aumentar el parámetro **packet-size** en la configuración general.

### Definición de ID de direccionadores OSPF

Cada direccionador de un dominio de direccionamiento OSPF debe tener asignado un ID de direccionador exclusivo de 32 bits. Elija el valor utilizado como ID de direccionador OSPF del siguiente modo:

- Si el mandato **set router ID** de configuración de IP, el valor configurado se utiliza como un ID de direccionador OSPF. El ID de direccionador OSPF configurado debe ser una de las direcciones IP del direccionador o la dirección interna.
- Si utiliza el mandato **set internal address** de configuración de IP, la dirección configurada se utiliza como el ID de direccionador OSPF. Se recomienda utilizar el mismo valor para el ID del direccionador y la dirección interna, si se define.
- Si no se ha configurado ni el ID de direccionador ni la dirección interna durante la configuración de IP, la dirección de la primera interfaz OSPF se utilizará como el ID de direccionador OSPF.

## Definición de áreas OSPF conectadas y de la red troncal

La Figura 34 en la página 366 muestra un diagrama de ejemplo de la estructura de un dominio de direccionamiento OSPF. Hay una división entre las subredes IP de dentro del dominio OSPF y las subredes IP externas al dominio OSPF. Las subredes que se incluyen en el dominio OSPF se subdividen en regiones denominadas *áreas*. Las áreas OSPF son grupos de subredes IP contiguas. La función de las áreas consiste en reducir la actividad general OSPF necesaria para encontrar rutas a destinos que están en otra área. La actividad general se reduce porque los direccionadores intercambian menos información y porque se necesitan menos ciclos de CPU para un cálculo de tabla de ruta menos complejo.

Cada dominio de direccionamiento OSPF debe tener al menos un *área de red troncal*. La red troncal siempre se identifica mediante el número de área 0.0.0.0. Para redes OSPF pequeñas, la red troncal es la única área necesaria. Para redes de mayor tamaño, con varias áreas, la red troncal ofrece un núcleo que conecta las áreas. A diferencia de otras áreas, las subredes de la red troncal pueden estar físicamente separadas. En este caso, la conectividad lógica de la red troncal se mantiene configurando *enlaces virtuales* entre direccionadores de las áreas de tránsito participantes que no son de la red troncal.

Los direccionadores que se conectan a más de una de un área funcionan como *direccionadores límite* del área. Todos los direcciones límite de área forman parte de la red troncal, de modo que un direccionador límite debe conectarse directamente a una subred IP de red troncal o a otro direccionador de red troncal sobre un enlace virtual. Además, debe haber una serie de subredes de red troncal y enlaces virtuales que se conectan a todos los direccionadores de red troncal.

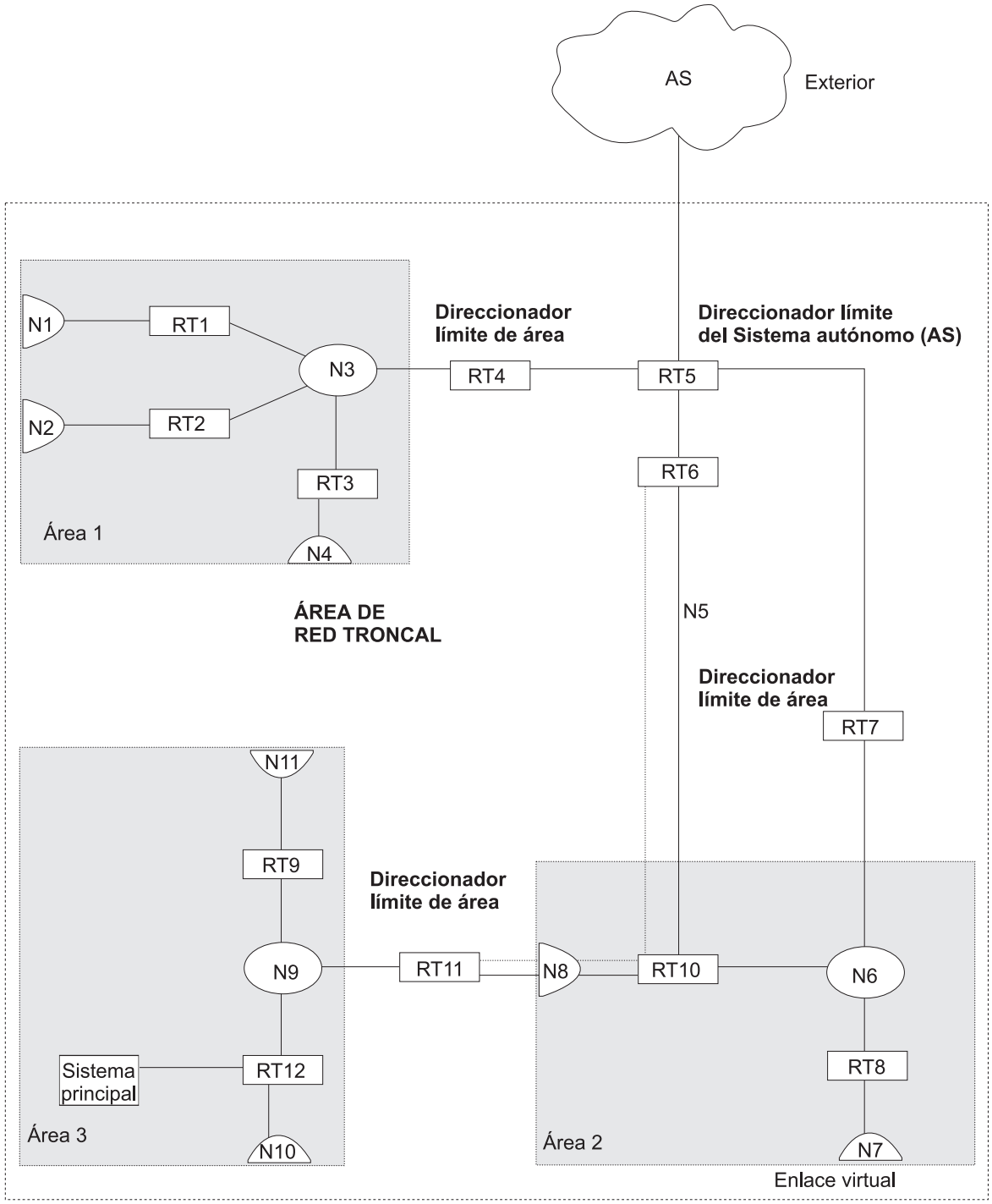



*Figura 34. Áreas de OSPF*

La información y algoritmos que utiliza OSPF para calcular rutas varía en función de si la subred IP de destino está dentro de la misma área, está en un área diferente del mismo dominio o es externa al dominio OSPF. Cada direccionador mantiene un mapa completo de todos los enlaces dentro de su área. Todos los enlaces de direccionador a red multiacceso, de red a direccionador multiacceso y de direccionador a direccionador se incluyen en el mapa. Se utiliza un algoritmo tipo primero la vía de acceso más corta para calcular las mejores rutas a destinos dentro del área a partir de este mapa. Las rutas entre áreas se calculan a partir

de anuncios de resumen originados por direccionadores límite de área para subredes IP, rangos de subredes IP y direccionadores límite externos del sistema autónomo (ASE) situados en otras áreas del dominio OSPF. Las rutas externas se calculan a partir de anuncios ASE que originan los direccionadores límite ASE y envían a través del dominio de direccionamiento OSPF.

La red troncal es la responsable de distribuir la información de direccionamiento entre áreas. El área de red troncal puede constar de:

- Redes que pertenecen al área 0.0.0.0
- Direccionadores conectados a dichas áreas
- Direccionadores pertenecientes a distintas áreas
- Enlaces virtuales configurados

Utilice el mandato **set area** para definir áreas a las que se conecta un direccionador. Si no utiliza el mandato **set area**, el valor por omisión consiste en que todas las interfaces del direccionador se conectan a la red troncal.

Cuando se configuran direccionadores límite de área, se pueden utilizar las opciones de los mandato **set area** y **add range** para controlar qué información de rutas OSPF cruza el límite de área.

Una opción consiste en utilizar el mandato **set area** para definir un área como un *apéndice*. Los anuncios ASE de OSPF nunca se envían a las áreas apéndice. Además, el mandato **set area** tiene una opción que sirve para suprimir la generación en el apéndice de anuncios resumen para rutas entre áreas. Los direccionadores límite de área anuncian rutas por omisión a las áreas apéndice. El tráfico interno del apéndice destinado a subredes IP desconocidas se reenvía al direccionador límite de área. El direccionador límite utiliza su información de direccionamiento más completa para reenviar el tráfico por una vía de acceso adecuada a su destino. Un área no se puede configurar como un apéndice si se utiliza como área de tránsito para enlaces virtuales.

La otra opción consiste en utilizar rangos de direcciones de subredes IP para limitar el número de anuncios de resumen que se utilizan para anuncios entre áreas de subredes de un área. Un rango se define mediante una dirección IP y una máscara de dirección. Se considera que una subred entra dentro del rango si la dirección IP de la subred y la dirección IP del rango coinciden una vez aplicada la máscara del rango a ambas direcciones.

Cuando se añade un rango correspondiente a un área a un direccionador límite de área, el direccionador límite suprime los anuncios de resumen correspondientes a subredes de las áreas incluidas en el rango. Los anuncios suprimidos se habrían originado para otras áreas a las que se conecta el direccionador límite. En su lugar, el direccionador límite de área puede originar un solo anuncio resumen para el rango o puede no emitir anuncios en absoluto, en función de la opción seleccionada con el mandato add range.

Tenga en cuenta que si el rango no se anuncia, no habrá rutas entre áreas correspondientes a ningún destino que quede dentro del rango. Tenga también en cuenta que no se pueden utilizar rangos para áreas que los enlaces virtuales utilizan como áreas de tránsito.

Para definir los parámetros correspondientes a un área OSPF, utilice el mandato **set area** y responda a las siguientes solicitudes:

```
Area number [0.0.0.0]? 0.0.0.1
Is this a stub area? [No]:  yes
Stub default cost? [0]:
Import summaries? [Yes]:
```

Defina un área como apéndice como:

1. No hay necesidad de que el área maneje tráfico de red troncal de tránsito.
2. Los direccionadores de área pueden utilizar un valor por omisión generado por el direccionador límite de área para el tráfico destinado fuera del AS.
3. No hay necesidad de que los direccionadores de área sean direccionadores límites AS (direccionadores OSPF que anuncian rutas de fuentes externas como anuncios externos AS).

En este caso, sólo los direccionadores límite de área y los direccionadores de red troncal tendrán que calcular y mantener rutas externas AS.

# Definición de interfaces OSPF

Las interfaces OSPF son un subconjunto de interfaces IP definidas durante la configuración de IP. Los parámetros configurados para las interfaces OSPF determinan la topología del dominio OSPF, las rutas que se seleccionarán a través del dominio y las características de la interacción entre direccionadores OSPF conectados directamente. El mandato **set interface** sirve para definir una interfaz OSPF y para especificar algunas de sus características. Otras características de la interfaz se especifican como respuesta a la solicitud **add address** durante la configuración de IP.

## Topología del dominio OSPF

La definición de la topología de un dominio OSPF depende de una definición sobre qué rutas se conectan directamente en el soporte técnico o la tecnología de subred del área de la que forman parte dichas conexiones. La topología básica consiste en que todos los direccionadores conectados a una subred física se conecten directamente, pero se pueden definir varias subredes IP sobre una sola subred física. En este caso, OSPF considera que los direccionadores se conectan directamente sólo si tienen interfaces OSPF conectadas a la misma subred IP. También hay casos en que los direccionadores conectados a la misma subred no tienen una conexión directa de capa de enlace.

En el caso de un soporte de LAN, los direccionadores OSPF conectados directamente se determinan a partir de la subred IP y el soporte físico asociados a una interfaz OSPF. La dirección IP de la interfaz OSPF se especifica como respuesta a la solicitud **Interface IP address**. Esta dirección debe coincidir con la dirección de una interfaz IP definida con el mandato **add address** durante la configuración de IP. La dirección IP, junto con la máscara de subred definida con el mandato **add address**, determina la subred IP a la que se conecta la interfaz OSPF. El *índice de red* asociado a la interfaz IP mediante el mandato add address determina la subred física a la que se conecta la interfaz OSPF. La función de difusión general de las LAN permite a OSPF utilizar mensajes Hello de difusión múltiple para descubrir otras rutas que tienen interfaces conectadas a la misma subred IP. Por lo tanto, los parámetros de la interfaz son todos los necesarios para que OSPF pueda determinar qué direccionadores están directamente conectados a través de una LAN.

Se pueden utilizar LAN para conectar un direccionador OSPF a sistemas principales IP. En este caso, sigue siendo necesario definir una interfaz OSPF con cualquier subred IP definida para la LAN. De lo contrario, OSPF no generará rutas con

dichas subredes IP como destino. Para evitar el tráfico de mensajes Hello de OSPF a las LAN que no tienen direccionadores conectados, la red se puede definir como una red multiacceso que no es de difusión general. El valor de la prioridad debe ser cero, puesto que no se necesita ningún direccionador designado.

Los requisitos para configurar interfaces OSPF que se conectan a líneas serie varían según la tecnología de la capa inferior.

Para líneas punto a punto, sólo se puede acceder a otro direccionador sobre la interfaz, de modo que el direccionador conectado directamente se puede determinar sin configuración adicional. De hecho, puesto que no es necesario configurar ninguna subred IP, las interfaces OSPF no numeradas se pueden utilizar para líneas punto a punto. En este caso, el mismo índice de red que se utiliza como dirección IP correspondiente al mandato add address de IP se utiliza como la dirección IP correspondiente al mandato set interface de OSPF.

Para tecnologías de subred como Frame Relay, ATM y X.25, que dan soporte a conexiones con varios direccionadores sobre una sola línea serie, la configuración de las interfaces OSPF es parecida a la de una LAN, pero, puesto que los direccionadores conectados directamente no se descubren de forma dinámica para estas tecnologías de subred, se necesita información adicional para especificar los direccionadores contiguos conectados directamente. Para obtener información sobre la configuración necesaria, consulte el tema “Configuración de subredes de área amplia” en la página 372.

## Costes de enlaces OSPF

OSPF calcula rutas buscando la vía de acceso de menor coste a un destino. El coste de cada vía de acceso es la suma de los costes correspondientes a distintos enlaces de la vía de acceso. El coste de un enlace con un direccionador conectado directamente se especifica en el mandato **set interface** para **Type of Service 0 cost**.

El hecho de configurar correctamente los costes de acuerdo con la necesidad de utilizar interfaces para el tráfico de datos resulta crítico para obtener las rutas deseadas a través de un dominio OSPF. Los factores que hacen que un enlace resulte más o menos adecuado pueden varias según las distintas redes, pero el objetivo común consiste en elegir rutas con el mínimo retardo y la mayor capacidad posibles. En general, esta política se puede conseguir haciendo que el coste de un enlace sea inversamente proporcional al ancho de banda del soporte utilizado para la subred física.

Un enfoque recomendado consiste en utilizar un coste igual a uno para la tecnología con mayor ancho de banda. Por ejemplo, utilice el valor 1 como el coste correspondiente a una interfaz que ejecuta ATM a 100 Mbps.

| *Tabla 22. Costes de ejemplo correspondientes a enlaces OSPF* | |
|---|---|
| Ancho de banda de la interfaz | Coste |
| ATM a 155 Mbps | 1 |
| Ethernet | 10 |
| Res en anillo a 16 Mbps | 6 |
| Red en anillo a 4 Mbps | 25 |
| Línea serie | Coste basado en el ancho de banda |
| Red en anillo emulada (vea la nota.) | 1 |
| Ethernet emulada (vea la nota.) | 1 |

**Nota:** Una Red en anillo o Ethernet emuladas funcionarán a la velocidad de la interfaz (por ejemplo, 155 Mbps), y se deben configurar con un coste igual a 1.

ATM se puede conectar a redes a una velocidad menor que la velocidad máxima de línea. Por ejemplo, si el direccionador tiene un puerto capaz de funcionar a 155 Mbps y un direccionador se conecta al mismo a 25 Mbps, este enlace se seguirá tratando como un enlace de coste igual a 1. La ponderación de OSPF se basa en interfaz.

El coste de una interfaz OSPF se puede modificar de forma dinámica desde el entorno de supervisión del direccionador. El nuevo coste se envía rápidamente a través del dominio de direccionamiento OSPF, y modifica el direccionamiento de forma inmediata.

Cuando un direccionador se vuelve a arrancar o a cargar, el coste de la interfaz pasa a ser el valor que se ha configurado en SRAM.

## Interacciones entre direccionadores contiguos

Varios de los valores configurados con el mandato **set interface** sirven para especificar parámetros que controlan la interacción de de direccionadores conectados directamente. Estos incluyen:

- Intervalo de retransmisión
- Retraso de transmisión
- Prioridad de direccionador
- Intervalo de Hello
- Intervalo de direccionador inactivo
- Circuito de demanda
- Supresión de Hello
- Intervalo de sondeo
- Clave de autentificación

En la mayoría de los casos, se pueden utilizar los valores por omisión.

**Nota:** El intervalo de Hello, el intervalo de direccionador inactivo y la clave de autentificación deben tener el mismo valor para todos los direccionadores OSPF que se conectan a la misma subred IP. Si los valores no coinciden, los direccionadores no podrán formar conexiones directas (adyacencias).

## Reenvío de difusiones múltiples

Para activar el direccionamiento de datagramas de difusión múltiple IP (clase D), utilice el mandato **enable multicast-routing**. Al activar el direccionamiento de difusión múltiple, se le solicitará si desea que el direccionador reenvíe difusiones múltiples entre áreas OSPF.

```
OSPF Config>enable multicast forwarding
Inter-area multicasting enabled?  [No]: yes
```

La primera vez que se invoca el mandato **enable multicast forwarding**, se activa la difusión múltiple en todas las interfaces OSPF con parámetros por omisión.

Si desea modificar los parámetros MOSPF, utilice el mandato **set interface**. Se le solicitarán parámetros de difusión múltiple únicamente si tiene activado el reenvío de difusiones múltiples.

En las redes basadas en un Sistema autónomo, en las que puede haber varios protocolos de direccionamiento de difusión múltiple (o varias instancias de un solo protocolo de direccionamiento de difusión múltiple), es posible que tenga que configurar el reenvío como difusiones individuales de enlace de datos para evitar la duplicación no deseada de datagramas. En cualquier caso, para todos los direccionadores conectados a una red común, los parámetros de interfaz forward multicast datagrams y forward as data-link unicasts se deben configurar de forma idéntica.

## Definición de parámetros de interfaz de red que no es de difusión general

Si el direccionador está conectado a una red multiacceso que no es de difusión general, como una X.25 PDN, tiene que configurar los siguientes parámetros para ayudar al direccionador a descubrir sus direccionadores OSPF contiguos. Esta configuración sólo es necesaria si el direccionador puede ser elegido como direccionador designado de la red que no es de difusión general.

Primero configure el intervalo de sondeo de OSPF con el siguiente mandato:

```
OSPF Config> set non-broadcast
Interface IP address [0.0.0.0]? 128.185.138.19
Poll Interval [120]?
```

Luego configure las direcciones IP de los demás direccionadores OSPF que se conectarán a la red que no es de difusión general. Para cada direccionador configurado, debe especificar también la probabilidad de elección como direccionador designado.

```
OSPF Config> add neighbor
Interface IP address [0.0.0.0]? 128.185.138.19
IP Address of Neighbor [0.0.0.0]? 128.185.138.21
Can that router become Designated Router [Yes]?
```

También puede utilizar la definición de red que no es de difusión general para forzar el envío de anuncios a una red que no tenga ningún otro direccionador OSPF. La prioridad del direccionador correspondiente a la interfaz debe ser cero y no se debe definir ningún direccionador contiguo.

## Configuración de subredes de área amplia

Frame Relay, IP clásico sobre ATM y X.25 permite conexiones directas entre distintos direccionadores sobre una sola línea serie. Se necesitan más pasos de configuración, además de los realizados con el mandato **set interface**, para las interfaces OSPF que se conectan a este tipo de red. Puesto que los mensajes del protocolo OSPF se envían directamente a un determinado direccionador contiguo en estas redes, se utiliza la configuración en lugar del descubrimiento dinámico para determinar las relaciones entre los direccionadores contiguos y el papel que juega cada direccionador.

**Nota:** Las configuraciones descritas en esta sección no se aplican a redes punto a punto.

OSPF puede adoptar uno de estos dos patrones para las conexiones directas entre direccionadores a través de estas subredes:

- Punto a multipunto
- Multiacceso no de difusión general (NBMA)

El factor clave que distingue estos dos patrones es si hay o no una conexión directa entre todos los pares de direccionadores que se conectan a la subred (*conectividad de malla completa*) o si algunos de los direccionadores sólo se pueden conectar a través de vías de acceso de varios saltos con otros direccionadores como intermediarios (*conectividad de malla parcial*).

El multiacceso no de difusión general (NBMA) necesita *conectividad de malla completa*, mientras que el patrón punto a multipunto sólo necesita *conectividad de malla parcial*.

Punto a multipunto es la opción por omisión, puesto que funciona tanto para conectividad de malla completa como para conectividad de malla parcial. Cuando se dispone de conectividad de malla completa, NBMA constituye una solución más eficiente.

### Configuración de subredes punto a multipunto

La configuración de punto a multipunto resulta más sencilla que la de NBMA, puesto que no hay DR, pero se tienen que configurar relaciones entre los direccionadores contiguos correspondientes a todos los pares de direccionadores que intercambiarán tráfico de datos directamente a través de la subred punto a multipunto. Cada par de direccionadores conectados directamente intercambiarán mensajes Hello, de modo que un extremo pueda descubrir al otro a través de estos mensajes. Sin embargo, el direccionador configurado para enviar el primer mensaje Hello debe tener la dirección IP de su direccionador contiguo configurado mediante el mandato **add neighbor**.

Es importante recordar que OSPF no calculará las rutas correctas si algunos de los direccionadores conectados a una subred la representa como NBMA y otros la representan como punto a multipunto. Por lo tanto, no utilice nunca el mandato **set non-broadcast** para una interfaz de una red punto a multipunto.

### Configuración de subredes NBMA

Para subredes IP NBMA, algún subconjunto de los direccionadores OSPF conectados se configuran como posibles direccionadores designados (DR). Cada direccionador que puede convertirse en DR envía periódicamente mensajes Hello a todos los direccionadores con posibilidad de convertirse en DR. El protocolo utiliza estos mensajes para elegir un DR y un DR de reserva. Tanto el DR como el DR de reserva intercambian periódicamente mensajes Hello con los demás direccionadores OSPF conectados a la subred IP NBMA. Además, el flujo de información de rutas OSPF a través de la subred IP NBMA sólo se produce entre cada uno de los direccionadores conectados y el DR o el DR de reserva.

Seleccione NBMA mediante el mandato **set non-broadcast** para las interfaces que se conectan a una subred NBMA. Este mandato se debe utilizar para todas las interfaces que se conectan a la red NBMA.

La configuración necesaria para un direccionador OSPF que se conecta a una subred NBMA depende de si el direccionador tiene o no posibilidades de convertirse en DR.

- Para un direccionador sin posibilidad de convertirse en un DR, se debe utilizar el mandato **set interface** para definir para la prioridad del direccionador el valor 0.
- Para un direccionador con posibilidad de convertirse en DR, se debe utilizar el mandato **set interface** para definir para la prioridad del direccionador un valor distinto de cero y el mandato **add neighbor** para identificar todos los direccionadores OSPF con interfaces conectadas a la subred NBMA y para indicar cuáles de estos pueden convertirse en DR.

**Nota:** En una configuración de estrella, utilice el mandato **add neighbor** en el concentrador (no hace falta configurar los direccionadores contiguos de la ubicación remota). El mandato **add neighbor** entra en vigor de forma inmediata sin necesidad de volver a arrancar el direccionador.

## Activación del direccionamiento límite AS

Para importar rutas aprendidas de otros protocolos (RIP e información configurada de forma estática) en el dominio OSPF, active el direccionamiento límite AS. Debe hacerlo incluso en el caso de que la ruta que desea importar sea la ruta por omisión (destino 0.0.0.0).

Al activar el direccionamiento límite AS, se le solicitará qué rutas desea importar. Puede seleccionar para importar, o para no importar, rutas pertenecientes a las siguientes categorías.

- Rutas BGP
- Rutas RIP
- Rutas estáticas
- Rutas directas

Por ejemplo, puede optar por importar duras BGP y directas, pero no rutas RIP ni estáticas.

Independientemente de las categorías externas anteriores, también puede configurar si importar o no rutas de subred en el dominio OSPF. El valor por omisión de este elemento de configuración es ENABLED (ACTIVADO: se importan subredes).

El tipo de métrica utilizado al importar rutas determina el modo en que el dominio OSPF capta el coste importado. Al comparar dos métricas de tipo 2, sólo se tiene en cuenta el coste externo al elegir la mejor ruta. Al comparar dos métricas de tipo 1, se realiza una combinación de costes interno y externo de la ruta antes de realizar la comparación. Por ejemplo, puede definir el direccionador de modo su valor por omisión se origine únicamente si se recibe una ruta a 10.0.0.0 procedente del AS número 12. Si define como número de AS el valor 0 significa “procedente de cualquier AS.” Si define el como número de red el valor 0.0.0.0 significa “cualquier ruta recibida.”

La sintaxis del mandato **enable** es la siguiente:

La sintaxis del mandato **enable** es la siguiente:

```
enable as boundary routing
Use route policy? [No]:
Import BGP routes? [No]
Import RIP routes? [No]
Import static routes? [No]
Import direct routes? [No] yes
Import subnet routes? [Yes]
Always originate default route? [No] yes
Originate as type 1 or 2 [2]? 2
Default route cost [1]?
Default forwarding address [0.0.0.0]? 10.1.1.1
```

Consulte el mandato **enable as boundary routing** en la página 387 para obtener información sobre cómo utilizar una política de filtro de rutas para definir parámetros del direccionamiento límite AS.

## Configuración de OSPF sobre ATM

Las opciones para configurar OSPF sobre una subred ATM dependen de si se utiliza Emulación de LAN o IP clásico sobre ATM para la capa IP. En el caso de Emulación de LAN, OSPF se configura del mismo modo que para una LAN real. Para IP clásico sobre ATM, las opciones de configuración de OSPF son las mismas que las correspondientes a subredes de área amplia. Consulte el tema “Configuración de subredes de área amplia” en la página 372. Se da soporte a configuraciones tanto NBMA como punto a multipunto.

## Configuración de OSPF sobre ATM (RFC 1577)

Para configurar OSPF sobre ATM que ejecuta RFC 1577 debe seguir los pasos siguientes::

1. Asigne una o más direcciones IP a la interfaz ATM mediante el mandato `IP Config>` **add address**. Cada dirección IP corresponde a una subred IP lógica (LIS) conectada.
2. Utilice el mandato `OSPF Config>` **set interface** para cada una de las direcciones IP configuradas en la interfaz ATM. Defina los parámetros de OSPF, incluida da posibilidad de elección como direccionador designado (DR).
3. Utilice el mandato `OSPF Config>` **set non-broadcast** para cada una de las direcciones IP configuradas en la interfaz ATM. Esto también se tiene que definir en todas las interfaces de cada direccionador conectado a una LIS ATM RFC 1577.
4. Utilice el mandato `OSPF Config>` **add neighbor** para definir los otros direccionadores de la subred IP lógica (LIS) con los que desea compartir información de direccionamiento OSPF.

**Nota:** Todos los direccionadores con posibilidad de convertirse en direccionadores designados (DR) se tienen que configurar con la información del direccionador contiguo. Sólo es necesario que un direccionador de cada LIS sea DR; sin embargo, si se configuran otros direccionadores con posibilidad de convertirse en DR, LIS tiene más capacidad de recuperación cuando se produce una anomalía.

# Otras tareas de configuración

## Definición de enlaces virtuales

Para mantener la conectividad de la red troncal, debe tener todos los direccionadores de la red troncal interconectados mediante enlaces permanentes o virtuales. Puede configurar enlaces virtuales entre dos direccionadores de límite de área cualesquiera que compartan un área común que no sea de apéndice ni de red troncal. Los enlaces virtuales se consideran como interfaces de direccionadores separadas que se conectan al área de red troncal. Por lo tanto, también se le solicitará que especifique muchos de los parámetros de la interfaz al configurar un enlace virtual.

El siguiente ejemplo ilustra la configuración de un enlace virtual. Se deben configurar enlaces virtuales en cada uno de los dos puntos finales del enlace. Observe que debe especificar los ID de direccionador OSPF con el mismo formato que las direcciones IP.

```
OSPF Config>set virtual
        Virtual endpoint (Router ID) [0.0.0.0]? 128.185.138.21
        Link's transit area [0.0.0.1]?
        Retransmission Interval (in seconds) [10]?
        Transmission Delay (in seconds) [5]?
        Hello Interval (in seconds) [30]?
        Dead Router Interval (in seconds) [180]?
        Authentication Type (0 - None, 1 - Simple) [0]? 1
        Authentication Key []? 41434545
        Retype Auth. Key []? 41434545
```

No se configura ningún coste para un enlace virtual porque el coste es el coste interno del área OSPF entre los puntos finales del enlace virtual a través del área de tránsito.

## Configuración de Comparaciones entre protocolos de direccionamiento

Si utiliza un protocolo de direccionamiento además de OSPF, o si cambia su protocolo de direccionamiento por OSPF, debe definir la Comparación entre protocolos de direccionamiento.

El direccionamiento OSPF de un AS se produce a estos tres niveles: dentro del área, entre áreas y exterior.

El direccionamiento dentro del área se produce cuando las direcciones de origen y de destino de un paquete residen en la misma área. La información sobre otras áreas no afecta a este tipo de direccionamiento.

El direccionamiento entre áreas se produce cuando las direcciones de origen y de destino del paquete residen en distintas áreas del mismo AS. OSPF lleva a cabo el direccionamiento entre áreas dividiendo la vía de acceso en tres piezas contiguas: una vía de acceso dentro del área desde el origen al direccionador límite del área; una vía de acceso de red troncal entre las áreas de origen y de destino; y otra vía

de acceso dentro del área al destino. Puede visualizar este alto nivel de direccionamiento como una topología de estrella con la red troncal como concentrador y cada una de las áreas como un radio.

Las rutas exteriores son vías de acceso a redes que quedan fuera del AS. Estas rutas se originan a partir de protocolos de direccionamiento, como el Protocolo de pasarela límite (BGP), o a partir de rutas estáticas que especifica el administrador de la red. La información de direccionamiento exterior que suministra BGP no interfiere con la información de direccionamiento interno que suministra el protocolo OSPF.

Los direccionadores límite AS pueden importar rutas exteriores en el dominio de direccionamiento OSPF. OSPF representa estas rutas como anuncios de enlaces externos AS.

OSPF importa las rutas externas en niveles separados. El primer nivel, denominado rutas de tipo 1, se utiliza cuando la métrica externa se puede comparar con la métrica de OSPF (por ejemplo, ambas calculan los retrasos en milisegundos). El segundo nivel, denominado rutas externas de tipo 2, da por supuesto que el coste externo es superior al coste de cualquier vía de acceso OSPF interna (estado de enlace).

Las rutas externas importadas se identifican con 32 bits de información. En un direccionador, este campo de 32 bits indica el número de AS del que se ha recibido la ruta. Esto permite un comportamiento más inteligente al determinar si se debe volver a anunciar la información externa a los demás sistemas autónomos.

OSPF tiene una jerarquía de direccionamiento de 4 niveles (consulte la Figura 35). El mandato **set comparison** indica al direccionador si las rutas BGP/RIP/estáticas se ajustan a la jerarquía de OSPF. Los dos niveles inferiores constan de las rutas internas OSPF. Las rutas dentro del área y entre áreas OSPF tienen preferencia sobre la información obtenida de otras fuentes, todas las cuales se encuentran en un solo nivel.

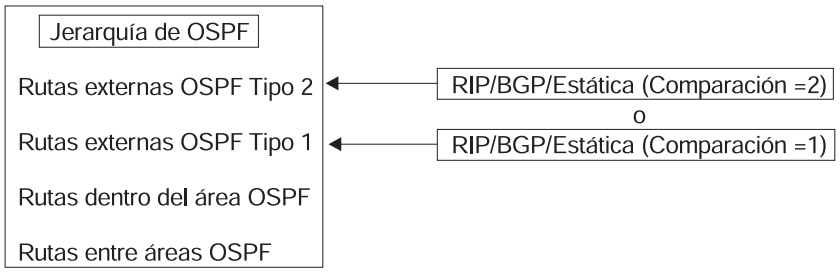



*Figura 35. Jerarquía de direccionamiento OSPF*

Para colocar las rutas BGP/RIP/estáticas al mismo nivel que rutas externas OSPF de tipo 1, defina para la comparación el valor 1. Para colocar las rutas BGP/RIP/estáticas al mismo nivel que las rutas externas OSPF tipo 2, defina para la comparación el valor 2. El valor por omisión es 2.

Por ejemplo, suponga que se define para la comparación el valor 2. En este caso, cuando se importan rutas RIP en el dominio OSPF, se importarán como rutas externas de tipo 2. Todas las rutas externas OSPF de tipo 1 prevalecen sobre las rutas RIP recibidas, independientemente de la métrica. Sin embargo, si las rutas RIP tienen un coste menor, las rutas RIP prevalecen sobre las rutas externas

OSPF de tipo 2. Los valores de comparación correspondientes a todos los direccionadores OSPF deben coincidir. Si los valores de comparación definidos para los direccionadores no son coherentes, el direccionamiento no funcionará correctamente.

La sintaxis del mandato **set comparison** es la siguiente:

```
OSPF Config> set comparison
Compare to type 1 or 2 externals [2]?
```

### Circuito de demanda

Se puede configurar un circuito de demanda para cualquier interfaz. No hay ninguna dependencia del soporte físico ni del modelo que utiliza OSPF para el cálculo de rutas. Cuando se configura el circuito de demanda y no hay problemas de compatibilidad:

- Sólo los Anuncios de estado de enlace (LSA) con cambios reales se anunciarán sobre la interfaz. Normalmente, el algoritmo fiable de envío de OSPF hace que los LSA se renueven con una nueva instancia cada 30 minutos, incluso si se han producido cambios en la topología.
- El bit DoNotAge no se definirá para los LSA enviados sobre la interfaz. Esto se debe a que no se renovarán sobre la interfaz.

### Solicitud de supresión de mensajes Hello

Este es un parámetro opcional que puede utilizar para configurar una interfaz de modo que solicite la supresión de mensajes Hello. Este parámetro influye sobre las interfaces punto a punto y punto a multipunto. Además, la subred a la que se conecta la interfaz debe ser capaz de notificar a OSPF que no se pueden distribuir datos sobre una conexión. Actualmente, las interfaces de marcación bajo demanda ATM e ISDN son los únicos tipos de interfaces que dan soporte a la supresión de mensajes Hello.

### Intervalo de sondeo

Cuando la supresión de mensajes Hello no está activa, el intervalo de sondeo sólo se utiliza con subredes multiacceso que no son de difusión general y se define con el mandato **set non-broadcast**. Puede configurar este parámetros una vez configurada una interfaz como un circuito de demanda y se ha solicitado la supresión de mensajes Hello. OSPF utilizará este parámetro para intentar restablecer una conexión cuando una línea punto a punto está inactiva debido a un error en la transmisión de datos pero parece que la red sigue estando operativa.

## Conversión de RIP a OSPF

Para convertir el Sistema autónomo de RIP a OSPF, instale OSPF en los direccionadores uno por uno, mientras se ejecuta RIP. Gradualmente, todas las rutas internas pasarán de aprenderse mediante RIP a que las aprenda OSPF (las rutas OSPF tienen preferencia sobre las rutas RIP). Si desea que las rutas tengan exactamente el mismo aspecto que tenían bajo RIP (a fin de comprobar que la conversión funciona correctamente), utilice el número de saltos como métrica de OSPF. Para ello, defina como coste de cada interfaz OSPF el valor 1.

Recuerde que se debe estimar el tamaño del sistema OSPF cuando se active el protocolo. Este tamaño estimado debe reflejar el tamaño final del dominio de direccionamiento OSPF.

Después de instalar OSPF en los direccionadores, active el direccionamiento límite AS en todos los direccionadores que tengan que aprender rutas mediante otros protocolos (BGP, RIP y rutas configuradas de forma estática). El número de estos direccionadores límite AS debe ser el mínimo.

Finalmente, puede desactivar la recepción de información RIP en todos los direccionadores que no son direccionadores límite AS.

## Cambio dinámico de parámetros de configuración de OSPF

Los parámetros de configuración de OSPF se pueden modificar de forma dinámica actualizando la configuración a través del recurso de configuración de OSPF y luego restableciendo el protocolo OSPF a través de la consola OSPF. Los direccionadores contiguos OSPF, las interfaces, las áreas y la política de direccionamiento límite AS se pueden añadir, suprimir o modificar mediante esta técnica. En la mayoría de los casos, estos cambios no detienen el funcionamiento normal. Por ejemplo, la adición de una interfaz OSPF no afecta a las demás interfaces OSPF (excepto a la generación de nuevos anuncios de estado de enlace de OSPF).

Los cambios que necesitan que se vuelvan a originar todos los anuncios OSPF de un direccionador hacen que se vuelva a arrancar OSPF. Estos incluyen:

- Activación/desactivación del reenvío de difusión múltiple OSPF (MOSPF)
- Activación/desactivación de circuitos de demanda (RFC 1793)
- Cambio del valor del ID del direccionador

En la mayoría de los casos, esto resulta transparente ante los usuarios puesto que el único momento en que se detiene el funcionamiento es cuando se restablecen las adyacencias de direccionadores contiguos OSPF.

Puesto que la memoria del direccionador está reservada para OSPF antes de asignar almacenamientos intermedios de entrada/salida, OSPF no se puede activar de forma dinámica a no ser que estuviera activado en el momento en que se volvió a arrancar el último direccionador. Además, la cantidad de memoria reservada para OSPF no se puede aumentar sin que se vuelva a arrancar el sistema. La cantidad de memoria reservada se determina mediante las estimaciones correspondientes a direccionadores y rutas externas AS especificadas en el mandato **enable OSPF**.

**Ejemplo:**

```
OSPF Config>enable OSPF
      Estimated # external routes [100]? 300
      Estimated # OSPF routers [50]? 100
      Maximum Size LSA [2048]?
```

## Migración desde programa de red multiprotocolo y procesador de red IBM 6611 Nways®

Las siguientes mejoras le permiten realizar una migración de IBM 6611 a 2210:

- **Rangos de áreas de menor coste**

  Para rangos de resumen de OSPF, el 6611 calcula el coste en función del coste menor de las redes de componentes, mientras que el 2210 calcula el coste del rango de resumen en función del coste mayor de las redes de com-

ponentes. **Rangos de áreas de menor coste** permite la opción de calcular rangos de menor coste.

- **Coste de direccionador contiguo punto a multipunto**

  El 6611 da soporte al concepto de enlaces lógicos Frame Relay punto a punto, pero no da soporte a punto a multipunto OSPF sobre Frame Relay. Punto a multipunto es más eficiente, pero no le permite especificar un coste distinto para cada direccionador contiguo. Se ha añadido **Coste de direccionador contiguo punto a multipunto** para permitirle especificar un coste TOS 0 alternativo para cada direccionador contiguo.

# Configuración y supervisión de OSPF

Este capítulo describe cómo configurar el protocolo Open Shortest Path First (OSPF). OSPF es un Protocolo de pasarela interior (IGP). El direccionador da soporte a los siguientes IGP para crear la tabla de direccionamiento IP: protocolo Open Shortest Path First (OSPF) y protocolo RIP. OSPF se basa en la tecnología de estado de enlace o algoritmo vía de acceso más corta primero (SPF). RIP se basa en el algoritmo Bellman-Ford o algoritmo de vector de distancia. Este capítulo incluye las siguientes secciones:

- "Cómo acceder al entorno de configuración de OSPF"
- "Mandatos de configuración de OSPF"
- "Cómo acceder al entorno de supervisión de OSPF" en la página 403
- "Mandatos de supervisión de OSPF" en la página 403

## Cómo acceder al entorno de configuración de OSPF

Para acceder al entorno de configuración de OSPF, especifique el siguiente mandato en el indicador `Config>`:

```
Config> protocol ospf
Open SPF-based Routing Protocol configuration monitoring
OSPF Config>
```

## Mandatos de configuración de OSPF

Antes de poder utilizar OSPF, debe configurarlo mediante los mandatos de configuración de OSPF. La siguiente sección resume y explica los mandatos de OSPF.

**Nota:** Excepto los mandatos del tema "Cambio dinámico de parámetros de configuración de OSPF" en la página 378, que hacen que OSPF se vuelva a arrancar de forma inmediata con los parámetros modificados, los mandatos de configuración de OSPF no entran en vigor de forma inmediata. Permanecen pendientes hasta que el usuario emite el mandato de Talk 5 **reset ospf**.

Entre estos mandatos en el indicador `OSPF config>`. La Tabla 23 en la página 382 muestra los mandatos.

*Tabla 23. Resumen de mandatos de configuración de OSPF*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Add | Añade información a la información OSPF existente. Puede añadir rangos a áreas y direccionadores contiguos a redes que no son de difusión general. |
| Delete | Suprime información de OSPF de SRAM. |
| Disable | Desactiva el protocolo OSPF completo, la función de direccionamiento límite AS, la función de circuito de demandao el direccionamiento de difusión múltiple IP.. |
| Enable | Activa el protocolo OSPF completo, la función de direccionamiento límite AS, la función de circuito de demandao el direccionamiento de difusión múltiple IP.. |
| Join | Configura el direccionador para que pertenezca a uno o más grupos de difusión múltiple. |
| Leave | Elimina el direccionador de grupos de difusión múltiple. |
| List | Muestra la configuración de OSPF. |
| Set | Establece o modifica la información de configuración correspondiente a áreas OSPF, interfaces, redes que no son de difusión general o enlaces virtuales. Este mandato también le permite definir el modo en que se comparan las rutas OSPF con información obtenida de otros protocolos de direccionamiento. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Respuesta a mandatos de configuración de OSPF

Excepto por los mandatos del tema “Cambio dinámico de parámetros de configuración de OSPF” en la página 378, que hacen que OSPF se vuelva a arrancar de forma inmediata con los parámetros modificados, los mandatos de configuración de OSPF (Talk 6) no entran en vigor de forma inmediata. Permanecen pendientes hasta que el usuario emite el mandato de Talk 5 **reset ospf**.

## Add

Utilice el mandato **add** para añadir información a la información OSPF ya existente. Con este mandato, puede añadir rangos a áreas, así como direccionadores contiguos a redes que no son de difusión general.

**Sintaxis:**

**add** range . . .
neighbor . .

**range** *núm. área dirección-IP máscara-dirección-IP*

Añade rangos a áreas OSPF. Las áreas OSPF se pueden definir en términos de rangos de direcciones. De forma externa al área, se anuncia una sola ruta para cada rango de direcciones. Por ejemplo, si un área OSPF debe consistir en todas las subredes de la red de clase B 128.185.0.0, se definirá como consistente en rango de una sola dirección. El rango de direcciones se especificará como una dirección igual a

128.185.0.0 con una máscara igual a 255.255.0.0. Fuera del área, la red entera con subredes recibirá anuncios como una sola ruta a la red 128.185.0.0.

Se pueden definir rangos para controlar qué rutas se anunciar de forma externa a un área. Hay dos opciones:

- Cuando se configura OSPF para que anuncie el rango, se anuncia una sola ruta entre áreas correspondiente al rango si al menos una ruta de componentes del rango está activa dentro del área.
- Cuando se configura OSPF para que no anuncie el rango, no se anuncia ninguna ruta entre áreas correspondiente a rutas que están dentro del rango.

No se pueden utilizar los rangos como áreas de tránsito para enlaces virtuales. Además, cuando se definen rangos para un área, OSPF no funcionará correctamente si el área está particionada pero está conectada por medio de la red troncal.

**Ejemplo:**

```
add range 0.0.0.2 128.185.0.0 255.255.0.0

inhibit advertisement ? [No]
```

1. El *número de área* tiene:

   **Valores válidos**: Cualquier número de área válido

   **Valor por omisión**: ninguno

2. La *dirección IP* tiene:

   **Valores válidos**: Cualquier dirección IP válida.

   **Valor por omisión**: ninguno

3. La *máscara de dirección IP* tiene:

   **Valores válidos**: Cualquier máscara de dirección IP válida.

   **Valor por omisión**: ninguno

**neighbor** Configura direccionadores contiguos adyacentes al direccionador sobre esta interfaz. En redes multiacceso que no son de difusión general, los direccionadores contiguos sólo se tienen que configurar en los direccionadores que tienen posibilidades de convertirse en el direccionador designado. En redes punto a multipunto, al menos un extremo de cada conexión lógica debe tener configurado un direccionador contiguo. Para redes punto a multipunto, se puede configurar un coste TOS 0 alternativo. Si no se configura ningún coste, se utiliza el coste de la interfaz.

**Ejemplo:** **`add neighbor`**

```
Interface IP address [0.0.0.0]? 128.185.138.19
IP Address of Neighbor [0.0.0.0]? 128.185.138.21
Can that router become Designated Router on this net [Yes]?
Alternate TOS 0 cost [0]? 100
```

1. *Interface IP address* tiene:

   **Valores válidos**: Cualquier dirección IP válida.

   **Valor por omisión**: Ninguno

2. *ID Address of Neighbor* tiene:

   **Valores válidos**: Cualquier dirección IP válida

   **Valor por omisión**: Ninguno

3. Respuesta a la pregunta `Can that router become designated router on this net?` Para interfaces punto a multipunto, este parámetro no se aplica y adopta el valor “No”.

   **Valores válidos**: Yes o No

   **Valor por omisión**: Yes

4. `Alternate TOS 0 cost` permite utilizar un coste alternativo.

   **Valores válidos**: 0 - 65534

   **Valor por omisión**: 0 (indica que se debe utilizar el coste de la interfaz).

## Delete

Utilice el mandato delete para suprimir información de OSPF de SRAM.

**Sintaxis:**

de**lete** range . . .
area . . .
interface . . .
neighbor . . .
non-broadcast . . .
virtual-link

**range** *núm. área dirección-IP*

Suprime rangos de áreas OSPF.

**Ejemplo:** `delete range 0.0.0.2 128.185.0.0 255.255.0.0`

1. El *número de área* del rango tiene:

   **Valores válidos**: Cualquier dirección de área válida

   **Valor por omisión**: ninguno

2. La *dirección IP del rango* tiene:

   **Valores válidos**: Cualquier dirección IP válida.

   **Valor por omisión**: ninguno

3. La *máscara de dirección IP del rango* tiene:

   **Valores válidos**: Cualquier máscara de dirección IP válida.

   **Valor por omisión**: ninguno

**area** *núm. área*

Suprime áreas OSPF de la configuración de OSPF actual.

**Ejemplo:** `delete area 0.0.0.1`

El *número de área* tiene:

**Valores válidos**: Cualquier número de área válido.

**Valor por omisión**: ninguno

**interface** *dirección-IP-interfaz*
Suprime una interfaz de la configuración de OSPF actual.

**Ejemplo:** `delete interface 128.185.138.19`

La *dirección IP de la interfaz* tiene:

**Valores válidos**: Cualquier dirección IP válida.

**Valor por omisión**: ninguno

**neighbor** *dirección-IP-interfaz dirección-IP-direccionador-contiguo*
Suprime direccionadores contiguos configurados de la configuración de OSPF actual.

**Ejemplo:** `delete neighbor`

```
Interface IP address [0.0.0.0]? 128.185.138.19
IP Address of Neighbor [0.0.0.0]? 128.185.138.21
```

1. La *dirección IP de la interfaz* tiene:

   **Valores válidos**: Cualquier dirección IP válida.

   **Valor por omisión**: ninguno

2. La *dirección IP del direccionador contiguo* tiene:

   **Valores válidos**: Cualquier dirección IP válida.

   **Valor por omisión**: ninguno

**non-broadcast** *dirección-IP-interfaz*
Suprime información de red que no es de difusión general de la configuración de OSPF actual.

**Ejemplo:** `delete non-broadcast 128.185.133.21`

1. La *dirección IP de la interfaz* tiene:

   **Valores válidos**: Cualquier dirección IP válida.

   **Valor por omisión**: ninguno

**virtual-link**
Suprime un enlace virtual definido mediante el mandato **set virtual-link**.

**Ejemplo:** `delete virtual-link`

```
Virtual endpoint (Router ID) [0.0.0.0]? 10.1.1.1
Link's transit area [0.0.0.1]? 0.0.0.2
```

1. *Virtual endpoint (router ID)*, que define el ID del direccionador contiguo virtual, tiene:

   **Valores válidos**: Cualquier dirección IP válida.

   **Valor por omisión**: ninguno

2. *Link's transit area* tiene:

   **Valores válidos**: Cualquier dirección de área válida.

   **Valor por omisión**: 0.0.0.1

## Disable

Utilice el mandato **disable** para desactivar el protocolo OSPF completo o sólo la función de direccionamiento límite AS.

**Sintaxis:**

**disable**
- as boundary routing
- demand-circuits
- least-cost-ranges
- multicast forwarding
- OSPF routing protocol
- RFC1583Compatibility
- subnet

**as boundary routing**

Desactiva la función de direccionamiento límite AS. Cuando está desactivada, el direccionador no importa información externa en el dominio OSPF.

**Ejemplo:** `disable as boundary routing`

**demand-circuits**

Desactiva la función circuito de demanda. Cuando está desactivada, el direccionador no indica que da soporte al proceso de circuitos de demanda en el Anuncio de estado de enlace (LSA) del enlace de su direccionador y no origina ningún LSA con el bit DoNotAge definido. Si un direccionador del dominio de direccionamiento o área apéndice de OSPF no da soporte a los circuitos de demanda, ninguno de los direccionadores del dominio de direccionamiento o área apéndice de OSPF origina LSA DoNotAge.

**Ejemplo:** `disable demand-circuits`

**least-cost-ranges**

Desactiva el cálculo de rangos de áreas OSPF basados en el coste de la red de componentes más cercana (de menor coste). Esta opción está desactivada por omisión.

**multicast forwarding**

Desactiva el direccionamiento de difusión múltiple IP en todas las interfaces. Cuando está desactivado, el direccionador no envía datagramas de difusión múltiple (Clase D).

**Ejemplo:** `disable multicast forwarding`

**OSPF routing protocol**

Desactiva el protocolo OSPF completo.

**Ejemplo:** `disable OSPF routing protocol`

**RFC1583 Compatibility**

Desactiva la selección de rutas externas AS que es compatible con RFC 1583. Se recomienda que no desactive la compatibilidad RFC1583 a no ser que pueda acceder a la misma ruta externa a través de más de un área OSPF y tenga problemas de bucles de direccionamiento parecidos a los descritos en RFC2178. El valor por omisión es que esté activada.

**Ejemplo:** `disable rfc1583Compatibility`

**subnet** Para una interfaz ante una línea serie punto a punto, esta opción desactiva el anuncio de una ruta apéndice a la subred que representa la línea serie en lugar de la ruta de sistema principal correspondiente a la dirección del otro direccionador. Debe especificar la dirección de este direccionador correspondiente a la interfaz para identificarlo.

**Ejemplo:**

```
OSPF Config> disable subnet
Interface IP address [0.0.0.0]? 8.24.3.1
```

*Interface IP address* tiene:

**Valores válidos**: Cualquier dirección IP válida.

**Valor por omisión**: ninguno

## Enable

Utilice el mandato **enable** para activar el protocolo OSPF o aspectos específicos de dicho protocolo, como el anuncio de un apéndice para dirigir a una subred o la función de direccionamiento límite AS.

**Sintaxis:**

en**able** as boundary routing
demand-circuits
least-cost-ranges
multicast forwarding
OSPF routing protocol
RFC1583Compatibility
send outage-only
subnet

**as boundary routing**

Activa la función de direccionamiento límite AS, que le permite importar rutas aprendidas a partir de otros protocolos (BGP, RIP e información configurada de forma estática) en el dominio OSPF. Para obtener información adicional sobre cómo utilizar el mandato **enable**, consulte el tema “Configuración de OSPF” en la página 363.

Una opción de este mandato le permite utilizar una política de filtro de rutas para determinar qué rutas se importan y los detalles específicos de su anuncio, incluido el tipo externo OSPF, la métrica y el valor de identificador (generalmente, el número del AS). Consulte el tema “Configuración de políticas de filtros de rutas” en la página 332 para obtener información sobre cómo configurar una política de filtro de rutas. El Ejemplo 1 muestra configuración de direccionamiento límite AS cuando no se utiliza ninguna política de filtro de rutas y el Ejemplo 2 muestra configuración de direccionamiento límite AS cuando se utiliza una política de filtro de rutas.

### Ejemplo 1:

```
 enable as boundary routing
 Use route policy? [No]:
 Import BGP routes? [No]
 Import RIP routes? [No]
 Import static routes? [No]
 Import direct routes? [No] yes
 Import subnet routes? [Yes]
 Always originate default route? [No] yes
 Originate as type 1 or 2 [2]? 2
 Default route cost [1]?
 Default forwarding address [0.0.0.0]? 10.1.1.1
```

### Ejemplo 2:

```
 enable as boundary routing
Use route policy? [No]: Yes
Router Policy Identifier [1-15 characters] [ ]? ospf-import
Always originate default route? [No]:
```

1. La pregunta *Use route policy* indica si se utiliza o no una política de rutas configurada para determinar qué rutas que no son de OSPF se importan en OSPF como rutas externas OSPF. Si la respuesta a esta pregunta es **yes**, muchas de las preguntas ya no aparecen puesto que no se aplican cuando hay una política de direccionamiento configurada. Una política de direccionamiento ofrece más granularidad al especificar qué rutas se importan.

   **Valores válidos**: yes o no

   **Valor por omisión**: no

2. La pregunta *Router Policy Identifier* solicita la serie de caracteres que identifica una política de filtro de rutas configurada.

   **Valores válidos**: una serie de caracteres ASCII de entre 1 y 15 caracteres

   **Valor por omisión**: ninguno

3. La pregunta *Import BGP* indica si las rutas BGP se importarán o no en OSPF como rutas externas OSPF.

   **Valores válidos**: Yes o No

   **Valor por omisión**: No

4. La pregunta *Import RIP* indica si las rutas RIP se importarán o no en OSPF como rutas externas OSPF.

   **Valores válidos**: Yes o No

   **Valor por omisión**: No

5. La pregunta *Import estatic* indica si las rutas estáticas se importarán o no en OSPF como rutas externas OSPF.

   **Valores válidos**: Yes o No

   **Valor por omisión**: No

6. La pregunta *Import direct* indica si las rutas directas se importarán o no en OSPF como rutas externas OSPF.

   **Valores válidos**: Yes o No

   **Valor por omisión**: No

7. La pregunta *Import subnet* indica si las rutas de subred se importarán o no en OSPF como rutas externas OSPF.

**Valores válidos**: Yes o No

**Valor por omisión**: Yes

8. La pregunta *Always originate default route* indica si se debe o no originar de forma incondicional una ruta por omisión en el formato de un anuncio externo OSPF.

   **Valores válidos**: Yes o No

   **Valor por omisión**: No

9. La pregunta *Originate as type 1 or 2* indica si el valor por omisión generado por OSPF tendrá un tipo de métrica externa AS de tipo 1 ó 2. Las métricas de tipo 1 se consideran en el mismo contexto que los costes de OSPF, mientras que las métricas de tipo 2 se consideran superiores a cualquier métrica de OSPF.

   **Valores válidos**: 1 ó 2

   **Valor por omisión**: 2

10. *Default route cost* es el parámetro que especifica el coste que OSPF asocia a la ruta por omisión a su direccionador límite de área. El coste sirve para determinar la vía de acceso más corta correspondiente a la ruta por omisión a su direccionador límite de área.

    **Valores válidos**: 0 to 16777215

    **Valor por omisión**: 1

11. *Default forwarding address* es el parámetro que especifica la dirección de reenvío que se utilizará en la ruta por omisión importada.

    **Valores válidos**: una dirección IP válida

    **Valor por omisión**: ninguno

**multicast forwarding**

Activa el reenvío de datagramas de difusión múltiple IP (Clase D). Cuando activa el direccionamiento de difusión múltiple, se le solicita si desea reenviar datagramas de difusión múltiple IP entre áreas OSPF. Para ejecutar MOSPF (OSPF con extensiones de difusión múltiple), un direccionador que actualmente ejecute OSPF sólo necesita utilizar este mandato. No es necesario que vuelva a especificar su información de configuración.

**Ejemplo:** `enable multicast forwarding`

```
Inter-area multicasting enabled (Yes or No): yes
```

**demand-circuits**

Activa el proceso de circuito de demanda correspondiente al direccionador. El direccionador indicará que da soporte al proceso de circuitos de demanda en el Anuncio de estado de enlace (LSA) del enlace de su direccionador. El valor por omisión es que este parámetro esté activado de modo que se puedan utilizar circuitos de demanda sin tener que volver a configurar cada direccionador en el dominio de direccionamiento OSPF.

```
OSPF Config> enable demand-circuits
```

**least-cost-ranges**

Activa el cálculo de rangos de áreas OSPF basados en el coste de la red de componentes más cercana (de menor coste). Es necesario activar este parámetro para la compatibilidad con IBM 6611 que actúen como Direccionadores límite de área (ABR) para la misma área. También se puede utilizar en situaciones en que al utilizar la red de componentes de menor coste se reduzca significativamente el número de regeneraciones de LSA de OSPF debido a cambios en el coste. Esta opción está desactivada por omisión.

**OSPF routing protocol**

Activa el protocolo OSPF completo. Al activar el protocolo de direccionamiento OSPF, debe especificar los dos siguientes valores que se utilizarán para estimar el tamaño de la base de datos de estado de enlace OSPF:

- Número total de rutas externas AS que se importarán en el dominio de direccionamiento OSPF. Un solo destino puede dar lugar a varias rutas externas si lo importan distintos direccionadores límite AS. Por ejemplo, si el dominio de direccionamiento OSPF tiene dos direccionadores límite AS, y ambos importan rutas a los mismos 100 destinos, debe definir como número de rutas externas AS el valor 200.

  **Valores válidos**: 0 a 65535

  **Valor por omisión**: 100

- Número total de direccionadores OSPF del dominio de direccionamiento.

  **Valores válidos**: 0 a 65535

  **Valor por omisión**: 50

- También puede especificar el tamaño máximo de LSA. Puede que tenga que aumentar este valor si tiene una ruta larga con muchos enlaces de marcación OSPF (por ejemplo, ISDN principal) en la misma área OSPF. Normalmente, 2048 es espacio más que suficiente para cualquier LSA único.

  **Valores válidos**: 2048 a 65535

  **Valor por omisión**: 2048

  **Ejemplo: `enable OSPF routing protocol`**

```
Estimated # external routes[100]? 200
Estimated # OSPF routers [50]? 60
Maximum LSA Size [2048]?
```

**RFC1583Compatibility**

Activa la selección de rutas externas AS que es compatible con RFC 1583. El valor por omisión es que esté activada.

**Ejemplo: `enable rfc1583Compatibility`**

**subnet** Para una interfaz ante una línea serie punto a punto, esta opción activa el anuncio de una ruta apéndice a la subred que representa la línea serie en lugar de la ruta de sistema principal correspondiente a la dirección del otro direccionador. Debe especificar la dirección de este direccionador correspondiente a la interfaz para identificarlo.

**Ejemplo:**

```
OSPF Config> enable subnet
Interface IP address [0.0.0.0]? 8.24.3.1
```

*Interface IP address* tiene:

**Valores válidos**: Cualquier dirección IP válida.

**Valor por omisión**: ninguno

## Join

Utilice el mandato **join** para configurar el direccionador como miembro de un grupo de difusión múltiple. Cuando el direccionador es miembro de un grupo de difusión múltiple, responde a mandatos PING y a consultas SNMP enviadas a la dirección del grupo.

Para solicitar que el direccionador forme parte de un grupo de forma más inmediata (no es necesario volverlo a arrancar ni volverlo a cargar), emita el mandato **join** desde el indicador de supervisión de OSPF. Además, desde el indicador de supervisión de OSPF, el mandato join mantiene un seguimiento del número de veces que se une un determinado grupo. Los grupos de difusión múltiple IP unidos a través del indicador de supervisión de OSPF no se retienen cuando el direccionador se vuelve a arrancar o a cargar.

**Sintaxis:**

j**oin** *dirección-grupo-difusión-múltiple*

**Ejemplo:** `join 224.185.0.0`

El parámetro *dirección grupo difusión múltiple* especifica la dirección de grupo/difusión múltiple IP de clase D.

**Valores válidos**: Direcciones IP de Clase D comprendidas entre 224.0.0.1 y 239.255.255.255

**Valor por omisión**: Ninguno

## Leave

Utilice el mandato **leave** para retirar el direccionador de un grupo de difusión múltiple. Esto evitará que que direccionador responda a mandatos PING y consultas SNMP enviadas a la dirección del grupo.

Para eliminar el direccionador del grupo de forma más inmediata (no es necesario volverlo a arrancar ni volverlo a cargar), emita el mandato **leave** desde el indicador de supervisión de OSPF. Además, desde el indicador de supervisión de OSPF, el direccionador no se elimina del grupo hasta que el número de mandatos leave ejecutados es igual al número de mandatos join ejecutados previamente.

**Sintaxis:**

le**ave** *dirección-grupo-difusión-múltiple*

**Ejemplo:** `leave 224.185.0.0`

El parámetro *dirección grupo difusión múltiple* especifica la dirección de grupo/difusión múltiple IP de clase D.

**Valores válidos**: Direcciones IP de Clase D comprendidas entre 224.0.0.1 y 239.255.255.255

**Valor por omisión**: ninguno

## List

Utilice el mandato **list** para visualizar información de configuración de OSPF.

**Sintaxis:**

**list** all
areas
interfaces
neighbors
non-broadcast
virtual-links

**all** Lista toda la información de configuración relacionada con OSPF.

**Ejemplo: `list all`**

```
        --Global configuration--
 OSPF Protocol:          Enabled
 # AS ext. routes:       300
 Estimated # routers:    100
 Maximum LSA Size:       2048
 External comparison:    Type 2
 RFC 1583 compatibility: Disabled
 AS boundary capability: Enabled
 Import external routes: BGP RIP STA DIR SUB
 Orig. default route:    No (0,0.0.0.0)
 Default route cost:     (1, Type 2)
 Default forward. addr.: 0.0.0.0
 Multicast forwarding:   Enabled
  Inter-area multicast:   Enabled
 Demand Circuits:        Enabled
 Least Cost Ranges:      Disabled
 LSA Max Random Initial Age:    0

        --Area configuration--
Area ID          AuType          Stub? Default-cost Import-summaries?
0.0.0.0          0=None          No         N/A           N/A


   --Interface configuration--
 IP address        Area    Cost  Rtrns  TrnsDly  Pri  Hello Dead
 128.185.184.11    0.0.0.1   1      5       1     1    10    60
 128.185.177.11    0.0.0.1   1      5       1     1    10    60
 128.185.142.11    0.0.0.0   1      5       1     1    10    60
```

| | |
|---|---|
| OSPF protocol | Muestra si OSPF está activado o desactivado. |
| # AS ext. routes | Muestra el número estimado de rutas externas del Sistema autónomo. El direccionador no puede aceptar más que este número de rutas externas AS. |
| Estimated # routers | Muestra el número estimado de direccionadores encontrados en la configuración OSPF. |
| Maximum LSA size | Muestra tamaño máximo de LSA que originará este direccionador. |
| External comparison | Muestra el tipo de ruta externa que utiliza OSPF al importar información externa en el dominio OSPF y al comparar rutas externas OSPF con rutas RIP/BGP. |
| RFC 1583 compatibility | Indica si la ruta externa AS de OSPF es o no compatible con RFC 1583. |
| AS boundary capability | Muestra si el direccionador importará o no rutas externas en el dominio OSPF. |

| | |
|---|---|
| Import external | Muestra las rutas que se importarán. |
| Orig default route | Muestra si el direccionador importará o no un valor por omisión en el dominio OSPF. Si este valor es “YES”, se muestra un número de red distinto de cero entre paréntesis. Esto indica que sólo se originará la ruta por omisión si está disponible una ruta a esta red. |
| Default route cost | Muestra el coste y el tipo que se utilizarán en la ruta por omisión importada. |
| Default forward addr | Muestra la dirección de reenvío que se utilizará para la ruta por omisión originada. |
| Multicast forwarding | Muestra si se reenviarán o no datagramas de difusión múltiple IP. |
| Demand circuits | Muestra si se da soporte al proceso de circuitos de demanda. |
| Least Cost Area Ranges | Muestra si se calculan los rangos de área de menor coste. |
| LSA Max Random Initial Age | Muestra la antigüedad inicial máxima para los LSA originados de forma automática. Si este valor es cero (valor por omisión), todos los LSA se originarán con una antigüedad igual a 0. |
| External comparison | Muestra el tipo de ruta externa que utiliza OSPF al importar información externa en el dominio OSPF y al comparar rutas externas OSPF con rutas RIP/BGP. |
| Inter-area multicast | Muestra si se reenviarán entre áreas datagramas de difusión múltiple IP. |
| Area-ID | Muestra el ID del área conectada (información de resumen de área) |
| AuType | Muestra el método utilizado para la autentificación de áreas. “Simple-pass” significa que se utiliza un solo esquema de contraseñas para la autentificación de áreas. |
| Stub area | Muestra si se el área que se está resumiendo es o no un área apéndice. Las áreas apéndice no contienen rutas externas, por lo que la base de datos de direccionamiento es menor. Sin embargo, las áreas apéndice no pueden contener direccionadores límite AS ni pueden dar soporte a enlaces virtuales configurados. |
| OSPF interfaces | Para cada interfaz, se muestra su dirección IP, junto con los parámetros configurados. “Area” es el área OSPF a la que se conecta la interfaz. “Cost” indica el coste 0 de TOS (o métrica) asociado a la interfaz. “Rtrns” es el intervalo de retransmisión, que es el número de segundos entre retransmisiones de información de direccionamiento con acuse de recibo. “TrnsDly” es el retraso de retransmisión, que es una estimación del número de segundos que se tarda en transmitir información de direccionamiento sobre la interfaz (debe ser mayor que 0). “Pri” es la Prioridad del direccionador de la interfaz, que se utiliza al seleccionar el direccionador designado.“Hello” es el número de segundos entre paquetes Hello enviados a la interfaz. “Dead” es el número de segundos que transcurren después de que se dejen de oír mensajes Hello para que se considere que el direccionador está inactivo. |

Virtual links — Lista todos los enlaces virtuales que se han configurado con este direccionador como punto final. “Virtual endpoint” indica el ID de direccionador OSPF del otro punto final. “Transit area” indica el área que no es de red troncal a través de la cual se configura el enlace virtual. Se considera que el protocolo OSPF trata a los enlaces virtuales de forma similar a las redes punto a punto. Los demás parámetros listados en el mandato (“Rtrns”, “TrnsDly”, “Hello” y “Dead”) se mantienen para todas las interfaces. Consulte el mandato de OSPF list interfaces para obtener más información.

**areas** Lista toda la información sobre las áreas OSPF configuradas.

**Ejemplo:** `list areas`

```
                              --Area configuration--
Area ID          AuType          Stub? Default-cost Import-summaries?
0.0.0.0          0=None           No         N/A           N/A
0.0.0.1          1=Simp-Pass      No         N/A           N/A
```

Area-ID — Muestra el ID del área conectada (información de resumen del área).

AuType — Muestra el método utilizado para la autentificación de áreas. “Simple-pass” significa que se utiliza un solo esquema de contraseñas para la autentificación de áreas.

Stub area — Muestra si se el área que se está resumiendo es o no un área apéndice. Las áreas apéndice no contienen rutas externas, por lo que la base de datos de direccionamiento es menor. Sin embargo, las áreas apéndice no pueden contener direccionadores límite AS ni pueden dar soporte a enlaces virtuales configurados.

Default-cost — Para áreas apéndice, el coste del valor por omisión que se originará como un Anuncio de estado de enlace (LSA) de resumen de OSPF (tipo 3). Para áreas de tránsito (por ejemplo, áreas que no son apéndice), este campo es N/A.

Import-summaries — Para áreas apéndice, indica si se van a originar o no Anuncios de estado de enlace de resumen de OSPF (tipo 3) en el área apéndice. Esta pregunta no se aplica al resumen por omisión. Para áreas de tránsito (por ejemplo, áreas que no son apéndice), este campo es N/A.

**interfaces**

Para cada interfaz, se muestra su dirección IP, junto con los parámetros configurados. “Area” es el área OSPF a la que se conecta la interfaz. “Cost” indica el coste 0 de TOS (o métrica) asociado a la interfaz. “Rtrns” es el intervalo de retransmisión, que es el número de segundos entre retransmisiones de información de direccionamiento con acuse de recibo. “TrnsDly” es el retraso de retransmisión, que es una estimación del número de segundos que se tarda en transmitir información de direccionamiento sobre la interfaz (debe ser mayor que 0). “Pri” es la prioridad del direccionador de la interfaz, que se utiliza al seleccionar el direccionador designado. “Hello” es el número de segundos entre paquetes Hello enviados a la interfaz. “Dead” es el número de segundos que transcurren después de que se dejen de oír mensajes Hello para que se considere que el direccionador está inactivo.

**Ejemplo:** `list interfaces`

```
OSPF Config>list interface

                        --Interface configuration--
IP address        Area            Auth   Cost  Rtrns  Delay  Pri  Hello   Dead
200.1.1.2         0.0.0.2           0      10      5     1     1     10     40
10.69.1.2         0.0.0.0           1       1      5     1     1     10     40
OSPF Config>list virtual-link

                        --Virtual link configuration--
Virtual endpoint     Transit area    Auth   Rtrns  Delay Hello  Dead
4.4.4.4              0.0.0.1           1       10    5     30   180
10.1.1.2             0.0.0.1           1       10    5     30   180
OSPF Config>
OSPF Config>list area

               --Area configuration--
Area ID         Stub? Default-cost Import-summaries?
0.0.0.2          No         N/A           N/A
0.0.0.0          No         N/A           N/A
0.0.0.1          No         N/A           N/A
0.0.0.3          Yes        10            Yes
```

**Nota:** Los parámetros de difusión múltiple no se visualizan si la difusión múltiple está desactivada. Los parámetros de circuito de demanda no se visualizan si ninguna de las interfaces está configurada como circuito de demanda.

**neighbors**

Lista direccionadores contiguos a redes que no son de difusión general. Muestra la dirección IP del direccionador contiguo y la dirección IP de la interfaz de dicho direccionador contiguo. También indica si el direccionador contiguo tiene posibilidades de convertirse en el "Direccionador designado" de la red y alterna el coste 0 de TOS para redes punto a multipunto.

**Ejemplo: `list neighbors`**

```
              --Neighbor configuration--
Neighbor Addr     Interface Address   DR eligible?      Alternate TOS 0 Cost
2.3.4.5           1.2.3.4             yes               0
2.5.6.7           5.6.7.8             no                100
```

**non-broadcast**

Lista toda la información relacionada con las interfaces conectadas a redes multiacceso que no son de difusión general. Para cada interfaz que no es de difusión general, y siempre que el direccionador tenga posibilidades de convertirse en el direccionador designado de la red conectada, se muestra el intervalo de sondeo junto con una lista de los direccionadores contiguos del direccionador en la red que no es de difusión general.

**Ejemplo: `list non-broadcast`**

```
              --NBMA configuration--
Interface Addr      Poll Interval
128.185.235.34      120
```

**virtual-links**

Lista todos los enlaces virtuales que se han configurado con este direccionador como punto final. "Virtual endpoint" indica el ID de direccionador OSPF del otro punto final. "Transit area" indica el área que no es de red troncal a través de la cual se configura el enlace virtual. Se considera que el protocolo OSPF trata a los enlaces virtuales de forma similar a las redes punto a punto. Los demás parámetros listados en el mandato ("Rtrns", "TrnsDly", "Hello" y "Dead") se mantienen para todas las interfaces. Consulte el mandato de OSPF **list interfaces** para obtener más información.

**Ejemplo: `list virtual-links`**

```
          --Virtual link configuration--
Virtual endpoint   Transit area   Rtrns  TrnsDly Hello Dead
0.0.0.0            0.0.0.1         10      5     30    180
```

## Set

Utilice el mandato **set** para visualizar o modificar información de configuración relacionada con áreas OSPF, interfaces, redes que no son de difusión general o enlaces virtuales. Este mandato le permite definir el modo en que se comparan las rutas OSPF con la información obtenida de otros protocolos de direccionamiento.

**Sintaxis:**

**set** area
comparison
interface
non-broadcast
virtual-link
max-random-initial-lsa-age

**area** Define los parámetros correspondientes a un área OSPF. Si no hay ninguna área definida, el software del direccionador da por supuesto que todas las redes conectadas directamente del direccionador pertenecen al área de red troncal (ID de área 0.0.0.0).

**Ejemplo: `set area`**

```
Area number [0.0.0.0]? 0.0.0.1
Is this a stub area? [No]:  yes
Stub default cost? [0]:
Import summaries? [Yes]:
```

- *Número de área* - es la dirección del área OSPF.
- *Designación de área apéndice.* Si especifica “Yes”:
  - El área no recibe ningún anuncio de enlace externo AS, lo que reduce el tamaño de la base de datos y reduce el uso de memoria correspondiente a los direccionadores del área apéndice.
  - No puede configurar enlaces virtuales a través de un área apéndice.
  - No puede configurar un direccionador dentro del área apéndice como un direccionador límite AS.

  *Direccionamiento externo en áreas apéndice.* No puede configurar la red troncal como un área apéndice. El direccionamiento externo en áreas apéndice se basa en una ruta por omisión. Cada direccionador de área límite que se conecta a un área apéndice origina una ruta por omisión con este objetivo. El coste de esta ruta por omisión también se puede configurar con el mandato **set area**.

**comparison**
Indica al direccionador dónde colocar las rutas BGP/RIP/estáticas en la jerarquía de OSPF. Los dos niveles inferiores constan de las rutas internas OSPF. Las rutas internas de OSPF tienen preferencia sobre la información obtenida de cualquier otra fuente, todas las cuales se encuentran en un solo nivel.

**Ejemplo: `set comparison`**

```
OSPF Config> set comparison
Compare to type 1 or 2 externals [2]?
```

**interface** Define los parámetros de OSPF correspondiente a las interfaces de red del direccionador.

1. *Interface IP address* corresponde a cada interfaz del direccionador.
2. *Attaches to area* es el área a la que se conecta la interfaz.
3. Los valores del temporizador son iguales para todos los direccionadores conectados a un segmento común de la red.
   a. *Retransmission interval* es el intervalo tras el cual se volverá a enviar una Petición de enlace correspondiente a uno o más anuncios de estado de enlace.

      **Valores válidos:** 1 a 65535 segundos

      **Valor por omisión:** 5

   b. *Transmission delay* es una estimación del número de segundos que se tarda en transmitir información de estado de enlace sobre la interfaz.

      Cada anuncio de estado de enlace tiene un tiempo de vida limitado que equivale a la constante MaxAge (1 hora). Puesto que cada anuncio de estado de enlace se envía a determinadas interfaces, caduca según el retraso de transmisión configurado. El retraso mínimo es 1 segundo.

      **Valores válidos**: 1 a 65535 segundos

      **Valor por omisión**: 1

   c. *Hello Interval* es el intervalo entre paquetes Hello enviados a la interfaz.

      **Valores válidos**: 1 a 65535 segundos

      **Valor por omisión**: 10

   d. *Dead Router Interval*

      Dead Router Interval es el intervalo tras el que un direccionador que no ha enviado un mensaje Hello se considera que está inactivo. El valor por omisión de Dead Router Interval es cuatro veces el intervalo Hello configurado. El valor de este parámetro debe ser superior al valor de Hello Interval.

      **Valores válidos**: 2 a ≥ 65535 segundos

      **Valor por omisión**: 40 (o cuatro veces el intervalo Hello configurado)

4. El valor de *Router Priority* sirve para que las redes de difusión general y las redes multiacceso que no son de difusión general elijan el direccionador designado. Para enlaces punto a punto, este valor debe ser **0**, lo que significa que este direccionador no se debe elegir como direccionador designado para su red.

   **Valores válidos**: 0 a 255

   **Valor por omisión**: 1

5. *Type of service 0 cost* es el coste que se utilizará para la interfaz cuando se calculen las rutas de vías de acceso más cortas correspondientes al área.

   **Valores válidos:** 1 a 65534

   **Valor por omisión:** 1

6. *Demand Circuit* indica si la interfaz se tratará o no como un circuito de demanda a fin de enviar LSA (Anuncios de estado de enlace). Sobre circuitos de demanda, los LSA se enviarán con el bit DoNotAge definido sobre esta interfaz y no se enviará a no ser que haya un cambio real en el LSA. Consulte RFC 1793 para obtener más información.

   **Valores válidos:** Yes o No

   **Valor por omisión:** No

7. *Hello Suppression* indica si los paquetes Hello se suprimirán o no en la interfaz cuando los direccionadores contiguos alcancen el estado de lleno. Los circuitos de demanda deben estar activados en la interfaz para que se solicite o se permita la supresión de mensajes Hello. Actualmente, la supresión de mensajes Hello sólo recibe soporte en enlaces ATM y de marcación bajo demanda ISDN. Consulte RFC 1793 para obtener más información.

   **Valores válidos:** Allow, Request o Disable

   **Valor por omisión:** Allow

   **Allow** Permite que un direccionador contiguo solicite la supresión de mensajes Hello.

   **Request** Solicita la supresión de mensajes Hello de un direccionador contiguo.

   **Disable** Desactiva la supresión de mensajes Hello y continúa enviando dichos mensajes.

8. *Demand Circuit Down Poll Interval* indica la duración entre sondeos hello enviados cuando no se pueden enviar datos en un circuito de demanda con la supresión de mensajes hello activa. Actualmente, la supresión de mensajes Hello sólo recibe soporte en enlaces ATM y de marcación bajo demanda ISDN. Consulte RCF 1793 para obtener más información.

   **Valores válidos:** 1 a 65535

   **Valor por omisión:** 60

9. *Authentication type* define el procedimiento de autentificación a utilizar para paquetes OSPF en la interfaz. Las opciones son 1, que indica una simple contraseña; o 0, que indica que no hace falta autentificación para intercambiar paquetes OSPF en la interfaz. Cuando se especifica 1, también se debe especificar la clave de autentificación.

   **Valores válidos**: 0, 1

   **Valor por omisión**: 0

10. *Authentication key* es el parámetro que define la contraseña utilizada para esta área OSPF. Si se utiliza autentificación de

contraseña, sólo se aceptan los paquetes con la clave de autentificación correcta.

**Valores válidos**: cualquier serie de entre 1 y 8 caracteres

**Valor por omisión**: una serie nula

**Ejemplo: `set interface`**

```
Interface IP address [0.0.0.0]? 10.69.1.2
Attaches to area [0.0.0.0]?
Retransmission Interval (in seconds) [5]?
Transmission Delay (in seconds) [1]? 1
Router Priority [1]? 1
Hello Interval (in seconds) [10]?
Dead Router Interval (in seconds) [40]?
Type Of Service 0 cost [1]?
Demand Circuit (Yes or NO) ?[No]:
Authentication Type (0 - none, 1 - simple) [0]? 1
Authentication Key []? AceeOSPF
Retype Auth.  Key []? AceeOSPF
```

Cuando responda a las solicitudes, especifique la dirección IP correspondiente a cada interfaz del direccionador y conteste a la pregunta siguiente. Para los siguientes parámetros, debe especificar el mismo valor para todos los direccionadores conectados a una red común:

- Hello interval
- Dead router interval
- Authentication key (si se utiliza una autentificación igual a 1)

La primera solicitud le pregunta por el área OSPF a la que se conecta la interfaz. Por ejemplo, suponga que la máscara de dirección de interfaz es 255.255.255.0, lo que indica que la interfaz se conecta a una subred (128.185.138.0) de la red 128.185.0.0. Los demás direccionadores OSPF conectados a la subred 128.185.138.0 también deben tener un *Hello interval* igual a 10, un *dead router interval* igual a 40 y *authentication key* de la interfaz igual a xyz_q.

Tenga en cuenta que las interfaces IP antes líneas punto a punto pueden no estar numeradas. En este caso, se configura un índice de red en lugar de una dirección IP. Esta implantación de OSPF funcionará con estas interfaces no numeradas, pero, para que funcione correctamente, ambos extremos de la línea punto a punto deben utilizar una interfaz no numerada.

En una configuración de direccionamiento de difusión múltiple (se ha activado la difusión múltiple), los parámetros MOSPF correspondientes a cada interfaz OSPF tienen los valores por omisión. Esto significa que:

- El reenvío de difusión múltiple está activado.
- Los datagramas de difusión múltiple se reenvían como difusiones múltiples de enlace de datos.
- La pertenencia a un sistema principal IGMP se envía a la interfaz cada 60 segundos.
- Las entradas de la base de datos de grupo local se eliminan transcurridos 180 segundos después de que la interfaz deja de recibir informes de pertenencia a sistema principal IGMP para grupo.

Si desea modificar los parámetros MOSPF, utilice el mandato **set interface**. Se le solicitarán parámetros de difusión múltiple (los cinco últimos parámetros que aparecen en el ejemplo de salida anterior) únicamente si tiene activado el reenvío de difusiones múltiples.

En las redes basadas en un Sistema autónomo, en las que puede haber varios protocolos de direccionamiento de difusión múltiple (o varias instancias de un solo protocolo de direccionamiento de difusión múltiple), es posible que tenga que configurar el reenvío como difusiones individuales de enlace de datos para evitar la duplicación no deseada de datagramas. En cualquier caso, para todos los direccionadores conectados a una red común, los parámetros de interfaz “forward multicast datagrams” y “forward as data-link unicasts” se deben configurar de forma idéntica.

**non-broadcast**

Modifica el valor por omisión de punto a multipunto para seleccionar redes NBMA para X.25, Frame Relay o ATM. Este parámetro especifica el intervalo que determina la frecuencia de mensajes Hello enviados a los direccionadores contiguos que están inactivos. Debe definir el parámetro non-broadcast de forma coherente entre todas las interfaces que se conectan a la misma subred para que OSPF funcione correctamente.

Sin embargo, para redes Frame Relay o ATM, se utiliza el mandato **set non-broadcast** para configurar una interfaz OSPF para que se conecte a una red multiacceso que no es de difusión general. Si no se utiliza el mandato **set non-broadcast**, se da por supuesto que la interfaz se conecta a una red punto a multipunto. En redes Frame Relay, todas las interfaces OSPF se deben configurar para que se conecten al mismo tipo de red (multiacceso que no es de difusión general o punto a multipunto), de modo que si se utiliza el mandato **set non-broadcast** para una interfaz del direccionador, se debe configurar en todas las interfaces correspondientes a todos los direccionadores que se conectan a la red.

**Ejemplo:** set non-broadcast

```
Interface IP address [0.0.0.0]? 128.185.138.19
Poll Interval [120]
```

*Interface IP address* tiene:

**Valores válidos**: Cualquier dirección IP válida.

**Valor por omisión**: ninguno
Poll Interval de NBMA sirve para enviar paquetes Hello a direccionadores contiguos inactivos. (Los direccionadores contiguos inactivos son aquellos de los que el direccionador no ha oído nada durante un periodo superior al valor del parámetro Dead Router Interval.) El direccionador sigue sondeando estos direccionadores contiguos a menor velocidad. Defina para el parámetro Poll Interval de NBMA un valor mucho mayor que el configurado para el parámetro Hello Interval correspondiente al direccionador.

**Valores válidos**: 1 a 65535 segundos

**Valor por omisión**: 120 segundos

**Ejemplo:** **`set non-broadcast`**

```
Interface IP address [0.0.0.0]? 128.185.138.19
Poll Interval [120]?
```

**virtual-link**

Configura enlaces virtuales entre dos direccionadores límite de área cualesquiera. Para mantener la conectividad de la red troncal, debe tener todos los direccionadores de la red troncal interconectados

mediante enlaces permanentes o virtuales. Los enlaces virtuales se consideran como interfaces de direccionadores separadas que se conectan al área de red troncal. Por lo tanto, también se le solicitará que especifique muchos de los parámetros de la interfaz al configurar un enlace virtual.

Se pueden configurar enlaces virtuales entre dos direccionadores de red troncal cualesquiera que tengan una interfaz con un área que no sea de red troncal común. Los enlaces virtuales sirven para mantener la conectividad de red troncal y se deben configurar en ambos puntos finales.

**Nota:** Esta implantación de OSPF da soporte al uso de enlaces virtuales cuando un extremo del enlace virtual puede ser una línea punto a punto no numerada. Para que esta configuración funcione, se debe utilizar el id del direccionador como dirección de origen en los mensajes del protocolo OSPF enviados sobre el enlace virtual. Se puede asegurar el uso del id del direccionador configurando la dirección IP interna con la dirección utilizada como el id del direccionador. Otro requisitos para que esta configuración funcione es que las implantaciones OSPF de ambos extremos del enlace virtual le den soporte.

1. *Virtual endpoint (router ID)* define el ID del direccionador contiguo virtual.

   **Valores válidos**: Cualquier dirección IP válida.

   **Valor por omisión**: ninguno

2. *Link's transit area* es el área que no es de red troncal ni apéndice a través de la que se configura el enlace virtual. Se pueden configurar enlaces virtuales entre dos direccionadores límite de área cualesquiera que tengan una interfaz con un área común que no sea de red troncal ni apéndice. Los enlaces virtuales se deben configurar en cada uno de los dos puntos finales del enlace.

   **Valores válidos**: 0.0.0.1 a 255.255.255.255

   **Valor por omisión**: 0.0.0.1

3. Los valores del temporizador son iguales para todos los direccionadores conectados a un segmento común de la red.

   a. *Retransmission interval* es el intervalo tras el cual se volverá a enviar una Petición de enlace correspondiente a uno o más anuncios de estado de enlace.

      **Valores válidos:** 1 a 65535 segundos

      **Valor por omisión:** 10

   b. El parámetro *Transmission delay* es una estimación del número de segundos que se tarda en transmitir información de estado de enlace sobre la interfaz.

      Cada anuncio de estado de enlace tiene un tiempo de vida limitado que equivale a la constante MaxAge (1 hora). Puesto que cada anuncio de estado de enlace se envía a determinadas interfaces, caduca según el

retraso de transmisión configurado. El retraso mínimo es 1 segundo.

**Valores válidos**: 1 a 65535 segundos

**Valor por omisión**: 5

c. *Hello Interval* es el intervalo entre paquetes Hello enviados a la interfaz.

**Valores válidos**: 1 a 255 segundos

**Valor por omisión**: 30

d. *Dead Router Interval* es el intervalo tras el que un direccionador que no ha enviado un mensaje Hello se considera que está inactivo. El valor por omisión de este parámetro es seis veces mayor que el parámetro Hello Interval configurado y debe tener un valor superior al de Hello Interval.

**Valores válidos**: 2 a 65535 segundos

**Valor por omisión**: 180

4. *Authentication type* define el procedimiento de autentificación a utilizar para paquetes OSPF en el enlace virtual. Las opciones son 1, que indica una simple contraseña; o 0, que indica que no hace falta autentificación para intercambiar paquetes OSPF en la interfaz. Cuando se especifica 1, también se debe especificar la clave de autentificación.

**Valores válidos**: 0, 1

**Valor por omisión**: 0

5. *Authentication key* define la contraseña utilizada para esta área OSPF. Si se utiliza autentificación de contraseña, sólo se aceptan los paquetes con la clave de autentificación correcta.

**Valores válidos**: cualquier serie de entre 1 y 8 caracteres

**Valor por omisión**: una serie nula

**Ejemplo:** `set virtual-link`

```
Virtual endpoint  (Router ID) [0.0.0.0]? 10.1.1.2
Link's transit area [0.0.0.1]?
Virtual link already exists - record will be modified.
Retransmission Interval (in seconds) [10]?
Transmission Delay (in seconds) [5]?
Hello Interval (in seconds) [30]?
Dead Router Interval (in seconds) [180]?
Authentication Type (0 - none, 1 - simple) [0] 1
Authentication Key []? AceeOSPF
Retype Auth. Key []? AceeOSPF
```

**max-random-initial-lsa-age**

Especifica la antigüedad inicial máxima para los LSA originados de forma automática. El valor por omisión es 0 y normalmente sólo se tiene que modificar si tiene problemas con la la sincronización de generación de LSA.

**Valores válidos**: 0 - 1770

**Valor por omisión**: 0

**Ejemplo:**

```
OSPF Config>  set max-random-initial-lsa-age
Maximum initial LSA age [0]?
```

## Cómo acceder al entorno de supervisión de OSPF

Utilice el siguiente procedimiento para acceder a los mandatos de supervisión de OSPF. Este proceso le ofrece acceso al proceso de *supervisión* de OSPF.

1. En el indicador OPCON, entre **talk 5**. (Para obtener más información sobre este mandato, consulte el tema “The OPCON Process and Commands” del manual *Guía del usuario de software*.) Por ejemplo:

   ```
   * talk 5
   +
   ```

   Una vez haya especificado el mandato **talk 5**, aparece el indicador GWCON (+) en el terminal. Si no aparece este indicador la primera vez que entre en la configuración, vuelva a pulsar **Intro**.

2. En el indicador +, entre el mandato **protocol ip** para que aparezca el indicador OSPF>.

   **Ejemplo:**

   ```
   + prot ospf
   OSPF>
   ```

## Mandatos de supervisión de OSPF

Esta sección resume y luego explica todos los mandatos de supervisión de OSPF. Estos mandatos le permite supervisar el protocolo de direccionamiento OSPF. La Tabla 24 contiene los mandatos de supervisión de OSPF.

Entre los mandatos de supervisión de OSPF en el indicador OSPF>.

*Tabla 24 (Página 1 de 2). Resumen de mandatos de supervisión de OSPF*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Advertisement | Muestra un anuncio de estado de enlace perteneciente a la base de datos OSPF. |
| Area summary | Muestra parámetros y estadísticas de áreas OSPF. |
| AS external | lista los anuncios externos AS pertenecientes a la base de datos de estado de enlace de OSPF. |
| Database summary | Muestra los anuncios pertenecientes a la base de datos de estado de enlace de un área OSPF. |
| Dump routing tables | Muestra las rutas OSPF contenidas en la tabla de direccionamiento. |
| Interface summary | Muestra parámetros y estadísticas de la interfaz OSPF. |
| Join | Configura el direccionador para que pertenezca a uno o más grupos de difusión múltiple. |

*Tabla 24 (Página 2 de 2). Resumen de mandatos de supervisión de OSPF*

| Mandato | Función |
|---|---|
| Leave | Elimina el direccionador de grupos de difusión múltiple. |
| Mcache | Muestra una lista de entradas de la antememoria de reenvíos de difusión múltiple actualmente activas. |
| Mgroups | Muestra la pertenencia a grupos de las interfaces conectadas del direccionador. |
| Mstats | Muestra distintas estadísticas de direccionamiento de difusión múltiple. |
| Neighbor summary | Muestra parámetros y estadísticas de direccionadores contiguos OSPF. |
| Ping | Envía continuamente peticiones de eco ICMP (o mandatos ping) a un determinado destino, mostrando una línea por cada respuesta recibida. |
| Policy | Muestra las políticas de importación de direccionadores límite AS configuradas. |
| Reset | Restablece la configuración de OSPF de forma dinámica. |
| Routers | Muestra los direccionadores límite AS y los direccionadores límite de área de OSPF a los que se puede llegar. |
| Size | Muestra el número de LSA que actualmente se encuentran en la base de datos de estado de enlace, clasificados por tipo. |
| Statistics | Muestra estadísticas de OSPF que detallan el uso de memoria y de red. |
| Traceroute | Muestra la ruta completa (salto a salto) a un determinado destino. |
| Weight | Modifica de forma dinámica el coste de una interfaz OSPF. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Advertisement Expansion

Utilice el mandato **advertisement expansion** para visualizar el contenido de un anuncio de estado de enlace contenido en la base de datos de OSPF. Para ver un resumen de los anuncios del direccionador, utilice el mandato **database**.

Un anuncio de estado de enlace se define por su tipo de estado de enlace, ID de estado de enlace y el direccionador que envía el anuncio. Hay una base de datos de estado de enlace para cada área OSPF. Al especificar un id de área en la línea de mandatos, indica al software en qué base de datos desea buscar. Los distintos tipos de anuncios, que dependen del valor especificado para el tipo de estado de enlace, son:

- Enlaces del direccionador - Contienen descripciones de una sola interfaz del solo direccionador.
- Enlaces de red - Contienen la lista de direccionadores conectados a una determinada interfaz.
- Redes resumen - Contienen descripciones de una sola ruta interna del área.
- Direccionadores límite AS resumen - Contienen descripciones de la ruta a un direccionador límite AS de otra área.
- Redes externas AS - Contienen descripciones de una sola ruta.

- Pertenencia a grupos de difusión general - Contienen descripciones de la pertenencia a un determinado grupo cercano al direccionador que envía el anuncio.

  **Nota:** Los ID de estado de enlace, los direccionadores que envían anuncios (especificados mediante sus ID de direccionador) y los ID de área tienen el mismo formato que las direcciones IP. Por ejemplo, el área de red troncal se puede especificar como 0.0.0.0.

El **Ejemplo 1** muestra una expansión de un anuncio de enlaces de direccionador. El ID del direccionador es 128.185.184.11. Es un direccionador límite AS que tiene tres interfaces con el área de red troncal (todas ellas con coste igual a 1). Se ha activado el direccionamiento de difusión múltiple. Con el ejemplo se suministran descripciones detalladas de los campos.

Este mandato también se ha mejorado de dos formas. En primer lugar, al visualizar los LSA del direccionador y los LSA de la red aparece el coste invertido de cada enlace direccionador a direccionador y de cada enlace direccionador a red de tránsito, así como el coste de reenvío que se visualizaba anteriormente. Esto se debe a que el direccionamiento de datagramas de difusión múltiple cuyo origen se encuentra en distintas áreas o sistemas autónomos se basa en el coste invertido en lugar de basarse en el coste de reenvío. En los casos en que no hay enlace invertido (lo que significa que el enlace nunca será utilizado por Dijkstra), el coste invertido que aparece es “1-way”.

Además, las opciones OSPF del LSA se visualizan del mismo modo que aparecen en el mandato **neighbor** detallado de OSPF.

También se pueden visualizar nuevos LSA de pertenencia a grupos. El “destino LS” de cada LSA de pertenencia a grupos es una dirección de grupo. Un direccionador origina un LSA de pertenencia a grupos para cada grupo que tiene miembros en una o más de las redes conectadas del direccionador. El LSA de pertenencia a grupos correspondiente al grupo lista las redes de tránsito conectadas que tienen miembros del grupo (los vértices de tipo “2”), y, cuando hay miembros que pertenecen a una o más redes apéndice conectadas, o si el direccionador es miembro del grupo de difusión múltiple, se incluye un vértice de tipo “1” cuyo ID es el ID del direccionador OSPF.

**Sintaxis:**

ad**vertisement** *tipo-ls id-estado-enlace direccionador-que-envía-anuncio id-área*

**Ejemplo 1:**
```
advertisement  1  128.185.184.11 0.0.0.0
```

```
LS age:     173
LS options:  E,MC,DC
LS type:     1
LS destination (ID): 128.185.184.11
LS originator:   128.185.184.11
LS sequence no:  0x80000047
LS checksum:     0x122
LS length:       60
Router type:  ASBR,W
# router ifcs:   3
         Link ID:          128.185.177.31
         Link Data:        128.185.177.11
         Interface type:   2
                  No. of metrics: 0
                  TOS 0 metric:   3 (0)
         Link ID:          128.185.142.40
         Link Data:        128.185.142.11
         Interface type:   2
                  No. of metrics: 0
                  TOS 0 metric:   4 (0)
         Link ID:          128.185.184.0
         Link Data:        255.255.255.0
         Interface type:   3
                  No. of metrics: 0
                  TOS 0 metric:   1
```

LS age — Indica la antigüedad del anuncio en segundos.

LS options — Indica las funciones de OSPF opcionales a las que da soporte el objeto OSPF correspondiente al anuncio. Estas funciones incluyen:

- **E** — Indica que se da soporte a los anuncios de tipo 5 (anuncios externos) en el área correspondiente al anuncio. Siempre se define para el tipo 5 (anuncios externos).
- **T** — Se da soporte al direccionamiento basado en TOS (Tipo de servicio) de IP.
- **MC** — Se da soporte al reenvío de difusión múltiple. Sólo se definirá en anuncios originados por direccionadores con MOSPF activado.
- **DC** — Se da soporte a los circuitos de demanda, tal como se describe en RFC 1793.

LS type — Clasifica los anuncios y especifica su contenido: 1 (anuncios de enlaces de direccionador), 2 (anuncio de enlace de red), 3 (anuncio de enlace de resumen), 4 (anuncio ASBR de resumen), 5 (enlace externo AS) y 6 (anuncio de pertenencia a grupos).

LS destination — Identifica lo describe el anuncio. Depende del tipo de anuncio. Para enlaces de direccionador y resúmenes ASBR, es el ID del direccionador OSPF. Para enlaces de red, es la dirección IP del direccionador designado de la red. Para enlaces de resumen y enlaces externos AS, es el número de red/subred. Para anuncios de pertenencia a grupos, es un determinado grupo de difusión múltiple.

LS originator — ID de direccionador OSPF del direccionador que origina el anuncio.

LS sequence number — Sirve para distinguir distintas instancias del mismo anuncio. Se debe considerar como un entero de 32 bits con signatura. Comienza en 0x80000001, y aumenta en uno cada vez que se actualiza el anuncio.

LS checksum — Una suma de comprobación del contenido del anuncio, que sirve para detectar un posible daño en los datos.

LS length — El tamaño del anuncio en bytes.

| | |
|---|---|
| Router type | Indica el nivel de función del direccionador. ASBR significa que el direccionador es un direccionador límite AS, ABR que es un direccionador límite de área y W que es un receptor comodín de difusión múltiple. |
| # Router ifcs | El número de interfaces del direccionador descritas en el anuncio. |
| Link ID | Indica a qué se conecta la interfaz. Depende del tipo de interfaz. Para interfaces a direccionadores (por ejemplo, enlaces punto a punto), el ID de enlace es el ID del direccionador contiguo. Para interfaces a redes de tránsito, es la dirección IP del direccionador designado de la red. Para interfaces a redes apéndice, es el número de red/subred de la red. |
| Link Data | 4 bytes de información adicional sobre el enlace; es la dirección IP de la interfaz (para interfaces ante redes punto a punto y redes de tránsito) o la máscara de subred (para interfaces ante redes apéndice). |
| Interface type | Uno de los siguientes valores: 1 (conexión punto a punto con otro direccionador), 2 (conexión con una red de tránsito), 3 (conexión con una red apéndice) o 4 (enlace virtual). |
| No. of metrics | El número de valores TOS distintos de cero para los que se ofrecen métricas correspondientes a esta interfaz. |
| TOS 0 metric | El coste de la interfaz. Entre paréntesis aparece el coste invertido del enlace (obtenido de otro anuncio). Si no hay enlace invertido, se muestra “1-way”. |

Los campos LS age, LS options, LS type, LS destination, LS originator, LS sequence no, LS checksum y LS length son comunes a todos los anuncios. Los campos Router type y # router ifcs sólo se muestran en anuncios de enlaces del direccionador. Cada enlace del anuncio del direccionador se describe mediante los campos Link ID, Link Data e Interface type. A cada enlace se le puede asignar un coste separado para cada Tipo de servicio (TOS) IP, que se describe mediante los campos No. of metrics y TOS 0 (el direccionador actualmente no direcciona según TOS, y sólo acepta el coste de TOS 0).

El **Ejemplo 2** muestra una expansión de un anuncio de pertenencia a grupos. Un anuncio de pertenencia a grupos correspondiente a una determinada combinación de grupo/direccionador que emite el anuncio lista las redes conectadas directamente al direccionador que emite el anuncio que tiene miembros de grupo. También lista si el direccionador forma parte del grupo especificado. El ejemplo siguiente muestra que la red 128.185.184.0 tiene miembros del grupo 224.0.1.1.

**Ejemplo 2:** `adv 6 224.0.1.1 128.185.184.114`

```
For which area [0.0.0.0]?

LS age:     168
LS options:  E
LS type:     6
LS destination (ID): 224.0.1.1
LS originator:   128.185.184.114
LS sequence no:  0x80000001
LS checksum:     0x7A3
LS length:       28
Vertex type: 2
Vertex ID:   128.185.184.114
```

| | |
|---|---|
| Vertex type | Describe el objeto que tiene miembros de grupo, y puede adoptar uno de los siguiente valores: 1 (el direccionador, o redes apéndice conectadas al direccionador) o 2 (una red de tránsito). |

Vertex ID — Cuando el tipo de vértice es 1, es siempre el ID del direccionador que emite el anuncio. Cuando el tipo de vértice es 2, es la dirección IP del direccionador designado de la red de tránsito.

## Area Summary

Utilice el mandato **area summary** para visualizar estadísticas y parámetros correspondientes a todas las áreas OSPF conectadas al direccionador.

En el ejemplo siguiente, el direccionador se conecta a una sola área (el área de red troncal). De utiliza un esquema de una sola contraseña para la autentificación del área. El direccionador tiene tres interfaces que se conectan al área y ha encontrado 4 redes de tránsito, 7 direccionadores y ningún direccionador límite de área al calcular el árbol SPF correspondiente a la red troncal.

**Sintaxis:**

ar**ea**

**Ejemplo:**

```
Area ID           #ifcs  #nets  #rtrs  #brdrs  DC-Status
          0.0.0.1                1      1       2       2      On
          0.0.0.0                3      0       3       2     Off
```

# ifcs — Indica el número de interfaces del direccionador conectadas al área determinada. Estas interfaces no están necesariamente operativas.

# nets — Indica el número de redes de tránsito encontradas al calcular el árbol SPF correspondiente a este área.

# rtrs — Indica el número de direccionadores encontrados al calcular el árbol SPF correspondiente a este área.

# brdrs — Indica el número de direccionadores límite de área encontrados al calcular el árbol SPF correspondiente a este área.

DC-Status — Indica si el proceso de circuitos de demanda está activo para este área.

## AS-external advertisements

Utilice el mandato **AS-external advertisements** para listar los anuncios externos al AS pertenecientes al dominio de direccionamiento OSPF. Se muestra una línea por anuncio. Cada anuncio se define mediante los tres siguientes parámetros: su tipo de estado de enlace (siempre 5 para anuncios externos al AS), su ID de estado de enlace (denominado Destino LS) y el direccionador que emite el anuncio (denominado Originador LS).

**Sintaxis:**

as**-external**

**Ejemplo: `as-external`**

```
Type LS-destination  LS-originator   Seq-Number  Age Unreach Xsum   Options
  5  10.13.64.0      10.1.62.1       0x80000385 1422         0x7791 E,DC
  5  10.14.64.0      10.1.62.1       0x80000385 1420         0x6B9C E,DC

               # advertisements:       2
               Checksum total:         0xE32D
```

Type — Siempre 5 para anuncios externos al AS.

| | |
|---|---|
| LS destination | Indica un número de red/subred IP. Estos números de red pertenecen a otro Sistema autónomo. |
| LS originator | Direccionador que emite el anuncio. |
| Unreach | Indica durante cuánto tiempo no se ha podido llegar al destino asociado a un Anuncio de estado de enlace (LSA) que es DoNotAge. Si el LSA es DoNotAge, aparecerá *DA* entre las columnas Age y Unreach. Si el LSA **no** es DoNotAge, aparecerán espacios en blanco. |
| Seqno, Age, Xsum | Es posible que haya varias instancias de un anuncio en el dominio de direccionamiento OSPF en un momento determinado. Sin embargo, sólo la instancia más reciente se mantiene en la base de datos de estado de enlace OSPF (que es la que muestra este mandato). Los campos LS sequence number (Seqno), LS age (Age) y LS checksum (Xsum) se comparan para ver qué instancia es la más reciente. El campo LS age se expresa en segundos. Su valor máximo es 3600. |
| Options | Son las opciones de estado de enlace, que son funciones opcionales de OSPF que reciben soporte del objeto OSPF correspondiente al anuncio. Estas funciones incluyen:<br>**E** Indica que se da soporte a los anuncios de tipo 5 (anuncios externos) en el área correspondiente al anuncio. Siempre se define para el tipo 5 (anuncios externos).<br>**T** Se da soporte al direccionamiento basado en TOS (Tipo de servicio) de IP.<br>**MC** Se da soporte al reenvío de difusión múltiple. Sólo se definirá en anuncios originados por direccionadores con MOSPF activado.<br>**DC** Se da soporte a los circuitos de demanda, tal como se describe en RFC 1793. |

Al final de la pantalla, aparece el número total de anuncios externos al AS, junto con un total de sumas de comprobación correspondiente a su contenido. El total de sumas de comprobación es simplemente la suma de 32 bits (se eliminan los restos) de los campos de suma de comprobación LS de cada anuncio. Esta información sirve para determinar con rapidez si dos direccionadores OSPF tienen bases de datos sincronizadas.

## Database Summary

Utilice el mandato **database summary** para visualizar una descripción del contenido de la base de datos de estado de enlace de una determinada área OSPF. Los anuncios externos al AS no aparecen en la pantalla. Se muestra una línea por anuncio. Cada anuncio se define mediante los tres siguientes parámetros: su tipo de estado de enlace (denominado Tipo), su ID de estado de enlace (denominado Destino LS) y el direccionador que emite el anuncio (denominado Originador LS).

**Sintaxis:**

da**tabase** *area-id*

**Ejemplo: `database 0.0.0.0`**

```
Type LS-destination  LS-originator   Seq-Number  Age Unreach Xsum   Options
  1  10.1.62.1       10.1.62.1       0x80004963  496         0xBC15 E,DC
  1  10.1.62.2       10.1.62.2       0x800250FF    6         0xCA6F E,DC
  ⋮
               # advertisements:       99
               Checksum total:         0x2CD102
```

| | |
|---|---|
| Type | Se muestran numéricamente los distintos tipos de LS: tipo 1 (anuncios de enlaces del direccionador), tipo 2 (anuncios de enlaces de la red), tipo 3 (resúmenes de la red), tipo 4 (resúmenes del direccionador límite AS) y tipo 6 (LSA de pertenencia a grupo). |
| LS destination | Indica lo que describe el anuncio. |
| LS originator | Direccionador que emite el anuncio. |
| Unreach | Indica durante cuánto tiempo no se ha podido llegar al destino asociado a un Anuncio de estado de enlace (LSA) que es DoNotAge. Si el LSA es DoNotAge, aparecerá *DA* entre las columnas Age y Unreach. Si el LSA **no** es DoNotAge, aparecerán espacios en blanco. |
| Seqno, Age, Xsum | Es posible que haya varias instancias de un anuncio en el dominio de direccionamiento OSPF en un momento determinado. Sin embargo, sólo la instancia más reciente se mantiene en la base de datos de estado de enlace OSPF (que es la que muestra este mandato). Los campos LS sequence number (Seqno), LS age (Age) y LS checksum (Xsum) se comparan para ver qué instancia es la más reciente. El campo LS age se expresa en segundos. Su valor máximo es 3600. |
| Options | Son las opciones de estado de enlace, que son funciones opcionales de OSPF que reciben soporte del objeto OSPF correspondiente al anuncio. Estas funciones incluyen:<br>**E** Indica que se da soporte a los anuncios de tipo 5 (anuncios externos) en el área correspondiente al anuncio. Siempre se define para el tipo 5 (anuncios externos).<br>**T** Se da soporte al direccionamiento basado en TOS (Tipo de servicio) de IP.<br>**MC** Se da soporte al reenvío de difusión múltiple. Sólo se definirá en anuncios originados por direccionadores con MOSPF activado.<br>**DC** Se da soporte a los circuitos de demanda, tal como se describe en RFC 1793. |

Al final de la pantalla, aparece el número total de anuncios del área, junto con un total de sumas de comprobación correspondiente a su contenido. El total de sumas de comprobación es simplemente la suma de 32 bits (se eliminan los restos) de los campos de suma de comprobación LS de cada anuncio. Esta información sirve para determinar con rapidez si dos direccionadores OSPF tienen bases de datos sincronizadas.

**Nota:** Al comparar direccionadores con soporte de difusión múltiple con direccionadores que no son de difusión múltiple, la suma de comprobación de base de datos anterior (y también el número de anuncio) no coincidirá necesariamente, puesto que los direccionadores que no son de difusión general no manejan ni guardan LSA de pertenencia a grupo. Además, si el proceso de circuitos de demanda está activo en el dominio de direccionamiento OSPF o en el área apéndice OSPF, es muy probable que la suma de comprobación de base de datos sea distinta entre los direccionadores con circuitos de demanda. Consulte RFC 1793 para obtener más información.

## Dump Routing Tables

Utilice el mandato **dump routing tables** para visualizar todas las rutas que ha calculado OSPF y que están ahora presentes en la tabla de direccionamiento. Su salida es parecida en formato a la del mandato dump routing tables de supervisión de IP.

**Sintaxis:**

d**ump**

**Ejemplo:** **dump**

```
Type   Dest net         Mask     Cost Age   Next hop(s)
SPE1   0.0.0.0          00000000  4    3    128.185.138.39
SPF*   128.185.138.0    FFFFFF00  1    1    Eth/0
Sbnt   128.185.0.0      FFFF0000  1    0    None
SPF    128.185.123.0    FFFFFF00  3    3    128.185.138.39
SPF    128.185.124.0    FFFFFF00  3    3    128.185.138.39
SPF    192.26.100.0     FFFFFF00  3    3    128.185.131.10
RIP    197.3.2.0        FFFFFF00  10   30   128.185.131.10
RIP    192.9.3.0        FFFFFF00  4    30   128.185.138.21
Del    128.185.195.0    FFFFFF00  16   270  None

Default gateway in use.

Type Cost Age  Next hop
SPE1 4    3    128.185.138.39

Routing table size: 768 nets (36864 bytes), 36 nets known
```

Type (tipo de ruta)
: Indica el modo en que se ha obtenido la ruta.

  Sbnt - Indica que la red tiene subredes; esta entrada es únicamente un área de retención de posición.

  Dir - Indica una red o subred directamente conectada.

  RIP - Indica que la ruta se ha aprendido a través del protocolo RIP.

  Del - Indica que la ruta se ha eliminado.

  Stat - Indica una ruta configurada de forma estática.

  BGP - Indica rutas aprendidas a través del protocolo BGP.

  BGPR - Indica rutas aprendidas a través del protocolo BGP que OSPF y RIP han vuelto a anunciar.

  Fltr - Indica un filtro de direccionamiento.

  SPF - Indica que la ruta es una ruta interna del área OSPF.

  SPIA - Indica que es una ruta entre áreas OSPF.

  SPE1, SPE2 - Indica rutas externas OSPF (de tipo 1 y de tipo 2 respectivamente).

  Rnge - Indica un tipo de ruta que es un rango de direcciones de área OSPF y que no se utiliza en el reenvío de paquetes.

Dest net
: Red/subred de destino IP.

Mask
: Máscara de dirección IP.

Cost
: Coste de la ruta.

Age
: Para rutas RIP y BGP, el tiempo transcurrido desde la última vez que se renovó la entrada de la tabla de direccionamiento.

| | |
|---|---|
| Next Hop | Dirección IP del siguiente direccionador de la vía de acceso hacia el sistema principal de destino. También se muestra el tipo de interfaz que utiliza el direccionador emisor para reenviar el paquete. |

Un asterisco (*) tras el tipo de ruta indica que la ruta tiene una reserva conectada de forma estática o directa. Un símbolo de porcentaje (%) tras el tipo de ruta indica que las actualizaciones RIP se aceptarán siempre para esta red/subred.

Un número entre paréntesis al final de la columna indica el número de rutas de igual coste hasta el destino. Los primeros saltos pertenecientes a estas rutas se pueden visualizar con el mandato de supervisión de IP **route**.

## Interface Summary

Utilice el mandato **interface summary** para visualizar estadísticas y parámetros relacionados con interfaces OSPF. Si no se especifica ningún argumento (consulte el Ejemplo 1), aparece una sola línea que resume cada interfaz. Si se especifica la dirección IP de una interfaz (consulte el Ejemplo 2), se muestran estadísticas detalladas sobre dicha interfaz.

**Sintaxis:**

**interface** *dirección-ip-interfaz*

**Ejemplo 1: `interface`**

```
Ifc Address      Phys    assoc. Area     Type   State   #nbrs #adjs
9.67.217.66      TKR/0   2.2.2.2        Brdcst   64        0    0
128.185.123.22   PPP/0   0.0.0.0        Brdcst   64        0    0
```

| | |
|---|---|
| Ifc Address | Dirección IP de la interfaz. |
| Phys | Muestra la interfaz física. |
| Assoc Area | ID del área conectada. |
| Type | Puede ser Brdcst (difusión general, como por ejemplo una interfaz Ethernet), P-P (una red punto a punto, como por ejemplo una línea serie síncrona), P-2-MP (punto a multipunto, como por ejemplo una red Frame-Relay), Multi (multiacceso que no es de difusión general, como por ejemplo una conexión X.25) o VLink (un enlace virtual OSPF). |
| State | Puede ser uno de los siguiente valores: 1 (inactivo), 2 (repetición de bucle), 4 (en espera), 8 (punto a punto) , 16 (DR otro) 32 (DR de reserva) o 64 (direccionador designado). |
| #nbrs | Número de direccionadores contiguos. Es el número de direccionadores de los que se han recibido mensajes hello más aquellos que se han configurado. |
| #adjs | Número de adyacencias. Es el número de direccionadores contiguos en estado de intercambio o superior. Son los direccionadores contiguos con los que ha sincronizado el direccionador o con los que está en proceso de sincronización. |

**Ejemplo 2:** `interface 128.185.125.22`

```
Interface address:      128.185.125.22
Attached area:          0.0.0.1
Physical interface:     Eth/1
Interface mask:         255.255.255.0
Interface type:         Brdcst
State:                  32
Authentication Type:    None
Designated Router:      128.185.184.34
            Backup DR:              128.185.184.11

DR Priority:       1  Hello interval:   10  Rxmt interval:     5
Dead interval:    40  TX delay:          1  Poll interval:     0
Demand Circuit   off  Max pkt size:   2044  TOS 0 cost:        1

# Neighbors:       0  # Adjacencies:     0  # Full adjs.:      0
# Mcast floods:    0  # Mcast acks:      0

MC forwarding:    on  DL unicast:      off  IGMP monitor:     on
# MC data in:      0  # MC data acc:     0  # MC data out:     0

Network Capabilities:    Broadcast    Real Network
IGMP polls snt:   75  IGMP polls rcv:    0  Unexp polls:       0

IGMP reports:     0
```

| | |
|---|---|
| Interface Address | Dirección IP de la interfaz. |
| Attached Area | ID del área conectada. |
| Physical interface | Muestra el tipo y número de la interfaz física. |
| Interface Mask | Muestra la máscara de subred de la interfaz. |
| Interface type | Puede ser Brdcst (difusión general, como por ejemplo una interfaz Ethernet), PP (una red punto a punto, como por ejemplo una línea serie síncrona), P-2-MP (punto a multipunto, como por ejemplo una red Frame-Relay), Multi (multiacceso que no es de difusión general, como por ejemplo una conexión X.25) y VLink (un enlace virtual OSPF). |
| State | Puede ser uno de los siguiente valores: 1 (inactivo), 2 (repetición de bucle), 4 (en espera), 8 (punto a punto) , 16 (DR otro) 32 (DR de reserva), 64 (direccionador designado) o 128 (lleno). |
| Authentication Type | Indica el tipo de autentificación activo para la interfaz. Los tipos a los que se da soporte son none o simple. |
| Designated Router | Dirección IP del direccionador designado. |
| Backup DR | Dirección IP del direccionador designado de reserva. |
| DR Priority | Muestra la prioridad asignada al direccionador designado. |
| Hello interval | Muestra el valor actual del intervalo hello. |
| Rxmt interval | Muestra el valor actual del intervalo de retransmisión. |
| Dead interval | Muestra el valor actual del intervalo de inactividad. |
| TX delay | Muestra el valor actual del retraso de transmisión. |
| Poll interval | Muestra el valor actual del intervalo de sondeo. |
| Max pkt size | Muestra el tamaño máximo correspondiente a un paquete OSPF enviado por esta interfaz. |
| Demand circuit | Indica si el proceso de circuitos de demanda está o no activo en la interfaz. |

| | |
|---|---|
| TOS 0 cost | Muestra el coste de TOS 0 de la interfaz. |
| # Neighbors | Número de direccionadores contiguos. Es el número de direccionadores de los que se han recibido mensajes hello más aquellos que se han configurado. |
| # Adjacencies | Número de adyacencias. Es el número de direccionadores contiguos en estado de intercambio o superior. |
| # Full adj | Número de adyacencias completas. El número de adyacencias completas es el número de direccionadores contiguos cuyo estado es Lleno (y, por lo tanto, con los que el direccionador tiene bases de datos sincronizadas). |
| # Mcast Floods | Número de actualizaciones de estado de enlace enviadas por la interfaz (sin contar las retransmisiones). |
| # Mcast acks | Número de acuses de recibo de estado de enlace enviados por la interfaz (sin contar las retransmisiones). |
| MC forwarding | Muestra si el reenvío de difusión múltiple está activado para la interfaz. |
| DL unicast | Muestra si los datagramas de difusión múltiple se deben enviar como difusiones múltiples de enlace de datos o como difusiones individuales de enlace de datos. |
| IGMP monitor | Muestra si IGMP está activado en la interfaz. |
| # MC data in | Muestra el número de datagramas de difusión múltiple recibidos en esta interfaz y luego reenviados de forma satisfactoria. |
| # MC data acc | Muestra el número de datagramas de difusión múltiple que se han reenviado de forma satisfactoria. |
| # MC data out | Muestra el número de datagramas que se han reenviado por la interfaz (como difusiones múltiples de enlace de datos o como difusiones individuales de enlace de datos). |
| Network Capabilities | Muestra las funciones de red correspondientes a la interfaz. |
| IGMP polls sent | Muestra el número de consultas de pertenencia a sistema principal IGMP enviadas por la interfaz. |
| IGMP polls rcv | Muestra el número de consultas de pertenencia a sistema principal IGMP recibidas en la interfaz. |
| Unexp polls | Muestra el número de consultas de pertenencia a sistema principal IGMP recibidas en la interfaz que no se esperaban (es decir, recibidas cuando el propio direccionador las estaba enviando). |
| IGMP reports | Muestra el número de informes de pertenencia a sistema principal IGMP recibidos en la interfaz. |
| Nbr node: tipo e ID | Muestra la identidad del nodo de donde proceden los datos si se suponía que el direccionador debía recibir datagramas en esta interfaz. Aquí el tipo es un entero comprendido entre 1 y 3: 1 indica direccionador, 2 indica red de tránsito y 3 indica red apéndice. |

## Join

Utilice el mandato **join** para establecer el direccionador como miembro de un grupo de difusión múltiple.

Este mandato se parece al mandato join de supervisión de configuración de OSPF con dos diferencias:

- El efecto sobre la pertenencia a grupo es inmediato si los mandatos se emiten desde el indicador de supervisión de OSPF (no hace falta volver a arrancar ni volver a cargar el direccionador). Paralelamente, los grupos IP unidos no se mantienen una vez se vuelve a arrancar o a cargar el direccionador.
- El mandato efectúa un seguimiento del número de veces que se emite un mandato “join” sobre un determinado grupo.

Cuando el direccionador es miembro de un grupo de difusión múltiple, responde a mandatos ping y a consultas SNMP enviadas a la dirección del grupo.

**Sintaxis:**

jo**in** *dirección-grupo-difusión-múltiple*

**Ejemplo:** `join 224.185.0.0`

## Leave

Utilice el mandato **leave** para que un direccionador deje de formar parte de un grupo de difusión múltiple. Este mandato hará que el direccionador deje de responder a mandatos ping y a consultas SNMP enviadas a la dirección del grupo.

Este mandato es parecido al mandato leave de supervisión de configuración de OSPF con dos diferencias:

- El efecto sobre la pertenencia a grupo es inmediato si los mandatos se emiten desde el indicador de supervisión de OSPF (es decir, no hace falta volver a arrancar ni volver a cargar el direccionador).
- El mandato no eliminará el direccionador del grupo hasta que el número de mandatos “leave” ejecutados sea igual al número de mandatos “joins” anteriormente ejecutados. Paralelamente, los grupos de difusión múltiple IP que queden no se mantienen una vez se vuelve a arrancar y a cargar el direccionador.

**Sintaxis:**

le**ave** *dirección-grupo-difusión-múltiple*

**Ejemplo:** `leave 224.185.0.0`

## Mcache

Utilice el mandato **mcache** para visualizar la lista de entradas de la antememoria de difusión múltiple actualmente activas. Las entradas de la antememoria de difusión múltiple se basan en la demanda, cuando se recibe el primer datagrama coincidente de difusión múltiple. Hay una entrada de antememoria (y, por lo tanto, una ruta) para cada combinación de red de origen de datagrama y grupo de destino.

Las entradas de la antememoria se borran tras cambios en la topología (por ejemplo, cuando se activa o desactiva una línea punto a punto en el sistema MOSPF) y tras cambios en pertenencia a grupos.

**Sintaxis:**

mc**ache**

**Ejemplo 1:** `mcache`

```
     0: TKR/0          1: SDLC/0         2: FR/0
     3: Internal

Source          Destination     Count   Upst    Downstream
133.1.169.2     225.0.1.10      8       Local   2 (4),3
133.1.169.2     225.0.1.20      8       Local   2 (4),3
3.3.3.3         225.0.1.10      8       2       3
```

| | |
|---|---|
| Source | Red/subred de origen de los datagramas coincidentes. |
| Destination | Grupo de destino de los datagramas coincidentes. |
| Count | Muestra el número de datagramas recibidos que coinciden con la entrada de antememoria. |
| Upst | Muestra el direccionador/red contiguo del que se debe recibir el datagrama para que se reenvíe. Cuando aparece el valor “none,” significa que el datagrama no se reenviará nunca. |
| Downstream | Muestra el número total de interfaces/direccionadores contiguos directos a los que se reenviará el datagrama. Cuando su valor es 0, significa que el datagrama no se reenviará. |

Una entrada de la antememoria de reenvíos de difusión múltiple contiene más información. Se puede visualizar en detalle una entrada de la antememoria especificando el origen y el destino de un datagrama coincidente en la línea de mandatos. Si no se encuentra ninguna entrada de la antememoria coincidente, se crea una. En el Ejemplo 2 se muestra un ejemplo de este mandato.

**Ejemplo 2:** `mcache 128.185.182.9 224.0.1.2`

```
source Net:     128.185.182.0
Destination:    224.0.1.2
Use Count:      472
Upstream Type:  Transit Net
Upstream ID:    128.185.184.114
Downstream:     128.185.177.11 (TTL = 2)
```

Además de la información que se muestra en el formato corto del mandato mcache, se visualizan los siguientes campos:

| | |
|---|---|
| Upstream Type | Indica el tipo de nodo del que se debe recibir el datagrama para que se reenvíe. Los valores posibles para este campo son “none” (indica que el datagrama no se reenviará), “router” (indica que el datagrama se debe recibir sobre una conexión punto a punto), “transit network,” “stub network,” y “external” (indican que se espera recibir el datagrama de otro Sistema autónomo). |
| Downstream | Muestra una línea para cada interfaz o direccionador contiguo al que se enviará el datagrama. También se muestra un valor TTL, que indica que los datagramas enviados por esta interfaz o recibidos en la misma deben tener al menos el valor TTL especificado en su cabecera IP. Cuando el direccionador es miembro de un grupo de difusión múltiple, aparece la línea “internal Application” como uno de los direccionadores contiguos/interfaces directos. |

## Mgroups

Utilice el mandato **mgroups** para visualizar la pertenencia a grupos de las interfaces conectadas al direccionador. Sólo se muestra una pertenencia a grupo para las interfaces en las que el direccionador es el direccionador designado o el direccionador designado de reserva.

**Sintaxis:**

mg**roups**

**Ejemplo:** **`mgroups`**

```
                Local Group Database
 Group              Interface                Lifetime (secs)

224.0.1.1         128.185.184.11 (Eth/1)       176
224.0.1.2         128.185.184.11 (Eth/1)       170
224.1.1.1         Internal                     1
```

Group — Muestra la dirección del grupo tal como se notifica (mediante IGMP) a una determinada interfaz.

Interface — Muestra la dirección de la interfaz a la que se ha notificado la dirección del grupo (mediante IGMP).

La pertenencia a un grupo interno del direccionador se indica mediante el valor “internal.” Para estas entradas, el campo Lifetime (consulte la explicación siguiente) indica el número de aplicaciones que han solicitado la pertenencia a un determinado grupo.

Lifetime — Muestra el número de segundos que la entrada permanece si se dejan de escuchar informes de pertenencia a grupo en la interfaz correspondiente al grupo especificado.

## Mstats

Utilice el mandato **mstats** para visualizar distintas estadísticas de direccionamiento de difusión múltiple. El mandato indica si el direccionamiento de difusión múltiple está activado y si el direccionador es un distribuidor entre áreas o un distribuidor de difusión general entre AS.

**Sintaxis:**

ms**tats**

**Ejemplo:** **`mstats`**

```
                MOSPF forwarding:       Enabled
                Inter-area forwarding:  Enabled
                DVMRP forwarding:       Disabled

Datagrams received:            2496  Datagrams (ext source):    0
Datagrams fwd (multicast):        0  Datagrams fwd (unicast):   0
Locally delivered:                0  No matching rcv interface: 0
Unreachable source:               3  Unallocated cache entries: 0
Off multicast tree:               0  Unexpected DL multicast:   0
Buffer alloc failure:             0  TTL scoping:               0

# DVMRP routing entries:          0  # DVMRP entries freed:     0
# fwd cache alloc:                1  # fwd cache freed:         0
# fwd cache GC:                   0  # local group DB alloc:    0
# local group DB free:            1
```

| | |
|---|---|
| MOSPF forwarding | Muestra si el direccionador reenviará datagramas de difusión múltiple IP. |
| Inter-area forwarding | Muestra si el direccionador reenviará datagramas de difusión múltiple IP entre áreas. |
| DVMRP forwarding | Muestra si el direccionador está configurado para utilizar DVMRP para el direccionamiento de difusión múltiple. |
| Datagrams received | Muestra el número de datagramas de difusión múltiple recibidos por el direccionador (los datagramas cuyos grupos de destino están en el rango 224.0.0.1 - 224.0.0.255 no se incluyen en este total). |
| Datagrams (ext source) | Muestra el número de datagramas recibidos cuyos orígenes están fuera del AS. |
| Datagrams fwd (multicast) | Muestra el número de datagramas que se han reenviado como difusiones múltiples de enlace de datos (esto incluye duplicaciones de paquetes, si es necesario, de modo que este número 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. |
| No matching rcv interface | Muestra el número de datagramas recibidos por un distribuidor de difusión múltiple que no es interno del AS en una interfaz que no es MOSPF. |
| Unreachable source | Muestra el número de datagramas cuyas direcciones de origen no se han podido alcanzar. |
| Unallocated cache entries | Muestra el número de datagramas cuyas entradas de antememoria no se han podido crear por falta de recursos. |
| Off multicast tree | Muestra el número de datagramas que no se han reenviado porque no había direccionador contiguo de procedencia o no había direccionadores contiguos/interfaces directos en la entrada de antememoria coincidente. |
| Unexpected DL multicast | Muestra el número de datagramas recibidos como difusiones múltiples de enlace de datos en interfaces que se han configurado para la difusión individual de enlace de datos. |
| Buffer alloc failure | Muestra el número de datagramas que no se han podido duplicar por falta de almacenamiento intermedio. |
| TTL scoping | Indica los datagramas que no se han podido reenviar porque su TTL indicaba que nunca podrían alcanzar un miembro del grupo. |
| DVMRP routing entries | Muestra el número de entradas de direccionamiento DVMRP |
| DVMRP entries freed | Indica el número de entradas DVMRP que se han liberado. El tamaño será el número de entradas de direccionamiento menos el número de entradas liberadas. |
| # fwd cache alloc | Indica el número de entradas de antememoria asignadas. El tamaño actual de la antememoria de reenvío es el número de entradas asignadas (“# fwd cache alloc”) menos el número de entradas de antememoria liberadas (“# fwd cache freed”). |
| # fwd cache freed | Indica el número de entradas de antememoria liberadas. El tamaño actual de la antememoria de reenvío es el número de entradas asignadas (“# fwd cache alloc”) menos el número de entradas de antememoria liberadas (“# fwd cache freed”). |

| | |
|---|---|
| # fwd cache GC | Indica el número de entradas de antememoria que se han borrado porque no se habían utilizado recientemente y la antememoria se había desbordado. |
| # local group DB alloc | Indica el número de entradas asignadas de la base de datos de grupo local. El número asignado ("# local group DB alloc") menos el número liberado ("# local group DB free") es igual al tamaño actual de la base de datos de grupo local. |
| # local group DB free | Indica el número de entradas liberadas de la base de datos de grupo local. El número asignado ("# local group DB alloc") menos el número liberado ("# local group DB free") es igual al tamaño actual de la base de datos de grupo local. |

El número de aciertos de antememoria se puede calcular como el número de datagramas recibidos ("Datagrams received") menos el total de datagramas eliminados debido a "No matching rcv interface," "Unreachable source" y "Unallocated cache entries," y menos "# local group DB alloc." El número de errores de antememoria es simplemente "# local group DB alloc."

## Neighbor Summary

Utilice el mandato **neighbor summary** para visualizar estadísticas y parámetros relacionados con direccionadores contiguos OSPF. Si no se especifica ningún argumento (consulte el Ejemplo 1), aparece una sola línea que resume cada direccionador contiguo. Si se especifica la dirección IP de un direccionador contiguo (consulte el Ejemplo 2), se muestran estadísticas detalladas sobre dicha direccionador.

**Sintaxis:**

n**eighbor** *dirección-ip-direccionador-contiguo*

**Ejemplo 1:** `neighbor`

```
Neighbor addr   Neighbor ID     State  LSrxl  DBsum  LSreq  Ifc
128.185.125.39  128.185.136.39  128      0      0      0   PPP/1
128.185.125.41  128.185.128.41    8      0      0      0   PPP/1
128.185.125.38  128.185.125.38    8      0      0      0   PPP/1
128.185.125.25  128.185.129.25    8      0      0      0   PPP/1
128.185.125.40  128.185.129.40  128      0      0      0   PPP/1
128.185.125.24  128.185.126.24    8      0      0      0   PPP/1
```

| | |
|---|---|
| Neighbor addr | Muestra la dirección del direccionador contiguo. |
| Neighbor ID | Muestra el ID del direccionador contiguo OSPF. |
| Neighbor State | Puede ser uno de los siguientes valores: 1 (inactivo), 2 (intento), 4 (iniz), 8 (2 vías), 16 (ExStart), 32 (intercambio), 64 (cargando) o 128 (lleno). |
| LSrxl | Muestra el tamaño de la lista actual de retransmisiones de estado de enlace correspondiente a este direccionador contiguo. |
| DBsum | Muestra el tamaño de la lista de resumen de bases de datos en espera de ser enviada al direccionador contiguo. |
| LSreq | Muestra el número de los anuncios más recientes que se solicitan del direccionador contiguo. |
| Ifc | Muestra la interfaz compartida por el direccionador y el direccionador contiguo. |

**Ejemplo 2:** `neighbor 128.185.138.39`

El significado de la mayoría de los campos que se visualizan se explica en la sección 10 de la especificación OSPF (RFC 2178).

```
            Neighbor IP address:    128.185.184.34
            OSPF Router ID:         128.185.207.34
            Neighbor State:         128
            Physical interface:     Eth/1
            DR choice:              128.185.184.34
            Backup choice:          128.185.184.11
            DR Priority:            1
            Nbr options:            E,MC
            Alternate TOS 0 cost:   5

DB summ qlen:      0  LS rxmt qlen:      0  LS req qlen: 0
Last hello:        7  No Hello         Off

# LS rxmits:     108  # Direct acks:    13  # Dup LS rcvd: 572
# Old LS rcvd:     2  # Dup acks rcv:  111  # Nbr losses:   29
# Adj. resets:    30
```

| | |
|---|---|
| Neighbor IP addr | Dirección IP del direccionador contiguo. |
| OSPF router ID | ID del direccionador contiguo OSPF. |
| Neighbor State | Puede ser uno de los siguientes valores: 1 (inactivo), 2 (intento), 4 (iniz), 8 (2 vías), 16 (ExStart), 32 (intercambio), 64 (cargando) o 128 (lleno). |
| Physical interface | Muestra el tipo y número de la interfaz física de la red común del direccionador y el direccionador contiguo. |
| DR choice, backup choice, DR priority | Indica los valores visualizados en el último mensaje hello recibido del direccionador contiguo. |
| Nbr options | Indica las funciones OSPF opcionales a las que da soporte el direccionador contiguo. Estas funciones se indican con una E (procesa componentes externos de tipo 5; cuando no está definido, el área a la que pertenece la red común se ha configurado como un apéndice), T (puede direccionador según TOS) y MC (puede reenviar datagramas de difusión múltiple IP). Este campo sólo es válido para los direccionadores contiguos en estado de intercambio o superior. |
| Alternate TOS 0 cost | Para interfaces punto a multipunto, indica un coste 0 de TOS alternativo para este direccionador contiguo. En el LSA de tipo 1 (enlaces del direccionador) del direccionador, se anunciará este coste en lugar del coste 0 de TOS de la interfaz. |
| DBsumm qlen | Indica el número de anuncios en espera de ser resumidos en paquetes de Descripción de base de datos. Debe ser cero excepto si el direccionador contiguo está en estado de intercambio. |
| LS rxmt qlen | Indica el número de anuncios que se han enviado al direccionador contiguo, pero de los que aún no se ha recibido acuse de recibo. |
| LS req qlen | Indica el número de anuncios que se solicitan al direccionador contiguo en estado Cargando. |
| Last hello | Indica el número de segundos desde que se recibió un mensaje hello procedente del direccionador contiguo. |
| # LS rxmits | Indica el número de retransmisiones producidas durante el envío. |
| # direct acks | Indica respuestas a anuncios de estado de enlace duplicados. |
| # Dup LS rcvd | Indica el número de retransmisiones duplicadas producidas durante el envío. |
| # Old LS rcvd | Indica el número de anuncios antiguos recibidos durante el envío. |

| | |
|---|---|
| # Dup acks rcvd | Indica el número de acuses de recibo duplicados recibidos. |
| # Nbr losses | Indica el número de veces que el direccionador contiguo ha pasado al estado Inactivo. |
| # Adj. resets | Cuenta las entradas en estado ExStart. |

## Ping

Consulte el tema “Ping” en la página 350 para ver una explicación del mandato **Ping**.

## Policy

Utilice el mandato **policy** de OSPF para visualizar la política de importación de rutas límite AS de OSPF correspondiente al direccionador.

**Sintaxis:**

p**olicy**

**Ejemplo:**

```
  AS Boundary Importation Policy - ospf
Checksum 0x9A23  Longest-Match Application

IP Address      IP Mask           Match  Index  Type
-----------------------------------------------------
9.0.0.0         255.0.0.0         Range  1      Include
10.0.0.0        255.0.0.0         Range  2      Exclude
    Match Conditions:  Protocol: BGP
10.1.1.0        255.255.255.0     Range  4      Include
0.0.0.0         0.0.0.0           Range  0      Include
0.0.0.0         0.0.0.0           Range  3      Include
    Match Conditions:  Protocol: Static
                       Gateway IP Address Range: 153.2.2.20/255.255.255.255
0.0.0.0         0.0.0.0           Range  7      Include
    Policy Actions:    Set Manual Tag: 0xACEEACEE
0.0.0.0         0.0.0.0           Range  8      Include
    Match Conditions:  Protocol: RIP
    Policy Actions:    Set Metric: 999
```

## Reset

Utilice el mandato **reset** de OSPF para modificar de forma dinámica la configuración de direccionamiento de OSPF sin tener que volver a arrancar el direccionador. Para obtener más información, consulte el tema “Cambio dinámico de parámetros de configuración de OSPF” en la página 378.

**Nota:** Durante un rearranque, las rutas OSPF se retienen en la tabla de direccionamiento para mantener el reenvío IP.

**Sintaxis:**

re**set** ospf

**Ejemplo:**

```
OSPF>interface

Ifc Address      Phys    assoc. Area     Type    State   Auth   #nbrs  #adjs
153.2.2.25       Eth/0   0.0.0.1         Brdcst   16     None       3      2
10.69.1.1        FR/0    0.0.0.0         P-2-MP    8     None       1      1

OSPF>
*t 6

OSPF Config>delete interface 10.69.1.1
OSPF Config>
*t 5

OSPF>reset ospf
OSPF>interface

Ifc Address      Phys    assoc. Area     Type    State   Auth   #nbrs  #adjs
153.2.2.25       Eth/0   0.0.0.1         Brdcst   16     None       3      2
```

## Traceroute

Consulte el tema “Traceroute” en la página 355 para ver una explicación del mandato **Traceroute**.

## Routers

Utilice el mandato **routers** para visualizar todas las rutas del direccionador que ha calculado OSPF y que están actualmente en la tabla de direccionamiento. Con el mandato **dump routing tables**, el campo Net indica que el destino es una red. El mandato routers cubre todos los demás destinos.

**Sintaxis:**

**routers**

**Ejemplo:**

```
DType RType Destination       AREA          Cost   Next hop(s)

 ASBR  SPF   128.185.142.9    0.0.0.1         1   128.185.142.9
 Fadd  SPF   128.185.142.98   0.0.0.1         1    0.0.0.0
 Fadd  SPF   128.185.142.7    0.0.0.1         1    0.0.0.0
 Fadd  SPF   128.185.142.48   0.0.0.1         1    0.0.0.0
 Fadd  SPF   128.185.142.111  0.0.0.1         1    0.0.0.0
 Fadd  SPF   128.185.142.38   0.0.0.1         1    0.0.0.0
 Fadd  SPF   128.185.142.11   0.0.0.1         1    0.0.0.0
   BR  SPF   128.185.142.9    0.0.0.2         1   128.185.142.9
   BR  SPF   128.185.142.9    0.0.0.2         2   128.185.184.114
 Fadd  SPF   128.185.142.47   0.0.0.2         1    0.0.0.0
```

DType — Indica el tipo de destino:

- Net — indica que el destino es una red
- ASBR — indica que el destino es un direccionador límite AS
- ABR — indica que el destino es un direccionador límite de área
- Fadd — indica una dirección de reenvío (para rutas externas)

RType — indica el tipo de ruta y el modo en que se ha obtenido la ruta:

- SPF — indica que la ruta es una ruta interna del área (procede del cálculo Dijkstra)
- SPIA — indica que es una ruta entre áreas (procede de tener en cuenta los anuncios de estado de resumen).

| | |
|---|---|
| Destination | ID OSPF del direccionador de destino. Para entradas de Tipo D, se visualiza una de las direcciones IP del direccionador (que corresponde a una ruta de otro AS). |
| Area | Muestra el área AS a la que pertenece. |
| Cost | Muestra el coste de la ruta. |
| Next hop | Dirección del siguiente direccionador de la vía de acceso hacia el sistema principal de destino. Un número entre paréntesis al final de la columna indica el número de rutas de igual coste hacia el destino. |

## Size

Utilice el mandato **size** para visualizar el número de LSA que hay actualmente en la base de datos de estado de enlace, clasificados por tipo.

**Sintaxis:**

si**ze**

**Ejemplo:**

```
# Router-LSAs:            6
# Network-LSAs:           2
# Summary-LSAs:           45
# Summary Router-LSAs:    6
# AS External-LSAs:       2
# Group-membership-LSAs:  11

# Intra-area routes:      11
# Inter-area routes:      15
# Type 1 external routes: 0
# Type 2 external routes: 2
```

## Statistics

Utilice el mandato **statistics** para visualizar estadísticas generadas por el protocolo de direccionamiento OSPF. Las estadísticas indican cómo está funcionando la implantación, incluida la utilización de memoria y de red. Muchos de los campos visualizados son una confirmación de la configuración de OSPF.

**Sintaxis:**

st**atistics**

### Ejemplo:

```
OSPF Router ID:        17.17.17.17
                    External comparison:    Type 2
                    RFC 1583 compatibility: Yes
                    Multicast OSPF [MOSPF]: Yes [Inter-Area Multicast Forwarder]
                    Demand circuit support: Yes
                    Least Cost Area Ranges: No
                    AS boundary capability: Yes
                    Import external routes: POLICY ospf
                    Orig. default route:    No [0,0.0.0.0]
                    Default route cost:     [1, Type 2]
                    Default forward. addr:  0.0.0.0

      Attached areas:                   2  Estimated # external routes:    400
      Estimated # OSPF routers:       100  Estimated heap usage:        104000
      OSPF packets rcvd:            16971  OSPF packets rcvd w/ errs:    16269
      Transit nodes allocated:        286  Transit nodes freed:            283
      LS adv. allocated:             1439  LS adv. freed:                 1421
      Queue headers alloc:             32  Queue headers avail:             32
      Maximum LSA size:              2048

      # Dijkstra runs:                 12  Incremental summ. updates:        0
      Incremental VL updates:           0  Buffer alloc failures:           0
      Multicast pkts sent:          16982  Unicast pkts sent:              10
      LS adv. aged out:                 0  LS adv. flushed:                 5
      Ptrs To Invalid LS adv:           0  Incremental ext. updates:       29
      LSA Max Random Initial Age:       0  LSA MINARRIVAL rejects:          1

      External LSA database:
      Current state:               Normal
      Number of LSAs:                  11  Number of overflows:             0
```

| | |
|---|---|
| OSPF Router ID | Muestra el ID OSPF del direccionador. |
| External comparison | Muestra el tipo de ruta externa que utiliza el direccionador al importar rutas externas. |
| RFC 1583 compatibility | Indica si el cálculo de rutas externas AS de OSPF será o no compatible con RFC 1583. |
| Import external routes | Muestra qué rutas externas se importarán. Si se ha configurado una política de importación de filtros de rutas para el direccionamiento límite AS, se visualizará dicha política. |
| Orig default route | Muestra si el direccionador anunciará o no una ruta OSPF por omisión. Si el valor es “Yes” y aparece un número distinto de cero entre paréntesis, significa que se anunciará una ruta por omisión sólo cuando exista una ruta a la red. |
| Default route cost | Muestra el coste y el tipo de la ruta por omisión (si se anuncia). |
| Default forward addr | Muestra la dirección de reenvío especificada en la ruta por omisión (si se anuncia). |
| Attached areas | Indica el número de áreas con las que el direccionador tiene interfaces activas. |
| Estimated heap usage | Indicación estimada del tamaño de la base de datos de estado de enlace de OSPF (en bytes). |
| Transit nodes | Asignado para guardar enlaces del direccionador y anuncios de enlaces de red. |
| LS adv. | Asignado para guardar anuncios de enlaces de resumen y de enlaces externos al AS. |

| | |
|---|---|
| Queue headers | Forma listas de anuncios de estado de enlace. Estas listas se utilizan en los procesos de envío e intercambio de bases de datos; si el número de cabeceras de cola asignados no es igual al número liberado, significa que se está procesando una sincronización de bases de datos con algún direccionador contiguo. |
| # Dijkstra runs | Indica el número de veces que se ha calculado la tabla de direccionamiento de OSPF a partir de datos de trabajo. |
| Maximum LSA size | El LSA de tamaño máximo que puede originar este direccionador. Es el mínimo entre el valor configurado a través de la configuración de OSPF y el tamaño máximo de paquete calculado o configurado a través de la configuración general. |
| Incremental summ updates, incremental VL updates | Indican que nuevos anuncios de estado de resumen han hecho que se volviera a crear parcialmente la tabla de direccionamiento. |
| Buffer alloc failures. | Indica errores de asignación de almacenamiento intermedio. El sistema OSPF se recuperará de la falta temporal de almacenamientos intermedios de paquetes. |
| Multicast pkts sent | Cubre paquetes de mensajes hello de OSPF y paquetes enviados durante un procedimiento de envío. |
| Unicast pkts sent | Cubre retransmisiones de paquetes OSPF y el procedimiento de intercambio de bases de datos. |
| LS adv. aged out | Cuenta el número de anuncios que han alcanzado los 60 minutos. Los anuncios de estado de enlace caducan transcurridos 60 minutos. Generalmente se renuevan antes de que transcurra este periodo. |
| LS adv. flushed | Indica el número de anuncios eliminados (y no sustituidos) de la base de datos de estado de enlace. |
| Ptrs to Invalid LS adv | Muestra el número de anuncios de la base de datos que no se han formado correctamente y no se han podido interpretar. |
| Incremental ext. updates. | Muestra el número de cambios en destinos externos que se han instalado de forma incremental en la tabla de direccionamiento. |
| LSA Max Random Initial Age | Muestra el número de antigüedad máxima aleatoria inicial para LSA que se originan de forma automática. |
| LSA MINARRIVAL Rejects | Muestra el número de LSA rechazados porque se ha recibido una instancia nueva en un intervalo inferior a MINARRIVAL (1 segundo). |
| External LSA database: | Ofrece información sobre la base de datos LSA:<br>Current state<br>Si la base de datos de LSA actuales externos al AS está en estado normal o de carga excesiva.<br>Number of LSA<br>El número de LSA externos que se encuentran actualmente en la base de datos<br>Number of overflows<br>El número de veces que la base de datos de LSA AS ha entrado en estado de carga excesiva. |

## Weight

Utilice el mandato **weight** para modificar el coste de una de las interfaces OSPF del direccionador. Este nuevo coste se envía de forma inmediata a través del dominio de direccionamiento OSPF, lo que hace que las rutas se actualicen en consecuencia.

El coste de la interfaz pasa a ser su coste configurado cuando se vuelve a arrancar o a cargar el direccionador. Para realizar un cambio permanente en el coste, debe volver a configurar la interfaz OSPF adecuada después de invocar el mandato weight. Este mandato hará que se origine un nuevo anuncio de enlaces del direccionador, a no ser que no se modifique el coste de la interfaz.

**Sintaxis:**

w**eight** *dirección-interfaz-ip nuevo-coste*

**Ejemplo:** `weight 128.185.124.22 2`

# Utilización de BGP4

Este capítulo describe cómo utilizar el Protocolo de pasarela límite (BGP) mediante los mandatos de configuración de BGP.

Este capítulo contiene la siguientes secciones:



## Visión general del Protocolo de pasarela límite

BGP es un protocolo de direccionamiento de pasarela exterior que sirve para intercambiar información sobre la posibilidad de alcanzar la red entre sistemas autónomos. Un AS es básicamente un grupo de direccionadores y nodos finales que funcionan bajo una sola organización administrativa. Dentro de cada AS, los direccionadores y los nodos finales intercambian información de direccionamiento mediante un protocolo de pasarela interior. El protocolo de pasarela interior puede ser RIP u OSPF.

BGP se incorporó en Internet en el intercambio libre de bucles de información de direccionamiento entre sistemas autónomos. Basado en el Direccionamiento entre dominios sin clase (CIDR), BGP ha evolucionado para dar soporte a la adición y reducción de información de direccionamiento.

Básicamente, CIDR es una estrategia diseñada para solucionar los siguientes problemas:

- Falta de espacio de direcciones de Clase B
- Crecimiento de la tabla de direccionamiento

CIDR elimina el concepto de clases de direcciones y ofrece un método para resumir *n* rutas diferentes en una sola ruta. Esto reduce significativamente la cantidad de información de direccionamiento que deben guardar e intercambiar los direccionadores BGP.

**Nota:** IBM sólo da soporte a la última versión de BGP, BGP4, que está definida en RFC 1654. Todas las referencias que se hacen a BGP en este capítulo y en la interfaz de direccionadores de IBM' son a BGP4, y no se aplican a versiones anteriores de BGP.

## Cómo funciona BGP4

BGP es un protocolo de direccionamiento entre sistemas autónomos. Básicamente, los direccionadores BGP recopilan de forma selectiva y anuncian información sobre la posibilidad de alcanzar direccionadores contiguos BGP de su propio sistema autónomo o de otros sistemas autónomos. La información sobre posibilidad de alcance consta de las secuencias de números de AS que forman las vías de acceso a determinados altavoces BGP y la lista de redes IP que se pueden alcanzar a través de cada vía de acceso anunciada. Un AS es un grupo administrativo de redes y direccionadores que comparten información sobre posi-

bilidad de alcance mediante uno o más Protocolos de pasarela interior (IGP), como RIP u OSPF.

Los direccionadores que ejecutan BGP se denominan altavoces BGP. Estos direccionadores funcionan como servidores con respecto a sus direccionadores contiguos BGP (clientes). Cada direccionador BGP abre una conexión TCP pasiva en el puerto 179 y escucha las conexiones entrantes procedentes de direccionadores contiguos de esta dirección conocida. El direccionador también abre conexiones TCP activas con direccionadores contiguos BGP activados. Esta conexión TCP permite a los direccionadores BGP compartir y actualizar información sobre posibilidad de alcance con direccionadores contiguos del mismo o de otros sistemas autónomos.

Las conexiones entre altavoces BGP del mismo AS se denominan conexiones BGP internas (IBGP), mientras que las conexiones entre altavoces BGP de distintos sistemas autónomos se denominan conexiones BGP externas (EBGP).

Un solo AS puede tener una o muchas conexiones BGP con sistemas autónomos externos. La Figura 36 muestra dos sistemas autónomos. El altavoz BGP que está en AS1 intenta establecer una conexión TCP con su direccionador contiguos de AS2. Una vez establecida la conexión, los direccionadores podrán compartir información sobre posibilidad de alcance.

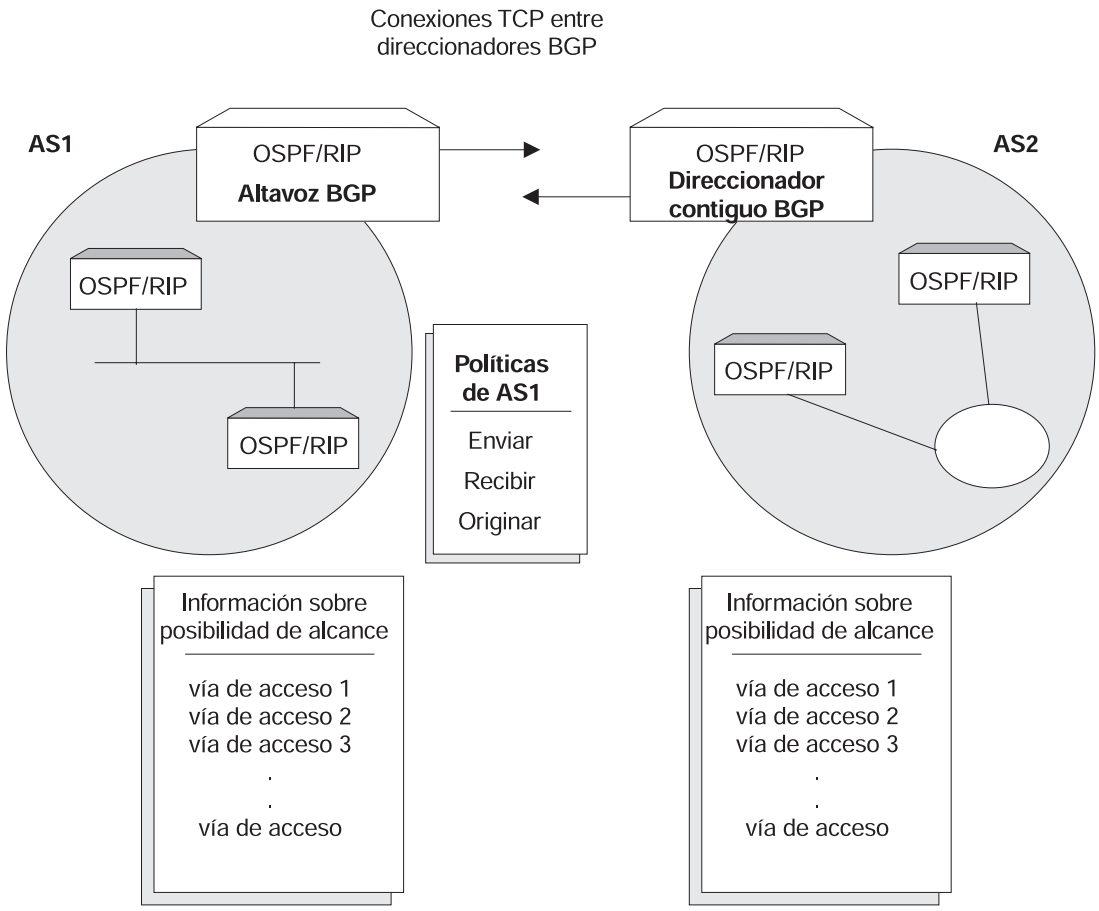



*Figura 36. Conexiones BGP entre dos sistemas autónomos. Cuando el altavoz BGP de AS1 establece una conexión TCP con su direccionador contiguo BGP de AS2, los dos direccionadores pueden intercambiar de forma selectiva información sobre posibilidad de alcance. La información que cada direccionador envía o acepta se determina mediante políticas definidas para cada direccionador.*

Aunque los sistemas autónomos de la Figura 36 sólo tienen un direccionador, cada uno puede tener varias conexiones con otros sistemas autónomos. Un ejemplo de este caso, la Figura 37 en la página 429, muestra tres sistemas autónomos interconectados. AS1 tiene tres conexiones BGP con sistemas autónomos externos: una con AS2, una con AS3 y una con ASx. Paralelamente, AS3 tiene conexiones con AS1, con AS2 y con ASy.

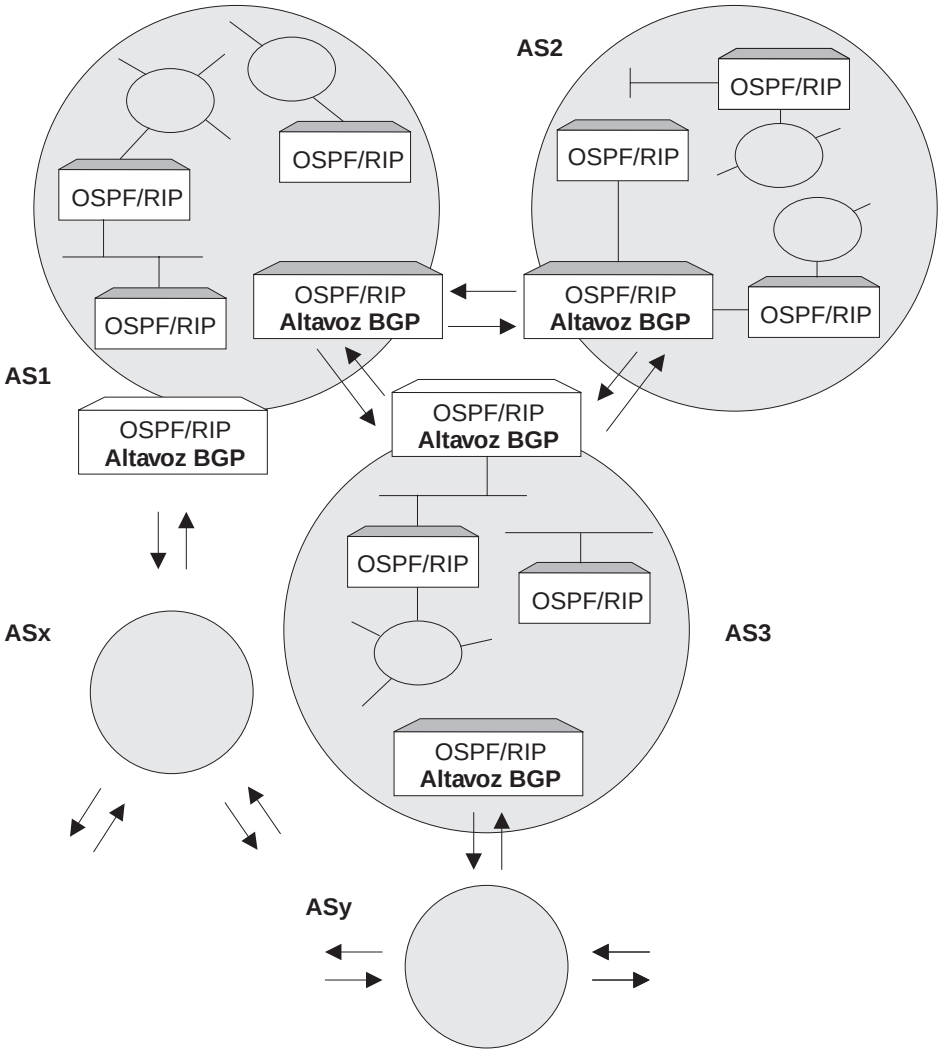



*Figura 37. Conexiones BGP entre tres sistemas autónomos. Observe que AS1 y AS3 tienen dos altavoces BGP.*

Una vez establecida una conexión TCP, el altavoz BGP que aparece en la Figura 36 en la página 428 puede enviar su tabla de direccionamiento completa a su direccionador contiguo BGP de AS2. Sin embargo, por seguridad o por otros motivos, puede no ser aconsejable enviar información sobre posibilidad de alcance en cada red a AS2. Paralelamente, puede no ser aconsejable que AS2 reciba información sobre posibilidad de alcance en cada red de AS1.

## Políticas de origen, envío y recepción

Las decisiones sobre qué información sobre posibilidad de alcance se debe anunciar (enviar) y qué información se debe aceptar (recibir) se toman según instrucciones de políticas definidas de forma explícita. La implantación BGP de IBM da soporte a tres tipos de instrucciones de políticas:

- Políticas de origen
- Políticas de envío - hay dos tipos de políticas de envío
  - Las políticas de envío basadas en AS se aplican únicamente a un determinado AS o a todos los AS. Si no hay ninguna política de envío configurada, la dirección de destino se elimina.
  - Las políticas de envío basadas en direccionadores contiguos se aplican sólo a un determinado direccionador o direccionadores contiguos. Si no hay ninguna política de envío basada en direccionadores contiguos configurada para un determinado direccionador contiguo, se aplican las políticas de envío basadas en AS. Si hay una política de envío basada en direccionadores contiguos configurada, la política de envío basada en AS se ignora.

  Cada instrucción de política de envío contiene el clasificador de anuncios de redes de destino y un grupo de acciones asociadas.

  La clasificación de redes de destino se basa en:

  - Red de destino exacta
  - Rango de redes de destino
  - Número de AS emisores de anuncios
  - Cualquier número de AS encontrado en el atributo de vía de acceso de AS

  Las acciones posibles son:

  - Excluir la red de destino de los anuncios
  - Incluir la red de destino en los anuncios a un determinado AS o a todos los AS (mediante la política basada en AS) o a un determinado direccionador contiguo (mediante la política basada en direccionadores contiguos)
  - Definir el valor MED
  - Relleno de vías de acceso AS

  **Nota:** MED y relleno de vías de acceso AS sólo se aplican a una política basada en direccionadores contiguos.

  El valor del atributo MED aconseja al direccionador contiguo BGP externo sobre su preferencia de ruta. Se preferirá la ruta que tenga el valor del atributo MED menor. Consulte el tema “Proceso de preferencia de rutas” en la página 437 para obtener más información.
- El relleno de vías de acceso AS le permite añadir un número de AS local adicional varias veces (1 a 10) a la vía de acceso AS de la ruta BGP. Se preferirá la ruta con el valor de vía de acceso AS menor. Consulte el tema “Proceso de preferencia de rutas” en la página 437 para obtener más información.
- Políticas de recepción - hay dos tipos de políticas de recepción.

- Las políticas de recepción basadas en AS se aplican únicamente a un determinado AS o a todos los AS. Si no hay ninguna política de recepción configurada, la dirección de destino se elimina.
- Las políticas de recepción basadas en direccionadores contiguos se aplican sólo a un determinado direccionador o direccionadores contiguos. Si no hay ninguna política de recepción basada en direccionadores contiguos configurada para un determinado direccionador contiguo, se aplican las políticas de recepción basadas en AS. Si hay políticas de recepción basadas en direccionadores contiguos configuradas, las políticas de recepción basadas en AS se pasan por alto.

Cada instrucción de política de recepción contiene el clasificador de anuncios de redes de destino y un grupo de acciones asociadas.

La clasificación de redes de destino se basa en:

- Red de destino exacta
- Rango de redes de destino
- Número de AS emisores de anuncios
- Cualquier número de AS encontrado en el atributo de vía de acceso de AS

Las acciones posibles son:

- Excluir la red de destino
- Incluir la red de destino procedente de un determinado AS o de todos los AS (mediante la política basada en AS) o de un determinado direccionador contiguo (mediante la política basada en direccionadores contiguos)
- Restablecer el valor MED
- Definir el valor de ponderación
- Definir el valor de métrica de IGP
- Definir un valor de preferencias local.

**Nota:** MED, ponderación y preferencias locales sólo se aplican a una política basada en direccionadores contiguos.

El valor de ponderación aconseja al direccionador BGP local que seleccione la ruta basada en el valor de ponderación más alto y pasa por alto el algoritmo de preferencia de rutas.

## Mensajes de BGP

Los direccionadores utilizan cuatro tipos de mensajes para comunicarse con sus direccionadores contiguos: mensajes OPEN, KEEP ALIVE, UPDATE y NOTIFICATION.

### OPEN

Los mensajes open son los primeros mensajes que se transmiten cuando se activa un enlace con un direccionador contiguo BGP y establece una conexión.

### KEEP ALIVE

Los direccionadores BGP utilizan los mensajes keep alive para notificarse entre sí que una determinada conexión está activa y en funcionamiento.

### UPDATE

Los mensajes update contienen la información de la tabla de direccionamiento interior. Los altavoces BGP sólo envían mensajes update cuando hay un cambio en sus tablas de direccionamiento.

### NOTIFICATION

Se envían mensajes notification siempre que un altavoz BGP detecta una condición que le fuerza a terminar una conexión existente. Estos mensajes se anuncian antes de que se transmita la conexión.

## Configuración de BGP4

Para configurar BGP hay que seguir tres pasos básicos:

1. "Activación de BGP".

   Para activar BGP debe especificar el número de AS exclusivo del direccionador BGP. Los números de AS los asigna el Stanford Research Institute Network Information Center.

2. "Cómo definir direccionadores contiguos BGP" en la página 433.

   Los *direccionadores contiguos BGP* son direccionadores BGP con los que un altavoz BGP establece una conexión TCP. Una vez definidos los direccionadores contiguos, por omisión se establecen conexiones con los mismos.

3. "Cómo añadir políticas" en la página 433.

   Las *políticas* que establece el usuario determinan qué rutas importará y exportará el altavoz BGP. Puede definir políticas para distintos objetivos. Consulte el tema "Ejemplos de definiciones de políticas" en la página 433 para obtener más información.

## Activación de BGP

Para activar BGP, utilice el mandato **enable BGP speaker**, tal como se muestra.

```
BGP Config> enable BGP speaker
AS [0]? 167
TCP segment size [1024]?
```

El *número de AS* debe estar comprendido entre 1 y 65535. *TCP segment* debe estar comprendido entre 1 y 65535. El valor por omisión de *TCP segment* es 1024. Este número representa el tamaño máximo de segmento que utilizará BGP para las conexiones TCP pasivas.

Después de emitir el mandato **enable bgp**, debe volver a arrancar el dispositivo para activar BGP.

## Cómo definir direccionadores contiguos BGP

Después de activar un altavoz BGP, debe definir sus direccionadores contiguos. Los direccionadores contiguos BGP pueden ser internos o externos. Los direccionadores contiguos internos se encuentran en el mismo AS no necesitan tener una conexión directa entre sí. Los direccionadores contiguos externos se encuentran en distintos sistemas autónomos. Deben tener una conexión directa entre sí.

Para definir direccionadores contiguos BGP internos o externos, utilice el mandato **add neighbor**. Debe especificar la dirección IP del direccionador contiguo y asignar un número de AS al direccionador contiguo, tal como se muestra a continuación. Los direccionadores internos deben tener el mismo número de AS que el altavoz BGP.

```
BGP Config> add neighbor 192.0.190.178
AS [0]? 178
Init timer [12]? 30
Connect timer [120]?
Hold timer [90]? 30
TCP segment size [1024]? 512
```

Utilice el mandato **reset neighbor** para activar el direccionador contiguo BGP especificado, según los parámetros de configuración de direccionadores contiguos guardados en la memoria de configuración.

## Cómo añadir políticas

La implantación BGP de IBM da soporte a tres mandatos de políticas:

- *Originate Policy*. Le permite seleccionar las redes del protocolo de pasarela interior (IGP) a exportar.
- *Receive Policy*. Le permite seleccionar la información de rutas a importar de similares BGP.
- *Send Policy*. Le permite seleccionar la información de rutas a exportar a similares BGP. Tenga en cuenta que la información de rutas que se puede exportar puede incluir información recopilada de sistemas autónomos de direccionadores contiguos, así como las rutas que se originan en el IGP.

Si ha añadido o modificado una política basada en direccionadores contiguos, utilice el mandato **reset neighbor** para activar la política de direccionadores contiguos. Si ha añadido o modificado una política basada en AS, debe volver a arrancar el dispositivo.

## Ejemplos de definiciones de políticas

Esta sección contiene una serie de ejemplos de algunas políticas específicas que puede configurar para un altavoz BGP. Todas las políticas se definan mediante el mandato **add** de BGP. Consulte el tema “Add” en la página 440 para ver la sintaxis del mandato **add**.

# Ejemplos de políticas de origen

### Incluir todas las rutas para anunciarlas

Este ejemplo incluye todas las rutas en la tabla de direccionamiento IGP del altavoz BGP para anunciarlas. En este sentido, puede ver este mandato como la instrucción de política de origen “por omisión” correspondiente a BGP.

Observe que el mandato especifica un rango de direcciones, en lugar de una sola dirección (exacta).

```
BGP Config> add originate-policy inclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Exact]? range
Tag [0]?
```

### Excluir un rango de rutas

Este ejemplo también especifica un rango, pero en este caso el objetivo es evitar que el altavoz BGP anuncie direcciones incluidas en este rango a los direccionadores contiguos.

Este ejemplo excluye todas las rutas del rango comprendido entre 194.10.16.0 y 194.10.31.255 de la tabla de direccionamiento IGP, que evita que se anuncien.

```
BGP Config> add originate-policy exclusive
Network Prefix [0.0.0.0]? 194.10.16.0
Network Mask [0.0.0.0]? 255.255.240.0
Address Match (Exact/Range) [Exact]? range
Tag [0]?
```

El identificador (tag) es la información RIP recibida. Puede seleccionar redes en función de un determinado valor de identificador para anunciarlas. Consulte la descripción del mandato **Set** en el tema “Configuración y supervisión de IP” en la página 273 para obtener información sobre cómo definir el valor del identificador.

### Incluir todas las rutas sin clase para anunciarlas

Por omisión, sólo las rutas con clase de la tabla de direccionamiento IGP del altavoz BGP se seleccionarán para ser anunciadas. Para seleccionar las rutas con y sin clase para el anuncio de subred, utilice el mandato **enable classless-bgp** o el mandato **patch bgp-subnets**.

# Ejemplos de políticas de recepción basadas en AS

### Importar todas las rutas de todos los direccionadores contiguos BGP

Este ejemplo asegura que el altavoz BGP importará todas las rutas de todos sus direccionadores contiguos en su tabla de direccionamiento IGP.

```
BGP Config> add receive-policy inclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Exact]? range
Originating AS# [0]?
Adjacent AS# [0]?
IGP-metric [0]?
```

*IGP-metric* especifica el valor de métrica con el que las rutas aceptadas se importan en la tabla de direccionamiento IGP del altavoz. Sólo se le solicitará que

especifique un valor para IGP-metric cuando defina una política para la inclusión de rutas.

Si *IGP-metric* es -1, estas rutas no se importarán en IGP; por lo tanto, las rutas no se pueden volver a anunciar.

### Bloqueo de determinadas rutas procedentes de un AS emisor

Este ejemplo evitará que el altavoz BGP importe las rutas originadas en el AS 168 en el direccionador contiguo AS 165. Puede utilizar este mandato si no desea que el altavoz BGP reciba rutas procedentes del AS 168 por motivos de seguridad.

```
BGP Config> add receive-policy exclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Exact]? range
Originating AS# [0]? 168
Adjacent AS# [0]? 165
```

### Bloqueo de una vía de acceso AS específica

Este ejemplo evitará que el altavoz BGP importe rutas que tengan AS 175 en su lista de vías de acceso AS.

```
BGP Config> add no-receive
Enter AS: [0]? 175
```

## Ejemplos de políticas de recepción basadas en direccionadores contiguos

### Importar todas las rutas de un determinado direccionador contiguo BGP, definir weight = 100

Este ejemplo le permitirá importar todas las rutas procedentes del direccionador contiguo BGP 192.0.190.178. Todas las rutas tendrán un valor de ponderación (weight) igual a 100 y un valor de IGP-metric igual a 1.

Defina el nombre de la lista de políticas correspondiente a la política de recepción.

```
BGP Config> add policy-list
Name[]?S1_100_r
Policy Type(Receive/Send)[Receive]?Receive
```

Conecte el nombre definido de la lista de políticas de recepción con un determinado direccionador contiguo.

```
BGP Config> attach policy-to-neighbor
Neighbor address [0.0.0.0]?192.0.190.178
First receive policy list name (none for global AS based policy)[]?S1_100_r
Second receive policy list name (none for exit)[]?
```

Añada políticas de recepción correspondientes al direccionador contiguo mediante el mandato **update** y el mandato **add**.

```
BGP Config>update policy S1_100_r
Policy-list S1_100_r Config>add
Policy type (Inclusive/Exclusive) [Exclusive]? inclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
MED [0]?
Weight [0]? 100
Local-Pref [0]?
IGP-metric [0]? 1
```

# Ejemplos de políticas de envío basadas en AS

## Restringir el anuncio de rutas a un determinado AS

Este ejemplo restringe el altavoz BGP. El altavoz no puede anunciar rutas en el rango de direcciones comprendido entre 143.116.0.0 y 143.116.255.255, que se originan en el AS 165, al sistema autónomo 168.

```
BGP Config> add send exclusive
Network Prefix [0.0.0.0]? 143.116.0.0
Network Mask [0.0.0.0]? 255.255.0.0
Address Match (Exact/Range) [Exact]? range
Tag [0]? 165
Adjacent AS# [0]? 168
```

## Anunciar todas las rutas conocidas

Este ejemplo asegura que el altavoz BGP anunciará todas las rutas originadas en su IGP y todas las rutas aprendidas a partir de sus sistemas autónomos contiguos.

```
BGP Config> add send policy inclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Exact]? range
Tag [0]?
Adjacent AS# [0]?
```

# Ejemplos de políticas de envío basadas en direccionadores contiguos

## Anunciar todas las rutas conocidas a un determinado direccionador contiguo con el valor del atributo MED = 100

Este ejemplo le permitirá anunciar todas las rutas al direccionador contiguo BGP 192.0.190.178. Todas las rutas anunciadas tendrán un valor de MED igual a 100.

Defina el nombre de la lista de políticas correspondiente a la política de envío.

```
BGP Config> add policy-list
Name[]?S1_100_s
Policy Type(Receive/Send)[Receive]?Send
```

Conecte el nombre o nombres definidos de listas de políticas de envío a un determinado direccionador contiguo.

```
BGP Config> attach policy-to-neighbor
Neighbor address [0.0.0.0]?192.0.190.178
First send policy list name (none for global AS based policy)[]?S1_100_s
Second send policy list name (none for exit)[]?
```

Añada las políticas de envío correspondientes al direccionador contiguo mediante los mandatos **update** y **add**.

```
BGP Config>update policy S1_100_s
Policy-list S1_100_s Config>add
Policy type (Inclusive/Exclusive) [Exclusive]?
Network prefix [0.0.0.0]?
Network mask [0.0.0.0]?
Address match (exact/range) [range]?
Originating AS# [0]?
TAG [0]?
MED [0]? 100
# of AS to pad [0]?
```

## Proceso de preferencia de rutas

Cuando el altavoz BGP recibe una vía de acceso a un determinado destino a partir de su similar, BGP pasa por el proceso de seleccionar la mejor vía de acceso posible:

- Aplica políticas de recepción basadas en la configuración.
- Si las políticas de recepción permiten un destino, calcula el Grado de preferencia correspondiente al destino recibido, basado en la longitud más corta de la vía de acceso AS y en el tipo de origen.
- Si hay varias vías de acceso al mismo destino, ejecuta el proceso de selección de vía de acceso. Selecciona la mejor vía de acceso posible comparando la nueva vía de acceso con la mejor vía de acceso seleccionada existente. Si la nueva vía de acceso se selecciona como la mejor vía de acceso, instala la nueva vía de acceso en la tabla de direccionamiento IP.
- BGP anuncia la mejor vía de acceso seleccionada a sus similares BGP externo e interno, según las políticas de envío.

## Proceso de selección de vía de acceso

La mejor vía de acceso se selecciona según el siguiente orden:

- Se prefiere la vía de acceso originada por este direccionador.
- Si este direccionador no ha originado ninguna vía de acceso, se prefiere la vía de acceso que tiene el valor de ponderación (Weight) configurado más alto.
- Si hay varias vías de acceso con el mismo valor de ponderación, se prefiere la vía de acceso que tenga el valor configurado de preferencia local (local-preference) más alto.
- Si hay varias vías de acceso con el mismo valor de preferencia local, se prefiere la vía de acceso que tenga el Grado de preferencia más alto.
  - La vía de acceso que tenga la longitud de vía de acceso AS más corta tiene el grado de preferencia más alto.
  - Si varias vías de acceso tienen la misma longitud de vía de acceso AS, se prefiere el IGP de tipo de origen sobre EGP e incompleto.
- Si hay varias vías de acceso con el mismo Grado de preferencia, se prefiere la vía de acceso que tenga el valor del atributo MED más bajo.
- Si hay varias vías de acceso con el mismo valor de atributo MED, se prefiere la ruta externa (EBGP) sobre la ruta interna (IBGP).
- Si continúa habiendo vías de acceso con los mismos valores, se prefiere la vía de acceso con el ID de BGP más bajo.

# Configuración y supervisión de BGP4

Este capítulo describe los mandatos de configuración y de supervisión de BGP e incluye las siguientes secciones:



## Cómo acceder al entorno de configuración de BGP4

Para acceder al entorno de configuración de BGP, entre el siguiente mandato en el indicador `Config>`:

```
Config> Protocol BGP
BGP Config>
```

## Mandatos de configuración de BGP4

Esta sección describe los mandatos de configuración de BGP. Estos mandatos le permiten modificar el comportamiento del protocolo BGP para que se ajuste a sus necesidades. Algunas de las tareas de configuración son obligatorias para que el direccionador BGP funcione por completo. Entre los mandatos de configuración de BGP en el indicador `BGP config>`.

*Tabla 25. Resumen de mandatos de configuración de BGP*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxxi. |
| Add | Añade políticas y direccionadores contiguos BGP. |
| Attach | Conecta una lista de políticas de recepción y envío a un determinado direccionador contiguo. |
| Change | Modifica información que se entró originalmente con el mandato **add**. |
| Delete | Suprime información de configuración de BGP entrada con el mandato **add**. |
| Disable | Desactiva determinadas características de BGP que se han activado mediante el mandato **enable**. |
| Enable | Activa altavoces BGP, direccionadores contiguos BGP o GBP sin clase. |
| List | Muestra elementos de configuración de BGP. |
| Move | Cambia el orden en que se han definido las políticas y agregados. |
| Set | Define el temporizador de exploración de la tabla de rutas IP. |
| Update | Manipula una política de un nombre de lista de políticas configuradas mediante los mandatos **add**, **delete**, **change** y **move** de submenú. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxii. |

## Add

Utilice el mandato **add** para añadir información de BGP a la configuración.

**Sintaxis**:

add
- aggregate . . .
- neighbor . . .
- no-receive asnum . . .
- originate-policy . . .
- policy-list . . .
- receive-policy . . .
- send-policy. . .

**aggregate** *prefijo red máscara red*

El mandato **add aggregate** hace que el altavoz BGP añada un bloque de direcciones y anuncie una sola ruta a sus direccionadores contiguos

BGP. Debe especificar el prefijo de red común a todas las rutas que se añaden y su máscara. El siguiente ejemplo ilustra cómo añadir un bloque de direcciones comprendidas entre la 194.10.16.0 y la 194.10.31.255.

1. *Network Prefix* es la dirección que se verá afectada. El prefijo es la primera dirección de un rango de direcciones especificado en una política BGP.

   **Valores válidos**: Cualquier dirección IP válida.
   **Valor por omisión**: ninguno

2. *Network Mask* se aplica a la dirección especificada en el prefijo de red para generar una dirección utilizada en una política BGP.

   **Valores válidos**: Cualquier dirección IP válida.
   **Valor por omisión**: ninguno

**Ejemplo:** **`add aggregate`**

```
Network Prefix [0.0.0.0]? 194.10.16.0
Network Mask [0.0.0.0]? 255.255.240.0
```

Al añadir una definición de agregado, recuerde definir una política para bloquear las rutas agregadas para que no se exporten. Si no lo hace, el direccionador anunciará tanto las rutas individuales como el agregado definido. Esto no se aplica cuando está añadiendo rutas, que se originan a partir de su tabla de direccionamiento IGP.

**neighbor** *dirección IP direccionador contiguo  núm. as temporizador inic  temporizador conexión  temporizador retención temporizador keep alive tamaño segmento tcp*

Utilice el mandato **add neighbor** para definir un direccionador contiguo BGP. El direccionador contiguo puede ser interno al AS del altavoz BGP o externo. Para activar este direccionador contiguo de forma dinámica, utilice el mandato **reset neighbor** desde el indicador de supervisión de BGP.

1. La dirección IP es la dirección del direccionador contiguo con el que desea establecer una conexión similar. Puede estar dentro de su propio sistema autónomo o en otro sistema autónomo. Si es un direccionador contiguo externo, ambos altavoces BGP deben compartir la misma red. Esta restricción no se aplica a los direccionadores contiguos internos. La dirección tiene:

   **Valores válidos**: Cualquier dirección IP válida.
   **Valor por omisión**: ninguno

2. El número de AS es el número de su propio sistema autónomo para el direccionador contiguo interno o el número del sistema autónomo del direccionador contiguo. El número de AS del direccionador contiguo tiene:

   **Valores válidos**: Un entero comprendido entre 0 y 65535
   **Valor por omisión**: ninguno

3. El temporizador de inicialización (*Init timer*) especifica el intervalo de tiempo que el altavoz BGP espera para inicializar recursos y volver a inicializar una conexión de transporte con el direccionador contiguo en el caso de que el altavoz haya pasado anteriormente al

estado IDLE debido a un error. Si el error persiste, este temporizador crece exponencialmente.

**Valores válidos**: 0 a 65535 segundos.
**Valor por omisión**: 12 segundos

4. El temporizador de conexión (*Connect timer*) especifica el intervalo de tiempo que espera el altavoz BGP para volver a iniciar una conexión de transporte con su direccionador contiguo, si la conexión TCP falla mientras está en estado CONNECT o ACTIVE. Mientras tanto, el altavoz BGP continúa escuchando para ver si su direccionador contiguo inicia alguna conexión.

   **Valores válidos**: 0 a 65535 segundos.
   **Valor por omisión**: 120 segundos

5. Entre el temporizador de retención (*Hold timer*) para especificar el intervalo de tiempo que el altavoz BGP espera antes de dar por supuesto que no se puede alcanzar el direccionador contiguo. Ambos direccionadores contiguos intercambian la información configurada en el mensaje OPEN y eligen el menor de los dos temporizadores como su valor de temporizador de retención negociado.

   Cuando los direccionadores contiguos han establecido la conexión BGP, intercambian mensajes Keepalive a intervalos frecuentes para asegurarse de que la conexión sigue activa y que los direccionadores contiguos se pueden alcanzar. El intervalo del temporizador Keep-Alive se calcula como un tercio del valor del temporizador de retención negociado. Por lo tanto, el valor del temporizador de retención debe ser cero o al menos tres segundos.

   Tenga en cuenta que, en líneas conmutadas, puede ser recomendable que el valor del temporizador de retención sera cero para ahorrar ancho de banda, al no enviar mensajes Keepalive a intervalos frecuentes.

   **Valores válidos**: 0 a 65535 segundos.
   **Valor por omisión**: 90 segundos

6. El tamaño de segmento TCP (*TCP segment size*) especifica el tamaño máximo de datos que se puede intercambiar en la conexión TCP con un direccionador contiguo. Este valor sirve para la conexión TCP activa con el direccionador contiguo.

   **Valores válidos**: 0 a 65535 bytes.
   **Valor por omisión**: 1024 bytes

**Ejemplo:** **`add neighbor`**

```
Neighbor address [0.0.0.0]? 192.0.251.165
AS [0]? 165
Init timer [12]?
Connect timer [120]?
Hold timer [90]?
TCP segment size [1024]?
```

**no-receive** *núm. as*

Utilice el mandato **add no-receive asnum** para excluir vías de acceso AS si el número de un determinado AS aparece en cualquier lugar dentro de la lista de vías de acceso AS.

El *número de AS* tiene:

**Valores válidos**: 0 a 65535
**Valor por omisión**: ninguno

**Ejemplo:** `add no-receive`

```
Enter AS: [0]? 178
```

**originate-policy** *(exclusive/ inclusive) prefijo red máscara red coincidencia dirección (Exact/Range) identificador*

Utilice el mandato **add originate-policy** para crear una política que determine si una determinada dirección, o rango de direcciones, se puede importar en la tabla de direccionamiento del altavoz BGP a partir de la tabla de direccionamiento IGP.

*Exclusive* Las políticas tipo exclusive evitan que se incluya información de rutas en la tabla de direccionamiento del altavoz BGP.

*Inclusive* Las políticas tipo inclusive aseguran que se incluyen determinadas rutas en la tabla de direccionamiento del altavoz BGP.

*Network prefix* El prefijo de red correspondiente a las direcciones que se verán afectadas.

*Address match* La dirección o rango de direcciones que se verán afectadas por la instrucción de política.

*Tag* El valor que se ha definido para un determinado AS. Todos los valores de identificador coinciden con el del AS del que se han aprendido.

Las políticas tipo exclusive evitan que se incluya información de rutas en la tabla de direccionamiento del altavoz BGP.

1. *Network Prefix* es la dirección que se verá afectada.

   **Valores válidos**: Cualquier dirección IP válida.
   **Valor por omisión**: ninguno

2. Entre el valor de *Network Mask* a aplicar a la dirección especificada en Network Prefix para generar una dirección utilizada en una política BGP.

   **Valores válidos**: Cualquier dirección IP válida.
   **Valor por omisión**: ninguno

3. Seleccione si *Address match* debe estar en un rango de direcciones o debe ser una dirección exacta.

4. *TAG* es el valor que se ha definido para un determinado AS. Los valores de Tag deben coincidir con el del AS del que se han aprendido.

   **Valores válidos**: 0 a 65535
   **Valor por omisión**: ninguno

El siguiente ejemplo incluye todas las rutas en la tabla de direccionamiento IGP del altavoz BGP para anunciar.

**Ejemplo:** **add originate-policy exclusive**

```
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Exact]? range
Tag [0]?
```

Consulte el tema “Ejemplos de políticas de origen” en la página 434 para ver ejemplos detallados de este mandato de política.

**policy-list**

Utilice el mandato **add policy-list** para configurar un grupo de políticas, que se pueden conectar a un determinado direccionador contiguo mediante el mandato **attach policy-to-neighbor**.

**Ejemplo: add policy-list**

```
Name[]? nbr1-rcv
Policy Type(Receive/Send)[Receive]?Receive
```

**Ejemplo: add policy-list**

```
Name[]? nbr1-snd
Policy Type(Receive/Send)[Receive]?Send
```

**Nota:** Consulte el tema “Ejemplos de políticas de recepción basadas en direccionadores contiguos” en la página 435 y el tema “Ejemplos de políticas de envío basadas en direccionadores contiguos” en la página 436 para ver ejemplos detallados de este mandato de política.

**receive-policy** *(exclusive/ inclusive) prefijo red máscara red coincidencia dirección núm. as emisor núm. as adyacente métricaigp (sólo inclusive)*

Utilice el mandato **add receive-policy** para determinar qué rutas se importarán en la tabla de direccionamiento del altavoz BGP.

Las políticas tipo exclusive evitan que se incluya información de rutas en la tabla de direccionamiento del altavoz BGP.

1. *Network Prefix* es la dirección que se verá afectada.

   **Valores válidos**: Cualquier dirección IP válida.
   **Valor por omisión**: ninguno

2. *Network Mask* se aplica a la dirección especificada en el prefijo de red para generar una dirección utilizada en una política BGP.

   **Valores válidos**: Cualquier máscara IP válida.
   **Valor por omisión**: ninguno

3. *Address match* es un rango de direcciones o una dirección exacta.

4. *Originating AS#* tiene:

   **Valores válidos**: 0 a 65535
   **Valor por omisión**: ninguno

5. *Adjacent AS#* especifica el número del AS del direccionador contiguo.

   **Valores válidos**: 0 a 65535
   **Valor por omisión**: ninguno

**Ejemplo:** **add receive-policy exclusive**

```
Network Prefix [0.0.0.0]? 10.0.0.0
Network Mask [0.0.0.0]?  255.0.0.0
Address Match (Exact/Range) [Exact]? range
Originating AS# [0]? 168
Adjacent AS# [0]? 165
```

Consulte el tema “Ejemplos de políticas de recepción basadas en AS” en la página 434 para ver ejemplos detallados de este mandato de política.

**send-policy** *(exclusive/ inclusive) prefijo red máscara red coincidencia dirección identificador núm. as adyacente*

Utilice el mandato **add send-policy** para crear políticas que determinen qué rutas aprendidas del altavoz BGP se anunciarán. Estas rutas pueden ser internas o externas al AS del altavoz BGP.

Las políticas tipo exclusive evitan que se incluya información de rutas en la tabla de direccionamiento del altavoz BGP.

1. *Network Prefix* corresponde a las direcciones que se verán afectadas.

   **Valores válidos**: Cualquier dirección IP válida.
   **Valor por omisión**: ninguno

2. *Network Mask* se aplica a la dirección especificada en el prefijo de red para generar una dirección utilizada en una política BGP.

   **Valores válidos**: Cualquier dirección IP válida.
   **Valor por omisión**: ninguno

3. *Address match* es un rango de direcciones o una dirección exacta.

4. *TAG* es el valor que se ha definido para un determinado AS. Los valores de Tag deben coincidir con el del AS del que se han aprendido.

   **Valores válidos**: 0 a 65535
   **Valor por omisión**: ninguno

5. *Adjacent AS#* especifica el número de AS del direccionador contiguo.

   **Valores válidos**: 0 a 65535
   **Valor por omisión**: ninguno

**Ejemplo:** `add send exclusive`

```
Network Prefix [0.0.0.0]? 180.220.0.0
Network Mask [0.0.0.0]? 255.255.0.0
Address Match (Exact/Range) [Exact]? range
Tag [0]?
Adjacent AS# [0]? 25
```

Consulte el tema “Ejemplos de políticas de envío basadas en AS” en la página 436 para ver ejemplos detallados de este mandato de política.

## Attach

Utilice el mandato **attach policy-to-neighbor** para conectar un nombre configurado de lista de políticas a un determinado direccionador contiguo. Puede conectar un máximo de tres nombres de listas de políticas de recepción y tres de envío.

**Sintaxis**:

a**ttach** policy-to-neighbor

**Ejemplo: attach policy-to-neighbor**

```
Neighbor address [0.0.0.0]? 192.0.251.165
First receive policy list name (none for global AS based policy)[]? nbr1-rcv
Second receive policy list name (none for exit)[]?
First send policy list name (none for global AS based policy)[]? nbr1-snd
Second send policy list name (none for exit)[]?
```

**Nota:** Consulte el tema de “Ejemplos de políticas de recepción basadas en direccionadores contiguos” en la página 435 y el tema “Ejemplos de políticas de envío basadas en direccionadores contiguos” en la página 436 para ver ejemplos detallados de este mandato de política.

## Change

Utilice el mandato **change** para modificar un elemento de la configuración de BGP antes instalado mediante el mandato add.

**Sintaxis**:

ch**ange** aggregate . . .

neighbor . . .

originate-policy . . .

policy-to-neighbor

receive-policy . . .

send-policy. . .

**aggregate** *núm. índice prefijo red máscara red*

Este ejemplo modifica el agregado actual (agregado 1). El cambio hace que el agregado 1 utilice otro prefijo de red y máscara de red para añadir todas las rutas pertenecientes al rango comprendido entre 128.185.0.0 y 128.185.255.255.

**Ejemplo:** **change aggregate 1**

```
Network Prefix [128.185.0.0]? 128.128.0.0
Network Mask [255.255.0.0]? 255.192.0.0
```

**neighbor** *dirección IP direccionador contiguo núm. as temporizador inic temporizador conexión temporizador retención temporizador keep alive tamaño segmento tcp*

El siguiente ejemplo cambia el valor del temporizador de retención por cero para el direccionador contiguo 192.0.251.165.

La *dirección del direccionador contiguo* a modificar tiene:

**Valores válidos**: Cualquier dirección IP válida.
**Valor por omisión**: ninguno

Para volver a activar este direccionador contiguo de forma dinámica utilice el mandato **reset neighbor** desde el indicador de supervisión de BGP.

**Ejemplo:** **change neighbor 192.0.251.165**

```
AS [165]?
Init timer [12]?
Connect timer [60]?
Hold timer [12]? 0
TCP segment size [1024]?
```

**originate-policy** *núm. índice (exclusive/ inclusive) prefijo red máscara red coincidencia dirección identificador*

Utilice el mandato **change originate-policy** para modificar una definición existente de política de origen.

Este ejemplo modifica la política de origen del altavoz BGP. En lugar de excluir las redes con el prefijo 194.10.16.0 de la tabla de direccionamiento IGP, la política incluirá todas las rutas.

**Ejemplo:** **change originate-policy**

```
Enter index of originate-policy to be modified [1]?
Policy Type (Inclusive/Exclusive) [Exclusive]? inclusive
Network Prefix [194.10.16.0]? 0.0.0.0
Network Mask [255.255.240.0]? 0.0.0.0
Address Match (Exact/Range) [Range]?
Tag [0]?
```

**policy-to-neighbor**

Utilice el mandato **change policy-to-neighbor** para modificar una conexión de una lista de políticas de un determinado direccionador contiguo.

**Ejemplo:** **change policy-to-neighbor**

```
Neighbor address [0.0.0.0]? 192.0.251.165
First receive policy list name to be changed[nbr1-rcv]?
Second receive policy list name to be changed[]?
Third receive policy list name to be changed[]?
First send policy list name to be changed[nbr1-snd]?
Second send policy list name to be changed[]?
Third send policy list name to be changed[]?
```

**receive-policy** *núm. índice (exclusive/inclusive) prefijo red máscara red coincidencia dirección núm. as emisor núm. as adyacente métricaigp (sólo inclusive)*

Utilice el mandato **change receive-policy** para modificar una definición existente de política de recepción.

Este ejemplo añade una restricción a la política de recepción del altavoz BGP. En lugar de importar información de rutas procedente de cada similar BGP en su tabla de direccionamiento IGP, evitará que se importen las rutas procedentes del AS 165.

**Ejemplo:** **change receive-policy**

```
Enter index of receive-policy to be modified [1]?
Policy Type (Inclusive/Exclusive) [Inclusive]? exclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Adjacent AS# [0]? 165
```

**send-policy** *núm. índice (exclusive/inclusive) prefijo red máscara red coincidencia dirección identificador núm. as adyacente*

Utilice el mandato **change send-policy** para modificar una política de envío existente por una que sea más tipo inclusive o más tipo exclusive.

Este ejemplo añade una restricción a la política de envío del altavoz BGP. La restricción asegura que todas las rutas del rango de direcciones comprendido entre 194.10.16.0 y 194.10.31.255 se excluirán de los anuncios emitidos al sistema autónomo 165.

**Ejemplo:** **change send-policy**

```
Enter index of send-policy to be modified [1]?
Policy Type (Inclusive/Exclusive) [Inclusive]? exclusive
Network Prefix [0.0.0.0]? 194.10.16.0
Network Mask [0.0.0.0]? 255.255.240.0
Address Match (Exact/Range) [Range]?
Tag [0]?
Adjacent AS# [0]? 165
```

## Delete

Utilice el mandato **delete** para suprimir un elemento de la configuración de BGP anteriormente instalado mediante el mandato **add**.

**Sintaxis:**

**delete** aggregate . . .
neighbor . . .
no-receive . . .
originate-policy . . .
policy-list . . .
policy-to-neighbor
receive-policy . . .
send-policy. . .

**aggregate** *núm. índice*
Debe especificar el número de índice del agregado que desea suprimir. El número de índice es equivalente al número de AS.

**Ejemplo: `delete aggregate 1`**

**neighbor** *dirección IP direccionador contiguo*
Utilice este mandato para suprimir un direccionador contiguo BGP. Debe especificar la dirección de red del direccionador contiguo.

La *dirección de red del direccionador contiguo a suprimir* tiene:

**Valores válidos**: Cualquier dirección IP válida.
**Valor por omisión**: ninguno

Para desactivar este direccionador contiguo de forma dinámica utilice el mandato **reset neighbor** desde el indicador de supervisión de BGP.

**Ejemplo: `delete neighbor 192.0.251.165`**

**no-receive** *as*
Utilice este mandato para suprimir de política que no es de recepción definida para un determinado AS. Debe especificar el número de AS.

El *número de AS* tiene:

**Valores válidos**: 0 a 65535
**Valor por omisión**: ninguno

**Ejemplo: `delete no-receive 168`**

**originate-policy** *núm. índice*
Utilice este mandato para suprimir una determinada política de origen. Debe especificar el número de índice asociado a la política.

**Ejemplo: `delete originate-policy 2`**

**policy-list**

Utilice el mandato **delete policy-list** para suprimir una lista de políticas.

**Ejemplo: `delete policy-list`**

```
Name of policy-list to delete []? nbr1-rcv
All policies defined for 'nbr1-rcv' will be deleted.
Are you sure you want to delete (Yes or [No]? Yes
Policy-list 'nbr1-rcv' is deleted.
```

La conexión de una lista de políticas a un direccionador contiguo se ajustará de la manera apropiada.

**policy-to-neighbor**

Utilice el mandato **delete policy-to-neighbor** para suprimir una conexión existente de un nombre de lista de políticas con un determinado direccionador contiguo.

**Ejemplo: `delete policy-to-neighbor`**

```
Neighbor address [192.0.251.165]?
Remove first receive policy-list name [nbr1-rcv]
Are you sure you want to remove (Yes or [No])? yes
Remove first send policy-list name [nbr1-snd]
Are you sure you want to remove (Yes or [No])? yes
```

**receive-policy** *núm. índice*

Utilice este mandato para suprimir una determinada política de recepción. Debe especificar el número de índice asociado a la política.

**Ejemplo: `delete receive-policy`**

```
Enter index of receive-policy to be deleted [1]?
```

**send-policy** *núm. índice*

Utilice este mandato para suprimir una determinada política de envío. Debe especificar el número de índice asociado a la política.

**Ejemplo: `delete send-policy 4`**

## Disable

Utilice el mandato **disable** para desactivar un altavoz o direccionador contiguo BGP anteriormente activado. Tenga en cuenta que los direccionadores contiguos se activan de forma implícita siempre que se añaden con el mandato **add**.

**Sintaxis**:

**disable** BGP speaker

classless-bgp

compare-med-from-diff-AS

neighbor . . .

**bgp speaker**

Utilice el mandato **disable bgp speaker** para desactivar el protocolo BGP.

**Ejemplo: `disable bgp speaker`**

**classless-bgp**

Utilice este mandato para que no se anuncie una ruta sin clase.

**Ejemplo: `disable classless-bgp`**

**Nota:** Asegúrese de que el mandato **patch bgp-subnets** está desactivado.

**compare-med-from-diff-AS**
Utilice este mandato para desactivar una comparación de MED entre distintos AS.

**Ejemplo:** `disable compare-med-from-diff-AS`

**neighbor** *dirección IP direccionador contiguo*
La *dirección del direccionador contiguo* tiene:

**Valores válidos**: Cualquier dirección IP válida.
**Valor por omisión**: ninguno

**Ejemplo:** `disable neighbor 192.0.190.178`

## Enable

Utilice el mandato **enable** para activar características, posibilidades e información de BGP añadida a la configuración de BGP.

**Sintaxis**:

**enable** BGP speaker

classless-bgp

compare-med-from-diff-AS

neighbor . . .

**bgp speaker** *núm. as tamaño segmento tcp*
Utilice el mandato enable bgp speaker para activar el protocolo BGP.

**Nota**: IBM sólo da soporte a la última versión de BGP, BGP4, que está definida en RFC 1654.

1. El *número de AS* se asocia con este grupo de direccionadores y nodos.

   **Valores válidos**: 0 a 65535
   **Valor por omisión**: ninguno

2. Entre *TCP segment size* para especificar el tamaño máximo de segmento que utilizará BGP para conexiones TCP pasivas.

   **Valores válidos**: 0 a 65535 bytes.
   **Valor por omisión**: 1024 bytes

**Ejemplo:** `enable bgp speaker`

```
AS [0]? 165
TCP segment size [1024]?
```

**classless-bgp neighbor**
Utilice este mandato para activar una ruta sin clase para anunciarla.

**Ejemplo:** `enable classless-bgp`

**compare-med-from-diff-AS**
Utilice este mandato para activar la comparación de MED entre distintos AS.

**Ejemplo:** `enable compare-med-from-diff-AS`

**neighbor** *dirección IP direccionador contiguo*
Utilice este mandato para activar un determinado direccionador contiguo BGP.

La *dirección del direccionador contiguo* tiene:

**Valores válidos**: Cualquier dirección IP válida.
**Valor por omisión**: ninguno

**Ejemplo:** `enable neighbor 192.0.190.178`

## List

Utilice el mandato **list** para visualizar distintas partes de los datos de configuración de BGP, según el submandato que invoque.

**Sintaxis**:

**list** aggregate
all
BGP speaker
neighbor
no-receive
originate-policy
policy-list . . .
policy-to-neighbor
receive-policy
send-policy

**aggregate**
Utilice el mandato **list aggregate** para visualizar todas las rutas añadidas definidas con el mandato **add aggregate**.

**Ejemplo:** `list aggregate`

```
Aggregation:
Index    Prefix              Mask
1         194.10.16.0       255.255.240.0
```

**all** Utilice el mandato **list all** para listar direccionadores contiguos BGP, políticas, rutas añadidas y registros no-receive-as de la configuración actual de BGP.

**Ejemplo:** `list all`

```
                    BGP Protocol:          Enabled
                    AS:                    167
                    TCP-Segment Size:      1024
                    Neighbors and their AS:

                                           Init    Conn    Hold    TCPSEG
Address             State     AS           Timer   Timer   Timer   Size
128.185.250.168     ENABLD    168          12      60      12      1024
192.0.251.165       ENABLD    165          12      60      12      1024

Receive-Policies:
Index  Type  Prefix       Mask       Match  OrgAS  AdjAS IGPmetric
1      INCL  0.0.0.0      0.0.0.0    Range  0      0      0

Send-Policies:
Index  Type  Prefix       Mask       Match  Tag    AdjAS
1      INCL  0.0.0.0      0.0.0.0    Range  0      0

Originate-Policies:
Index  Type  Prefix       Mask             Match  Tag
1      EXCL  194.10.16.0  255.255.240.0    Range  0

Aggregation:

Index  Prefix             Mask
1      194.10.16.0        255.255.240.0
No no-receive-AS records in configuration.
```

**bgp speaker**

Utilice el mandato **list bgp speaker** para obtener información sobre el altavoz BGP. La información que se ofrece es la siguiente:

**Ejemplo: `list BGP speaker`**

```
BGP Protocol:          Enabled
AS:                    165
TCP-Segment Size:      1024
```

**neighbor** Utilice el mandato **list neighbor** para obtener información sobre direccionadores contiguos BGP.

**Ejemplo: `list neighbor`**

```
Neighbors and their AS:

                                       Init    Conn    Hold    TCPSEG
Address             State     AS       Timer   Timer   Timer   Size

128.185.252.168     ENABLD    168      12      60      12      1024
192.0.190.178       DISBLD    178      12      60      12      1024
192.0.251.167       ENABLD    167      12      60      12      1024
```

**no-receive**

Utilice el mandato **list no-receive** para obtener información sobre definiciones no-receive-AS añadidas a la configuración de BGP.

**Ejemplo: `list no-receive`**

```
AS-PATH with following autonomous systems will be discarded:
AS  178
AS  165
```

**originate-policy** *all index prefix*

Utilice el mandato **list originate-policy** para obtener información sobre las políticas de origen añadidas a la configuración de BGP.

**Ejemplo: `list originate-policy`**

```
Originate-Policies:
Index  Type  Prefix           Mask             Match  Tag
1      EXCL  194.10.16.0      255.255.240.0    Range  0
2      INCL  0.0.0.0          0.0.0.0          Range  0
```

**policy-list**

Utilice el mandato **list policy-list** para listar nombres configurados de listas de políticas.

**Ejemplo: `list policy-list`**

```
BGP Config>li policy list
Policy list:
nbr1-rcv  Receive
nbr1-snd  Send
```

**policy-to-neighbor**

Utilice el mandato **list policy-to-neighbor** para listar políticas conectadas a direccionadores contiguos.

**Ejemplo: `list policy-to-neighbor`**

```
Neighbor addrs  receive          send
192.0.251.165   nbr1-rcv         nbr1-snd
```

**receive-policy adj-as-number** *all* **o** *index* **o** *prefix*

Utilice el mandato **list receive-policy** para obtener información sobre las políticas de recepción añadidas a la configuración de BGP. Puede visualizar todas las políticas de recepción definidas para un AS o visualizar políticas por número de índice o de prefijo.

**Ejemplo: `list receive-policy`**

```
Receive-Policies:
Index  Type  Prefix      Mask        Match  OrgAS  AdjAS  IGPmetric
1      EXCL  0.0.0.0     0.0.0.0     Range  178    165
2      INCL  0.0.0.0     0.0.0.0     Range  0      0      0
```

**send-policy adj-as-number** *all* **o** *index* **o** *prefix*

Utilice el mandato **list send-policy** para visualizar información sobre políticas de envío definidas para determinados sistemas autónomos. También puede visualizar todas las políticas de envío definidas para un AS o visualizar políticas por número de índice o de prefijo.

**Ejemplo: `list send-policy`**

```
Send-Policies:
Index  Type  Prefix      Mask           Match Tag    AdjAS
1      EXCL  194.10.16.0 255.255.240.0  Range   0    165
2      INCL   0.0.0.0    0.0.0.0        Range   0    0
```

## Move

Utilice el mandato **move** para modificar el orden en que se han definido políticas y agregados. Esto modifica el orden en que el direccionador aplica las políticas existentes a la información sobre rutas. Antes de utilizar este mandato, se recomienda utilizar el mandato **list** para ver qué políticas se han definido.

**Sintaxis:**

**move** *aggregate* u *originate-policy* o *receive-policy* o *send-policy*

**Ejemplo:**

```
move originate-policy
Enter index of originate-policy to move [1]? 3
Move record AFTER record number [0]?
```

## Set

Utilice el mandato **set** para definir el temporizador de exploración de la tabla de rutas IP (IP-route-table-scan-timer). El valor de IP-route-table-scan-timer sirve para definir el intervalo de tiempo de exploración de la tabla de reenvío IP correspondiente a actualizaciones BGP.

**Sintaxis:**

**set** ip-route-table-scan-timer

**Ejemplo:**

```
set ip-route-table-scan-timer
```

# Update

Utilice el mandato **update** y sus submandatos para manipular políticas.

**Sintaxis:**

**update** *policy-list*

**Ejemplo de política de recepción:**

```
update policy-list
Name[]? nbr1-rcv
```

## Add

Utilice el mandato **Add** para añadir políticas de recepción del mandato **update**.

```
BGP nbr1-rcv: Receive Config>add
Policy type (Inclusive/Exclusive) [Exclusive]? inclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
MED [0]?
Weight [0]?
Local-Pref [0]?
IGP-metric [0]?
```

**Nota:** No se le solicitarán los parámetros MED, Local-pref, Weight ni IGP-metric para políticas de recepción de tipo exclusive. Se utilizarán los valores de MED y Local-pref de los anuncios recibidos si se han configurado con el valor '0'. El valor '0' para el parámetro weight indica que se debe pasar por alto el valor de weight en el proceso de selección de rutas.

## Change

Utilice el mandato **Change** para cambiar políticas del mandato **update**.

**Ejemplo:**

```
Enter index of receive-policy to be modified [1]?
```

## Delete

Utilice el mandato **delete** para suprimir políticas del mandato **update**.

**Ejemplo:**

```
Enter index of receive-policy to be deleted [1]?
```

## Move

Utilice el mandato **move** para mover políticas del mandato **update**.

### Ejemplo:

```
Enter index of receive-policy to move [1]?
Move record after record number [0]?
```

## List

Utilice el mandato **list policy-list** para listar políticas de recepción del mandato **update**.

### Ejemplo: list policy-list

```
Receive policy list for 'name':
                   T Prefix             Match OrgAS AnyAS MED   Weight Lpref IGPmetric
               1   I 0.0.0.0/0          Range 0     0     0     0      0     1
```

### Ejemplo de política de envío:

```
update policy-list
Name[]? nbr1-rcv
```

## Add

Utilice el mandato **Add** para añadir políticas de envío del mandato **update**.

```
BGP nbr1-rcv: Send Config>add
Policy type (Inclusive/Exclusive) [Exclusive]? inclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
TAG [0]
MED [0]?
# of AS to pad[0]?
```

**Nota:** No se le solicitarán los parámetros MED ni ASpad para políticas de envío de tipo exclusive. El valor 0 del parámetro MED indica que el atributo MED no se incluye en el anuncio. El valor 0 correspondiente al parámetro ASpad indica que no se insertará ningún número de AS local adicional en la vía de acceso AS.

## Change

Utilice el mandato **Change** para cambiar políticas del mandato **update**.

### Ejemplo:

```
Enter index of send-policy to be modified [1]?
```

## Delete

Utilice el mandato **delete** para suprimir políticas del mandato **update**.

### Ejemplo:

```
Enter index of send-policy to be deleted [1]?
```

### Move

Utilice el mandato **move** para mover políticas del mandato **update**.

**Ejemplo:**

```
Enter index of send-policy to move [1]?
Move record after record number [0]?
```

### List

Utilice el mandato **list policy-list** para listar políticas de envío del mandato **update**.

**Ejemplo:** list policy-list

```
Send policy list for 'name':
                    T Prefix             Match OrgAS AnyAS Tag   MED    ASpad
                1   I 0.0.0.0/0          Range 0     0     0     0      0
```

## Cómo acceder al entorno de supervisión de BGP

Para acceder al entorno de supervisión de BGP, entre el siguiente mandato en el indicador `Config>`:

```
Config> Protocol BGP
BGP>
```

## Mandatos de supervisión de BGP4

Esta sección describe los mandatos de supervisión de BGP. Estos mandatos le permiten modificar el comportamiento del protocolo BGP para que se ajuste a sus necesidades. Algunas de las tareas de configuración son obligatorias para que el direccionador BGP funcione por completo. Entre los mandatos de supervisión de BGP en el indicador de supervisión `BGP>`.

*Tabla 26. Resumen de mandatos de supervisión de BGP*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Destinations | Muestra todas las entradas de la tabla de direccionamiento BGP. |
| Disable neighbor | Desactiva un determinado direccionador contiguo o todos los direccionadores contiguos. |
| Dump routing tables | Lista el contenido de la tabla de direccionamiento BGP. |
| Enable neighbor | Activa un determinado direccionador contiguo o todos los direccionadores contiguos. |
| Neighbors | Muestra los direccionadores contiguos actualmente activos. |
| Parameter | Muestra los valores globales de BGP instalados en el sistema BGP. |
| Paths | Muestra todas las vías de acceso disponibles de la base de datos. |
| Ping | Envía solicitudes de eco ICMP a otro sistema principal una vez por segundo y espera una respuesta. Este mandato se puede utilizar para identificar un problema en un entorno de interredes. |
| Policy-list | Muestra la política actualmente instalada para un determinado direccionador contiguo y estadísticas sobre el uso de cada política. |
| Reset neighbor | Restablece un determinado direccionador contiguo. |
| Traceroute | Muestra la vía de acceso completa (salto por salto) a un determinado destino. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Destinations

Utilice el mandato **destinations** para realizar un vuelco de todas las entradas de la tabla de direccionamiento BGP o para visualizar información sobre rutas que se anuncian a determinadas direcciones (destinos) de direccionadores contiguos BGP o sobre rutas recibidas de dichas direcciones.

**Sintaxis**:

destinations *dirección red/máscara dirección red*
advertised-to *dirección red*
received-from *dirección red*

**Ejemplo: destination**

```
Network/MaskLen    NextHop         MED   Weight LPref AAG AGRAS ORG AS-Path
142.4.0.0/16       192.0.251.165   100   0      0     No  0     IGP seq[165-178]
```

**destinations** *dirección red*

Muestra información detallada sobre la ruta especificada o la red de destino. El mandato muestra el modo en que se ha aprendido una determinada ruta, la mejor vía de acceso a un destino específico, la métrica asociada a la ruta y más información.

**Ejemplo: destinations 142.4.0.0**

```
Network/MaskLen   NextHop        MED  Weight LPref     AAG AGRAS ORG ASPath
142.4.0.0/16      192.0.251.165  100  0      0         No  0     IGP seq[165-178]

Dest:142.4.0.0/16, Age:180, Upd#:13,LastSent:0001:53:32

Eligible paths: 2
PathID: 8  (Best Path)
        ASpath: seq[165-178]
        Origin: IGP, Pref: 507, LocalPref: 0
        Metric: 0, Weight: 0, MED: 100
        NextHop: 192.0.251.165, Neighbor: 192.0.251.165
        AtomicAggr: No

PathID: 21
        ASpath: seq[168-165-178]
        Origin: IGP, Pref: 505, LocalPref: 0
        Metric: 0, Weight: 0, MED: 0
        NextHop: 128.185.250.168, Neighbor: 128.185.250.168
        AtomicAggr: No
```

**ASpath** Enumera los sistemas autónomos que hay en la vía de acceso.

- -seq: Secuencia de sistemas autónomos en orden en la vía de acceso
- -set: Grupo de sistemas autónomos en la vía de acceso.

**Origin** El originador del destino. Puede ser EGP, IGP o Incomplete (originado por otros métodos desconocidos).

**LocalPref** El grado de preferencia del direccionador originador correspondiente al destino.

**Metric** La métrica de la vía de acceso con la que se ha importado la ruta.

**Weight** La ponderación de la vía de acceso.

**MED** El valor del discriminador de varias salidas, que sirve para establecer una discriminación entre diversos puntos de entrada/salida al mismo AS.

**NextHop** La dirección del direccionador a utilizar como la dirección de reenvío correspondiente a destinos que se pueden alcanzar a través de una determinada vía de acceso.

**AtomicAggr** Indica si el direccionador que anuncia la vía de acceso ha incluido o no la vía de acceso en un agregado atómico.

**destinations** *dirección red  máscara red*

Muestra información detallada sobre la ruta especificada o la red de destino. El mandato muestra el modo en que se ha aprendido una determinada ruta, la mejor vía de acceso a un destino específico, la métrica asociada a la ruta y más información.

Este mandato resulta útil cuando hay varias direcciones de red con el mismo prefijo y distintas máscaras. En estos casos, especificar la máscara de red reduce la cantidad de información presentada.

**Ejemplo: `destinations 194.10.16.0 255.255.240.0`**

```
Dest:194.10.16.0/21, Age:0, Upd#:3, LastSent:0002:00:00

Eligible paths: 1
PathID: 0 - (Best Path)
        ASpath:
        Origin: IGP, Pref: 0, LocalPref: 0
        Metric: 0, Weight: 0, MED: 0
        NextHop: 194.10.16.167, Neighbor: 194.10.16.167
        AtomicAggr: No, Aggregator AS167/194.10.16.167
```

**destinations advertised-to** *dirección red*

Lista todas las rutas anunciadas al direccionador contiguo BGP especificado.

**Ejemplo: `destinations advertised-to`**

```
BGP neighbor address [0.0.0.0]? 192.0.251.165

        Destinations advertised to BGP neighbor 192.0.251.165

Network         NextHop         MED  Weight  LPref      AAG AGRAS ORG ASPath
194.10.16.0/20  194.10.16.167   0    0       0          No  167   IGP
192.0.190.0/24  192.0.251.165   0    0       0          No  0     IGP seq [165]
142.4.0.0/16    192.0.251.165   0    0       0          No  0     IGP seq [165-178]
143.116.0.0/16  128.185.250.168 0    0       0          No  0     IGP seq [168]
```

**destinations received-from** *dirección red*

Lista todas las rutas recibidas del direccionador contiguo BGP especificado.

**Ejemplo: `destinations received-from`**

```
BGP neighbor address [0.0.0.0]? 128.185.250.167

        Destinations obtained from BGP neighbor 128.185.250.167

Network             NextHop         MED Weight  LPref      AAG AGRAS ORG ASPath
194.10.16.0/20      128.185.250.167 0   0       0          No  167   IGP seq[167]
192.0.190.0/24      128.185.250.167 0   0       0          No  0     IGP seq[167-165]
142.4.0.0/16        128.185.250.167 0   0       0          No  0     IGP seq[167-165-178]
```

## Disable Neighbor

Utilice el mandato **disable neighbor** para desactivar un determinado direccionador contiguo o todos los direccionadores contiguos que se han activado. Este mandato desactiva las sesiones BGP y elimina las rutas aprendidas a partir de dicho direccionador contiguo.

**Sintaxis**:

**disable neighbor** *dirección internet*

**Ejemplo: `disable neighbor`**

```
Neighbor address (255.255.255.255 for all) [0.0.0.0]? 128.185.250.167
```

## Dump Routing Tables

Para ver una explicación completa del mandato **dump routing tables**, consulte el tema “Dump Routing Table” en el capítulo “IP de supervisión” del manual *Consulta de configuración y supervisión de protocolos Volumen 1*

## Enable Neighbor

Utilice el mandato **enable neighbor** para activar un determinado direccionador contiguo o todos los direccionadores contiguos que se han desactivado. Este mandato inicia la sesión BGP con el direccionador contiguo.

**Sintaxis**:

**enable neighbor** *dirección internet*

**Ejemplo**:

```
Neighbor address (255.255.255.255 for all) [0.0.0.0]? 128.185.250.167
```

## Neighbors

Utilice el mandato **neighbors** para visualizar información sobre todos los direccionadores contiguos activos BGP.

**Sintaxis:**

**neighbors** *dirección internet*

**Ejemplo:** **neighbors**

```
IP-Address       Status   State        DAY-HH:MM:SS  BGPID           AS     Upd#

128.185.252.168  ENABLD  Established  00000:48:52  128.185.142.168  168     16
192.0.190.178    ENABLD  Established  00002:01:49  142.4.140.178    178     16
192.0.251.167    DISBLD  Established  00002:01:45  194.10.16.167    167     16
```

**IP-Address**
Especifica la dirección IP del direccionador contiguo BGP.

**State** Especifica el estado de la conexión. Los estados posibles son:

- **Connect** En espera de que finalice la conexión TCP con el direccionador contiguo.
- **Active** En el caso de que se produzca un error en la conexión TCP, el estado pasa a Active y continúa el intento de conseguir el direccionador contiguo.
- **OpenSent** En este estado se ha enviado un mensaje OPEN y BGP espera un mensaje OPEN procedente del direccionador contiguo.
- **OpenConfirm** En este estado, se ha enviad un mensaje KEEPALIVE en respuesta a un mensaje OPEN del direccionador contiguo y se espera un mensaje KEEPALIVE/NOTIFICATION del direccionador contiguo.
- **Established** Se ha establecido una conexión BGP satisfactoriamente y ahora se puede comenzar a intercambiar mensajes UPDATE.

**BGP-ID** Especifica el número de identificación BGP del direccionador contiguo.

**AS** Especifica el número de AS del direccionador contiguo.

**Upd#** Especifica el número de secuencia del último mensaje UPDATE enviado al direccionador contiguo.

**dirección-internet**

Utilice el mandato **neighbor** para visualizar datos detallados sobre un determinado direccionador contiguo BGP.

**Ejemplo: `neighbor 192.0.251.167`**

```
Active Conn: Sprt:1026  Dprt:179    State: Established KeepAlive/Hold
Time: 4/12
Passve Conn: None
TCP connection errors: 0          TCP state transitions: 0

BGP Messages:     Sent       Received                    Sent
Received
Open:             1          1          Update:          11         11
Notification:     0          0          KeepAlive:       1828       1830
Total Messages:   1840       1842

Msg Header Errs:  Sent       Received                    Sent
Received
Conn sync err:    0          0          Bad msg length:  0          0
Bad msg type:     0          0

Open Msg Errs:    Sent       Received                    Sent
Received
Unsupp versions:  0          0          Unsupp auth code: 0          0
Bad peer AS ident:0          0          Auth failure:    0          0
Bad BGP ident:    0          0          Bad hold time:   0          0

Update Msg Errs:  Sent       Received                    Sent
Received
Bad attr list:    0          0          AS routing loop:  0          0
Bad wlkn attr:    0          0          Bad NEXT_HOP atr: 0          0
Mssng wlkn attr:  0          0          Optional atr err: 0          0
Attr flags err:   0          0          Bad netwrk field: 0          0
Attr length err:  0          0          Bad AS_PATH attr: 0          0
Bad ORIGIN attr:  0          0

Total Errors:     Sent       Received                    Sent
Received
Msg Header Errs:  0          0          Hold Timer Exprd: 0          0
Open Msg Errs:    0          0          FSM Errs:        0          0
Update Msg Errs:  0          0          Cease:           0          0
```

## Parameter

Utilice el mandato **parameter** de BGP para visualizar los globales BGP instalados en el sistema BGP.

**Sintaxis:**

**parameter**

**Ejemplo:**

```
BGP> parameter

classless-bgp is enabled.
compare-med-from-diff-as is enabled.
IP-route-table-scan-timer value is 5 seconds.
```

## Paths

Utilice el mandato **paths** de BGP para visualizar vías de acceso guardadas en la base de datos de descripciones de vías de acceso.

**Sintaxis:**

**paths**

**Ejemplo:**

```
paths
PathId   NextHop    MED  AAG   AGRAS  RefCnt   ORG   ASPath
0        10.2.0.3    0   No     0      2       IGP
4        192.2.0.2   0   No     0      2       IGP    seq[2]
5        192.2.0.2   0   No     2      1       IGP    seq[2]
6        192.2.0.2   0   No     0      1       IGP    seq[2-1]
7        10.2.0.168  0   No     0      4       IGP
8        192.3.0.1   0   No     0      2       IGP    seq[1]
9        192.2.0.2   0   No     2      1       IGP    seq[2]
10       10.2.0.3    0   No     0      1       IGP
```

**PathId** Identificador de vía de acceso

**NextHop** La dirección del direccionador a utilizar como dirección de reenvío para los destinos que se pueden alcanzar a través de una determinada vía de acceso.

**MED** El discriminador de varias salidas que sirve para establecer una discriminación entre diversos puntos de entrada/salida al mismo AS.

**AAG** Indica si la vía de acceso se ha agregado de forma atómica, es decir, si el direccionador que anuncia esta vía de acceso ha seleccionado una ruta menos específica sobre una más específica cuando se ha presentado con rutas que se solapaban.

**AGRAS** Indica el número de AS del altavoz BGP que ha agregado las rutas.

**RefCnt** Indica el número de entidades de vías de acceso que hacen referencia al descriptor.

**ORG** Especifica el originador de los destinos anunciados en la vía de acceso especificada: EGP, IGP o Incomplete (originado por otros métodos desconocidos).

**AS Path** Enumera los sistemas autónomos que hay en la vía de acceso.

- **seq:** Secuencia de sistemas autónomos en orden en la vía de acceso.
- **set:** Grupo de sistemas autónomos en la vía de acceso.

## Ping

Para ver una explicación completa del mandato **ping**, consulte el mandato Ping en el capítulo “Configuración y supervisión de IP” del manual *Consulta de configuración y supervisión de protocolos Volumen 1*.

## Policy-List

Utilice el mandato **policy-list** para visualizar la política actualmente instalada para un determinado direccionador contiguo y estadísticas sobre el uso de cada política.

**Ejemplo: policy-list**

```
Neighbor address[0.0.0.0]? 192.0.251.167
Policy Type(Receive/Send/Origin)[All]?Receive
```

Ejemplo correspondiente a la configuración de una política basada en direccionadores contiguos:

```
Receive policy list for neighbor '192.0.251.167':
Idx T Prefix            Match OrgAS AnyAS MED   Weight LPref IGPmet Usage
1   I 0.0.0.0/0         Range 0     0     0     0      0     1      1
```

Ejemplo correspondiente a la configuración de una política basada en AS:

```
Receive policy :
Idx Type  Prefix            Match OrgAS AdjAS IGPmetric Usage
1   INCL  0.0.0.0/0         Range 0     0     1         1
```

### Ejemplo: policy-list

```
Neighbor address[0.0.0.0]? 192.0.251.167
Policy Type(Receive/Send/Origin)[All]?Send
```

Ejemplo correspondiente a la configuración de una política basada en direccionadores contiguos:

```
send policy list for neighbor '0.0.0.0': 192.0.251.167
Idx T Prefix            Match OrgAS AnyAS TAG   MED   ASpad Usage
1   I 0.0.0.0/0         Range 0     0     0     0     0     1
```

Ejemplo correspondiente a la configuración de una política basada en AS:

```
send policy :
Idx Type  Prefix            Match OrgAS AdjAS TAG   Usage
1   INCL  0.0.0.0/0         Range 0     0     0     1
```

### Ejemplo: policy-list

```
Neighbor address[0.0.0.0]? 192.0.251.167
Policy Type(Receive/Send/Origin)[All]?Origin

Origin policy list for neighbor '0.0.0.0':
Idx T Prefix            Match TAG   Usage
1   I 0.0.0.0/0         Range 0     1
```

## Reset Neighbor

Utilice el mandato **reset neighbor** para restablecer el direccionador contiguo BGP especificado, en función de los parámetros de configuración del direccionador contiguo guardados en la memoria de configuración.

**Sintaxis**:

**reset neighbor** *dirección internet*

**Ejemplo:** **reset neighbor**

```
Neighbor address[0.0.0.0]? 128.185.250.167
```

## Sizes

Utilice el mandato **sizes** de BGP para visualizar el número de entradas guardadas en diversas bases de datos.

**Sintaxis:**

**sizes**

**Ejemplo:** **sizes**

```
# Paths:                                11
# Path descriptors:                      7
  Update sequence#:                     22
# Routing tbl entries (allocated):       6
# Current tbl entries (not imported):    0
# Current tbl entries (imported to IGP): 3
```

**Paths** Número total de vías de acceso que se pueden elegir para todas las rutas de la tabla de direccionamiento BGP.

**Path descriptors**
Número total de descriptores de vías de acceso en la base de datos que se utiliza para albergar información común de vías de acceso.

**Update sequence#**
Indica el número actual de secuencia de actualización.

**Routing tbl entries (allocated)**
Indica el número de entradas en la tabla de direccionamiento BGP.

**Current tbl entries (not imported)**
Indica el número de rutas BGP que no se han importado en IGP.

**Current tbl entries(imported to IGP)**
Indica el número de rutas BGP importadas en IGP.

## Traceroute

Para ver una explicación completa del mandato **traceroute**, consulte “Configuración y supervisión de IP” en el manual *Consulta de configuración y supervisión de protocolos Volumen 2*.

# Configuración y supervisión de DVMRP

Este capítulo describe cómo configurar y supervisar la actividad del protocolo DVMRP (Protocolo de direccionamiento de difusión múltiple de vector de distancia). Incluye las siguientes secciones:

- "Cómo acceder al entorno de configuración de DVMRP"
- "Mandatos de configuración de DVMRP"
- "Mandatos de supervisión de DVMRP" en la página 470

## Cómo acceder al entorno de configuración de DVMRP

Para acceder al entorno de configuración de DVMRP, entre el siguiente mandato en el indicador `Config>`:

```
Config> protocol dvmrp
Distance Vector Multicast Routing Protocol config monitoring
DVMRP Config>
```

## Mandatos de configuración de DVMRP

Esta sección describe los mandatos de configuración de DVMRP. Los mandatos se entran en el indicador `DVMRP Config>`.

*Tabla 27. Resumen de mandatos de configuración de DVMRP*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxxi. |
| Add | Añade información a la información existente de DVMRP. Puede añadir una interfaz física o una interfaz de túnel IP-IP. |
| Change | Modifica información de DVMRP en SRAM. Puede modificar el coste o el umbral de un interfaz física, túnel IP-IP, la interfaz MOSPF o los puntos finales de un túnel IP-IP. |
| Delete | Suprime información de DVMRP de la configuración estática. |
| Disable | Desactiva el protocolo DVMRP completo o la interfaz MOSPF. |
| Enable | Activa el protocolo DVMRP completo o la interfaz MOSPF. |
| List | Muestra la configuración de DVMRP. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxii. |

## Add

Utilice el mandato **add** para añadir información a la información de DVMRP existente. Puede añadir una interfaz física o un túnel IP-IP.

**Sintaxis:**

a**dd** interface *dirección-ip coste umbral*

tunnel *origen-túnel destino-túnel cose umbral*

**interface** Añade o actualiza una interfaz DVMRP

**dirección-ip**
Especifica la dirección IP de la interfaz DVMRP.

**Valores válidos**: Cualquier dirección IP válida

**Valor por omisión**: Ninguno

**coste** Especifica el coste (en términos de número de saltos) de utilizar la interfaz.

**Valores válidos**: Cualquier entero mayor que 0

**Valor por omisión**: 1

**umbral** Especifica el tiempo de vida necesario para alcanzar el direccionador contiguo más cercano de la interfaz.

**Valores válidos**: Cualquier entero mayor que 0

**Valor por omisión**: 1

**tunnel** Añade o actualiza un túnel IP-IP a través de una red que no es de difusión múltiple. Hay que configurar túneles cuando el tráfico de difusión múltiple tiene que atravesar una red que no da soporte a datagramas de difusión múltiple o que no ejecuta ningún protocolo de direccionamiento de difusión múltiple.

**dirección-origen**
Especifica la dirección IP del origen del túnel.

**Valores válidos**: Cualquier dirección IP válida

**Valor por omisión**: Ninguno

**dirección-destino**
Especifica la dirección IP del destino del túnel.

**Valores válidos**: Cualquier dirección IP válida

**Valor por omisión**: Ninguno

**coste** Especifica el coste (en términos de número de saltos) de utilizar el túnel.

**Valores válidos**: Cualquier entero mayor que 0

**Valor por omisión**: 1

**umbral** Especifica el tiempo de vida necesario para alcanzar el direccionador contiguo más cercano de la interfaz.

**Valores válidos**: Cualquier entero mayor que 0

**Valor por omisión**: 1

## Change

Utilice el mandato **change** para modificar la información existente de DVMRP. Puede modificar los valores de coste o interfaz de la interfaz física, túneles IP-IP o la interfaz MOSPF.

**Sintaxis:**

c**hange** interface *dirección-ip coste umbral*

tunnel *origen-túnel destino-túnel cose umbral*

mospf *coste umbral*

**interface** Modifica una interfaz DVMRP

**dirección-ip**

**Valores válidos**: Cualquier dirección IP válida

**Valor por omisión**: Ninguno

**coste** Especifica el coste (en términos de número de saltos) de utilizar la interfaz.

**Valores válidos**: Cualquier entero mayor que 0

**Valor por omisión**: 1

**umbral** Especifica el tiempo de vida necesario para alcanzar el direccionador contiguo más cercano de la interfaz.

**Valores válidos**: Cualquier entero mayor que 0

**Valor por omisión**: 1

**tunnel** Modifica un túnel IP-IP.

**dirección-origen**

**Valores válidos**: Cualquier dirección IP válida

**Valor por omisión**: Ninguno

**dirección-destino**

**Valores válidos**: Cualquier dirección IP válida

**Valor por omisión**: Ninguno

**coste** Especifica el coste (en términos de número de saltos) de utilizar la interfaz.

**Valores válidos**: Cualquier entero mayor que 0

**Valor por omisión**: 1

**umbral** Especifica el tiempo de vida necesario para alcanzar el direccionador contiguo más cercano de la interfaz.

**Valores válidos**: Cualquier entero mayor que 0

**Valor por omisión**: 1

**mospf** Modifica una interfaz MOSPF.

**coste** Especifica el coste (en términos de número de saltos) de utilizar la interfaz.

**Valores válidos**: Cualquier entero mayor que 0

**Valor por omisión**: 1

**umbral** Especifica el tiempo de vida necesario para alcanzar el direccionador contiguo más cercano de la interfaz.

**Valores válidos**: Cualquier entero mayor que 0

**Valor por omisión**: 1

## Delete

Utilice el mandato **delete** para eliminar información de DVMRP existente de la memoria estática.

**Sintaxis:**

de**lete** interface *dirección-ip*

tunnel *origen-túnel destino-túnel*

**interface** Suprime una interfaz DVMRP.

**dirección-ip**

**Valores válidos**: Cualquier dirección IP válida

**Valor por omisión**: Ninguno

**tunnel** Suprime un túnel IP-IP.

**dirección-origen**

**Valores válidos**: Cualquier dirección IP válida

**Valor por omisión**: Ninguno

**dirección-destino**

**Valores válidos**: Cualquier dirección IP válida

**Valor por omisión**: Ninguno

## Disable

Utilice el mandato **disable** para desactivar el protocolo DVMRP completo o la interfaz MOSPF.

**Sintaxis:**

di**sable** dvmrp

mospf

**dvmrp** Desactiva el protocolo DVMRP. Cuando está desactivado, el dispositivo no participa como direccionador de difusión múltiple DVMRP.

**mospf** Desactiva la interfaz ante el protocolo de direccionamiento MOSPF. Cuando está desactivado, el protocolo DVMRP no reenvía datagramas de difusión múltiple al protocolo de direccionamiento MOSPF ni los recibe del mismo.

## Enable

Utilice el mandato **enable** para activar el protocolo DVMRP completo o la interfaz MOSPF.

**Sintaxis:**

**enable** dvmrp

mospf *coste umbral*

**dvmrp** Activa el protocolo DVMRP. Todas las interfaces configuradas que no tienen MOSPF activado y la interfaz MOSPF se activan.

**mospf** Activa la interfaz ante el protocolo de direccionamiento MOSPF correspondiente a DVMRP. Esta interfaz permite a DVMRP reenviar datagramas de difusión múltiple al protocolo de direccionamiento MOSPF. Esta interfaz se trata como una interfaz física.

**coste** Especifica el coste (en términos de número de saltos) de utilizar la interfaz.

**Valores válidos**: Cualquier entero mayor que 0

**Valor por omisión**: 1

**umbral** Especifica el tiempo de vida necesario para alcanzar el direccionador contiguo más cercano de la interfaz.

**Valores válidos**: Cualquier entero mayor que 0

**Valor por omisión**: 1

## List

Utilice el mandato **list** para visualizar la configuración actual de DVMRP. La salida muestra el estado actual de DVMRP (activado o desactivado), información sobre la configuración de la interfaz física, información sobre la configuración del túnel e información sobre la configuración de MOSPF.

**Sintaxis:**

**list**

**Ejemplo:**

```
DVMRP config> list

          DVMRP on
          phyint 128.185.138.19 1 1
          phyint 128.185.177.19 2 4
          tunnel 128.185.138.19 128.185.138.21 4 4
```

La siguiente información se muestra para cada interfaz listada:

**Protocolo DVMRP**
Muestra si DVMRP está activado o desactivado

**Interfaces físicas de DVMRP**
Para cada interfaz física, se muestra su dirección IP y los valores correspondientes a coste y umbral.

**Interfaces del túnel DVMRP**
Para cada interfaz del túnel, se muestran los puntos finales configurados del túnel, el coste y el umbral.

**Interfaz MOSPF de DVMRP**
Para la interfaz MOSPF, se muestra el coste y el umbral.

## Mandatos de supervisión de DVMRP

Los mandatos de supervisión de DVMRP le permiten ver parámetros y estadísticas de redes que tienen DVMRP activado.

Entre los mandatos de supervisión de DVMRP en el indicador **DVMRP>**.

*Tabla 28. Resumen de mandatos de supervisión de DVMRP*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Dump routing tables | Muestra las rutas DVMRP contenidas en la tabla de direccionamiento. |
| Interface summary | Muestra parámetros y estadísticas de la interfaz DVMRP. |
| Join | Configura el direccionador para que pertenezca a uno o más grupos de difusión múltiple. |
| Leave | Elimina el direccionador de grupos de difusión múltiple. |
| Mcache | Muestra una lista de entradas de la antememoria de reenvíos de difusión múltiple actualmente activas. |
| Mgroups | Muestra la pertenencia a grupos de las interfaces conectadas del direccionador. |
| Mstats | Muestra distintas estadísticas de direccionamiento de difusión múltiple. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Dump Routing Tables

Utilice el mandato **dump routing tables** para visualizar el grupo de orígenes conocidos de difusión múltiple DVMRP. Cada origen se muestra junto con el direccionador DVMRP a partir del cual se ha aprendido, un coste asociado y el número de segundos transcurridos desde que se renovó la entrada de la tabla de direccionamiento.

**Sintaxis:**

**dump**

**Ejemplo:** `dump`

```
Multicast Routing Table
Type   Origin-Subnet   From-Gateway    Metric  Age  In  Out-Vifs
Direct 18.26.0.0       192.35.82.97      10     30   1    0  2*
Direct 18.58.0.0       192.35.82.97       4     30   1    0  2*
DVMRP  18.85.0.0       192.35.82.97       4     30   1    0  2*
DVMRP  18.180.0.0      192.35.82.97       3     30   1    0  2*
DVMRP  36.8.0.0        192.35.82.97       9     30   1    0  2*
DVMRP  36.56.0.0       192.35.82.97       7     30   1    0  2*
DVMRP  36.103.0.0      192.35.82.97       9     30   1    0  2*
DVMRP  128.61.0.0      192.35.82.97       8     30   1    0  2*
DVMRP  128.89.0.0      192.35.82.97      10     30   1    0  2*
DVMRP  128.109.0.0     192.35.82.97       4     30   1    0  2*
DVMRP  128.119.0.0     192.35.82.97       4     30   1    0  2*
DVMRP  128.150.0.0     192.35.82.97       6     30   1    0  2*
```

**Type** Muestra el tipo de orígenes de la difusión múltiple (por ejemplo, DVMRP)

**Origin-Subnet**
Muestra la dirección IP de la subred de origen.

**From-Gateway**
Muestra la dirección IP de la pasarela de la que proviene la entrada.

**Metric** Muestra el coste asociado de esta ruta.

**Age** Muestra la antigüedad de la entrada de la tabla de direccionamiento como el número de segundos transcurridos desde que se renovó la entrada de la tabla de direccionamiento.

**In** Muestra la VIF de DVMRP en la que se tiene que recibir este datagrama de difusión múltiple procedente del origen.

**Out-Vifs** Muestra las VIF que enviarán datagramas de difusión múltiple. Las VIF marcadas con un asterisco indican que sólo se reenviará un datagrama si hay miembros del grupo en la red conectada.

## Interface Summary

Utilice el mandato **interface summary** para visualizar la lista actual de interfaces DVMRP (o VIF).

**Sintaxis:**

**interface** *dirección-ip-interfaz*

**Ejemplo: `interface`**

```
Virtual Interface Table
Vif  Local-Address                          Metric  Thresh  Flags
0   10.1.153.22      subnet: 10.1.153.0       1       1    querier
1   10.1.154.22      subnet: 10.1.154.0       1       1    down
```

**Vif** Muestra el número asignado a las interfaces DVMRP (o VIF). Cada VIF tiene un número asignado, que sirve para identificar la VIF en otros mandatos.

**Local Address**
Muestra la dirección IP local de la interfaz DVMRP.

**Metric** Muestra el coste asociado de la ruta.

**Threshold**
Refleja la capacidad de una red de controlar flujo externo de paquetes de difusión múltiple externos a la red.

**Flags** Muestra si la VIF está desactivada o si el direccionador es el emisor de consultas de pertenencia a grupo de sistema principal IGMP en la interfaz.

## Join

Utilice el mandato **join** para establecer el direccionador como miembro de un grupo de difusión múltiple.

Este mandato se parece al mandato join de supervisión de configuración de OSPF con dos diferencias:

- El efecto sobre la pertenencia a grupo es inmediato si los mandatos se emiten desde el indicador de supervisión (es decir, no hace falta volver a arrancar ni volver a cargar el direccionador).
- El mandato efectúa un seguimiento del número de veces que se emite un mandato “join” sobre un determinado grupo.

Cuando el direccionador es miembro de un grupo de difusión múltiple, responde a mandatos ping y a consultas SNMP enviadas a la dirección del grupo.

**Sintaxis:**

**join** *dirección-grupo-difusión-múltiple*

**Ejemplo:** `join 224.185.00.00`

## Leave

Utilice el mandato **leave** para que un direccionador deje de formar parte de un grupo de difusión múltiple. Este mandato hará que el direccionador deje de responder a mandatos ping y a consultas SNMP enviadas a la dirección del grupo.

Este mandato es parecido al mandato **leave** de supervisión de configuración de OSPF con dos diferencias:

- El efecto sobre la pertenencia a grupo es inmediato si los mandatos se emiten desde el indicador de supervisión (es decir, no hace falta volver a arrancar ni volver a cargar el direccionador).
- El mandato no eliminará el direccionador del grupo hasta que el número de mandatos “leave” ejecutados sea igual al número de mandatos “joins” anteriormente ejecutados.

**Sintaxis:**

**leave** *dirección-grupo-difusión-múltiple*

**Ejemplo:** `leave 224.185.00.00`

## Mcache

Utilice el mandato **mcache** para visualizar la lista de entradas de la antememoria de difusión múltiple actualmente activas. Las entradas de la antememoria de difusión múltiple se basan en la demanda, cuando se recibe el primer datagrama coincidente de difusión múltiple. Hay una entrada de antememoria (y, por lo tanto, una ruta) para cada combinación de red de origen de datagrama y grupo de destino.

Las entradas de la antememoria se borran tras cambios en la topología (por ejemplo, cuando se activa o desactiva una línea punto a punto en el sistema DVMRP) y tras cambios en pertenencia a grupos.

**Nota:** Los números que se muestran en la descripción que aparece en la parte superior de la salida NO se refieren directamente a las VIF, sino a interfaces físicas (que pueden ejecutar DVMRP o MOSPF) y túneles.

**Nota:**

**Sintaxis:**

**mcache**

**Ejemplo:**

```
mcache
0: Eth/0           1: TKR/0           2: Internal
3: 128.185.246.17  4: 192.35.82.97

Source          Destination     Count   Upst    Downstream
128.185.146.0   239.0.0.1       1       0       2,4
128.119.0.0     224.2.199.198   9       4       3
128.9.160.0     224.2.127.255   1       4       3
13.2.116.0      224.2.0.1       27      4       3
140.173.8.0     224.2.0.1       31      4       3
128.165.114.0   224.2.0.1       25      4       3
132.160.3.0     224.2.158.99    11      4       3
132.160.3.0     224.2.170.143   56      4       3
128.167.254.0   224.2.199.198   27      4       3
129.240.200.0   224.2.0.1       21      4       3
131.188.34.0    224.2.0.1       28      4       3
131.188.34.0    224.2.199.198   28      4       3
```

**Source** Red/subred de origen de los datagramas coincidentes.

**Destination**
Grupo de destino de los datagramas coincidentes.

**Count** Muestra el número de entradas procesadas correspondientes a este grupo de difusión múltiple.

**Upstream**
Muestra el direccionador/red contiguo del que se debe recibir el datagrama para que se reenvíe. Cuando aparece el valor “none”, significa que el datagrama no se reenviará nunca.

**Downstream**
Muestra el número total de interfaces/direccionadores contiguos directos a los que se reenviará el datagrama. Cuando su valor es *none*, el datagrama no se reenviará.

Una entrada de la antememoria de reenvíos de difusión múltiple contiene más información. Se puede visualizar en detalle una entrada de la antememoria especificando el origen y el destino de un datagrama coincidente en la línea de mandatos. Si no se encuentra ninguna entrada de la antememoria coincidente, se crea una. A continuación se muestra un ejemplo de este mandato:

**Ejemplo:**

```
mcache 128.185.182.9  224.0.1.2
source Net:     128.185.182.0
Destination:    224.0.1.2
Use Count:      472
Upstream Type:  Transit Net
Upstream ID:    128.185.184.114
Downstream:     128.185.177.11 (TTL = 2)
```

Además de la información que se muestra en el formato corto del mandato mcache, se visualizan los siguientes campos:

**Upstream Type** Indica el tipo de nodo del que se debe recibir el datagrama para que se reenvíe. Los valores posibles para este campo son “none” (indica que el datagrama no se reenviará), “router” (indica que el datagrama se debe recibir sobre una conexión punto a punto), “transit network”, “stub network” y “external” (indican que se espera recibir el datagrama de otro Sistema autónomo).

**Downstream** Muestra una línea para cada interfaz o direccionador contiguo al que se enviará el datagrama. También se muestra un valor TTL, que indica que los datagramas enviados por esta interfaz o recibidos en la misma deben tener al menos el valor TTL especificado en su cabecera IP. Cuando el direccionador es miembro de un grupo de difusión múltiple, aparece la línea *internal application* como uno de los direccionadores contiguos/interfaces directos.

## Mgroups

Utilice el mandato **mgroups** para visualizar la pertenencia a grupos de las interfaces conectadas al direccionador. Sólo se muestra una pertenencia a grupo para las interfaces en las que el direccionador es el direccionador designado o el direccionador designado de reserva.

**Sintaxis:**

**mgroups**

**Ejemplo:**

```
mgroups
Local Group Database
Group             Interface                Lifetime (secs)

224.0.1.1         128.185.184.11 (Eth/1)       176
224.0.1.2         128.185.184.11 (Eth/1)       170
224.1.1.1         Internal                     1
```

**Group** Muestra la dirección del grupo tal como se notifica (mediante IGMP) a una determinada interfaz.

**Interface** Muestra la dirección de la interfaz a la que se ha notificado la dirección del grupo (mediante IGMP).

La pertenencia a un grupo interno del direccionador se indica mediante el valor“internal”. Para estas entradas, el campo Lifetime (consulte la explicación siguiente) indica el número de aplicaciones que han solicitado la pertenencia a un determinado grupo.

**Lifetime** Muestra el número de segundos que la entrada permanece si se dejan de escuchar informes de pertenencia a grupo en la interfaz correspondiente al grupo especificado.

## Mstat

Utilice el mandato **mstat** para visualizar distintas estadísticas de direccionamiento de difusión múltiple. El mandato indica si el direccionamiento de difusión múltiple está activado y si el direccionador es un distribuidor entre áreas o un distribuidor de difusión general entre AS.

**Sintaxis:**

**mstats**

**Ejemplo:**

```
mstats
              MOSPF forwarding:       Enabled
              Inter-area forwarding:  Enabled
              DVMRP forwarding:       Enabled

Datagrams received:           45476  Datagrams (ext source):    0
Datagrams fwd (multicast):        0  Datagrams fwd (unicast):   0
Locally delivered:                0  No matching rcv interface: 0
Unreachable source:               4  Unallocated cache entries: 0
Off multicast tree:               0  Unexpected DL multicast:   0
Buffer alloc failure:             0  TTL scoping:               0

# DVMRP routing entries:          0  # DVMRP entries freed:     0
# fwd cache alloc:                5  # fwd cache freed:         0
# fwd cache GC:                   0  # local group DB alloc:    6
# local group DB free:            0
```

**MOSPF forwarding**
Muestra si el direccionador reenviará datagramas de difusión múltiple IP.

**Inter-area forwarding**
Muestra si el direccionador reenviará datagramas de difusión múltiple IP entre áreas.

**DVMRP forwarding**
Muestra si el direccionador reenviará datagramas de difusión múltiple IP.

**Datagrams received**
Muestra el número de datagramas de difusión múltiple recibidos por el direccionador (los datagramas cuyos grupos de destino están en el rango 224.0.0.1 - 224.0.0.255 no se incluyen en este total).

**Datagrams (ext source)**
Muestra el número de datagramas recibidos cuyos orígenes están fuera del AS.

**Datagrams fwd (multicast)**
Muestra el número de datagramas que se han reenviado como difusiones múltiples de enlace de datos (esto incluye duplicaciones de paquetes, si es necesario, de modo que este número 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.

**No matching rcv interface**
Muestra el número de datagramas recibidos por un distribuidor de difusión múltiple que no es interno del AS en una interfaz que no es MOSPF.

**Unreachable source**
Muestra el número de datagramas cuyas direcciones de origen no se han podido alcanzar.

**Unallocated cache entries**
Muestra el número de datagramas cuyas entradas de antememoria no se han podido crear por falta de recursos.

**Off multicast tree**
Muestra el número de datagramas que no se han reenviado porque no había direccionador contiguo de procedencia o no había direccionadores contiguos/interfaces directos en la entrada de antememoria coincidente.

**Unexpected DL multicast**
Muestra el número de datagramas recibidos como difusiones múltiples de enlace de datos en interfaces que se han configurado para la difusión individual de enlace de datos.

**Buffer alloc failure**
Muestra el número de datagramas que no se han podido duplicar por falta de almacenamiento intermedio.

**TTL scoping**
Indica los datagramas que no se han podido reenviar porque su TTL indicaba que nunca podrían alcanzar un miembro del grupo.

**DVMRP routing entries:**
Muestra el número de entradas de direccionamiento DVMRP.

**DVMRP entries freed:**
Indica el número de entradas DVMRP que se han liberado. El tamaño será el número de entradas de direccionamiento menos el número de entradas liberadas.

**# fwd cache alloc**
Indica el número de entradas de antememoria asignadas. El tamaño actual de la antememoria de reenvío es el número de entradas asignadas (“# fwd cache alloc”) menos el número de entradas de antememoria liberadas (“# fwd cache freed”).

**# fwd cache freed**
Indica el número de entradas de antememoria liberadas. El tamaño actual de la antememoria de reenvío es el número de entradas asignadas (“# fwd cache alloc”) menos el número de entradas de antememoria liberadas (“# fwd cache freed”).

**# fwd cache GC**
Indica el número de entradas de antememoria que se han borrado porque no se habían utilizado recientemente y la antememoria se había desbordado.

**# local group DB alloc**

Indica el número de entradas asignadas de la base de datos de grupo local. El número asignado (“# local group DB alloc”) menos el número liberado (“# local group DB free”) es igual al tamaño actual de la base de datos de grupo local.

**# local group DB free**

Indica el número de entradas liberadas de la base de datos de grupo local. El número asignado (“# local group DB alloc”) menos el número liberado (“# local group DB free”) es igual al tamaño actual de la base de datos de grupo local.

El número de aciertos de antememoria se puede calcular como el número de datagramas recibidos (“Datagrams received”) menos el total de datagramas eliminados debido a “No matching rcv interface,” “Unreachable source” y “Unallocated cache entries” y menos “# local group DB alloc.” El número de errores de antememoria es simplemente “# local group DB alloc.”

# Utilización de RSVP

Resource ReSerVation Protocol (RSVP) es un protocolo de señalización que utilizan las aplicaciones para marcar sus requisitos de calidad de servicio (QoS). RSVP está diseñado para dar soporte a sesiones entre varios emisores y varios receptores. Cuando la señalización RSVP activa la gestión del tráfico, el resultado es una reserva dinámica de recursos de la red (por ejemplo, ancho de banda y almacenamientos intermedios) que consiguen una QoS deseada para la distribución de paquete. RSVP está orientado al receptor, es decir, la aplicación que recibe el flujo de QoS es la responsable de iniciar la señalización RSVP que reserva recursos de la red. Por lo tanto, la QoS en RSVP se consigue estableciendo reservas a través de cada salto de la vía de acceso entre el receptor y el emisor. Una reserva consta de una serie de valores de parámetros que determinan la QoS correspondiente a un flujo de tráfico. El emisor y el receptor, que son aplicaciones de sistema principal activadas para RSVP, crean la reserva enviando mensajes RSVP entre sí. Una mejora de IBM permite que para algunas aplicaciones no activadas para RSVP su direccionador del primer salto realice la función de señalización RSVP en su nombre. RSVP funciona en IPv4 en direccionadores IBM y da soporte a tráfico IP tanto de difusión individual como de difusión múltiple. Encontrará una descripción completa de RSVP en RFC 2205.

Para cada flujo de tráfico IP para el que se ha establecido una reserva, RSVP, tal como se implanta en el 2210, ofrece calidad de servicio de Carga controlada. La QoS de Carga controlada está definida en el modelo denominado Integrated Services de Internet Engineering Task Force (IETF) (RFC 2211). Incluso cuando la red está congestionada, la QoS de Carga controlada continúa ofreciendo el nivel de servicio que el flujo de tráfico recibe cuando la red no está congestionada.

Este capítulo incluye las siguientes secciones:

- "Cómo funciona RSVP"
- "Tipos de enlaces que reciben soporte de RSVP" en la página 484
- "Configuración de ejemplo" en la página 485

## Cómo funciona RSVP

La Figura 38 muestra la secuencia de mensajes que RSVP utiliza para establecer una reserva que ofrece QoS a un determinado flujo de tráfico. En este ejemplo, se da por supuesto que ya se han establecido flujos de tráfico IP Best Effort entre los direccionadores.

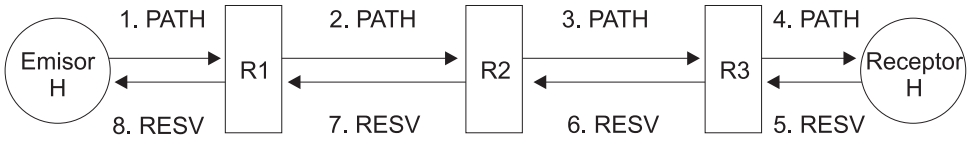



*Figura 38. Reservas RSVP - Todos los direccionadores dan soporte a RSVP*

El establecimiento de una reserva an comienza cuando un emisor con RSVP activado envía mensajes *PATH* a los receptores del flujo de tráfico de datos. El mensaje PATH contiene información sobre el tráfico que describe el flujo. Cuando los direccionadores reciben un mensaje PATH (examinando el campo ALERT

Option de la cabecera IP), establecen y mantienen un estado dinámico correspondiente a dicho mensaje PATH. Un direccionador RSVP también marcará el mensaje PATH que envía en dirección al destino con su propia dirección IP, lo que se denomina salto anterior o salto-a. Un receptor con RSVP activo puede responder a un mensaje PATH enviando un mensaje *RESV*. El mensaje RESV solicita que se reserven recursos de la red, como ancho de banda, a través de cada enlace de la vía de acceso. El mensaje RESV se envía junto con la vía de acceso inversa por la que ha pasado el mensaje PATH. El primer direccionador (Direccionador R3) recibe el mensaje RESV en la vía de acceso inversa. Este direccionador intenta reservar recursos en la interfaz de salida, es decir, en el enlace entre R3 y el sistema principal receptor. Si los recursos solicitados están disponibles, se reservan para este flujo y la cantidad de recursos disponibles se reduce en la cantidad correspondiente. Si los recursos solicitados no están disponibles, la reserva falla en dicho nodo y es posible que se envíe un mensaje RESVERR al sistema principal receptor. Por ahora, supondremos que la reserva resulta satisfactoria.

El Direccionador R3 envía el mensaje RESV al siguiente direccionador (R2) de la vía de acceso hacia el emisor. R2 define una reserva en el enlace entre sí mismo y R3 y envía el mensaje RESV a R1. R1 define una reserva en el enlace entre sí mismo y R2 y envía el mensaje RESV al sistema principal emisor. En este ejemplo, el sistema principal emisor da soporte a RSVP. Define una reserva en el enlace entre sí mismo y R1. Ahora una vía de acceso de enlaces reservados forma una reserva que se ha establecido entre el emisor y el receptor.

Ahora supongamos que tenemos una red en la que no todos los nodos dan soporte a RSVP, tal como se muestra en la Figura 39.

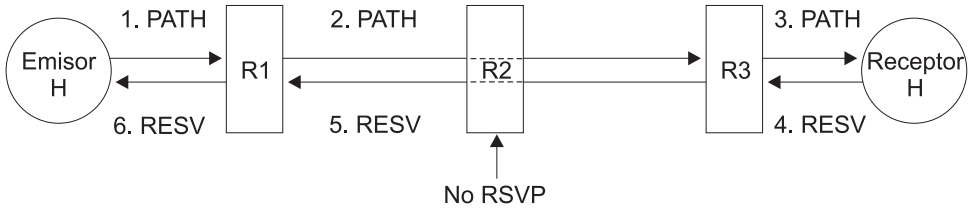



*Figura 39. Reservas RSVP - No todos los direccionadores dan soporte a RSVP*

En concreto, supongamos que R2 no da soporte a RSVP. Cuando R2 recibe el mensaje PATH, lo trata como un paquete normal y lo reenvía hacia R3. R2 no cambia el salto-a contenido en el mensaje PATH.

Al igual que antes, cuando el mensaje PATH llega al sistema principal receptor, comienza el proceso de reserva enviando un mensaje RESV a R3. El salto-anterior que R3 ve en el mensaje RESV es la dirección de R1 porque R2 no suministró su salto anterior en el mensaje PATH. R3 envía el mensaje RESV a R1 y realiza la reserva en el enlace entre sí mismo y el sistema principal receptor. Cuando R1 recibe el mensaje RESV procedente de R3, realiza la reserva entre sí mismo y R3. Ahora, existen en reservas (en dirección al emisor) en el emisor, R1 y R3. Los paquetes pasarán a través de R2 como paquetes normales Best effort. De este modo, se puede utilizar RSVP en una red en la que no todos los direccionadores dan soporte a RSVP.

## Gestor de recursos de circuito virtual

Gestor de recursos de circuito virtual (VCRM) es una característica que se activa cuando RSVP está activado. Basado en la petición de reserva procedente de RSVP, VCRM crea la conexión para el flujo de datos sobre la interfaz física. Para ello, VCRM debe determinar si hay suficiente ancho de banda para albergar la reserva.

**Nota:** Si utiliza interfaces de WAN como Frame Relay o X.25, debe definir la velocidad de línea para que VCRM sepa la cantidad de ancho de banda disponible. El procedimiento para definir la velocidad de línea se describe en los capítulos sobre configuración de interfaz Frame Relay y X.25 del manual *Guía del usuario de software*.

Si un enlace subyacente de la red da soporte al tráfico QoS, como el soporte ATM de SVC QoS, VCRM aprovecha esta capacidad de enlace para establecer un SVC ATM que utilizará el tráfico de datos correspondiente a este flujo. Cundo el enlace subyacente no da soporte a QoS, la planificación del tráfico y los almacenamientos intermedios entre las capas de enlace de datos y red añaden los flujos QoS y los diferencian del tráfico best-effort.

Si un enlace subyacente es un enlace WAN con soporte de DiffServ, VCRM solicitará a DiffServ que asigne el recurso de enlace para los flujos de DOS y que añada las marcas DiffServ TOS como flujos de tráfico a través del dispositivo.

Para obtener más información sobre VCRM, consulte el tema “Configuring and Monitoring VCRM” del manual *Utilización y configuración de las características*.

## Flujos de tráfico y sesiones RSVP

Una vía de acceso del direccionador y el estado dinámico de reserva definen la existencia de una reserva RSVP y que el flujo de tráfico se está transmitiendo de acuerdo con dicha reserva. Una sesión RSVP consta de todos los flujos de tráfico procedentes de uno o más emisores que se envían sobre vías de acceso reservadas a la misma dirección de sesión IP, que puede ser una dirección IP individual o de difusión múltiple. Por ejemplo, en la Figura 41 en la página 483 la sesión incluye los flujos de tráfico entre el emisor S1 y el receptor Rec 1 así como los flujos de tráfico entre el emisor S2 y el receptor Rec 1. Esta sesión se identifica mediante la dirección IP del receptor Rec 1.

Los emisores y receptores mantienen la existencia de cada vía de acceso y reserva de la sesión enviando mensajes de renovación que reafirman la existencia del flujo de tráfico reservado. Estos mensajes de renovación son simplemente copias de los mensajes PATH y RESV. Los temporizadores que se pueden configurar definirán tiempos de espera y harán que los nodos que mantienen el estado dinámico desactiven la reserva si el nodo final no recibe un mensaje de renovación dentro de un periodo de tiempo determinado.

Hay dos tipos de mensajes de desactivación - RSVTEAR y PATHTEAR. El mensaje RSVTEAR, que envía el receptor, desactiva la reserva pero no el flujo de tráfico, que continúa con servicio best-effort. El mensaje PATHTEAR desactiva la vía de acceso entre el emisor y la dirección de la sesión. PATHTEAR desactiva tanto la reserva como el estado dinámico de la vía de acceso. El tráfico Best effort continúa fluyendo.

## Estilos de reservas

La Figura 38 en la página 479 muestra el establecimiento de una reserva RSVP, que reserva enlaces correspondientes a una corriente de tráfico entre un determinado emisor y un determinado receptor. Si varios emisores envían al mismo receptor, habrá varios flujos de tráfico IP, uno entre cada emisor y el receptor. En esta situación, los distintos emisores pueden o no compartir reservas sobre algunos de los enlaces con el receptor, en función del *estilo de reserva* seleccionado.

La Figura 40 muestra dos emisores S1 y S2 para los que el receptor ha solicitado un estilo de reserva de filtro fijo (FF). En este estilo de reserva, cada emisor tiene su propia reserva. El sistema principal S3 no participa en RSVP, pero recibe tráfico Best Effort.

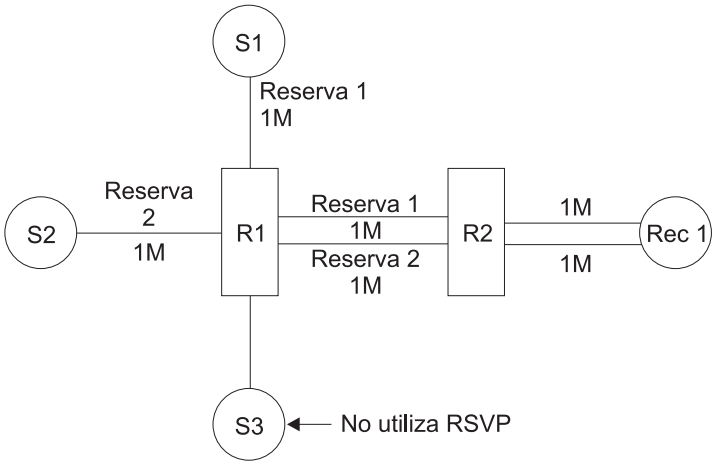



*Figura 40. Estilo de reserva de filtro fijo*

En el estilo de reserva explícita compartida (SE), los emisores identificados como miembros de un determinado grupo pueden compartir parte de los enlaces reservados. El receptor define los emisores de un grupo de acuerdo con la información que los emisores envían en el mensajes PATH, como la dirección IP del emisor. En la Figura 41 en la página 483, el emisor S1 y el emisor S2 han incluido una sesión RSVP que se identifica por la dirección de destino del receptor Rec 1. Los emisores del grupo comparten la reserva en cuanto se fusionan las vías de acceso entre los emisores y el receptor. En este caso, la reserva común se amplía del direccionador R1 al receptor.

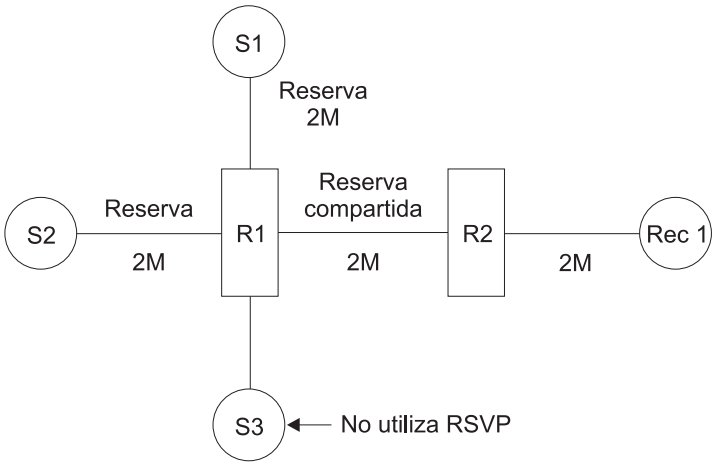



*Figura 41. Estilo de reserva explícita compartida*

En el tercer estilo de reserva, de filtro comodín (WF), todos los emisores que envían mensajes *PATH* a la dirección de la sesión comparten la misma reserva, tal como se ilustra en la Figura 42.

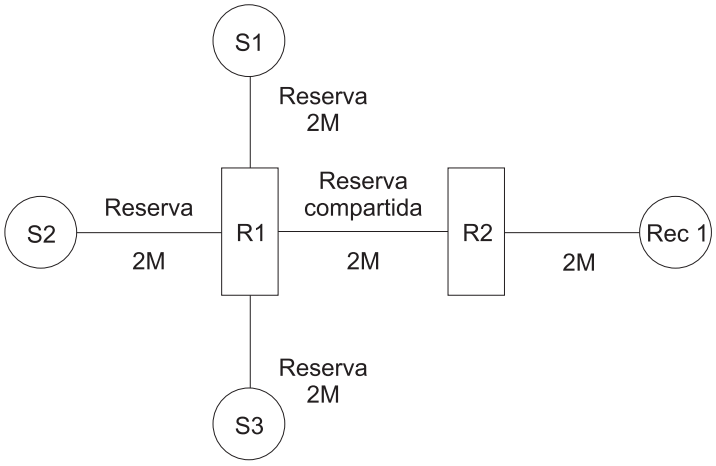



*Figura 42. Estilo de reserva de filtro comodín*

## OPWA

One-Path With Advertising (OPWA) es una característica opcional de RSVP. Permite al receptor obtener un registro de los valores QoS, como ancho de banda, que están disponibles a partir de cada enlace a lo largo de la vía de acceso de reserva. Por ejemplo, si los direccionadores R1 y R3 que se muestran en la Figura 38 en la página 479 están configurados para OPWA, se les notificarán las características de cada enlace. Esta información les permite ajustar la información del mensaje PATH de acuerdo con la capacidad del enlace con la menor cantidad de recursos posible.

Por ejemplo, en el contexto de la Figura 38 en la página 479, supongamos que un emisor empieza a enviar mensajes PATH hacia un receptor a una velocidad media de 1 Mbps y una velocidad punta de 10 Mbps. Supongamos también que el enlace entre R2 y R3 es un enlace PPP con una velocidad de línea de 2 Mbps. OPWA en R2 modificará la velocidad punta del mensaje PATH para que baje a 2 Mbps,

puesto que no hay razón para que los nodos directos reserven una velocidad punta superior a 2 Mbps.

## Tipos de enlaces que reciben soporte de RSVP

Los tipos de enlaces a los que RSVP da soporte incluyen:

- SVC punto a punto ATM.
- Enlaces PPP. RSVP da soporte a PPP sobre todos los tipos de enlaces soportados, como V.35, T1/E1 e ISDN, que se basan en una conexión permanente. Los enlaces utilizados en marcación bajo demanda, restauración de WAN, modalidad de retención corta o en configuraciones de equilibrio de cargas no se deben utilizar para RSVP.
- PVC Frame Relay. Al igual que con PPP, todos los tipos de enlaces soportados darán soporte a RSVP, pero sólo los enlaces que se basan en una conexión permanente se deben utilizar para RSVP. Los enlaces utilizados en marcación bajo demanda, restauración de WAN, modalidad de retención corta o en configuraciones de equilibrio de cargas no se deben utilizar con RSVP.
- SVC Frame Relay. Recibe el mismo soporte que PVC Frame Relay; es decir, RSVP no puede definir distintos DLCI para el tráfico QoS, pero utilizará parte del DLCI por omisión para la asignación de ancho de banda de QoS.
- Todos los enlaces de LAN:
  - Ethernet
  - Red en anillo

  **Nota:** Para redes de soporte compartido como LAN, se necesitan otros métodos, como diseño de tráfico para coordinar la compartición del ancho de banda de la LAN. RSVP controla el uso del ancho de banda de un determinado direccionador, pero no coordina el uso del ancho de banda de la LAN por parte de diversos direccionadores y sistemas principales.
- X.25. Reciben el mismo soporte que PPP o PVC Frame Relay. RSVP no puede definir distintos VC para el tráfico QoS; utiliza parte del VC por omisión para la asignación de ancho de banda de QoS.

**Notas:**

1. RSVP se direcciona de acuerdo con las tablas normales de direccionamiento IP. No aprovecha el Protocolo de direccionamiento del siguiente salto (NHRP) en ATM porque NHRP utiliza la antememoria de reenvío de vía de acceso rápida de IP, no el direccionamiento IP, para realizar un seguimiento de sus rutas.
2. Para evitar conflictos, RSVP se desactiva en enlaces PPP o FR que se han configurado para el Sistema de reserva de ancho de banda (BRS).
3. RSVP puede utilizar las funciones de planificación y gestión de colas DiffServ con enlaces PPP o FR que se han configurado para DiffServ.

## Configuración de ejemplo

Como guía para configurar RSVP, se incluye un ejemplo de configuración de interfaz de línea de mandatos talk 6. consulte el tema “Configuración y supervisión de RSVP” en la página 489 para ver descripciones de los mandatos y parámetros de RSVP. Los pasos siguientes describen una configuración de ejemplo de RSVP:

1. Active RSVP en el direccionador mediante el mandato de talk 6 **enable rsvp** desde el indicador `RSVP config>`. RSVP sólo se puede activar en interfaces configuradas para IP. Este mandato define para los parámetros del direccionador RSVP valores por omisión, e incluye 0 como el ancho de banda por omisión en las interfaces. Tendrá que activar interfaces determinadas y definir en las mismas en ancho de banda para que RSVP se pueda ejecutar sobre dichas interfaces.
2. Utilice el mandato **enable interface** para activar cada interfaz para RSVP.
3. Utilice el mandato de talk 5 **reset interface** si desea que RSVP entre en vigor de inmediato en esta interfaz.
4. Se le solicitará que defina el ancho de banda para cada interfaz. Si para el ancho de banda de una determinada interfaz se deja el valor 0 (el valor por omisión), no se pueden hacer reservas RSVP sobre dicha interfaz.
5. Utilice el mandato **enable opwa-all** si desea activar OPWA en todas las interfaces con soporte de RSVP. Utilice el mandato **enable opwa** y el número de interfaz si desea activar OPWA en una interfaz. Asegúrese de activar RSVP sobre la interfaz antes de activar OPWA. Si intenta activar OPWA sobre una interfaz que aún no se ha activado para RSVP, aparecerá el mensaje `Cannot find RSVP i/f rec`.
6. Los demás parámetros son opcionales y RSVP se puede ejecutar con valores por omisión.
7. Si lo desea, puede utilizar los mandatos **add sender** y **add receiver** para crear emisores o receptores estáticos para el direccionador. El emisor y receptor estáticos generarán señalización RSVP para una aplicación de sistema principal que no utilice RSVP. La dirección IP del puerto configurado para el emisor y receptor estáticos identifica el origen y el destino del flujo de tráfico IP por el que el direccionador enviará mensajes RSVP. Si no se ha configurado ningún emisor ni receptor estático, el direccionador reenvía mensajes RSVP y establece enlaces de reserva, pero no origina mensajes RSVP. Consulte el tema “Configuración de ejemplo de un emisor y receptor estáticos” en la página 486 para obtener más información.

**Ejemplo:**

```
Config> protocol rsvp
Resource ReSerVation Protocol config console
RSVP Config> enable rsvp
RSVP Config> enable interface
Interface [0]?
Creating RSVP i/f record...
Set Link Reservable Bandwidth (bits) [0]? 5000000

Interface enabled.
  To take effect immediately, use talk-5 RSVP's 'reset interface'
RSVP Config> enable interface
Interface [0]? 1
Creating RSVP i/f record...
Set Link Reservable Bandwidth (bits) [0]? 1024000

Interface enabled.
    To take effect immediately, use talk-5 RSVP's 'reset interface'
RSVP Config>enable opwa
Interface [0]?
Controlled Load installed on interface 0
take effect immediately?(Yes or [No]): y
RSVP Config>enable opwa
Interface [0]? 1
Controlled Load installed on interface 1
take effect immediately?(Yes or [No]): y
Interface enabled.

RSVP Config>list interface

RSVP Interfaces:

If      IP address   RSVP-enabled  Encaps.  max_res_bw SRAM_rec
0       5.0.31.5        Y          IP       5000000      1
1       5.0.31.3        Y          IP       1024000      2

RSVP Config>list opwa

OPWA configuration:

Network OPWA    CTL-LOAD
0       Y       Y
1       Y       Y
```

Una vez finalizada la configuración, puede activar RSVP con los mandatos de talk 5 **reset rsvp** o **reset interface** o volviendo a arrancar el direccionador.

## Configuración de ejemplo de un emisor y receptor estáticos

Si configura RSVP tal como se describe en el tema “Configuración de ejemplo” en la página 485, aplicaciones con soporte de RSPV de sistemas principales que estén conectados al direccionador establecerán de forma dinámica flujos de tráfico RSVP y sesiones. Cuando hay una aplicación de sistema principal que no da soporte a RSVP y que envía paquetes a un puerto y dirección IP conocidos, se puede configurar un emisor y receptor estáticos para que el direccionador genere señalización RSVP correspondiente a este flujo.

Primero, configure el emisor mediante el mandato **add sender** desde el indicador `RSVP config>`.

```
Config> protocol rsvp
Resource ReSerVation Protocol config console
RSVP Config> add sender
Session> IP Address: [0.0.0.0]? 5.0.31.1  1
Session> Port Number: [1]? 5004
Session> Protocol Type (UDP/TCP): [UDP]?
Sender> IP Address: [0.0.0.0]? 5.0.27.27  2
Sender> Src Port: [1]? 5005
Tspec> Peak Rate (in byte/sec) [250000]? 25000
Tspec> Average Rate (in byte/sec) [200000]? 20000
Tspec> Burst Size (in bytes) [2000]?
Tspec> Max. Pkt Size [1500]?
Tspec> Min Pkt Size [53]?
```

**1** Si el flujo de tráfico es de difusión individual, la dirección IP de la sesión es la dirección de difusión individual del receptor del flujo de tráfico IP. Si el flujo de tráfico es de difusión múltiple, la dirección IP de la sesión es la dirección de difusión múltiple del destino del flujo de tráfico IP.

**2** La dirección IP del emisor es la dirección de difusión individual del emisor del flujo de tráfico IP. Si el emisor y el receptor no son direccionadores, son sistemas principales que están conectados a direccionadores. Los direccionadores en este caso actúan como proxies para los sistemas principales.

Después de utilizar el mandato **list sender** para comprobar que se han configurado los valores correctos, puede configurar un receptor estático en un segundo direccionador remoto que actuará como receptor. En el ejemplo, el direccionador emisor tiene la dirección IP 5.0.27.27 y el direccionador receptor tiene la dirección IP 5.0.31.1. Para configurar el receptor estático, utilice el mandato **add receiver**.

```
RSVP Config>add receiver
RESV requestor IP Address: [0.0.0.0]? 5.0.31.1
Session> IP Address: [5.0.31.1]?  1
Session> Port Number: [1]? 5004
Session> Protocol Type (UDP/TCP): [UDP]?
Style> (WF, FF, SE): [FF]? wf  2
Need confirmation?(Yes or [No]):
Service Type: CTL-LOAD
Tspec> Peak Rate (in byte/sec) [250000]? 5000
Tspec> Average Rate (in byte/sec) [200000]? 20000
Tspec> Burst Size (in bytes) [2000]?
Tspec> Max. Pkt Size [1500]?
Tspec> Min Pkt Size [53]?
```

**1** Observe que la dirección de sesión IP, puerto y protocolo del receptor coinciden con la dirección de sesión IP, puerto y protocolo del emisor. El emisor y el receptor deben identificar el mismo flujo de tráfico. El receptor, no el emisor, determina qué ancho de banda intentarán establecer en cada enlace los direccionadores de la vía de acceso.

**2** Las letras *wf* significan filtro comodín. Es uno de los tres estilos de reserva de RSVP. Consulte el tema “Estilos de reservas” en la página 482 para obtener más información.

# Configuración y supervisión de RSVP

Este capítulo describe cómo configurar y reservar el Resource ReSerVation Protocol (RSVP) y cómo utilizar los mandatos de supervisión de RSVP. Incluye las siguientes secciones:



## Cómo acceder al entorno de configuración de RSVP

Para acceder al entorno de configuración de RSVP, entre el siguiente mandato en el indicador `Config>`:

```
Config> protocol rsvp
Resource ReSerVation Protocol config console
RSVP Config>
```

## Mandatos de configuración de RSVP

Esta sección describe los mandatos de configuración de RSVP. Entre estos mandatos en el indicador `RSVP Config>`.

*Tabla 29. Resumen de mandatos de configuración de RSVP*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxxi. |
| Add | Añade emisores y receptores. |
| Delete | Suprime emisores y receptores. |
| Disable | Desactiva RSVP u One-Path With Advertising (OPWA). |
| Enable | Activa RSVP u One-Path With Advertising (OPWA). |
| List | Muestra información sobre la configuración de RSVP. |
| Set | Define parámetros del sistema RSVP. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxii. |

## Add

Utilice el mandato **add** para añadir emisores y receptores RSVP estáticos al direccionador. Los emisores y receptores estáticos permiten al direccionador enviar o recibir mensajes RSVP. En la mayoría de los casos, si el direccionador envía o recibe mensajes RSVP, actúa como un proxy en nombre de una aplicación del sistema principal que no está configurada para RSVP. La dirección IP del emisor, en este caso, es la dirección de la aplicación del sistema principal y la dirección IP de la sesión es la dirección de destino del flujo de datos. Si no hay ningún emisor o receptor estático configurado para el direccionador, este reenvía mensajes RSVP de forma dinámica, define reservas y ofrece QoS, pero no origina mensajes RSVP.

Las definiciones de emisores y receptores se guardan en la configuración como registros SRAM numerados. El mandato **activate** de talk 5 sirve para activar cada registro.

**Sintaxis:**

| | |
|---|---|
| a**dd** | sender ... |
| | receiver ... |

**sender**
Palabra clave que sirve para especificar que los parámetros que vienen a continuación se aplican al emisor del mensaje *path* de RSVP.

**receiver**
Palabra clave que sirve para especificar que los parámetros que vienen a continuación se aplican al receptor, el cual devuelve el mensaje *resv* de RSVP al emisor.

La mayoría de los siguientes parámetros se especifican tanto para el emisor como para el receptor. Los parámetros que son exclusivos del emisor o del receptor se identifican en sus descripciones.

**session-ip-address**
Es la dirección IP de destino de difusión individual o de difusión general de los flujos de datos IP procedentes de uno o más emisores. Cuando los flujos de tráfico son de difusión individual, esta dirección es la dirección del receptor; cuando los flujos de tráfico son de difusión múltiple, esta dirección es una dirección de difusión múltiple; el receptor debe ser miembro del grupo identificado por la dirección de difusión múltiple. Los emisores y el receptor utilizan la dirección IP de sesión junto con el número de puerto de sesión y el protocolo para identificar la sesión RSVP en la que se establece QoS.

**Valores válidos**: Direcciones IPv4 válidas. No puede ser 0.0.0.0. Cuando RSVP está activo, el emisor y el receptor deben ser capaces de acceder a esta dirección.

**Valor por omisión**: ninguno

**session-port**
El número de puerto IP de la sesión que va a reservar RSVP. Es el número de puerto UDP o el número de zócalo TCP de la aplicación de destino.

**Valores válidos**: 0 - 65535

**Valor por omisión**: 1

**session-protocol**
UDP o TCP.

**Valores válidos**: UDP o TCP

**Valor por omisión**: UDP

**sender-ip-address**
La dirección del emisor, que es la aplicación emisora que origina el flujo de datos que se va a reservar. Este parámetro debe ser una dirección de difusión individual.

**Valores válidos**: Direcciones IPv4 válidas.

**Valor por omisión**: ninguno

**sender-port**
El número de puerto IP del emisor del flujo IP que se va a reservar para QoS. Es el número de puerto UDP o el número de zócalo TCP de la aplicación emisora.

**Valores válidos**: 0 - 65535

**Valor por omisión**: 1

**receiver-ip-address**
La dirección IP del receptor que emite el mensaje *resv*. En el caso de una sesión de difusión individual, esta dirección es la misma que la dirección IP de la sesión. En el caso de una sesión de difusión múltiple, esta dirección es la dirección de difusión individual de la aplicación que realiza la reserva para la dirección de la sesión de difusión múltiple. Si es una sesión de difusión múltiple, el receptor debe pertenecer al grupo de difusión múltiple representado por esta dirección de difusión múltiple.

**Valores válidos**: Direcciones IPv4 válidas.

**Valor por omisión**: ninguno

**peak-rate**
Especifica la velocidad punta de datos de la sesión IP. Esta velocidad se define como la velocidad de generación de tráfico punta del emisor, si se conoce y se controla, la velocidad de línea de la interfaz física, si se conoce, o infinito (X'FFFFFFFF', decimal 4 294 967 295) si no se dispone de otro valor mejor. La velocidad de tráfico punta debe ser mayor o igual que la velocidad media de tráfico.

Si el receptor solicita una velocidad de datos punta distinta de la velocidad que ofrece el emisor, el direccionador intenta cumplir la petición del receptor.

**Valores válidos**: 1 - 4 294 967 295 bytes/segundo

**Valor por omisión**: 250 000

**average-rate**
Especifica la velocidad media de datos que el emisor debe enviar o que el receptor debe recibir en la sesión IP. Esta velocidad se define como la velocidad media de generación de tráfico del emisor, si se conoce y se controla, como la velocidad de línea de la interfaz física, si se conoce, o 200 000 bytes/segundo por omisión.

Si el receptor solicita una velocidad media diferente de la que ofrece el emisor, el direccionador intenta cumplir la petición del receptor.

**Valores válidos**: 1 - 4 294 967 295 bytes/segundo

**Valor por omisión**: 200 000

**data-burst-size**
Especifica el número de bytes que se pueden enviar sin tener en cuenta la velocidad punta ni la velocidad media. Por ejemplo, si la velocidad punta es 50 000 bytes/segundo, y el tamaño de ráfaga de datos es 2000, se pueden enviar 2000 bytes en una determinada instancia, aunque la ráfaga haga que la velocidad punta supere los 50 000 bytes/segundo en esta instancia.

Si el receptor solicita una velocidad distinta a la del emisor, el direccionador intenta cumplir la petición del receptor.

**Valores válidos**: 1 - 4 294 967 295 bytes

**Valor por omisión**: 2000

**max-packet-size**

Especifica el tamaño máximo de paquete que el emisor enviará en el flujo IP o que el receptor recibirá del flujo IP. Para el emisor, este valor se debe definir como el tamaño del paquete mayor generado por la aplicación emisora. Para el receptor, se debe definir como la MTU de vía de acceso de menor tamaño, que el receptor aprende de la información que llega en paquetes One-Path With Advertisement (OPWA) de RSVP o por otro método.

Si el tamaño máximo de paquete es superior que la MTU de un enlace de la vía de acceso, la petición de reserva se rechazará en este punto. Por ejemplo, si un enlace de la vía de acceso de reservas tiene una MTU igual a 1500 y el tamaño máximo de paquete solicitado es 2000, la petición de reserva se rechazará.

Si el receptor solicita un tamaño máximo de paquete distinto al del emisor, el direccionador intenta cumplir la petición del receptor.

El tamaño máximo de paquete se debe configurar con un valor no inferior que el tamaño mínimo de paquete. Por ejemplo, si el tamaño mínimo de paquete es 64 bytes, el tamaño máximo de paquete debe ser igual o superior a 64 bytes.

**Valores válidos**: 1 - 4 294 967 295 bytes

**Valor por omisión**: 1500

**min-packet-size**

Especifica el tamaño mínimo de paquete que el emisor enviará en el flujo IP o que el receptor recibirá del flujo IP. Para el emisor, este valor se debe definir como el tamaño del paquete menor generado por la aplicación emisora.

Este tamaño de paquete no debe superar el tamaño máximo de paquete. Por ejemplo, si el tamaño máximo de paquete es 1500 bytes, el tamaño mínimo de paquete debe ser igual o inferior a 1500. Este tamaño de paquete incluye datos de la aplicación y todas las cabeceras de protocolo al nivel IP o superior, como IP, TCP o UDP, pero no incluye ninguna cabecera a nivel de enlace.

**Nota:** Este valor sirve para estimar la actividad generan de reserva de recursos. Cuanto menor es el tamaño mínimo de paquete, mayor es la actividad general de reserva.

**Valores válidos**: 1 - 4 294 967 295 bytes

**Valor por omisión**: 48

**reservation-style**

Este parámetro sólo se configura para receptores. Especifica el estilo de reserva que el receptor recibirá en el flujo IP. Una reserva RSVP garantiza un manejo especial de los paquetes de un flujo de tráfico IP a fin de ofrecer una determinada QoS sobre cada enlace o serie de enlaces que forman una vía de acceso entre el emisor y el receptor. Los tres estilos de reserva que se ofrecen son los siguientes:

**Filtro fijo (FF)**

Especifica que el receptor recibirá tráfico de datos de un determinado emisor en el flujo IP. Se establece una reserva por emisor.

**Explícita compartida (SE)**
Especifica que el receptor recibirá tráfico de datos procedente de un grupo de emisores del mismo grupo, que define el receptor. Los miembros de este grupo comparten la reserva. Cada emisor del grupo puede compartir la reserva en cuanto su enlace se fusiona en una vía de acceso común hacia el receptor.

**Filtro comodín (WF)**
Especifica que el receptor recibirá tráfico de datos procedente de todos los emisores. Cada emisor puede compartir la reserva en cuanto su enlace se fusiona en una vía de acceso común hacia el receptor.

Consulte el tema “Estilos de reservas” en la página 482 para obtener más información.

**Valores válidos**: FF, SE y WF

**Valor por omisión**: FF

**confirm-reservation**
Especifica si el receptor desea recibir un mensaje *reservation confirm*. Este mensaje se envía de nuevo al receptor que envió el mensaje resv cuando la petición se fusiona en una reserva mayor existente o se distribuye a la aplicación emisora.

**Valores válidos**: Yes o No

**Valor por omisión**: No

## Delete

Utilice el mandato **delete** para suprimir un emisor o un receptor.

**Sintaxis:**

de**lete**
sender *registro-sram*
receiver *registro-sram*

**sender o receiver** *registro-sram*
Cada emisor o receptor se identifica mediante un registro SRAM que se muestra cuando utiliza el mandato **delete**. Si entra el número de registro SRAM del emisor o receptor a suprimir, se suprime dicho emisor o receptor de la configuración.

## Disable

Utilice el mandato **disable** para desactivar RSVP u OPWA en una interfaz o en todas las interfaces.

**Sintaxis:**

di**sable**
interface
opwa
opwa-all
rsvp

**interface** *número-interfaz*
Desactiva la función RSVP en una determinada interfaz. Los mensajes de control de RSVP pueden fluir sobre esta interfaz, pero no se realizará ninguna reserva RSVP en esta interfaz. Este mandato también desactiva la posibilidad de esta interfaz de definir QoS.

**Valores válidos**: Cualquier número de interfaz válido.

**Valor por omisión**: 0

**OPWA** *número-interfaz*
Desactiva OPWA en una determinada interfaz.

**Valores válidos**: Cualquier número de interfaz válido.

**Valor por omisión**: 0

**OPWA-all**
Desactiva OPWA en todas las interfaces.

**RSVP** Desactiva la función RSVP dentro del direccionador. Por omisión, RSVP está desactivado.

## Enable

Utilice el mandato **enable** para activar RSVP u OPWA en una interfaz o en todas las interfaces.

**Sintaxis:**

**enable**
interface
opwa
opwa-all
rsvp

**interface** *número-interfaz*
Activa la función RSVP en una determinada interfaz. Este mandato permite a esta interfaz responder a mensajes RSVP y reenviarlos, pero no originarlos. Tiene que configurar emisores y receptores estáticos para originar mensajes RSVP.

Se le solicitará que defina el ancho de banda en la interfaz activada. También puede utilizar el mandato **set bandwidth** posteriormente para modificar el valor de ancho de banda. Este mandato sólo funciona si el direccionador da soporte a RSVP y la interfaz especificada está activada y configurada para IP.

Consulte el tema “Tipos de enlaces que reciben soporte de RSVP” en la página 484 para ver una lista de enlaces que dan soporte a RSVP.

**Valores válidos**: Cualquier número de interfaz válido.

**Valor por omisión**: 0

**OPWA** *número-interfaz*
Activa OPWA en una determinada interfaz. OPWA indica al receptor si la vía de acceso entre el emisor y el receptor se puede reservar en cada salto y la cantidad de ancho de banda disponible en cada salto de la vía de acceso. Esta operación sólo está permitida si la interfaz da soporte a RSVP.

**Valores válidos**: Cualquier número de interfaz válido.

**Valor por omisión**: 0

**OPWA-all**

Activa OPWA en todas las interfaces. RSVP debe estar activado en el direccionador para que este mandato tenga efecto.

**RSVP** Activa la función RSVP dentro del direccionador. Si es la primera vez que se activa RSVP, se inicializarán también una serie de parámetros por omisión correspondientes a RSVP.

El habilitar RSVP no lo activa. Para activar RSVP en este direccionador, tiene que utilizar el mandato **set bandwidth** para definir el ancho de banda en al menos una interfaz que vaya a utilizar RSVP. Luego tiene que volver a arrancar el direccionador para RSVP. Para ello, puede utilizar el mandato **reset rsvp** de talk 5 o puede volver a arrancar el direccionador. Consulte el mandato **reset rsvp** de talk 5 para obtener más información.

## List

Utilice el mandato **list** para visualizar parámetros de RSVP. Estos grupos de parámetros se pueden listar por separado:

- Todos los parámetros
- Parámetros de interfaz
- Valores de OPWA correspondientes a todas las interfaces
- Registros del receptor o del emisor
- Parámetros RSVP a nivel de sistema

**Nota:** El mandato **list** lista los registros los emisores y receptores configurados. Estos registros no identifican los flujos de tráfico RSVP activos, que se definen mediante la dirección del emisor y la dirección del receptor. Utilice el mandato **show rsvp flows** de talk 5 para ver los flujos RSVP actualmente activos.

**Sintaxis:**

**list ...**
all
interface
opwa
receiver
sender
system

**Ejemplo:**

```
RSVP Config>list all

Software Version:

RSVP Control: IBM RSVP Router Release 1.0 (RFC 2205)


RSVP Configuration:

RSVP Status:                    Enabled
Maximum RSVP Msg Size:          1500 (bytes)
Refresh Interval:               30 (sec)
Allowed Successive Msg Loss:    3 (frame)
Flow Life-Time:                 158 (sec)
Refresh Slew Max:               30 (percent)
Total system reservable b/w:    4294967 (kbps)

RSVP Interfaces:

If      IP address   RSVP-enabled  Encaps.  max_res_bw SRAM_rec
0       5.0.27.2        Y          IP       5000000      1
5       5.0.28.2        Y          IP       8000000      2
4       5.0.25.101      Y          IP       1024000      3
2       5.0.45.2        Y          IP       1024000      4

OPWA configuration:

Network OPWA    CTL-LOAD
0       Y       Y
5       Y       Y
4       Y       Y
2       Y       Y

Following senders/receivers are defined in SRAM:
Rec.No   Type     DestAddr [1]      Dest Port   Protocol   Src Addr        Src Port

1    Sender(PATH) 5.0.25.100      25          17         5.0.25.101      25
2    Receiv(RESV) 5.0.25.101      26          17         0.0.0.0         0
```

**1** La dirección de destino que se visualiza es la dirección de la sesión IP. Consulte el mandato **add session-ip-address** de talk 6 para ver la definición de la dirección de sesión IP.

## Set

Define los parámetros del sistema RSVP. Consulte el ejemplo del mandato **list all** de talk 6 para ver algunos valores típicos de estos parámetros.

**Sintaxis:**

**set ...**
- allowed-successive-msg-loss ...
- bandwidth ...
- default
- encapsulation ...
- lifetime ...
- max-msg-size ...
- refresh-interval ...
- slew ...
- total ...

**allowed-successive-msg-loss** *pérdidas-mens*

Este parámetro define el número de mensajes de renovación path y resv correspondiente sucesivos que se pueden perder antes de que RSVP considere que ha transcurrido el tiempo de espera de la vía de acceso y se defina el estado de reserva para el flujo de tráfico RSVP. Cuando transcurre el tiempo de espera de RSVP de la vía de acceso y se define el estado de reserva para un determinado flujo de tráfico, dicho flujo deja de suministrar QoS. El emisor y el receptor tienen que volver a establecer la reserva.

**Valores válidos**: 1 - 9999

**Valor por omisión**: 3

**bandwidth** *interfaz bps*

Este parámetro define el ancho de banda que se puede reservar de una interfaz. Normalmente, el ancho de banda que se puede reservar es una pequeña parte del ancho de banda total del enlace. Un valor recomendable es uno inferior al 30%. El ancho de banda que se puede reservar sólo se puede definir en una interfaz que dé soporte a RSVP.

Este mandato de talk 6 puede entrar en vigor de forma inmediata y de forma dinámica sin que afecte a los valores de otros parámetros.

**interfaz**

Número de interfaz de red.

**Valores válidos**: Cualquier número de interfaz de red válido.

**Valor por omisión**: 0

**bps** Bits por segundo (bps) de ancho de banda que se puede reservar en esta interfaz.

**Valores válidos**: 1 - 4 294 967 295 bps (representa cantidad ilimitada)

**Valor por omisión**: 0

**default**

Este parámetro define para todos los parámetros de RSVP su valor por omisión original que se establece al utilizar el mandato **enable rsvp**. El mandato **set default** altera temporalmente cualquier valor de parámetro configurado anteriormente en cada una de las interfaces. Puesto que el valor por omisión de ancho de banda de cada interfaz es 0, lo que significa que no se establecerán reservas RSVP en dicha interfaz, tiene que utilizar el mandato **set bandwidth** para cada interfaz que utilice RSVP para preparar RSVP para que vuelva a funcionar.

**encapsulation** *interfaz estilo*

Este parámetro define el estilo de encapsulado de mensajes RSVP en una interfaz, que puede ser IP, UDP o Both. Normalmente, los mensajes de control de RSVP, como los mensajes path y resv, se encapsulan en tramas IP nativas con el tipo de protocolo 46. En el caso de que un sistema principal conectado a este direccionador sólo pueda utilizar paquetes UDP para enviar los mensajes RSVP, el estilo de encapsulado sobre la interfaz que se conecta a este sistema principal debe ser UDP. Si algunos sistemas principales que utilizan IP y algunos que utilizan UDP envían mensajes RSVP sobre el mismo enlace, debe definir para el estilo de encapsulado el valor Both. Esta operación sólo se permite si RSVP está activado en la interfaz especificada.

Este mandato de talk 6 puede entrar en vigor de forma inmediata y de forma dinámica sin que afecte a los valores de otros parámetros.

**interfaz**
Número de interfaz de red.

**Valores válidos**: Cualquier número de interfaz de red válido.

**Valor por omisión**: 0

**estilo**
Estilo de encapsulado de los mensajes RSVP.

**Valores válidos**: IP, UDP o Both

**Valor por omisión**: IP

**lifetime**
Este parámetro define el tiempo de vida en segundos de una vía de acceso y estado de reserva, que mantiene un flujo de tráfico RSVP establecido. Este tiempo debe ser lo suficientemente largo para que RSVP observe el número de pérdidas de mensajes de renovación que se especifica mediante el valor del parámetro de pérdidas permitidas de mensajes sucesivos. Para calcular aproximadamente este tiempo, utilice esta fórmula: 1,5 x refresh-interval x (allowed-successive-msg-losses + 0,5).

Si transcurre el tiempo de espera del estado de reserva, pero no el estado de vía de acceso, la reserva se elimina y el flujo de tráfico IP continúa con servicio best effort. Si transcurre el tiempo de espera del estado de vía de acceso, tanto la reserva como el flujo de tráfico IP finalizan.

Este mandato de talk 6 puede entrar en vigor de forma inmediata y de forma dinámica sin que afecte a los valores de otros parámetros. Se espera que el valor por omisión de este parámetro funcione sin modificación.

**Valores válidos**: 1 - 2 147 483 647 segundos

**Valor por omisión**: 158 segundos

**max-msg-size**
Este parámetro define el tamaño máximo general de mensajes de control de RSVP del direccionador. Este valor no puede ser superior al menor de los tamaños de MTU que reciben soporte de las interfaces con soporte de RSVP de la vía de acceso. Se espera que el valor por omisión de este parámetro funcione sin modificación.

**Valores válidos**:64 - 2 147 483 647 bytes (representa cantidad ilimitada)

**Valor por omisión**: 1500 bytes

**refresh-interval**
Este parámetro define el intervalo de tiempo en segundos que transcurre entre mensajes de renovación para mantener una vía de acceso y un estado de reserva (un flujo de tráfico RSVP) entre el receptor y el emisor.

**Valores válidos**: 10 - 600 segundos

**Valor por omisión**: 30 segundos

**slew-max**
Este parámetro limita cuánto se puede modificar el intervalo de renovación dentro de un ciclo de renovación. Se espera que el valor por omisión de este parámetro funcione sin modificación. Sin embargo, es posible que tenga que modificar el valor de este parámetro para evitar errores de sincronización.

Por ejemplo, si slew-max es 30% y el intervalo de renovación es 30 segundos, puede modificar el intervalo de renovación un máximo de 9 segundos (30% of 30) dentro de un intervalo de renovación. Para realizar un cambio mayor, debe cambiar el intervalo de renovación por segunda vez. Por ejemplo, cuando el intervalo de renovación sea 39, puede sumarle o restarle 11 dentro de un intervalo de renovación. También puede aumentar slew-max y luego realizar el cambio. Por ejemplo, si el intervalo de renovación es 30 y desea cambiarlo por 50, puede primero aumentar slew-max al 70% (lo que le ofrece la posibilidad de sumar o restar 21 a 30) y luego aumentar el intervalo de renovación a 50.

Este mandato de talk 6 puede entrar en vigor de forma inmediata y de forma dinámica sin que afecte a los valores de otros parámetros.

**Valores válidos**: 0 - 100%

**Valor por omisión**: 30%

**total**

Puesto que la suma de anchos de banda de enlaces de todas las interfaces puede ser superior al rendimiento total del direccionador, es posible que tenga que definir un límite en el ancho de banda total que se puede reservan del direccionador. Por ejemplo, la suma de anchos de banda de la suma de enlaces puede ser de 250.000.000 bps, mientras que el rendimiento total del direccionador puede ser de 200.000.000 bps. Si el ancho de banda total que se puede reservar se define en 200.000.000 bps y hay 200.000.000 bps actualmente reservados entre todas las interfaces, no se pueden establecer más reservas IP de RSVP hasta que se elimine alguna.

Este mandato de talk 6 puede entrar en vigor de forma inmediata y de forma dinámica sin que afecte a los valores de otros parámetros.

**Valores válidos**: 1 a 4 294 967 295 bps

**Valor por omisión**: 4 294 967 295 bps (representa cantidad ilimitada)

## Cómo acceder al entorno de supervisión de RSVP

Para acceder al entorno de supervisión de RSVP, escriba **t 5** en el indicador OPCON (*):

```
* t 5
```

Luego, entre el siguiente mandato en el indicador **+**:

```
+ protocol rsvp
RSVP>
```

## Mandatos de supervisión de RSVP

Esta sección describe los mandatos de supervisión de RSVP. Entre estos mandatos en el indicador RSVP>.

| *Tabla 30. Resumen de mandatos de supervisión de RSVP* | |
|---|---|
| Mandato | Función |
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Activate | Activa un emisor o receptor definido de forma estática. |
| List | Lista información de RSVP. |
| Reset | Restablece de forma dinámica RSVP y características de RSVP. |
| Send | Envía varios mensajes RSVP, que incluyen *data-packet, ip ping, path, ptear, resv* y *rtear*. |
| Show | Muestra información sobre los flujos RSVP activos. |
| Stop-RSVP | Detiene la función RSVP en el direccionador. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Activate

Utilice el mandato **activate** para activar de forma dinámica un emisor o receptor configurado.

**Sintaxis:**

a**ctivate**
*número-registro*

Este mandato le permite activar de forma dinámica emisores y receptores definidos mediante los mandatos de talk 6 **add sender** y **add receiver** y que se han habilitado con el mandato adecuado de talk 6 **enable**.

**número-registro**

Al utilizar el mandato **activate**, se mostrarán los emisores y receptores configurados y actualmente habilitados y cada uno se identificará mediante un número de registro. El especificar un número de registro, dicho receptor o emisor se activará de forma automática. Un emisor o receptor activado se puede detener en talk 5 mediante el mandato **send ptear**, **send rtear** o **reset rsvp** o volviendo a arrancar el direccionador.

Para obtener información sobre cómo configurar emisores y receptores estáticos, consulte el tema “Mandatos de configuración de RSVP” en la página 489 para ver una descripción de los mandatos de talk 6 **add sender**, **add receiver** y **enable**.

## List

Utilice el mandato **list** para visualizar información sobre la configuración de RSVP que se está ejecutando.

**Nota:** Utilice el mandato de talk 5 **show rsvp flow** para ver los flujos de tráfico RSVP existentes.

**Sintaxis:**

**list** interface
opwa
sender/receiver-records-in-sram
system

**interface** Este mandato muestra interfaces RSVP y su estado actual. El estado *bwCtrl* indica un enlace que se encuentra bajo control del ancho de banda de RSVP; se puede reservar ancho de banda en esta interfaz para QoS de RSVP. El estado *notCnf* indica un enlace que no está configurado para RSVP. El estado *up* indica que hay un enlace configurado para RSVP, pero el ancho de banda se encuentra bajo el control de la función QoS a nivel de enlace (como por ejemplo la característica Differentiated Services).

**Ejemplo:**

```
RSVP> list int

RSVP Interfaces:

If      IP address      b/w(K)  res'able  curr-res     state
0/Eth   5.0.27.2        10000   5000      0      Kbps  bwCtrl
2/PPP   5.0.45.2        0       1024      0      Kbps  notCnf
4/PPP   5.0.25.101      2048    1024      0      Kbps  up
 5/TKR   5.0.28.2        16000   8000      0      Kbps  bwCtrl
```

**opwa** Este mandato muestra interfaces RSVP y su estado OPWA actual.

**Ejemplo:**

```
RSVP>list opwa

OPWA running configuration
Network OPWA    CTL-LOAD
0       Y       Y
2       Y       Y
4       Y       Y
5       Y       Y
```

**sender/receiver-records-in-sram**
Este mandato muestra la lista de emisores y receptores que se han configurado de forma estática.

**Ejemplo:**

```
RSVP> list sender

Following senders/receivers are defined in SRAM:
Rec.No   Type     DestAddr       Dest Port   Protocol   Src Addr        Src Port
1    Sender(PATH) 5.0.25.100      25         17         5.0.25.101      25
2    Receiv(RESV) 5.0.25.101      26         17         0.0.0.0         0
3    Receiv(RESV) 5.0.25.101      5006       17         0.0.0.0         0
```

**system** Este mandato muestra los valores actualmente en vigor de los parámetros del sistema RSVP, que serán distintos de los de SRAM si alguno de ellos se ha modificado de forma dinámica mediante mandatos de talk 5.

**Ejemplo:**

```
RSVP> list system

RSVP running configuration:
RSVP Status:                    Running
Current Existing Flows:         0
Current Existing Sessions:      0
Maximum RSVP Msg Size:          1500 (bytes)
Refresh Interval:               30 (sec)
Allowed Successive Msg Loss:    3 (frame)
Flow Life-Time:                 158 (sec)
Refresh Slew Max:               30 (percent)
System resv Max:                unlimited
System current resv:            0 (kbps)
```

## Reset

Utilice el mandato **reset** para restablecer diversos aspectos de la configuración de RSVP. El mandato **reset** prevalece sobre cualquier parámetro configurado de forma dinámica mediante mandatos de talk 5 y sustituye a los últimos valores configurados mediante mandatos de talk 6.

**Sintaxis:**

**reset**
- interface
- queue-stat
- rsvp
- system-parameters

**interface** Actualiza los parámetros de interfaz de RSVP con los datos de configuración guardados en SRAM. El mandato le solicitará el número de interfaz.

Las reservas sobre esta interfaz se perderán y se volverán a establecer la próxima vez que se emitan mandatos de renovación path y resv, en función de la disponibilidad de los recursos. Existe el riesgo de que se pierdan algunas reservas si los recursos necesarios para renovarlas, como por ejemplo el ancho de banda, no están disponibles.

**queue-stat**
Borra las colas de control de flujos de todas las interfaces configuradas para RSVP.

**rsvp** Detiene RSVP en el direccionador y vuelve a arrancar RSVP si está activado en SRAM.

Todos los mensajes path y resv del direccionador se borrarán cuando se detenga RSVP. Cuando se vuelva a arrancar RSVP, las reservas se volverán a arrancar la próxima vez que se emitan mensajes de renovación path y resv, según la disponibilidad de los recursos. Existe el riesgo de que se pierdan algunas reservas si los recursos necesarios para renovarlas, como por ejemplo el ancho de banda, no están disponibles.

**system-parameters**
Actualiza los parámetros del sistema RSVP con los datos de configuración creados con mandatos de talk 6 y guardados en SRAM. Los parámetros del sistema RSVP son los que se definen mediante el mandato de talk 6 **set**.

## Send

Utilice el mandato **send** para enviar de forma dinámica mensajes RSVP y ping de IP.

**Sintaxis:**

**send**
- data-packet
- ip-ping
- path
- ptear
- resv

rtear

**data-packet**

Este mandato sirve para enviar datos de prueba sobre un flujo IP definido. Puede enviar varios paquetes por segundo, según los límites de velocidad del direccionador y de los recursos. Aparece un mensaje cada vez que se envía el paquete número diez.

**Ejemplo:**

```
RSVP>send data
IP Dest Address: [0.0.0.0]? 5.0.25.100
Destination UDP port: [1]? 100
IP Srce Address: [5.0.25.101]? 1
Source UDP port: [1]? 100
Number of pings per second: [1]?
UDP packet length: [56]?
RSVP send data 1 to 5.0.25.100 protocol 17 source port 100 dest port 100.
.........RSVP send data 11 to 5.0.25.100 protocol 17 source port 100 dest port
100.
.........RSVP send data 21 to 5.0.25.100 protocol 17 source port 100 dest port
100.
RSVP>
```

**1** Es la dirección IP del direccionador que envía este flujo IP.

**ip-ping**

Envía un mensaje ping de IP (echo de ICMP). Consulte el mandato **ping** en el capítulo “Configuración y supervisión de IP” del manual *Consulta de configuración y supervisión de protocolos Volumen 1*.

**path**

Envía un mensaje *path* de RSVP, a sí mismo o como proxy a otro sistema principal. El formato de entrada de este mandato es el mismo que para el mandato de talk 6 **add sender**. Consulte el mandato de talk 6 **add sender** para ver descripciones de los parámetros necesarios.

Por omisión, estos mensajes se envían cada 30 segundos. La vía de acceso sigue existiendo hasta que la elimina con el mandato **send ptear** o hasta que restablece RSVP.

Este mandato puede añadir de forma dinámica un emisor a la configuración. Puede utilizar talk 2 para ver el rastreo ELS de renovaciones de vías de acceso.

**ptear**

Envía un mensaje *ptear* de RSVP, a sí mismo como como proxy a otro sistema principal. Si se elimina una vía de acceso mediante el mandato **send ptear** se elimina tanto el flujo de tráfico como la reserva. Se le solicitarán parámetros que identifiquen la vía de acceso, como por ejemplo la dirección de destino IP y la dirección de sesión IP. Consulte el mandato de talk 6 **add** para ver una descripción de los parámetros solicitados.

El estado de la vía de acceso especificado en el mandato **send ptear** debe existir o se generará un mensaje de error de ELS. Puede utilizar talk 2 para ver los mensajes ELS asociados a este mandato.

**resv**

Envía un mensaje *resv* de RSVP, a sí mismo o como proxy a otro sistema principal. Se le solicitarán parámetros que identifiquen la vía de acceso, como por ejemplo la dirección de destino IP y la dirección de sesión IP. Consulte el mandato de talk 6 **add** para ver una descripción de los parámetros solicitados. Puede utilizar talk 2 para ver los mensajes ELS asociados a este

mandato. Para ver estos mensajes de rastreo, debe activarlos mediante estos mandatos desde el indicador de talk 6 o de talk 5:

**Ejemplo:**

```
Config>event
ELS config>disp sub rsvp all
```

Si intenta emitir este mandato para un receptor que no ha definido ninguna sesión RSVP, este mandato muestra el mensaje `Inputting session does not exist`. Utilice el mandato **show rsvp flow** para ver los flujos RSVP existentes.

**Ejemplo:**

```
RSVP>send resv
RESV requestor IP Address: [0.0.0.0]? 5.0.25.101
Session > IP Address: [5.0.25.101]?
Session > Port Number: [1]? 201
Session> Protocol Type (UDP/TCP): [UDP]?
Inputting session does not exist.
RSVP>
RSVP>show rsvp flow

Number of flows:        1

Num To (Session)    From            Prot DPrt  SPrt In-If Out-If Rsvd Nhop's
-------------------------------------------------------------------------------
1   5.0.25.101      5.0.25.100      UDP  26    26    4     6      N    0
RSVP>
RSVP>send resv
RESV requestor IP Address: [0.0.0.0]? 5.0.25.101 1
Session > IP Address: [5.0.25.101]? 2
Session > Port Number: [1]? 26
Session> Protocol Type (UDP/TCP): [UDP]?
Style> (WF, FF, SE): [FF]?
Need confirmation?(Yes or [No]):
Service Type: CTL-LOAD
Tspec> Peak Rate (in byte/sec) [250000]? 25000
Tspec> Average Rate (in byte/sec) [200000]? 20000
Tspec> Burst Size (in bytes) [2000]?
Tspec> Max. Pkt Size [1500]?
Tspec> Min Pkt Size [53]?

Existing Filters:
Filter 1 (sender-address : sender-port):  5.0.25.100:26

Make reservation to all senders?(Yes or [No]): Y
A new RESV message will be sent from 5.0.25.101:26 to 5.0.25.100:26
RESV message sent
RSVP>
RSVP>sh r flow

Number of flows:        1

Num To (Session)    From            Prot DPrt  SPrt In-If Out-If Rsvd Nhop's
-------------------------------------------------------------------------------
1   5.0.25.101      5.0.25.100      UDP  26    26    4     6      Y 3    0
RSVP>

*t 2 4
43:56:28 RSVP.074: Send RESV refresh for session 5.0.25.101:26
43:56:28 RSVP.073: --RSVP send IP pkt to 5.0.25.100 on net 4, return code=0
```

**1** la dirección del solicitando debe ser una dirección de difusión individual IP.

**2** La dirección de sesión IP, que es la dirección de destino correspondiente a la sesión, puede ser la dirección de difusión individual IP del receptor o una dirección de difusión múltiple IP de un grupo de difusión múltiple al que pertenece el receptor.

**3** Observe que el campo *Rsvd* (Reservado) de la entrada de flujo pasa de N (No) a Y (Yes) cuando se establece la reserva. Si el valor es N, significa que existe un flujo, pero no hay reserva. El flujo se envía mediante QoS best effort.

**4** Por omisión, el rastreo de ELS de talk 2 muestra las renovaciones de reservas que se envían cada 30 segundos.

**rtear**

Envía un mensaje *rsvtear* de RSVP, a sí mismo o como proxy a otro sistema principal. Este mandato desconecta un flujo de tráfico RSVP, pero no elimina la vía de acceso del emisor, de modo que el flujo de tráfico IP continúa con QoS best effort. El mandato le solicita los parámetros que identifican un flujo de tráfico RSVP, como por ejemplo la dirección de destino IP del receptor y la dirección de sesión IP. Consulte el mandato de talk 6 **add** para ver una descripción de los parámetros solicitados.

El flujo de tráfico IP especificado en el mandato **send rtear** debe existir o se generará un mensaje de error de ELS. Puede utilizar talk 2 para ver los mensajes ELS asociados a este mandato.

## Show

Utilice el mandato **show** para ver diversos aspectos de RSVP.

**Sintaxis:**

**show**
- adspec
- classifier
- ds
- flowspec
- queue
- rsvp
  - flows
  - senders
  - sessions
  - reservations
  - requests
- vc

**adspec**

Muestra especificaciones de anuncios (adspec) de todos los flujos. Adspec es la salida de OPWA; lista información sobre los recursos reservados en cada enlace a lo largo de la vía de acceso de la sesión RSVP activa.

**classifier**

Muestra todas las entradas del flujo QoS actual que hay en el clasificador de paquetes RSVP y/o en la antememoria IP.

**ds** Muestra las reservas actuales sobre enlaces Differentiated Services (DS). El campo streamID permite al usuario correlacionar las reservas con las que muestra el mandato **show stream** de la característica DS.

**flowspec**

Muestra las tspec del emisor, las tspec de reservas y las tspec de solicitud que hay actualmente en las tablas de estado de RSVP.

**queue**

Muestra las estadísticas actuales sobre colas de software de RSVP. Se aplica sólo a enlaces que no son ATM.

**rsvp**

Muestra aspectos del estado de la conexión RSVP actual.

**flows** Muestra los flujos de tráfico RSVP activos. Consulte el ejemplo del mandato de talk 5 **send resv** para ver un ejemplo de este mandato.

**senders** Muestra los emisores RSVP. Los emisores están configurados, pero no necesariamente activados.

**sessions** Muestra las sesiones RSVP, tanto las sesiones activas que tienen flujos reservados como las inactivas que existen pero no tienen reservas en este momento.

**reservations**
Muestra las reservas RSVP.

**requests** Muestra las peticiones RSVP.

**vc** Muestra los SVC de ATM actualmente establecidos que ha reservado RSVP.

## Stop-RSVP

Utilice el mandato **stop-rsvp** para detener la función RSVP en el direccionador.

**Sintaxis:**

**stop**
rsvp

# Utilización de SNMP

Este capítulo describe SNMP. Contiene la siguientes secciones:

- "Gestión de red"
- "Gestión de SNMP"

## Gestión de red

Consulte el manual *IBM 2210 Introduction and Planning Guide* para obtener información sobre la gestión de red.

## Gestión de SNMP

El IBM 2210 ofrece una interfaz Simple Network Management Protocol (SNMP) ante aplicaciones y plataformas de gestión de red, como por ejemplo los productos Nways Campus Manager.

SNMP sirve para gestionar y supervisar sistemas principales IP de una red IP y utiliza un software denominado agente SNMP para permitir que los sistemas principales puedan leer y modificar algunos de los parámetros operativos del IBM 2210. De este modo, SNMP establece funciones de gestión de red para la comunidad IP.

Debe tener en cuenta los siguientes aspectos de SNMP cuando configure SNMP para su IBM 2210.

**Comunidad**

La comunidad le permite definir la dirección IP de la estación de gestión de IP que tiene acceso a la información de la Base de información de gestión (MIB) del agente SNMP. Puede definir un nombre de comunidad que se utilizará para acceder a MIB.

**Autentificación**

El nombre de comunidad se utiliza como esquema de autentificación para evitar que los usuarios no autorizados obtengan información sobre un agente SNMP o que modifiquen sus características.

Este esquema implica el definir uno o más grupos de datos MIB (a los que se denomina vistas MIB) y asociar un privilegio de acceso (sólo lectura, lectura y grabación), una máscara IP y un nombre de comunidad a cada vista MIB. La máscara IP define qué direcciones IP pueden originar solicitudes de acceso sobre una determinada vista MIB y el nombre de comunidad sirve como contraseña que deben comparar las peticiones SNMP. El nombre de comunidad se incluye en cada mensaje SNMP y el agente SNMP de IBM 2210 lo verifica. Una petición SNMP se rechazará si no ofrece el nombre de comunidad correcto, no coincide con la máscara IP o intenta un acceso que no concuerda con el privilegio de acceso asignado.

**Contraseña SNMP**

La contraseña SNMP sirve para cifrar y autentificar objetos MIB sensibles a la seguridad, como clave de cifrado o contraseña, en la sección de perfiles de la característica de autentificación. Si se define como contraseña SNMP una serie de longitud cero, significa que no se puede acceder a los datos sensibles a la seguridad. Cuando el valor de la contraseña SNMP es *clear*, signi-

fica que SNMP puede acceder a los datos sin cifrado. Cuando el valor de la contraseña SNMP es otra serie de caracteres, los datos se pueden recuperar son cifrado y autentificación utilizando una clave derivada de la contraseña SNMP. Para obtener más información, consulte la definición de MIB.

**Soporte de MIB**

Una MIB es un almacén de información virtual que ofrece acceso a la información de gestión. Esta información se define como objetos MIB a los que se puede acceder y los cuales, en determinados casos, se pueden modificar mediante herramientas de gestión de red.

IBM 2210 ofrece una amplia gama de MIB estándares, MIB específicos de empresa para supervisar y gestionar recursos y archivos Readme.

Encontrará los archivos Readme que documentan el soporte de MIB de IBM 2210 accediendo al directorio del release adecuado en World Wide Web en la siguiente dirección:

- **ftp://ftp.nways.raleigh.ibm.com/pub/netmgmt/2210/**

Para recibir una copia de una determinada MIB, entre el mandato **get** con el nombre de la MIB. Por ejemplo, el mandato **get ibm.mib** coloca una copia de la MIB especificada en el directorio desde el que se ha conectado al servidor FTP.

Puede acceder a la siguiente información desde la dirección ftp:

- MIB estándares
- MIB de empresa
- Rupturas genéricas de SNMP
- MIB específicas de empresa
- Valores que se pueden definir

Rupturas genéricas de SNMP, MIB de empresa y Valores que se pueden definir se encuentran en los archivos Readme.

Todos los objetos MIB se implantan como objetos de SÓLO LECTURA, incluso aunque su cláusula de acceso se defina como lectura y grabación o lectura y creación, excepto los objetos MIB identificados en el archivo Readme que dan soporte a mandatos SET sobre objetos que tienen su cláusula de acceso definida como de lectura y grabación o como de lectura y creación.

**Mensajes de ruptura**

Los mensajes de ruptura son mensajes no solicitados enviados por el agente SNMP del dispositivo a un gestor SNMP como respuesta a una condición del dispositivo o de la red, como por ejemplo cuando se ha vuelto a cargar un dispositivo o cuando la red no está operativa.

# Configuración y supervisión de SNMP

Este capítulo describe los mandatos de configuración y de supervisión de SNMP. Incluye las siguientes secciones:



## Cómo acceder al entorno de configuración de SNMP

Para acceder al entorno de configuración de SNMP, entre el siguiente mandato en el indicador `Config>`:

```
Config> protocol snmp
SNMP user configuration
SNMP Config>
```

## Mandatos de configuración de SNMP

Esta sección describe los mandatos de configuración de SNMP.

La Tabla 31 en la página 510 lista los mandatos de configuración de SNMP. Los mandatos de configuración de SNMP le permiten especificar parámetros que definen la relación entre el agente SNMP y la estación de gestión de red. La información que especifique entra en vigor de forma inmediata cuando se vuelve a arrancar o a cargar el IBM 2210.

Entre los mandatos de configuración de SNMP en el indicador `SNMP Config>`.

*Tabla 31. Resumen de mandatos de configuración de SNMP*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Add | Añade una comunidad a la lista de comunidades SNMP, una dirección IP con máscara a una comunidad o un subárbol a una vista MIB. |
| Delete | Elimina una comunidad de la lista de comunidades SNMP, una dirección IP con máscara de una comunidad o un subárbol de una vista MIB. |
| Disable | Desactiva el protocolo SNMP y las rupturas asociadas a las comunidades especificadas. |
| Enable | Activa el protocolo SNMP y las rupturas asociadas a las comunidades especificadas. |
| List | Muestra las comunidades actuales con sus modalidades de acceso, rupturas activadas, direcciones IP y vistas asociadas. También muestra todas las vistas y sus subárboles MIB asociados. |
| Set | Define una modalidad de acceso o vista de una comunidad. La modalidad de acceso de una comunidad puede ser una de las siguientes:<br>Lectura y generación de rupturas<br>Lectura, grabación y generación de rupturas<br>Sólo generación de rupturas<br>Este mandato también sirve para definir un puerto UDP de rupturas y para definir la contraseña utilizada para cifrar y autentificar datos sensibles a la seguridad. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

*Tabla 32 (Página 1 de 2). Resumen de opciones de los mandatos de configuración de SNMP*

| MANDATO | PARÁM 1 | PARÁM 2 | PARÁM 3 | PARÁM 4 | VALOR OMISIÓN |
|---|---|---|---|---|---|
| add | community | <nombre_comun> | | | Ninguno |
| | address | <nombre_comun> | <direcciónIp> | <máscaraIp> | |
| | sub_tree | <nombre_texto_vista> | <oid> | | |
| delete | community | <nombre_comun> | | | |
| | address | <nombre_comun> | <direcciónIp> | <máscaraIp> | |
| | sub_tree | <nombre_texto_vista> | <oid> | | |
| disable | snmp | | | | |
| | trap | all | <nombre_comun> | | |
| | | cold_start | <nombre_comun> | | |
| | | warm_start | <nombre_comun> | | |
| | | link_down | <nombre_comun> | | |
| | | link_up | <nombre_comun> | | |

*Tabla 32 (Página 2 de 2). Resumen de opciones de los mandatos de configuración de SNMP*

| MANDATO | PARÁM 1 | PARÁM 2 | PARÁM 3 | PARÁM 4 | VALOR OMISIÓN |
|---|---|---|---|---|---|
| | | auth_fail | <nombre_comun> | | |
| | | enterprise | <nombre_comun> | | |
| enable | snmp | | | | |
| | trap | all | <nombre_comun> | | |
| | | cold_start | <nombre_comun> | | |
| | | warm_start | <nombre_comun> | | |
| | | link_down | <nombre_comun> | | |
| | | link_up | <nombre_comun> | | |
| | | auth_fail | <nombre_comun> | | |
| | | enterprise | <nombre_comun> | | |
| list | all | | | | |
| | community | access | | | access |
| | | traps | | | |
| | | address | | | 255.255.255.255 |
| | | view | | | all |
| | views | | | | |
| set | community | access | read_trap | <nombre_comun> | |
| | | | write_read_trap | <nombre_comun> | |
| | | | trap_only | <nombre_comun> | |
| | | view | <comunidad> | all | all |
| | | | | <nombre_texto_vista> | |
| | trap_port | <númPuertoUdp> | | | |
| | password | | | | |
| exit | | | | | |

## Add

Utilice el mandato **add** para añadir un nombre de comunidad a la lista de comunidades SNMP, para añadir una dirección a una comunidad o para asignar una parte de la MIB (subárbol) a una vista.

**Sintaxis:**

**add** community
address
sub_tree

**community**

Utilice el mandato **add community** para crear una comunidad. Se creará con valor de acceso por omisión igual a read_trap, una vista de

todo, todas las rupturas desactivadas y todas las direcciones IP permitidas.

**Nota:** Para seleccionar tipo de acceso o control de rupturas, utilice el mandato **set community access** para asignar tipos de acceso a comunidades SNMP existentes y utilice el mandato **enable trap** o el mandato **disable trap** para el control de rupturas.

**community name**

Ofrece el nombre de comunidad que utilizará el cliente SNMP. Este nombre de comunidad se utiliza al acceder a la base de información de gestión (MIB) del dispositivo desde el sistema principal especificado mediante el parámetro Community IP address.

**Valores válidos**: Una serie de caracteres de entre 1 y 31 caracteres alfanuméricos. No se da soporte a caracteres como espacios, tabuladores o secuencias de teclas <ESC>.

**Valor por omisión**: ninguno

**Ejemplo:**

```
SNMP Config>  add community
Community Name  []? comm01
Community added successfully
```

**address** Utilice el mandato **add address** para añadir a la definición de comunidad una dirección de una estación de gestión de red de la red que deberá ser capaz de comunicarse con este recuadro. Debe especificar el nombre de la comunidad y la dirección de la red (en notación a.b.c.d estándar). También puede especificar una máscara de red para restringir el acceso a un determinado sistema principal (máscara = 255.255.255.255) o a una red de sistemas principales. Se puede añadir más de una dirección a una comunidad; entre el mandato cada vez que desee añadir otra dirección.

Si no especifica una dirección correspondiente a una comunidad, las peticiones se manejan desde cualquier sistema principal.

Las direcciones también especifican los sistemas principales que reciben rupturas. Si no se especifica ninguna dirección, no se genera ninguna ruptura.

**community name**

**Valores válidos**: Una serie de caracteres de entre 1 y 31 caracteres alfanuméricos. No se da soporte a caracteres como espacios, tabuladores o secuencias de teclas <ESC>.

**Valor por omisión**: ninguno

**IP address**

**Valores válidos**: Cualquier dirección IP válida.

**Valor por omisión**: 0.0.0.0

**ip mask** Puede especificar una máscara para restringir el acceso a un determinado sistema principal (máscara = 255.255.255.255) o a una red de sistemas principales.

**Valores válidos**: 0.0.0.0 - 255.255.255.255

**Valor por omisión**: 255.255.255.255

**Ejemplo:**

```
SNMP Config> add address
Community Name []?
IP Address [0.0.0.0]?
IP Mask [255.255.255.255]?
```

**sub_tree** Utilice el mandato **add sub_tree** para añadir una parte de la MIB a una vista o para crear una vista nueva. El valor por omisión es la MIB entera. El mandato **add sub_tree** sirve para gestionar vistas MIB. Se puede añadir más de un subárbol a una vista definida por <nombre_texto_vista>.

**view name**

Especifica el nombre de la vista que se va a crear.

**Valores válidos**: Cualquier serie de caracteres alfanuméricos con una longitud máxima de 31 caracteres. No se aceptan caracteres como espacios, tabuladores o secuencias de teclas <Esc>.

**Valor por omisión**: ninguno

**Nota:** Debe asignar una vista a una o más comunidades mediante el mandato **set community view** para que entre en vigor. Las definiciones de subárbol son inclusivas; es decir, el OID del subárbol especificado y cualquier OID lexicográficamente superior al OID especificado se consideran parte de la vista MIB.

Si se añade una comunidad mediante el mandato **add community**, todas las vistas MIB soportadas se asignan a la comunidad a no ser que se utilice el mandato **set community view** para asignar vistas específicas a la comunidad.

**MIB OID name**

Especifica el ID del objeto MIB correspondiente al subárbol. Se debe especificar como un valor numérico, no como un valor simbólico.

Este parámetro contiene un nombre de subárbol MIB incluido en la vista definida con el parámetro View name. Todos los hijos de un subárbol MIB especificado se incluyen también en la vista.

Por ejemplo, para ofrecer una vista que daría acceso al grupo del sistema en MIB-II, especifique **1.3.6.1.2.1.1**.

**Valores válidos**:

Un identificador de objeto en el formato <elemento1>.<elemento2>.<elemento3>. . ., donde:

- Necesita al menos 1 elemento. Puesto que todos los OID de MIB comienzan por *1.3.6.1*, el número mínimo de elementos que debe especificar para que la vista sea diferente de *all* es 5 (1.3.6.1.X).

- Puede definir un máximo de 31 caracteres, incluidos los separadores ..
- Todos los elementos que van detrás de los cuatro primeros (*1.3.6.1*) son enteros comprendidos entre 0 y 127.

**Nota:** Este valor debe ser numérico en notación con puntos, *no* un valor simbólico.

**Valor por omisión**: ninguno

**Ejemplo:**

```
SNMP Config> add sub_tree
View Name  []? view01
MIB OID name []? 1.3.6.1.1
Subtree added successfully
```

## Delete

Utilice el mandato **delete** para suprimir una comunidad y todas sus direcciones, una dirección específica a un subárbol de una vista.

**Sintaxis:**

**delete** community
address
sub_tree

**community**

Elimina una comunidad y su dirección IP.

**community name**

Especifica un nombre de comunidad utilizado por el cliente SNMP. Este nombre de comunidad se utiliza al acceder a la base de información de gestión (MIB) del dispositivo desde el sistema principal especificado mediante el parámetro Community IP address.

**Valores válidos**: Una serie de caracteres de entre 1 y 31 caracteres alfanuméricos. No se da soporte a caracteres como espacios, tabuladores o secuencias de teclas <ESC>.

**Valor por omisión**: ninguno

**Ejemplo:**

```
SNMP Config> delete community
Community Name []?
```

**address** Elimina una dirección de una comunidad. Debe especificar el nombre.

**community name**

Especifica el nombre de la comunidad de la que se tiene que eliminar una dirección. Este nombre de comunidad se utiliza al acceder a la base de información de gestión (MIB) del dispositivo desde el sistema principal especificado mediante el parámetro Community IP address.

**Valores válidos**: Una serie de caracteres de entre 1 y 31 caracteres alfanuméricos. No se da soporte a caracteres como espacios, tabuladores o secuencias de teclas <ESC>.

**Valor por omisión**: public

**IP address**

Especifica la dirección IP a suprimir.

**Valores válidos**: Cualquier dirección IP válida.

**Valor por omisión**: ninguno

**Ejemplo:**

```
SNMP Config>  delete address
Community Name []?
IP address []?
```

**sub_tree** Elimina una MIB o una parte de la MIB de una vista. Debe especificar el nombre del subárbol. Si se suprimen todos los subárboles, también se suprime la vista MIB y todas las referencias a la misma desde cualquier comunidad SNMP asociada.

**view name** Especifica la vista que utiliza la comunidad definida en el parámetro **community name**. Esta vista determina los objetos MIB a los que puede acceder esta comunidad. Si no se especifica ninguna vista, la comunidad puede acceder a todos los objetos conocidos por el agente SNMP del dispositivo.

Este parámetro se debe responder si decide que una comunidad no pueda acceder a la MIB entera gestionada por el agente SNMP del dispositivo.

**Valor por omisión**: ninguno

**MIB OID name** Especifica el ID del objeto MIB correspondiente al subárbol. Se debe especificar como un valor numérico, no como un valor simbólico.

Este parámetro contiene un nombre de subárbol MIB incluido en la vista definida con el parámetro View name. Todos los hijos de un subárbol MIB especificado se incluyen también en la vista.

**Valores válidos**: Un identificador de objeto en el formato <elemento1>.<elemento2>.<elemento3>.  . ., donde:

- Necesita al menos 1 elemento. Puesto que todos los OID de MIB comienzan por *1.3.6.1*, el número mínimo de elementos que debe especificar para que la vista sea diferente de *all* es 5 (1.3.6.1.X).
- Puede definir un máximo de 31 caracteres, incluidos los separadores ..
- Todos los elementos que van detrás de los cuatro primeros (*1.3.6.1*) son enteros comprendidos entre 0 y 127.

**Valor por omisión**:ninguno

**Ejemplo:**

```
SNMP Config> delete sub_tree
View name[]?
MIB OID[]?
```

## Disable

Utilice el mandato **disable** para desactivar el protocolo SNMP o determinadas rupturas en el dispositivo.

**Sintaxis:**

**disable** snmp
trap
sram-write

**snmp** Desactiva SNMP.

**Ejemplo:** `disable snmp`

**trap** *tipo ruptura*
Desactiva las rupturas especificadas o todas las rupturas.

**tipo ruptura**
Especifica el tipo de ruptura que se va a desactivar. Los tipos de ruptura válidos se muestran en la Tabla 33.

**community name**

**Valores válidos**: Una serie de caracteres de entre 1 y 31 caracteres alfanuméricos. No se da soporte a caracteres como espacios, tabuladores o secuencias de teclas <ESC>.

**Valor por omisión**: ninguno

**Ejemplo:**

```
SNMP Config> disable trap link_up
Community name []?
```

**sram-write**

*Tabla 33 (Página 1 de 2). Tipos de rupturas SNMP*

| Tipo ruptura | Descripción |
|---|---|
| all | Especifica todas las rupturas de comunidad especificada. |
| cold_start | Una ruptura de arranque en frío significa que el dispositivo transmisor se está volviendo a inicializar y que la configuración del agente o la implantación de la entidad del protocolo se han podido modificar. |
| warm_start | Una ruptura de arranque en caliente significa que el dispositivo transmisor se está volviendo a inicializar, pero la configuración o la implantación del protocolo no se han modificado. Especifique el nombre de la comunidad como parte de la línea de mandatos. |
| link_down | Una ruptura link_down reconoce un error en uno de los enlaces de comunicaciones representados en la configuración del agente. link_down trap-PDU contiene el nombre y valor de la instancia ifIndex correspondiente al enlace afectado como el tercer elemento de sus vinculaciones variables. |
| link_up | Una ruptura link_up reconoce que se ha activado en la red un enlace que antes estaba inactivo. link_up trap-PDU contiene el nombre y el valor de la instancia ifIndex correspondiente al enlace afectado como el primer elemento de sus vinculaciones variables. |

*Tabla 33 (Página 2 de 2). Tipos de rupturas SNMP*

| Tipo ruptura | Descripción |
|---|---|
| auth_fail | Las rupturas de error de autentificación indican que el emisor de una petición SNMP no tiene el permiso adecuado para establecer comunicación con el agente SNMP de este recuadro. |
| enterprise | Las rupturas específicas de empresa indican que se ha producido algún suceso específico de la empresa. El campo specific-trap identifica la ruptura producida. Por ejemplo, cuando se han configurado para ello, se envían mensajes de sucesos ELS en rupturas específicas de empresa. |

## Enable

Utilice el mandato **enable** para activar el protocolo SNMP o determinadas rupturas en el dispositivo.

**Sintaxis:**

enable snmp

trap

sram-write

**snmp** Activa SNMP

**Ejemplo:** `enable snmp`

**trap** *tipo ruptura*
Activa las rupturas especificadas o todas las rupturas.

**tipo ruptura**
Especifica el tipo de ruptura que se va a activar. Los tipos de ruptura válidos se muestran en la Tabla 33 en la página 516.

**community name**

**Valores válidos**: Una serie de caracteres de entre 1 y 31 caracteres alfanuméricos. No se da soporte a caracteres como espacios, tabuladores o secuencias de teclas <ESC>.

**Valor por omisión**: ninguno

**sram-write**

## List

Utilice el mandato **list** para visualizar la configuración actual de comunidades SNMP, modalidades de acceso, rupturas, direcciones de red y vistas.

**Sintaxis:**

**list** all

community

views

**list all** Muestra la configuración actual de las comunidades SNMP correspondiente a Acceso, Rupturas, Dirección y Vista. Consulte la descripción del mandato **list community** para obtener detalles sobre las opciones.

**Ejemplo: `list all`**

```
SNMP Config>list all

   SNMP is enabled
   Trap UDP port: 162
   SRAM write is enabled

            Community Name                 Access
   -------------------------------  ------------------
   oxnard                           Read, Write, Trap
   public                           Read, Trap


          Community Name              IP Address         IP Mask
   -------------------------------  ---------------  ---------------
   oxnard                           1.1.1.2          255.255.255.255
   public                           All              N/A


          Community Name                  Enabled Traps
   -------------------------------  -------------------------------
   oxnard                           Link Down, Cold Restart
   public                           None


            Community Name                    View
   -------------------------------  -------------------------------
   oxnard                           mib2
   public                           All

             View Name                    Sub-Tree
   -------------------------------  -------------------------------
   mib2                             1.3.6.1.2

   Password is set. (security data flow encrypted)
```

**list community** *opción*

Muestra los atributos actuales de una comunidad SNMP. Las opciones son access, address, traps, view.

| Opción | Descripción |
|---|---|
| Access | Muestra las modalidades de acceso correspondiente a la comunidad. |
| Address | Muestra la dirección de red correspondiente a la comunidad. |
| Traps | Muestra los tipos de rupturas generados para la comunidad. |
| View | Muestra la vista MIB correspondiente a la comunidad. |

**Ejemplo:**

```
SNMP Config  list community access

          Community Name   Access
          public           Read, Write, Trap
          oxnard           Read, Trap
```

**Ejemplo:**

```
SNMP Config>  list community address

          Community Name   IP Address   IP Mask
          public           All          N/A
          oxnard           1.1.1.2      255.255.255.255
```

**Ejemplo:**

```
SNMP Config  list community traps

            Community Name   Enabled Traps
            public           Link Down, Cold Restart
            oxnard           NONE
```

**Ejemplo:**

```
SNMP Config>  list community view

             Community Name   View
            public           All
            oxnard           mib2
```

**list views**

Muestra las vistas actuales correspondientes a una comunidad SNMP especificada.

**Ejemplo:**

```
SNMP Config  list views

            View Name   Sub-Tree
            mib2        1.3.6.1.2.1
```

## Set

Utilice el mandato **set** para asignar una vista MIB a una comunidad, para definir el número de puerto de rupturas UDP de SNMP o para definir la modalidad de acceso de la comunidad  o contraseña SNMP.

**Sintaxis:**

**set** community access

community view

trap_port

password

**community access**

Utilice el mandato **set community access** para asignar uno de los tres tipos de acceso a una comunidad. Debe especificar el nombre de la comunidad y el tipo de acceso.

**opciones** Elija una opción de la siguiente lista:

**read_trap**
Permite un acceso de lectura y generación de rupturas a la comunidad especificada.

**write_read_trap**
Permite un acceso de grabación y lectura y de generación de rupturas a la comunidad especificada.

**trap_only**
Indica que la comunidad sólo se utiliza al enviar una ruptura SNMP.

**nombre_comun**

El **nombre de comunidad** tiene:

**Valores válidos**: Una serie de caracteres de entre 1 y 31 caracteres alfanuméricos.

No se da soporte a caracteres como espacios, tabuladores o secuencias de teclas <ESC>.
**Valor por omisión**: ninguno

**Ejemplo:** `set community access <opciones> nombre_comun`

**community view**

Utilice el mandato **set community view** para asignar una vista MIB a una comunidad.

**nombre_comun**

**Valores válidos**: Una serie de caracteres de entre 1 y 31 caracteres alfanuméricos. No se da soporte a caracteres como espacios, tabuladores o secuencias de teclas <ESC>.

**Valor por omisión**: ninguno

**all** Permite el acceso a todos los objetos MIB correspondientes a la comunidad especificada. All es el valor por omisión.

**nombre_texto_vista**
Asigna una determinada vista MIB a la comunidad especificada.

**Ejemplo:** `set community view nombre_comun <all o nombre_texto_vista>`

**trap_port** Utilice el mandato **set trap_port** para especificar un número de puerto UDP, que no sea el puerto estándar por omisión 162, al que enviar rupturas.

**Valor por omisión**: puerto estándar

**Ejemplo:** `set trap_port núm puertoudp`

**Número de puerto UDP**
Especifica un puerto del Protocolo de datagramas de usuario distinto del puerto UDP estándar.

**Valor por omisión**: 162

**password**

Utilice el mandato password para especificar la contraseña a cifrar y autentificar los objetos MIB sensibles a la seguridad que están definidos en la MIB. Si define como contraseña una serie de longitud cero, especifica la seguridad máxima, puesto que no permite ningún acceso ni definición de objetos MIB sensibles a la seguridad. Si define como contraseña el valor "clear", especifica la menor cantidad de seguridad, puesto que permite que los datos fluyan sin autentificación. Si define como contraseña cualquier otra serie de caracteres, permite el acceso y definición de los objetos MIB sensibles a la seguridad que están cifrados y autentificados con esta contraseña.

**Ejemplos**:

(a) definición como contraseña de una serie de longitud cero:

```
SNMP Config>set pa
Password:
Remove password? (Yes, No): y
Password is set to NULL. (security data are not accessible)
```

(b) definición como contraseña del valor "clear":

```
SNMP Config>set pa
Password:
to verify Enter password again:
Password is set to "clear". (WARNING: security data flow in clear)
```

(c) definición como contraseña del valor "test":

```
SNMP Config>set pa
Password:
to verify Enter password again:
Password is set. (security data flow encrypted)
```

## Cómo acceder al entorno de supervisión de SNMP

Para acceder al entorno de supervisión de SNMP, entre el siguiente mandato en el indicador **+** (GWCON):

```
+ protocol snmp
SNMP>
```

## Mandatos de supervisión de SNMP

Esta sección describe los mandatos de supervisión de SNMP.

La Tabla 34 en la página 522 contiene los mandatos de supervisión de SNMP. Los mandatos de supervisión de SNMP le permiten ver los parámetros de configuración de SNMP y algunas estadísticas relacionadas con el agente SNMP.

Los cambios temporales en los parámetros SNMP de ejecución se pueden hacer mediante mandatos de supervisión. Afectarán inmediatamente al funcionamiento del agente SNMP. Si desea convertir en permanentes los cambios temporales, utilice el mandato SAVE. Si tiene que restablecer la configuración SNMP original, utilice el mandato **reset**.Este mandato le permite modificar temporalmente el comportamiento del agente SNMP, sin modificar la configuración de forma permanente. Para que los cambios temporales entren en vigor, debe salir (EXIT) del proceso de supervisión de SNMP.

Entre los mandatos de supervisión de SNMP en el indicador `SNMP>`.

| *Tabla 34. Resumen de mandatos de supervisión de SNMP* | |
|---|---|
| Mandato | Función |
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Add | Añade una comunidad a la lista de comunidades SNMP, una dirección IP con máscara a una comunidad o un subárbol a una vista MIB. |
| Delete | Elimina una comunidad de la lista de comunidades SNMP, una dirección IP con máscara de una comunidad o un subárbol de una vista MIB. |
| Disable | Desactiva las rupturas asociadas a las comunidades especificadas. La desactivación de SNMP o SRAM_write se debe realizar desde el entorno de configuración `SNMP Config>`. |
| Enable | Activa las rupturas asociadas a las comunidades especificadas. La activación de SNMP o SRAM_write se debe realizar desde el entorno de configuración `SNMP Config>`. |
| List | Muestra la configuración actual de comunidades SNMP, vistas, modalidades de acceso, rupturas y direcciones de red. |
| Reset | Actualiza la configuración de SNMP con los valores de la configuración de SNMP actualmente guardada. |
| Save | Guarda de forma temporal los cambios especificados en la configuración de SNMP. |
| Set | Define una modalidad de acceso o vista de una comunidad. La modalidad de acceso de una comunidad puede ser una de las siguientes:<br>• Lectura y generación de rupturas<br>• Lectura, grabación y generación de rupturas<br>• Sólo generación de rupturas<br><br>También permite definir la contraseña y el puerto UDP de las rupturas. Consulte 520 para obtener más información. |
| Statistics | Muestra estadísticas sobre el agente SNMP. |
| Reset | Actualiza la configuración de SNMP con los valores de la configuración de SNMP actualmente guardada. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Add

Utilice el mandato **add** para añadir un nombre de comunidad a la lista de comunidades SNMP, para añadir una dirección a una comunidad o para asignar una parte de la MIB (subárbol) a una vista.

Para obtener información sobre cómo utilizar el mandato **add**, consulte el tema “Add” en la página 511.

## Delete

Utilice el mandato **delete** para suprimir:

- Una determinada dirección.
- Una comunidad y todas sus direcciones.
- Un subárbol de una vista.

Para obtener información sobre cómo utilizar el mandato **delete**, consulte el tema "Delete" en la página 514.

## Disable

Utilice el mandato **disable** para desactivar determinadas rupturas en el dispositivo.

Para obtener información sobre cómo utilizar el mandato **disable**, consulte el tema "Disable" en la página 516.

## Enable

Utilice el mandato **enable** para activar determinadas rupturas en el dispositivo.

Para obtener información sobre cómo utilizar el mandato **enable**, consulte el tema "Enable" en la página 517.

## List

Utilice el mandato **list** para visualizar la configuración actual de comunidades SNMP, vistas, modalidades de acceso, rupturas y direcciones de red.

**Sintaxis:**

| | |
|---|---|
| **list** | all |
| | community |
| | views |

Para obtener información sobre cómo utilizar el mandato **list**, consulte el tema "List" en la página 517.

## Reset

Utilice el mandato **reset** de SNMP para actualizar la configuración de SNMP con los valores de la configuración de SNMP actualmente guardada. Esta acción permite realizar cambios en la configuración actual de SNMP cuando el dispositivo se vuelve a arrancar o a cargar.

## Save

Utilice el mandato **save** para guardar de forma permanente los cambios especificados.

## Set

Para obtener información sobre cómo utilizar el mandato **set**, consulte el tema “Set” en la página 519.

## Statistics

Utilice el mandato **statistics** para visualizar estadísticas sobre el agente SNMP.

**Sintaxis:**

**statistics**

**Ejemplo: `statistics`**

```
               Max       Current    Current
              Alloc      Alloc       In Use

SNMP agent:  512000      181144     133120

SNMP MIBs:  1048576       57976      19712
```

Se muestra la siguiente información:

**Max Alloc**
La cantidad máxima de memoria (en bytes) que está reservada para el componente SNMP.

**Current Alloc**
A medida que se necesita memoria, se toma de la agrupación reservada (designada mediante MAX ALLOC) y se pasa a una agrupación de memoria "activa". El tamaño de esta agrupación de memoria "activa" se indica mediante el valor de CURRENT ALLOC.

**Current In Use**
Este valor representa la memoria actualmente asignada de la agrupación de memoria "activa" (designada mediante CURRENT ALLOC) que está utilizando el componente SNMP.

# Utilización de DLSw

Este capítulo describe Data Link Switching (DLSw), una implantación del protocolo Data Link Switching (DLSw). Los cambios realizados en el indicador `Config>` no entran en vigor de forma inmediata, pero pasan a formar parte de la configuración de SRAM que se utiliza la siguientes veces vez que se vuelve a arrancar el direccionador. Para ver una descripción de cambios en la configuración temporales, pero inmediatos, consulte la página 598.

El 2210 ofrece una amplia gama de funciones que le permiten integrar tráfico Systems Network Architecture (SNA) y Network Basic Input/Output System (NetBIOS) en redes de área amplia heterogéneas.

Las siguientes secciones explican cómo configurar el direccionador para DLSw:



## Acerca de DLSw

DLSw es un mecanismo de reenvío para los protocolos LLC2, SDLC y QLLC (SNA sobre X.25). Se basa en la función de conexión por puente del direccionador, el protocolo Switch-to-Switch (SSP) y TCP/IP para ofrecer un transporte fiable de tráfico SNA sobre internet. DLSw no ofrece todas las funciones de direccionamiento, pero ofrece conmutación en la capa de enlace de datos. En lugar de conectar por puente tramas LLC2, DLSw encapsula sus datos en tramas TCP y reenvía los mensajes resultantes sobre el enlace WAN a un direccionador DLSw similar para que los distribuya a las direcciones de estaciones finales de destino.

## DLSw y ATM

Varios productos entre redes ATM y Frame Relay permiten distribuir tráfico en redes que contienen dispositivos Frame Relay y ATM. Normalmente, los dispositivos Frame Relay funcionan a velocidades T1 (1,544 Mbps), mientras que las velocidades ATM suelen ser uno o dos órdenes de magnitud más rápidas. DLS puede jugar un papel importante al acomodar este diferencial de velocidad.

DLS es una alternativa a conectar por puente tráfico SNA. Si tiene dos redes de alta velocidad conectadas a un enlace de WAN T1 lento, debe decidir entre conexión por puente y DLS. El efecto secundario negativo de la conexión por puente es que todo el tráfico de difusión general se reenviará a través del enlace T1, utilizando valioso ancho de banda. Por otro lado, DLSw termina las sesiones de forma local y no utiliza la WAN para el tráfico de difusión general, lo que da lugar a un uso más eficiente del enlace de WAN lento, lo que a su vez mejora el rendimiento.

# Cómo funciona DLSw

LLC2, SDLC y QLLC con protocolos orientados a la conexión. DLSw ofrece las características dinámicas de protocolos direccionables ***y*** conserva tanto la fiabilidad de extremo a extremo como las características de control para una comunicación eficiente.

## Problemas de la solución de conexión por puente

La Figura 43 ilustra el enfoque tradicional de conectar por puente tramas LLC2 a través de enlaces de la WAN. Con el enfoque tradicional, se producen retrasos de red con mucha más frecuencia en la WAN que en una LAN. Estos retrasos pueden deberse a una simple congestión de la red, a velocidades de línea bajas o a otros factores. Cualquiera que sea la causa, estos retrasos aumentan la posibilidad de que se agoten los tiempos de espera de sesiones y de que los datos no lleguen a su destino.

Además, los protocolos de LAN, como LLC2, utilizan tiempos de respuesta de retransmisión significativamente menores que los de la WAN. Por lo tanto, las conexiones de extremo a extremo a través de un enlace de WAN resultan extremadamente difíciles de mantener y es mucho más probable que se agoten los tiempos de espera de las sesiones.

Además de los tiempos de espera de las sesiones, existen un problema significativo cuando los datos se retrasan mientras atraviesan la WAN. Una estación emisora puede volver a enviar datos que se han retrasado (pero no se han perdido); esto puede dar lugar a que las estaciones finales LLC2 reciban datos duplicados. Los datos duplicados ocasionan confusión en los procedimiento LLC2 del lado receptor, lo que puede dar lugar a un uso poco eficiente del enlace de la WAN.

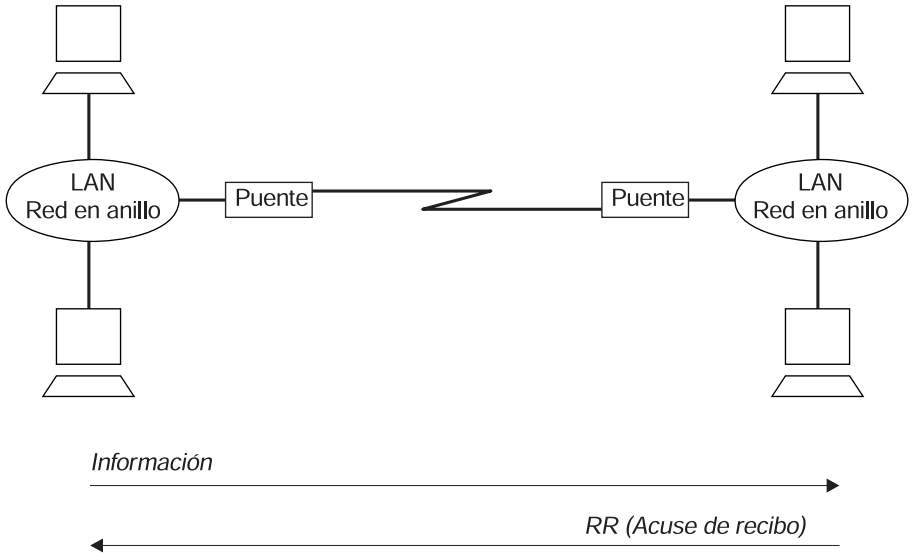



*Figura 43. Enfoque tradicional de la conexión por puente a través de enlaces de la WAN*

El ejemplo anterior muestra una conexión por puente tradicional, que incluye control de enlace de datos de extremo a extremo. Al igual que un protocolo sin conexión, la conexión por puente no toma ninguna medida para asegurar la integridad del tráfico LLC en la WAN.

### Simulación de protocolo

Para reducir la posibilidad de que se agoten los tiempos de espera y para mantener la apariencia de la conectividad de extremo a extremo para las estaciones emisoras, DLSw funciona terminando o “simulando” conexiones LLC2 en el direccionador local. Cuando recibe una trama LLC2, el direccionador envía un acuse de recibo a la estación emisora. Este acuse de recibo indica al emisor que los datos que se han transmitido anteriormente se han recibido.

El acuse de recibo evita que la estación vuelva a transmitir los datos. A partir de este punto, el asegurar que los datos llegan a su destino es responsabilidad del software DLSw. Para ello, el software encapsula los datos en tramas IP direccionables y luego los transporta (mediante TCP) a un similar DLSw. El direccionador DLSw similar elimina las cabeceras TCP, determina la dirección del receptor de destino de los datos y establece una nueva conexión LLC2 con esta estación final.

La Figura 44 ilustra esta relación entre dos direccionadores DLSw similares, cada uno de los cuales está conectado a una red en anillo.

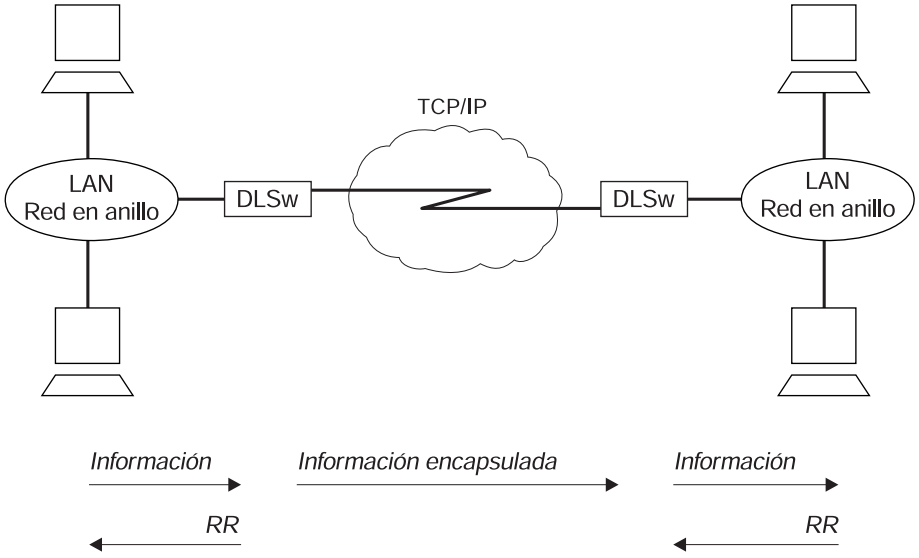



*Figura 44. Conmutación de enlace de datos sobre la WAN*

DLSw termina la conexión LLC2 en el direccionador. Esto significa que las conexiones LLC2 no atraviesan la red de área amplia. Esto reduce los tiempos de espera excedidos de sesiones y los acuses de recibo (RR) que de otro modo atravesarían los enlaces de área del área amplia.

## Ventajas de DLSw

Puesto que DLSw termina la conexión DLC en el dispositivo local (consulte la Figura 44 ), resulta especialmente eficaz para eliminar tiempos de espera excedidos de sesiones SNA y para reducir la actividad general de la WAN en circuitos compartidos. El protocolo ofrece las siguientes ventajas principales:

- Reduce la posibilidad de que se agoten los tiempos de espera de sesiones al terminar el tráfico de control LLC2, SDLC y QLLC en el dispositivo local.

- Reduce la actividad general de la red WAN al eliminar la necesidad de transmitir acuses de recibo (RR) sobre el área amplia. Los RR se configuran en las LAN locales para cada direccionador DLSw.
- Ofrece control del flujo y de congestiones, y control de difusión general de paquetes de búsqueda, entre los direccionadores DLSw y sus estaciones finales conectadas.
- Aumenta los límites de número de saltos de la conexión por puente de direccionamiento de origen.
- Permite la conversión de protocolo entre LLC2, SDLC y QLLC.
- Da soporte al tráfico NetBIOS.

## Utilización de características de DLSw

Las siguientes secciones tratan sobre el uso de diversas características de DLSw:



## Conexiones TCP, descubrimiento de direccionadores contiguos y exploración de difusión múltiple

DLSw utiliza TCP para ofrecer una distribución fiable y en secuencia de información de usuario final a través de una red IP. Los formatos de mensajes DLSw permiten transportar varias sesiones de estaciones finales, o circuitos, a través de una sola conexión de transporte TCP. Hay dos formas de configurar qué direccionadores con soporte de DLSw deben tener conexiones de transporte TCP entre sí para permitir la conectividad deseada de estaciones finales:

- Configurar la dirección IP del direccionador contiguo en uno de los dos direccionadores, o en ambos. Este es el método más básico y recibe soporte de todos los proveedores de direccionadores DLSw.
- Configurar la pertenencia a un grupo de difusión múltiple en cada direccionador, lo que permite que cada direccionador descubra la dirección IP de los demás de forma dinámica. Esta es una característica especial de DLSw de este producto, que facilita la tarea de configurar direcciones IP de direccionadores contiguos.

### Configuración de direccionadores contiguos TCP

Para configurar una dirección IP de direccionador contiguo en un direccionador, utilice el mandato **add tcp** una vez por cada uno de los direccionadores contiguos del direccionador. No es necesario que cada uno de los dos direccionadores contiguos de una relación de direccionador contiguo configure la dirección IP del otro direccionador. Sólo es necesario que un direccionador tenga la dirección del otro, y el otro direccionador se puede configurar para que acepte conexiones TCP dinámicas procedentes de direccionador contiguos no configurados. Utilice el mandato

**enable dynamic-neighbors** para configurar este comportamiento y utilice el mandato **set dynamic-tcp** para configurar los parámetros necesarios para estas conexiones dinámicas. La activación de conexiones TCP dinámicas puede resultar especialmente útil para direccionadores “concentradores” que desea volver a configurar al definir nuevos direccionadores remotos de sucursal que se conectan al concentrador.

Además de la dirección IP, el mandato **add tcp** le permite configurar varios parámetros correspondientes al direccionador contiguo y la propia conexión TCP. El parámetro *Keepalive* controla si la capa TCP sondea ocasionalmente su capa TCP similar en ausencia de tráfico de datos de usuario. Al activar mensajes Keepalive, se notifican antes errores de conexión TCP, pero se puede aumentar la actividad general de la WAN y puede dar lugar a que se notifiquen errores que se podrían haber vuelto a direccionador satisfactoriamente.

El parámetro NetBIOS SessionAlive Spoofing controla si las tramas NetBIOS SessionAlive se reenvían o no al similar DLSw. Este parámetro es importante cuando se han establecido sesiones NetBIOS a través de similares DLSw sobre un enlace ISDN. Si este parámetro está activado y el parámetro Keepalive está desactivado, no pasará tráfico DLSw entre los asociados DLSw si se establecen sesiones NetBIOS desocupadas entre similares DLSw. Esto permitiría que una conexión ISDN subyacente terminara mientras se mantuviera una sesión NetBIOS desocupada sobre DLSw.

El parámetro *connectivity setup type* controla cuándo DLSw está activo y desactiva la conexión TCP. Cuando uno o ambos direccionadores contiguos tienen para CST el valor *active*, DLSw intenta activar la conexión al arrancar el sistema y a intervalos regulares hasta que se activa. Una vez establecida la conexión TCP, DLSw intenta mantenerla activa en todo momento intentando volverla a activar si falla. Si ambos direccionadores contiguos tienen para CST el valor *passive*, DLSw activa la conexión TCP únicamente cuando realmente se necesita para establecer una sesión de estación final DLSw. Cuando finaliza la última sesión DLSw y no se arranca ninguna nueva sesión durante un periodo de tiempo que se puede configurar (*neighbor inactivity timer*), DLSw desconecta la conexión TCP y libera los recursos internos asociados.

## Configuración de grupos para el descubrimiento de direccionadores contiguos

Para evitar el tener que configurar direcciones IP de direccionadores contiguos en uno de cada par de direccionadores contiguos, o en ambos, defina DLSw para que utilice IP de difusión múltiple para descubrir la dirección IP de los direccionadores contiguos a los que se debe conectar. Utilice el mandato **join-group** en cada direccionador para que pase a formar parte de uno o más grupos DLSw y para asignarle un papel dentro del grupo. El papel puede ser “cliente”, “servidor” o “similar”. DLSw utiliza IP de difusión múltiple para descubrir las direcciones IP de todos los direccionadores DLSw que son miembros de los mismos grupos y que tienen el papel complementario (es decir, clientes descubren servidores dentro de un grupo y viceversa, y similares descubren otros similares).

Cuando DLSw aprende las direcciones IP de sus direccionadores contiguos de cada grupo, utiliza el “tipo de configuración de conectividad” de su pertenencia a grupo y el de cada direccionador contiguo del grupo para determinar cuándo se debe activar una conexión TCP con dicho direccionador contiguo. Al igual que con los direccionadores contiguos individuales configurados, cuando el valor de CST es

*active*, DLSw activa la conexión TCP con el direccionador contiguo descubierto en cuanto le es posible e intenta mantener la conexión activa en todo momento. Cuando el valor de ambos CST es *passive*, DLSw activa la conexión TCP únicamente cuando hace falta para llevar sesiones DLSw, y utiliza el parámetro *neighbor inactivity timer* para desconectar la conexión TCP cuando no se utiliza.

## Exploración de difusión múltiple y reenvío de tramas

DLSw utiliza los servicios IP de difusión múltiple para algo más que para descubrir las direcciones IP de los direccionadores contiguos. Utiliza los mismos servicios para reenviar mensajes DLSw en busca de recursos de estaciones finales (por ejemplo, direcciones MAC o nombres de NetBIOS) y para reenviar tráfico de datagramas NetBIOS. Esta característica permite aumentar significativamente la escalabilidad de redes DLSw, puesto que no hace falta que las conexiones TCP estáticas con todos los direccionadores contiguos lleven mensajes de búsqueda y de datagramas. Además, DLSw no necesita enviar una copia distinta de cada mensaje de difusión general en cada conexión TCP, sino que puede enviar una sola copia que se duplica dentro de la infraestructura IP de difusión múltiple.

Para utilizar IP de difusión múltiple para la exploración y reenvío de tramas, emita el mandato **join-group** y defina como *tipo de configuración de conectividad* el valor *passive*. DLSw determina de forma automática cuáles de los otros miembros del grupo dan soporte a la difusión múltiple y cuáles utilizan su pertenencia al grupo simplemente para descubrir direcciones IP de direccionadores contiguos y activar conexiones TCP estáticas. DLSw trabaja simultáneamente con ambos tipos de direccionadores contiguos cuando busca recursos de estaciones finales, reenvía datagramas NetBIOS y establece sesiones DLSw.

Cuando emite el mandato **join-group**, selecciona uno de dos métodos de direccionamiento para describir el grupo al que se une. Cuando especifica un ID de grupo y el papel cliente/servidor/similar tal como se ha descrito anteriormente, el direccionador construye las direcciones IP de difusión múltiple correspondientes y se puede comunicar con otros direccionadores de IBM que utilizan este método. También puede especificar directamente las direcciones IP de difusión múltiple a utilizar y si cada dirección se puede leer, se puede grabar en la misma o ambos. Este método se incorporó para dar soporte a RFC 2166 y permitir la interoperatividad de difusión múltiple con otros productos compatibles con DLSw Versión 2.

Un determinado direccionador puede ser miembro de grupos tradicionales y simultáneamente leer direcciones de difusión múltiple DLSw Versión 2 y grabar en las mismas. Las nuevas direcciones de difusión múltiple también se pueden utilizar para el descubrimiento de direccionadores contiguos, pero debe asegurarse de que para cada par de direccionadores que desea formen una conexión TCP, un direccionador tiene como *tipo de configuración de conectividad* el valor *active* en una dirección con capacidad de grabación que el otro direccionador está leyendo. Tanto si lleva a cabo la función de descubrimiento de direccionadores contiguos como si no es así, la especificación de direcciones de difusión múltiple necesita una planificación de la configuración más cuidadosa, para asegurar la posibilidad de alcance, que la utilización de ID de grupos y el modelo cliente/servidor/similar.

***Reducción del tráfico de exploración:*** Si la cantidad de tráfico de exploración que se reenvía entre direccionadores contiguos DLSw es demasiado alta, hay varias formas de reducir este tráfico de exploración.

SAP abiertos de DLSw
: Cada DLSw envía una lista de todos los SAP abiertos en cualquier interfaz a sus direccionadores contiguos DLSw mediante el intercambio de funciones de DLSw. Los direccionadores contiguos DLSw pueden utilizar esta lista de SAP para limitar el tráfico de exploración enviado a este DLSw.

Listas de direcciones MAC de DLSw
: Cada DLSw puede configurar una lista de direcciones MAC locales. Esta lista se define como de tipo exclusive (representa todas las direcciones MAC a las que se puede acceder a través de este DLSw) o no exclusive (representa una serie de direcciones MAC a las que se puede acceder a través de este DLSw). Cada entrada de la lista contiene una máscara de dirección MAC y un valor de dirección MAC. La lista de direcciones MAC entera y un tipo de exclusividad se envían a todos los direccionadores contiguos DLSw a través del intercambio de funciones de DLSw. Los direccionadores contiguos DLSw pueden utilizar esta lista de direcciones MAC para limitar el tráfico de exploración enviado a este DLSw.

  Las listas de direcciones MAC funcionan de forma similar que las listas de nombres NetBIOS. Para obtener información sobre las listas de nombres NetBIOS, consulte el tema “Listas de nombres NetBIOS” en la página 161.

Entradas de antememoria MAC de DLSw
: Un DLSw puede configurar entradas individuales de la antememoria MAC que correlacionan una determinada dirección MAC con un determinado direccionador contiguo DLSw. Se pueden utilizar varias entradas de la antememoria MAC para correlacionar una determinada dirección MAC con varios direccionadores contiguos DLSw. El DLSw utiliza esta lista de forma local para limitar dónde se envían exploradores DLSw destinados a una dirección MAC configurada.

Filtros de direcciones MAC
: Los filtros de direcciones MAC configurados para la interfaz de red del puente se aplican al tráfico DLSw. Estos filtros de direcciones MAC de entrada de la red del puente se pueden utilizar para limitar el tráfico que se ofrece a DLSw, limitando así el tráfico de exploración enviado a asociados DLSw. Para obtener más información sobre los filtros MAC, consulte los temas “Using and Configuring Mac Filtering” y “Monitoring MAC Filtering” del manual *Guía del usuario de software*.

Limitación de exploradores por cola de transporte
: Ocasionalmente, el rendimiento de una sesión TCP ante un asociado DLSw se puede ver significativamente afectado por una ráfaga de tráfico o por problemas de la red. En estos casos, DLSw puede colocar en cola tráfico de exploración (SNA y NetBIOS) en espera de ser enviado al asociado DLSw. Si hay gran cantidad de datos en la cola, puede tener un efecto negativo en la memoria. A fin de reducir este efecto, DLSw tiene dos parámetros de configuración que controlan la cantidad de tramas exploradoras de SNA que se pueden colocar simultáneamente en cola en un solo asociado DLSw y la cantidad de tramas exploradoras de NetBIOS que se pueden colocar simultáneamente en cola en un solo asociado DLSw. Estos parámetros son 'Maximum SNA explorers per transport queue' y 'Maximum NetBIOS explorers per transport queue'.

## Soporte de dispositivos LLC

DLSw da soporte a estaciones finales SNA y NetBIOS conectadas al direccionador mediante interfaces de LAN y de WAN de conexión por puente remota. Estaos estaciones finales y el direccionador ejecutan el Control lógico de enlaces (LLC) estándar ISO 8802-2 (IEEE 802.2) a fin de ofrecer secuencia de datos y distribución fiable. El direccionador actualmente da soporte al tráfico LLC conectado por puente sobre los siguientes tipos de interfaces, y todas se pueden utilizar para el flujo de tráfico entre estaciones finales DLSw y LLC:

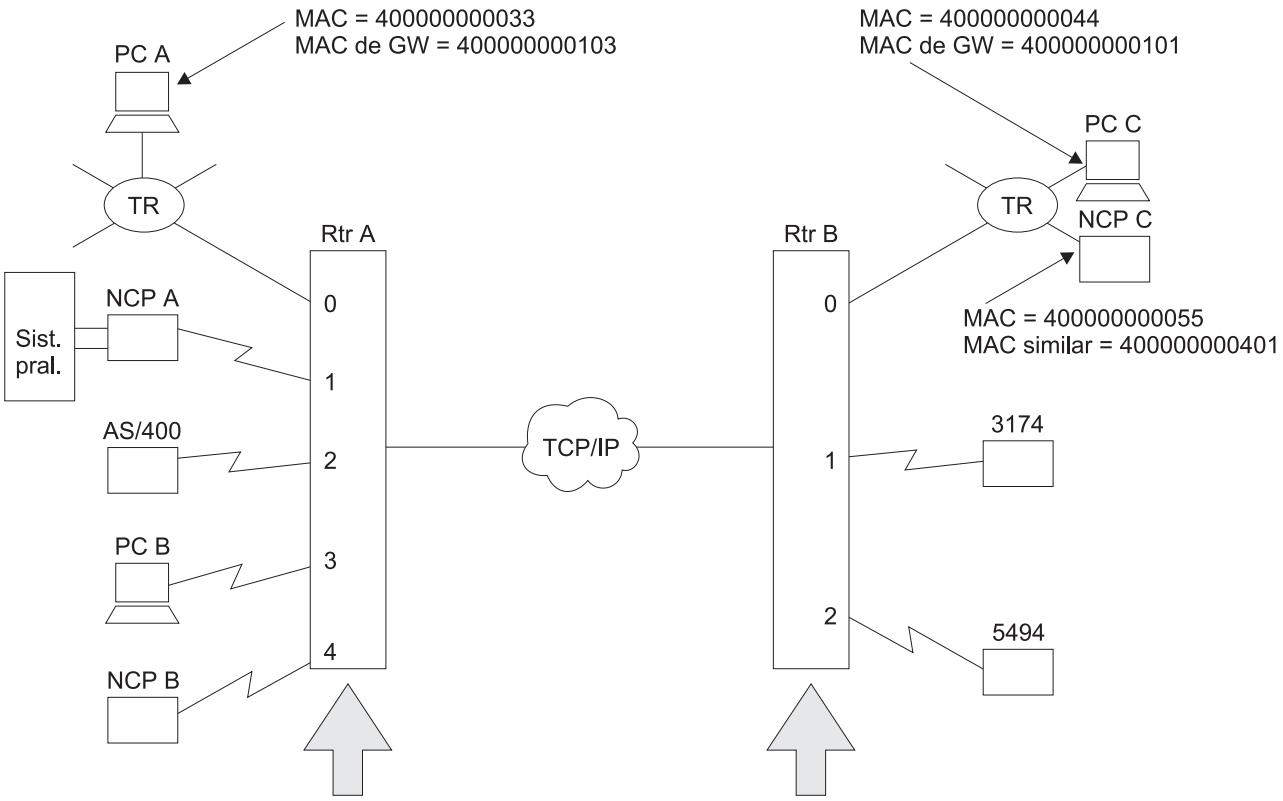
- Red en anillo
- Ethernet/802.3
- ATM (como un cliente de emulación de LAN)
- Frame Relay (utilizando formatos de tramas conectadas por puente RFC 1490/2427)
- PPP
- Circuitos de marcación que utilizan tramas PPP o FR (por ejemplo, ISDN)

Puesto que DLSw utiliza las direcciones MAC y SAP disponibles en tramas conectadas por puente, no hay necesidad de configurar en DLSw ninguna información sobre estaciones finales LLC individuales. DLSw recibe tráfico de difusión general enviado por estas estaciones finales, y utiliza los métodos normales de difusión general de LAN/puente para establecer el contacto inicial con las mismas. Sin embargo, debe configurar el soporte de conexión por puente para cada interfaz que vaya a utilizar DLSw y configurar dentro de DLSw los SAP que se van a utilizar en cada interfaz.

## Soporte de dispositivos SDLC

DLSw da soporte a estaciones finales SDLC que pueden ser SNA PU de tipo 1, 2.0, 2.1, 4 (para tráfico NCP-NCP) o 4/5 (un sistema principal o NCP que realiza la función límite de SNA). El direccionador puede adoptar un papel de estación de enlace SDLC primaria o secundaria, en función del papel configurado para la interfaz SDLC o en función de la negociación de XID de SNA. En el papel primario, el direccionador puede dar soporte a varios dispositivos SDLC de distintos tipos de PU en la misma línea física SDLC multipunto. En el papel secundario, el direccionador puede representar varias estaciones secundarias SDLC en una sola interfaz física SDLC. También da soporte a la función de sondeo de grupos de IBM 3174 en el papel secundario.

**Nota:** DLSw da soporte a dispositivos SDLC PU1 que se comunican con dispositivos conectados a SDLC o conectados a LAN que dan soporte a dispositivos PU1 (por ejemplo, 3745). Pero no da soporte a dispositivos SDLC PU1 que se comunican con dispositivos que no dan soporte a dispositivos PU1 (por ejemplo, AS/400).




| Interfaz | Direcc. SDLC | Tipo PU | MAC origen | MAC dest. |
|---|---|---|---|---|
| 1 (sec) | 01 | 2 | 400000000101 | 400000000044 |
| | 02 | 5 | 400000000102 | 4011111101C1 |
| | 03 | 5 | 400000000103 | 400000000033 |
| | 04 | 2 | 400000000104 | 400000000301 |
| 2 (neg) | 01 | 2 | 400000000201 | 4011111102C1 |
| 3 (neg) | 01 | 2 | 400000000301 | 000000000000 |
| 4 (neg) | 01 | 4 | 400000000401 | 400000000055 |

| Interfaz | Direcc. SDLC | Tipo PU | MAC origen | MAC dest. |
|---|---|---|---|---|
| 1 (pri) | C1 | 2 | 4011111101C1 | 000000000000 |
| 2 (neg) | C1 | 2 | 4011111102C1 | 400000000201 |

*Figura 45. Configuraciones SDLC de DLSw de ejemplo*

La Figura 45 ilustra algunas de las configuraciones SDLC que reciben soporte de DLSw y muestra un subconjunto de la configuración DLSw necesaria para establecer una correlación entre direcciones SDLC y DLSw (MAC y SAP). El diagrama muestra sesiones DLSw *locales* (dentro de un solo direccionador) y *remotas* (entre dos direccionadores y una red IP).

Están configuradas las siguientes sesiones DLSw:

- NCP A a PC A, B y C y al 3174

  Para que NCP A pueda comunicarse con estas 4 PU, el Direccionador A debe tener una estación de enlace secundaria configurada en la Interfaz 1 por cada PU. Esta interfaz se debe configurar en un SDLC como secundaria, dúplex completo y punto a punto. Se recomienda el sondeo de grupos siempre que hay varias estaciones secundarias en la misma interfaz, a fin de reducir el sondeo no productivo.

  En este ejemplo, NCP A se comunica con el PC C mediante la dirección de estación SDLC 01, con el 3174 mediante la dirección 02, con el PC A mediante la dirección 03 y con el PC B mediante la dirección 04. Observe que las sesiones de PC A y C incluyen conversión SDLC-a-LLC, en una configu-

ración local y remota respectivamente. La sesión con el PC B es una sesión SDLC-a-SDLC local, lo cual resulta poco usual.

Para las estaciones de enlace secundarias definidas en el Direccionador A, un tipo de PU igual a 5 indica que el dispositivo SDLC es un sistema principal (cuyo componente frontal es un controlador) que realiza la función BNN de SNA con un dispositivo PU2.0 directo. Aquí, un tipo de PU igual a 2 indica que es sistema principal SDLC/FEP actúa como un nodo T2.1 que se comunica con otro nodo T2.1 en la red DLSw.

- AS/400 con el 5494

  Aquí, estos dispositivos funcionarán como nodos T2.1 y los enlaces SDLC de sus respectivos direccionadores están configurados como negociables (los nodos T2.1 también reciben soporte en enlaces de papel fijo, y DLSw restringe la negociación de papeles en consecuencia). Las estaciones realizarán la negociación XID completa, incluida la determinación de papeles y la resolución de direcciones SDLC (si el direccionador y la estación final del mismo enlace están ambos configurados con distintas direcciones de estaciones SDLC). Observe que no hay relación en las configuraciones SDLC-SDLC remotas entre las direcciones de estaciones SDLC utilizadas en los dos enlaces SDLC distintos. Las estaciones SDLC-a-LLC remotas también reciben soporte entre dispositivos T2.1.

- NCP B a NCP C

  El NCP B está configurado como PU tipo 4, lo que indica que esta sesión DLSw debe llevar tráfico de subárea INN entre los NCP, no tráfico BNN de un NCP a un dispositivo PU 2. El ejemplo muestra una sesión SDLC-a-LLC remota, pero se da soporte a sesiones similar a similar. La función INN de DLSw no da soporte a TG de varios enlaces ni a funciones de carga/vuelco remoto de NCP.

## Correlación de direcciones

La configuración DLSw ofrece una correlación entre direcciones de estaciones SDLC de un solo byte y las direcciones MAC y SAP mediante los que DLSw identifica estaciones finales. La dirección MAC de origen correspondiente a una estación SDLC representa el dispositivo SDLC ante el resto de la red DLSw. Es la dirección de origen correspondiente a tramas procedentes del dispositivo y la dirección de destino correspondiente a tramas destinadas al dispositivo. La dirección MAC de origen es necesaria para que el dispositivo SDLC pueda comunicarse a través de DLSw.

La dirección MAC de destino especifica la estación final de la red DLSw a la que este dispositivo SDLC se debe conectar cuando empiece a establecer comunicación. Los dispositivos SDLC que van a ser siempre el destino de nuevas sesiones y nunca los iniciadores deben tener una dirección MAC de destino igual a cero. Cuando el direccionador se configura como una estación de enlace secundaria, es importante definir una dirección MAC de destino para que la conexión del salida del sistema principal sea satisfactoria. Esto se debe a que una estación de enlace secundaria no puede iniciar un contacto con el sistema principal en nombre de una estación final DLSw remota que se conecta, sino que debe esperar al sondeo. Observe que cuando la estación final DLSw remota es SDLC (por ejemplo, el 3174 del Direccionador B de la Figura 45 en la página 533) y está emparejada con una estación secundaria local, la estación remota puede tener una dirección

MAC de destino igual a cero para reflejar su dependencia de la conexión de salida del sistema principal.

## Configuración DLSw y configuración SDLC

Para utilizar DLSw sobre una interfaz SDLC, debe configurar la correlación de direcciones como parte de la configuración DLSw y debe configurar también una parte de la información como parte de la configuración SDLC. Como requisito mínimo en SDLC, debe definir la interfaz para que sea SDLC y configurar otros parámetros a nivel de interfaz como el papel del enlace. Los parámetros de interfaz SDLC ofrecen valores por omisión para todas las estaciones de enlace SDLC de esta interfaz, pero si desea tener valores exclusivos para una estación, puede configurar información individual de estación SDLC.

El par de direcciones *número de interfaz, dirección de estación SDLC* es la clave común que enlaza información de correlación de direcciones DLSw con la configuración a nivel de estación de SDLC. El software del direccionador realiza esta asociación en el momento de la inicialización. Si DLSw intenta inicializar una estación de enlace cuya dirección de estación SDLC no está configurada en SDLC en la interfaz que especifica DLSw, SDLC crea una definición de estación de enlace de forma dinámica y utiliza los valores por omisión de los parámetros de SDLC para dicha interfaz.

## Relación con la función SDLC Relay

SDLC Relay es una función del direccionador que encapsula tramas SDLC completas en paquetes IP, que luego se direccionan a otro direccionador que también dé soporte a SDLC Relay. El direccionador de destino elimina la cabecera IP y distribuye las tramas SDLC sin modificar a un enlace SDLC de destino.

Esta función difiere del soporte SDLC de DLSw en lo siguiente:

- Con SDLC Relay, no hay ninguna estación de enlace SDLC funcionando dentro del direccionador. Las tramas de control (por ejemplo, RR) fluyen a través de la red IP. Con DLSw, el soporte SDLC del direccionador termina la conexión SDLC. Sólo los datos procedentes de tramas SDLC fluyen a través de la red IP. Como resultado, DLSw puede ofrecer una mejor utilización del ancho de banda de la WAN y es menos sensible a tiempos de espera excedidos de enlaces debidos a retrasos de la WAN.
- Las tramas de control y de datos de SDLC pasan de forma transparente a través de SDLC Relay, mientras que DLSw tiene que interpretar y modificar algunos de ellos. Junto con el hecho de que DLSw termina la conexión SDLC, esto significa que determinadas configuraciones y funciones de productos (por ejemplo, TG de varios enlaces entre NCP) no reciben soporte de DLSw.
- SDLC Relay necesita que el tipo de datos de ambas estaciones finales que se comunican sea SDLC. DLSw ofrece una función de conversión de protocolos, de modo que el tipo de datos de la otra estación final puede ser LLC, SDLC, QLLCo cualquier otro tipo de datos que reciba soporte de un producto DLSw.
- DLSw es un estándar desarrollado por APPN Implementers Workshop y documentado en un IETF RFC. Como tal, recibe soporte de varios proveedores. SDLC Relay actualmente sólo recibe soporte de determinados direccionadores de IBM y compatibles.

Debe utilizar DLSw cuando:

- Necesite una conversión de protocolos de SDLC a LLC o QLLC
- Desee restringir el tráfico de control (por ejemplo, tramas RR) que fluye fuera de la red IP

Debe utilizar SDLC Relay cuando:

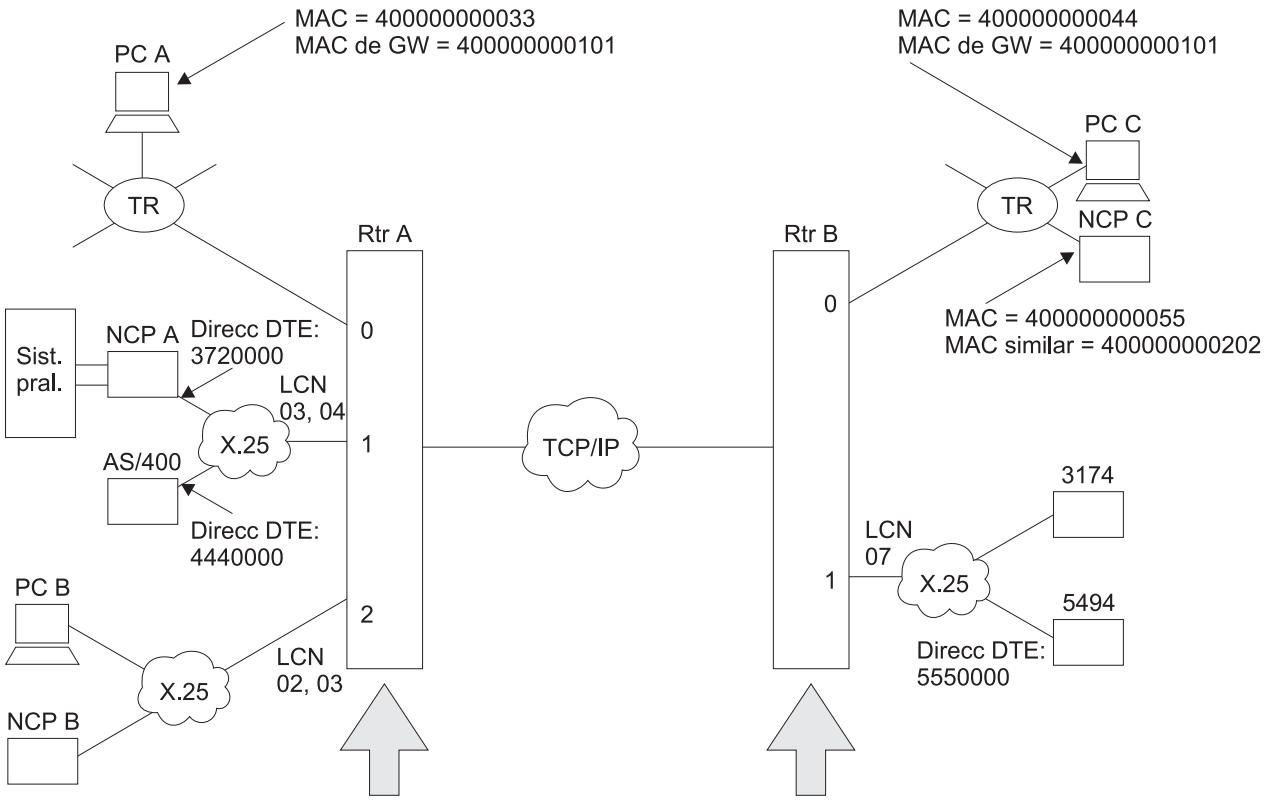
- Necesite una de las funciones SDLC-SDLC o configuraciones que no recibe soporte actualmente de DLSw

En otras configuraciones SDLC-SDLC, elija la función que mejor se ajuste a sus requisitos de facilidad de configuración, utilización de la WAN y soporte del entorno actual de estaciones finales. Para obtener más información sobre SDLC Relay, consulte el manual *Guía del usuario de software*

## Soporte de dispositivos QLLC

QLLC es un protocolo que funciona sobre el protocolo de capa de paquetes de X.25 a fin de ofrecer un aspecto de estación parecido a SDLC ante dispositivos SNA y redes X.25. QLLC da soporte a una sola PU SNA por circuito virtual (PVC o SVC). La multiplexación de canal X.25 permite la conexión de varios circuitos virtuales o PU a través de una sola interfaz física con la red X.25. La arquitectura QLLC define papeles de estaciones primaria, secundaria y similar, pero esto es menos importante que en SDLC, puerto que no afecta a la transmisión de datos de usuario final. Los datos correspondientes a todos los circuitos virtuales fluyen en una sola conexión de enlace de capa 2 LAPB, que funciona en una modalidad de equilibrio. Ambos extremos tienen permiso de envío en todo momento mientras el enlace esté conectado.

DLSw da soporte a estaciones finales QLLC que pueden ser PU SNA tipo 2.0, 2.1, 4 (para el tráfico NCP-NCP) o 4/5 (un sistema principal o NCP que realiza la función límite SNA). Las estaciones finales pueden conectarse mediante PVC configurados, SVC configurados o SVC dinámicos, resultantes de una llamada entrante. El direccionador puede adoptar un papel de estación de enlace QLLC primario o secundario, en función del papel configurado para la interfaz X.25 y en función de la negociación de XID de SNA. Distintos tipos de PU pueden coexistir en distintos circuitos virtuales de la misma interfaz física, pero sólo se da soporte a un papel de estación de enlace por interfaz.




| Interfaz | Tipo VC | Direcc LCN/DTE | Tipo PU | MAC origen | MAC dest |
|---|---|---|---|---|---|
| 1 (neg) | PVC | 03 | 5 | 400000000102 | 401111110101 |
| | PVC | 04 | 5 | 400000000105 | 400000000201 |
| | SVC | 3720000 | 5 | 400000000101 | 000000000000 |
| | SVC | 4440000 | 2 | 400000000104 | 000000000000 |
| 2 (neg) | PVC | 02 | 2 | 400000000201 | 400000000105 |
| | PVC | 03 | 4 | 400000000202 | 400000000055 |

Interfaces activadas para llamadas entrantes
1

| ID conexión | MAC dest |
|---|---|
| PCA | 400000000033 |
| PCC | 400000000044 |

| Interfaz | Tipo VC | Direcc LCN/DTE | Tipo PU | MAC origen | MAC dest |
|---|---|---|---|---|---|
| 1 (pri) | PVC | 07 | 2 | 401111110101 | 400000000102 |

Interfaces activadas para llamadas entrantes
1

| ID conexión | MAC dest |
|---|---|
| AS400 | 400000000104 |

*Figura 46. Ejemplo de configuraciones QLLC de DLSw*

La Figura 46 ilustra algunas de las configuraciones QLLC que reciben soporte de DLSw y muestra un subconjunto de la configuración DLSw necesaria para establecer una correlación entre direcciones QLLC y DLSw (MAC y SAP). El diagrama muestra sesiones DLSw *locales* (dentro de un solo direccionador) y *remotas* (entre dos direccionadores y una red IP). No se muestra ningún par QLLC-a-SDLC, pero reciben soporte en configuraciones tanto locales como remotas.

Están configuradas las siguientes sesiones DLSw:

- NCP A a PC A, B y C y al 3174

  El NCP A está conectado a la Interfaz 1 del Direccionador A mediante 2 PVC y 2 SVC; cada circuito virtual representa una PU. Los PVC se direccionan dentro de una interfaz mediante un *Número de canal lógico* y los SVC mediante la dirección DTE (número de teléfono) del dispositivo X.25 conectado. Al igual

que con SDLC, la configuración DLSw correlaciona estas direcciones DLC "nativas" (dirección LCN o DTE) con direcciones DLSw (MAC y SAP).

En este ejemplo, el NCP A se comunica con el 3174 (QLLC-QLLC remoto) mediante PVC 03, y con el PC B (QLLC-QLLC local) mediante PVC 04. Estos LCN son realmente locales para el Direccionador A; NCP puede utilizar distintos LCN para sus PVC correspondientes en la red X.25. El Direccionador A se conecta al NCP A con PC C (QLLC-LLC remoto) y con el PC A (QLLC-LLC local) mediante dos SVC entre la dirección DTE 3720000 para el NCP A y la dirección DTE correspondiente a la interfaz 1 del Direccionador A. Puesto que el Direccionador A debe poder aceptar llamadas procedentes del NCP A, tiene la Interfaz 1 activada para llamadas entrantes ante DLSw. El NCP A utiliza *ID de conexión*, que se describen a continuación, para establecer conexión de salida con los PC A y C.

En el Direccionador B, el PC C no está configurado porque está conectado a LLC/LAN, El 3174 se conecta mediante la Interfaz 1 LCN 07, que no tiene relación con la Interfaz ni número LCN utilizado en el Direccionador interfaz.

- AS/400 con el 5494

  Además de NCP A, el AS/400 también está conectado al Direccionador A mediante la Interfaz 1. A diferencia de SDLC, no hay ninguna ventaja en rendimiento derivada de limitar el número de estaciones en una determinada interfaz. Puede haber varias estaciones en un enlace, independientemente del papel del enlace. Si el papel es negociable y las estaciones son nodos T2.1 o PU4, cada estación puede negociar independientemente para pasar a ser primaria o secundaria.

  El AS/400 no tiene ninguna dirección MAC de destino configurada en el Direccionador A, y por lo tanto no puede establecer conexión de salida con el 5494. El 5494 no está configurado en el Direccionador B, por lo que será un SVC dinámico. El 5494 utiliza un ID de conexión para indicar que desea conectarse al AS/400. El Direccionador B tiene la Interfaz 1 activada para llamadas entrantes ante DLSw, de modo que puede recibir llamadas procedentes del 5494.

- NCP B a NCP C

  El NCP B está configurado como PU tipo 4, lo que indica que esta sesión DLSw debe llevar tráfico de subárea INN entre los NCP, no tráfico BNN de un NCP a un dispositivo PU 2. El ejemplo muestra una sesión QLLC-a-LLC remota, pero también se da soporte las sesiones similar a similar y a las sesiones en las que interviene SDLC. La función INN de DLSw no da soporte a TG de varios enlaces ni a funciones de carga/vuelco remoto de NCP.

## Correlación de direcciones

DLSw ofrece una correlación entre los pares MAC/SAP para direccionar entidades de estación final en el dominio DLSw y entre los pares *interfaz, LCN* (PVC) o *interfaz, dirección DTE* (SVC) que se utilizan en el dominio X.25. Esta correlación tiene lugar en el momento de establecer la conexión, pero utiliza información de direccionamiento configurada en el direccionador y en los productos de la estación final.

## Conexión de salida (a estaciones QLLC)

DLSw recibe un mensaje CUR_ex o CUR_cs dirigido a un determinado MAC y SAP de destino. Busca entre sus estaciones finales QLLC una cuyo SMAC y SSAP (SAP sólo se comprueba para CUR_cs) coincida con este MAC/SAP de destino. Debe haber una coincidencia o bien ninguna, puesto que los SMAC son exclusivos dentro del direccionador.

Si se encuentra una coincidencia, DLSw comienza el establecimiento de conexión con la estación QLLC utilizando la interfaz correspondiente y LCN para un PVC, o la interfaz y número de teléfono para un SVC. DLSw puede realizar varias llamadas de salida a la misma dirección DTE utilizando una sola definición de estación QLLC (SVC). Esto permite conectar varios dispositivos DLSw al mismo destino con un mínimo esfuerzo de configuración.

## Conexión de entrada (procedente de estaciones QLLC)

Para los **PVC**, QLLC recibe una trama que comienza el establecimiento de circuito desde la estación final conectada. QLLC y DLSw comparan con la interfaz y LCN en los que se ha recibido la trama con una entrada de la lista de estaciones QLLC. Se encuentra una coincidencia o bien ninguna, puesto que los LCN deben ser exclusivos dentro de una interfaz. Si no se encuentra ninguna coincidencia o si la entrada no tiene DMAC/DSAP definido, la conexión de entrada falla. De lo contrario, se inicia una conexión con el DMAC/DSAP definido. El MAC/SAP de origen correspondiente a la conexión es el SMAC/SSAP de la misma entrada de la lista.

Para los **SVC**, DLSw obtiene direcciones MAC/SAP utilizando la dirección del emisor de la llamada X.25 o un *id de conexión* (bytes 4-11) del campo de datos de usuario de llamada del paquete Call_Request recibido. Si la dirección del emisor de la llamada está disponible, en primer lugar DLSw la compara con todas sus direcciones DTE de SVC configuradas correspondientes a la interfaz llamada. Se encuentra una coincidencia o bien ninguna, porque las direcciones DTE deben ser exclusivas dentro de una interfaz. Si se encuentra una coincidencia y la entrada de la lista de estaciones QLLC tiene un DMAC/DSAP distinto de cero, DLSw utiliza este DMAC/DSAP como la dirección de destino para el establecimiento de la conexión. El MAC/SAP de origen correspondiente a la conexión es el SMAC/SSAP de la misma entrada de la lista.

Si no hay ninguna dirección de emisor de llamada disponible, si hay una pero coincide con una entrada que no tiene DMAC/DSAP definido, o bien si no coincide con ninguna dirección DTE definida para la interfaz llamada, DLSw comprueba si algún id de conexión (CID) recibido en el paquete Call_Request coincide con alguno definido en los registros de destino QLLC de DLSw. El CID se interpreta como una serie de un máximo de 8 caracteres alfanuméricos EBCDIC.

Si hay una coincidencia de CID, DLSw utiliza el DMAC/DSAP asociado en el Registro de destino como la dirección de destino para el establecimiento del circuito. Si también hay una coincidencia de dirección de emisor de la llamada (sin DMAC/DSAP definido), DLSw utiliza el SMAC/SSAP de la entrada coincidente de la lista de estaciones. Si no es así, DLSw asigna de forma dinámica el SMAC y SSAP. Para el SMAC, DLSw elige la siguiente dirección MAC disponible (en sentido rotatorio) del rango definido por los parámetros de configuración de DLSw *QLLC base MAC address* y *Max dynamic addresses*. El SSAP definido de forma dinámica siempre es 0x04.

Si no hay coincidencia de dirección de emisor de la llamada o de id de conexión, DLSw no toma la llamada. Observe que los CID son el único método con que una sola dirección de emisor de llamada puede efectuar llamadas a diversos destinos.

APPN y DLSw pueden ambos aceptar llamadas QLLC procedentes de la misma dirección de emisor de llamada. DLSw obtiene el primer acceso a la llamada porque est más restrictivo en cuanto a las llamadas que acepta. Si DLSw no encuentra ninguna coincidencia de emisor de la llamada o de id de conexión, DLSw no borra la llamada, sino que permite que se presente a APPN.

Por lo tanto, para que se acepte una llamada entrante, la dirección del emisor de la llamada o un id de conexión deben estar definidos ante DLSw. Aunque esto es necesario principalmente para ofrecer correlación de direcciones, también ofrece un elemento de seguridad frente a llamadas entrantes procedentes de partícipes no autorizados. Otras medidas posibles de seguridad incluyen no activar una interfaz para llamadas entrantes ante DLSw y definir el número de direcciones MAC de origen dinámicas posibles en cero. El primero evita que entren llamadas en esta interfaz, incluso procedentes de direcciones DTE configuradas en DLSw. El último evita únicamente la entrada de llamadas dinámicas procedentes de direcciones DTE no configuradas.

Para permitir que DLSw acepte cualquier emisor de la llamada (independientemente de la dirección DTE o CID ) y lo correlacione con un determinado DMAC y DSAP (uno por recuadro), puede configurar un registro Destino de QLLC con un valor CID igual a "ANYCALL" y el DMAC y DSAP deseados. DLSw asigna de forma dinámica el SMAC y SSAP. Si se utiliza esta característica, DLSw acepta todas las llamadas. No se presenta ninguna llamada ante APPN y todas las características de seguridad asociadas a la correlación de direcciones se pasan por alto.

## Configuración DLSw y configuración X.25

Para utilizar el soporte de QLLC de DLSw sobre una determinada interfaz X.25, debe configurar la correlación de direcciones como parte de la configuración DLSw y debe configurar también la siguiente información como parte de la configuración de la interfaz X.25. Consulte el tema “Configuración de interfaces X.25” en la página 550 para ver un ejemplo de estos pasos y consulte el capítulo “Using the X.25 Network Interface” del manual *Guía del usuario de software* para obtener información adicional.

1. Configure la interfaz para que sea X.25 y configure sus parámetros básicos de interfaz X.25.
2. Añada DLS como un protocolo soportado.
3. Configure los PVC que va a utilizar DLSw y asócielos a DLSw.
4. Configure direcciones DTE de SVC estáticas que DLSw va a utilizar y asócielas a DLSw. Son las mismas direcciones que se han configurado en DLSw. No es necesario configurar las direcciones DTE de las estaciones finales QLLC que pueden efectuar llamadas de entrada de forma dinámica.

A diferencia de SDLC, X.25 no tiene capacidad para crear de forma dinámica una definición de estación de enlace (circuito virtual) basada en la información configurada en DLSw.

## Relación con la función XTP

El Protocolo de transporte X.25 (XTP) es una función del direccionador que toma paquetes procedentes de circuitos virtuales X.25 y los transporta a través de TCP/IP a otro direccionador que también dé soporte a XTP. Luego el direccionador de destino elimina la información de cabecera XTP y distribuye los paquetes a un circuito virtual X.25 de destino.

Esta función se puede comparar con el soporte de QLLC de DLSw en que:

- Ambas funciones utilizan TCP/IP para establecer comunicación entre direccionador similares y pueden multiplexar la información procedente de diversos circuitos virtuales (o sesiones DLSw) en una sola conexión TCP.
- Con ambas funciones, el direccionador termina las conexiones de capa de paquete de capa 3 y de LAPB de capa 2 con la estación final X.25. Las tramas de control LAPB no fluyen a través de TCP/IP.
- XTP sólo da soporte a la comunicación entre dos estaciones finales X.25. DLSw realiza la conversión de protocolo entre LLC (conectado por puente de forma remota o en una LAN), SDLC, QLLC y cualquier otro tipo de datos soportado por un producto DLSw.
- XTP no se ve afectado por el tipo de LLC (por ejemplo, QLLC o PAD) que funciona sobre la capa de paquete. Siempre que ambas estaciones finales X.25 den soporte al mismo tipo de LLC, pueden comunicarse a través de XTP. El soporte de QLLC de DLSw sólo se puede comunicar con estaciones finales SNA que ejecuten QLLC.
- Con XTP, hay una asociación configurada entre un circuito virtual de una red X.25, un direccionador similar y un circuito virtual de otra red X.25. Sólo para los SVC, se pueden definir varios direccionadores similares e intentar activar una conexión a través de un direccionador secundario en el caso de que el direccionador primario debe de estar disponible, pero XTP no realiza búsquedas paralelas ni intentos de establecimiento de conexión. Por otro lado, DLSw correlaciona un circuito virtual con una dirección MAC y SAP y luego realiza una búsqueda completamente dinámica entre varios similares a fin de localizar la estación de destino. Con el soporte de difusión múltiple de DLSw, no hace falta configurar las direcciones IP similares individuales a buscar.
- XTP puede correlacionar un PVC únicamente con otro PVC, y un SVC únicamente con otro SVC. En configuraciones QLLC-a-QLLC de DLSw, se puede correlacionar un PVC con un SVC. En la práctica esto resulta poco útil, puesto que DLSw intentará activar el SVC siempre que el protocolo QLLC esté activo en el PVC.
- Con XTP que utiliza SVC, las llamadas se emiten a direcciones DTE de estaciones finales X.25 y se reciben de las mismas. Es posible que se tenga que configurar un conmutador X.25 o una suscripción de red para permitir que el direccionador represente varias direcciones DTE. Con DLSw, las llamadas se reciben de estaciones finales en la dirección DTE de la interfaz del direccionador y viceversa.
- DLSw es un estándar desarrollado por APPN Implementers Workshop y documentado en un IETF RFC. Como tal, recibe soporte de varios proveedores. Actualmente, XTP sólo recibe soporte de determinados direccionadores de IBM y compatibles.

Debe utilizar DLSw cuando:

- Necesite una conversión de protocolos de QLLC a SDLC o LLC
- Necesite varias vías de acceso simultáneas a un destino

Debe utilizar XTP cuando:

- Ejecute un protocolo que no sea QLLC sobre X.25

En otras configuraciones QLLC-a-QLLC, seleccione el protocolo que mejor se ajuste a los requisitos de su red. Para obtener más información sobre XTP, consulte el capítulo “Using, Configuring, and Monitoring XTP” del manual *Guía del usuario de software*.

## Soporte de interfaz APPN

DLSw tiene una interfaz interna con APPN que conecta APPN a estaciones finales conectadas a direccionadores DLSw remotos. Los direccionadores remotos no tienen que dar soporte a APPN, lo que puede reducir la cantidad de memoria que necesitan. Tal como se muestra en la Figura 47, esta interfaz interna es el equivalente de ocultar una conexión DLC (por ejemplo, LLC sobre una LAN) en una sola interfaz de software.

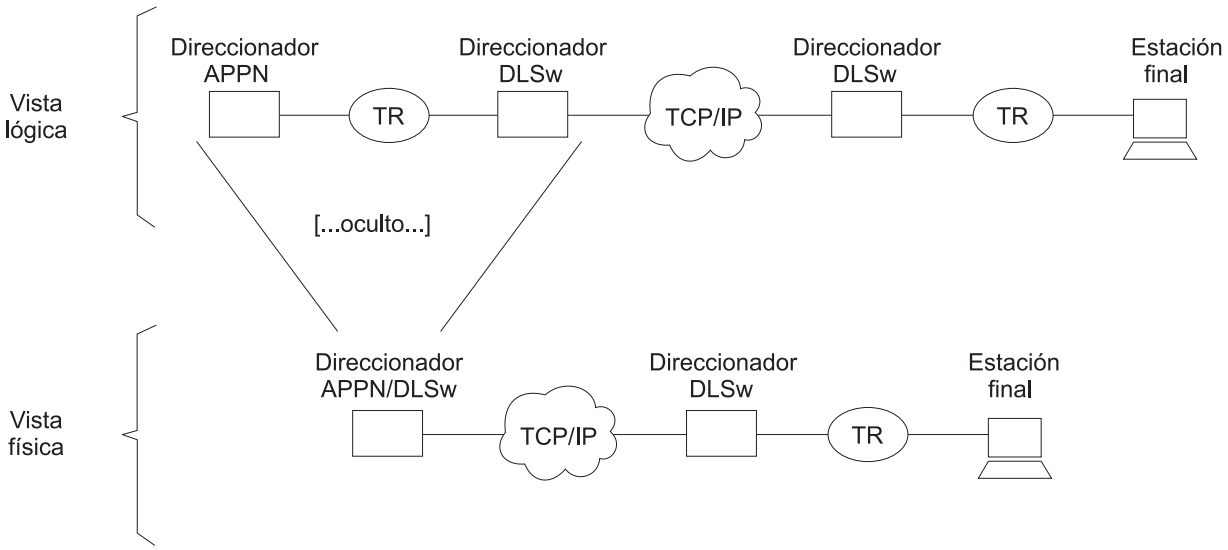



*Figura 47. Interfaz de software APPN-a-DLSw*

APPN no puede utilizar la interfaz de software DLSw para alcanzar las estaciones finales conectadas de forma local al direccionador APPN/DLSw. Debe utilizar su soporte DLC nativo para establecer comunicación con estos dispositivos.

No se necesita ninguna configuración DLSw adicional para dar soporte a la interfaz APPN. Debe activar los mensajes Keepalive de TCP en el direccionador remoto DLSw a fin de activar la detección de la pérdida de las estaciones de enlace en el puerto DLSw. Debe configurar APPN para que utilice una interfaz virtual DLSw para alcanzar una determinada estación final. Para obtener información sobre cómo implementar APPN a través de DLSw, consulte el capítulo sobre configuración de APPN del manual *Consulta de configuración y supervisión de protocolos Volumen 2.*

## Utilización de la característica de prioridad de direccionador contiguo

Muchas configuraciones de red DLSw ofrecen varias vías de acceso entre un direccionador DLSw de origen y estaciones finales de destino haciendo que las estaciones finales sean locales para más de un direccionador DLSw de destino. Para ofrecer control adicional sobre qué direccionador DLSw remoto se utiliza para nuevos circuitos, puede asignar una prioridad (alta, media o baja) a cada direccionador contiguo definido. Aunque los valores permitidos son parecidos, la prioridad de direccionador contiguo ***no*** es igual que las prioridades para equilibrar tráfico SNA y NetBIOS que se describen en el tema “Equilibrio del tráfico SNA y NetBIOS” en la página 544.

Para la prioridad de direccionador contiguo, el usuario asigna una prioridad al definir un direccionador contiguo mediante los mandatos **add tcp** o **join group**. Heredan una prioridad de grupo todas las conexiones de transporte activadas dentro de dicho grupo.

Cuando DLSw está originando un circuito y descubre que la dirección MAC de destino o el nombre de NetBIOS se puede alcanzar a través de varios direccionadores DLSw remotos, establece el circuito a través del direccionador contiguo que tiene la prioridad más alta. Si hay varios direccionadores remotos que comparten esta prioridad más alta, DLSw utiliza un método “rotatorio” de asignar nuevos circuitos entre estos direccionadores.

Mediante la prioridad de direccionador contiguo, puede establecer una relación de primario/reserva entre los direccionadores remotos. Un direccionador de prioridad más baja no se utiliza a no ser que el direccionador de prioridad más alta deje de estar disponible. Además, el método rotatorio permite equilibrar la carga entre los direccionadores con la misma prioridad.

**Notas:**

1. Cuando se recibe una trama SNA destinada a una dirección MAC que no tiene información en antememoria para que los direccionadores contiguos puedan alcanzar la dirección SNA, se envía un mensaje de exploración de SNA a todos los direccionadores contiguos DLSw. Las respuestas al mensaje de exploración de SNA se recopilan durante el periodo de tiempo especificado en el parámetro “neighbor priority wait timer”. Una vez transcurrido este periodo de tiempo, la entrada de antememoria de direcciones MAC se actualiza con la información de las respuestas procedentes de los direccionadores contiguos con la prioridad más alta. Se elige uno de estos direccionadores contiguos para que maneje este circuito SNA y se envía una respuesta a la trama SNA original recibida. Las siguientes peticiones del circuito SNA correspondientes a esta dirección MAC utilizarán uno de los direccionadores contiguos con prioridad más alta colocados en antememoria para activar el circuito.
2. Cuando se recibe una trama NetBIOS destinada a un nombre de NetBIOS que no tiene ninguna entrada actual de información en la antememoria correspondiente a este nombre de NetBIOS, se envía un mensaje de exploración de NetBIOS a todos los direccionadores contiguos DLSw que dan soporte a NetBIOS. A diferencia de en SNA, se recopilan respuestas durante un periodo de tiempo especificado antes de que se envíe la respuesta a la trama NetBIOS original. Los temporizadores de estaciones finales no suelen permitir un retraso de espera en el direccionador.

Por lo tanto, la primera respuesta al mensaje de exploración de NetBIOS se guarda. Este direccionador contiguo se utiliza para activar este circuito NetBIOS y se envía una respuesta a la trama NetBIOS original recibida. En este intervalo, las siguientes respuestas al mensaje de exploración de NetBIOS se utilizan para actualizar la antememoria de nombres de NetBIOS.

- Si se recibe una respuesta de un direccionador contiguo de igual prioridad a la información que actualmente está en antememoria, se añade a la antememoria.
- Si se recibe una respuesta de un direccionador contiguo de prioridad superior a la información que actualmente está en antememoria, la información que actualmente está en antememoria se elimina y se añade la información correspondiente al nuevo direccionador contiguo de prioridad más alta.
- Si se recibe una respuesta de un direccionador contiguo de prioridad más baja a la información que actualmente está en antememoria, se pasa por alto. Las siguientes peticiones del circuito NetBIOS correspondientes al nombre de NetBIOS utilizarán uno de los direccionadores contiguos de prioridad más alta colocados en antememoria para activar el circuito.

Se puede desactivar la característica de prioridad de direccionador contiguo correspondiente a todas las direcciones MAC o a determinados grupos de direcciones MAC. Para desactivarla para todas las direcciones MAC, defina para el parámetro *wait neighbor priority timer* el valor 0. Para desactivarla para un grupo de direcciones MAC, cree una modificación de explorador de antememoria MAC y defina para su parámetro *wait neighbor priority timer* el valor 0.

Si la característica de prioridad de direccionador contiguo está desactivada, la información sobre asociados DSLw no se coloca en antememoria para la dirección MAC. Siempre se envían exploradores SNA y NetBIOS a todos los asociados DLSw aplicables y el primer asociado DSLw se utiliza para establecer la sesión DLSw (independientemente de su prioridad).

## Equilibrio del tráfico SNA y NetBIOS

Con la introducción del soporte DLSw para tráfico NetBIOS, el usuario debe controlar la combinación de tráfico SNA y NetBIOS dentro de las conexiones de transporte DLSw. Sin este control, las transferencias de archivos NetBIOS tienen tendencia a interrumpir el tráfico SNA inactivo durante periodos de tiempo demasiado largos, especialmente si las conexiones TCP se ejecutan sobre enlaces de WAN relativamente lentos. Puede controlar esta combinación de tráfico mediante los parámetros de configuración del mandato **set priority**. Con estos parámetros, puede:

- Establecer una proporción de número de tramas procedentes de cada protocolo transmitidas a una conexión TCP durante periodos de congestión
- Establecer un tamaño máximo de trama correspondiente a tramas NetBIOS de modo que una trama grande no consuma un enlace de WAN lento.

Para definir una proporción de tramas SNA y NetBIOS, puede seleccionar de forma global uno de entre cuatro valores (critical, high, medium o low) para cada protocolo. En el momento de la configuración del circuito, el direccionador utiliza el mecanismo de prioridades de circuito de DLSw Versión 1 (RFC 1795) para intentar negociar cada nueva prioridad de circuito con el valor correspondiente al protocolo

que va a utilizar el circuito. El direccionador DLSw que inicia el circuito elegirá la prioridad de circuito a utilizar. Si el direccionador DLSw local inicia el circuito, la prioridad de circuito que elige se basa en los valores por omisión configurados de prioridad de circuito y en las modificaciones de la prioridad de circuito. Si el direccionador DLSw remoto inicia el circuito, el direccionador DLSw local notificará al direccionador DLSw remoto de su necesidad de utilizar una prioridad de circuito basada en los valores por omisión configurados y en las modificaciones, pero el direccionador DLSw remoto puede elegir otro valor. En cualquier caso, el direccionador que inició el establecimiento de este circuito asigna a cada circuito establecido una de las cuatro prioridades.

Durante periodo de congestión de TCP, el direccionador coloca en cola tramas (procedentes de circuitos que tienen datos para transmitir) en una de cuatro colas: una cola para cada posible prioridad de circuito. Las tramas se colocan en cola según el método FIFO dentro de cada prioridad. Para alimentar el proceso de transmisión TCP, el direccionador selecciona tramas de cada cola de prioridad según lo indicado en el parámetro “message allocation by priority”. El valor por omisión es 4/3/2/1, lo que significa que se toman, como máximo, cuatro mensajes de la cola de prioridad crítica, seguidos de un máximo de tres mensajes de la cola de prioridad media, y así sucesivamente. Si una cola está vacía, pierde su turno en el ciclo.

Para evitar que una sola trama NetBIOS grande domine un enlace lento durante un periodo de tiempo largo, puede utilizar el parámetro “NetBIOS maximum frame size” para definir un límite superior del tamaño de una sola trama NetBIOS. Este valor se pasa a ambas estaciones finales NetBIOS durante el establecimiento del circuito utilizando los bits de Trama más larga (LF) de la cabecera MAC de direccionamiento de origen. Las estaciones finales NetBIOS de direccionamiento de origen observan los valores LF y no generan tramas que superen el valor especificado.

Hay cuatro prioridades de circuito por omisión que se pueden configurar:

- Prioridad de circuito de tráfico de exploración de SNA por omisión
- Prioridad de circuito de tráfico de sesión SNA por omisión
- Prioridad de circuito de tráfico de exploración de NetBIOS por omisión
- Prioridad de circuito de tráfico de sesión NetBIOS por omisión

Estos distintos valores permiten asignar distintas proporciones de tráfico SNA y NetBIOS y de exploración y de sesión.

En algunos casos puede resultar recomendable asignar una determinada prioridad de circuito a un tráfico específico. Por ejemplo, es posible que desee asignar al tráfico destinado a una determinada dirección MAC de SNA una prioridad superior a la del resto del tráfico. Esto se puede conseguir utilizando modificaciones de prioridad de circuito (mandato **add priority**). Esto permite asignar una prioridad de exploración y de circuito de sesión a un determinado rango de direcciones MAC y SAP de origen y de direcciones MAC y SAP de destino. Estas modificaciones de prioridad de circuito se evalúan en el orden en que se han configurado. La prioridad de circuito se define con el valor de la primera coincidencia encontrada de modificación de prioridad de circuito. Si no se encuentra ninguna coincidencia de modificación de prioridad de circuito, se utiliza la prioridad de circuito por omisión.

# Configuración de DLSw

Las siguientes secciones explican los procedimientos de configuración de DLSw:

- “Requisitos de la configuración de DLSw”
- “Definición de almacenamientos intermedios globales”
- “Configuración de la Conexión por puente de ruta de origen adaptable (ASRT) para DLSw”
- “Configuración del Protocolo Internet (IP) para DLSw” en la página 548
- “Configuración de OSPF para DLSw” en la página 549
- “Configuración de interfaces SDLC” en la página 549
- “Configuración de interfaces X.25” en la página 550
- “Configuración de DLSw” en la página 551

Además, se ha incluido una configuración DLSw de ejemplo con notas explicativas (consulte la Figura 48 en la página 553).

## Requisitos de la configuración de DLSw

Para utilizar DLSw, configure los siguientes protocolos: ASRT, IP y DLSw. Además, puede que tenga que configurar los protocolos que aparecen en la Tabla 35.

*Tabla 35. Protocolos opcionales de DLSw*

| Protocolo opcional | Cuándo se utiliza |
|---|---|
| LLC2 | Cuando se tienen que utilizar parámetros LLC2 distintos de los parámetros por omisión |
| SDLC | Para establecer conexión con dispositivos que utilizan SDLC |
| OSPF | Para el direccionamiento dinámico o para utilizar grupos de difusión múltiple DLSw |
| X.25 | Para establecer conexión con dispositivos que utilizan QLLC |

Las siguientes secciones explican paso a paso cómo configurar estos protocolos necesarios y opcionales.

## Definición de almacenamientos intermedios globales

AL ejecutar DLSw en un 2210 con 4M de DRAM, es posible que sea necesario aumentar la memoria para DLSw reduciendo el número de almacenamiento intermedios globales de paquetes. Entre el mandato **set global** en el indicador `Config>` y a continuación entre el número de almacenamientos intermedios globales de paquetes. (el número recomendado para un 2210 de 4M de DRAM es 50).

## Configuración de la Conexión por puente de ruta de origen adaptable (ASRT) para DLSw

Puesto que el direccionador DLSw aparece como un puente ante las estaciones finales conectadas, tiene que configurar la conexión por puente de ruta de origen. Para ello, siga estos pasos:

1. Entre en el proceso de configuración de ASRT (Conexión por puente de rutas de origen adaptables). Utilice el mandato **protocol asrt** desde el indicador `Config>`.

2. Active la conexión por puente en el direccionador mediante el mandato **enable bridge**. Cada puente debe tener tener una dirección de puente exclusiva en cada DLSw.
3. Añada un puerto de puente con el mandato **add port**. Se le solicitará un número de interfaz y un número de puerto.
   - ***Para interfaces de red en anillo:***

     Para ejecutar DLSw sobre red en anillo solo puede haber una conexión por puente de ruta de origen presente en el puerto de puente designado. Por lo tanto, debe desactivar la conexión por puente transparente. Para ello, utilice el mandato **disable transparent**. Luego, emita el mandato **enable source routing** para activar el direccionamiento de origen correspondiente al puerto del puente.
   - ***Para interfaces Ethernet:***

     Asegúrese de que la conexión por puente transparente está activada en el puerto del puente. Emita el mandato **enable transparent**.
4. Si está configurando el direccionador para la ***conexión por puente simultánea y DLSw:***

   Cree un filtro de protocolo contra los SAP (puntos de acceso de servicio) que desea que utilice DLSw. Si el direccionador está llevando a cabo operaciones de conexión por puente y además están reenviando paquetes a través de DLSw, este paso resulta esencial. Si no lo hace, los paquetes DLSw que recibe el puente serán reenviados por DLSw y conectados por puente por el direccionador. La idea consiste en evitar que los paquetes DLSw se reenvíen (conecten por puente) en paralelo con direccionamiento DLSw.

   Para crear un filtro SAP, emita el mandato **add protocol-filter dsap 4** en el indicador `Config ASRT>`.

   Además de este mandato, debe especificar el puerto de puente al que se aplica. Este mandato indica al direccionador que filtre todo el tráfico que tiene un DSAP de 4 excepto en el puerto designado para DLSw. (Observe que se da por supuesto que ha elegido un SAP de 4 para el tráfico DLSw. Esto se especifica durante la configuración de DLSw.)
5. Active DLSw con el mandato **enable dls**. Esto activa el protocolo DLSw en el puerto de puente que ha designado.
6. Compruebe la configuración de ASRT. Este paso no es obligatorio, pero resulta recomendable para comprobar la configuración del puente antes de continuar. Utilice el mandato **list bridge** para comprobar la configuración del protocolo ASRT. El siguiente ejemplo muestra el resultado del mandato list bridge después de configurar ASRT.

```
                Source Routing Transparent Bridge Configuration
                ===============================================

 Bridge:                 Enabled                 Bridge Behavior: Unknown
                      +----------------------------+
 --------------------| SOURCE ROUTING INFORMATION |-------------------------------
                      +----------------------------+
 Bridge Number:          01                       Segments: 1
 Max ARE Hop Cnt:        14                      Max STE Hop cnt:  14
 1:N SRB:                 Not Active              Internal Segment:  0x000
 LF-bit interpret:        Extended

                      +--------------------+
 --------------------| SR-TB INFORMATION |----------------------------------------
                      +--------------------+
SR-TB Conversion:        Disabled
TB-Virtual Segment:      0x000                   MTU of TB-Domain:  0

                    +-----------------------------------+
-------------------| SPANNING TREE PROTOCOL INFORMATION |----------------------
                    +-----------------------------------+
Bridge Address:          Default                 Bridge Priority:   32768/0x8000
STP Participation:       IEEE802.1d

                    +-------------------------+
-------------------| TRANSLATION INFORMATION |---------------------------------
                    +-------------------------+
 FA<=>GA Conversion:      Enabled                 UB-Encapsulation :  Disabled
 DLS for the bridge:      Enabled

                      +------------------+
 --------------------| PORT INFORMATION |----------------------------------------
                      +------------------+
 Number of ports added: 1
 Port:   1      Interface:       0      Behavior:    SRB Only STP:  Enabled
```

## Configuración del Protocolo Internet (IP) para DLSw

Tiene que configurar IP para que el direccionador DLSw local pueda establecer conexiones TCP con otros similares DLSw. Para ello:

1. Entre en el proceso de configuración de IP emitiendo el mandato **protocol ip** desde el indicador `Config>`.
2. Asigne la dirección IP a la interfaz de hardware. Utilice el mandato **add address** para asignar la dirección IP a la interfaz de hardware que utiliza para establecer conexión con el otro similar DLSw.
3. ***Active el direccionamiento dinámico***. Debe elegir OSPF o RIP como protocolo de direccionamiento. Se recomienda utilizar OSPF porque necesita menor actividad general de la red que RIP.
   - Para activar OSPF: consulte el tema “Configuración de OSPF para DLSw” en la página 549.
   - Para activar RIP: entre **enable RIP** en el indicador `IP Config>`.
4. Defina la dirección IP interna. Utilice el mandato **set internal-ip-address** para definir la dirección que pertenece al direccionador como un conjunto, no a una interfaz en particular. El direccionador utiliza la dirección ip interna al establecer la conexión TCP con el otro similar DLSw.
   - Si utiliza RIP, elija una de las direcciones de interfaz como dirección ip interna.
   - Si utiliza OSPF, elija una dirección que tenga una subred distinta de las que se están utilizando en la red.

## Configuración de OSPF para DLSw

Si desea utilizar OSPF como protocolo de direccionamiento, lo tiene que configurar del siguiente modo:

1. *Entre en el proceso de configuración de OSPF*. Utilice el mandato **protocol ospf** desde el indicador `Config>`.
2. *Asigne la dirección OSPF a la interfaz de hardware*. Utilice el mandato **set interface** para asignar la dirección OSPF a la interfaz de hardware que utiliza para establecer conexión con el otro similar DLSw.
3. *Active el direccionamiento dinámico*. Utilice el mandato **enable ospf** para activar el direccionamiento. Si utiliza la función de grupo de DLSw, debe activar el protocolo de direccionamiento OSPF y el direccionamiento de difusión múltiple OSPF desde el indicador `Config>` de OSPF. Todos los valores por omisión de OSPF funcionan correctamente. Sólo tiene que activar OSPF y OSPF de difusión múltiple después de utilizar el mandato **join-group** en lugar de utilizar add TCP neighbor para definir de forma explícita la conexión TCP.

## Configuración de interfaces SDLC

El mandato de configuración de SDLC le permite crear o modificar la configuración de la interfaz SDLC como parte del proceso de configuración de DLSw.

**Nota:** Si SDLC es el encapsulador correspondiente a V.25bis, los parámetros de enlace físico no se pueden definir al nivel de SDLC y se deben configurar al nivel de V.25bis. En este caso, no debe configurar los siguientes parámetros de SDLC:

- Role - Debe ser el primario.
- Group - No puede definir una dirección de sondeo de grupos.
- Type - Debe ser punto a punto.
- Duplex
- Idle state
- Clocking
- Speed
- Cable
- Encoding
- Inter-frame delay

Debe configurar enlaces SDLC si tiene intención de dar soporte a SDLC sobre DLSw. Esta sección explica cómo acceder a la consola de configuración de SDLC y describe los mandatos relacionados con SDLC.

Si hay un dispositivo SDLC conectado directamente, configure el protocolo SDLC del siguiente modo:

1. Defina el enlace de datos con SDLC: En el indicador `Config>`, utilice el mandato **set data-link SDLC** para configurar el tipo de enlace de datos correspondiente a la interfaz serie. Se le solicitará un número de interfaz.
2. Entre en el proceso de configuración de SDLC: Utilice el mandato **network** en el indicador `Config>` para entrar en el proceso de configuración de SDLC. Se le solicitará un número de interfaz.
3. Al configurar DLSw, añade estaciones SDLC y el software asigna los siguientes valores por omisión a las estaciones:
   - El número máximo de BTU es el máximo que permite la interfaz

- Tx y Rx Windows son 7 para Mod 8 y 127 para Mod 128

4. El valor por omisión del papel del enlace es primario. Si es necesario, cambie el papel del enlace por secundario o negociable mediante el mandato **set link role**.
5. Puede definir el sondeo de grupos correspondiente a estaciones secundarias del enlace. Para ello, defina la dirección de sondeo de grupos con el mandato **set link group-poll** y utilice los mandatos **add station** y **set station group-inclusion** para incluir estaciones en la lista de sondeo de grupos.
6. Defina el origen de sincronización de enlaces (opcional): Si desea establecer conexión directa con un dispositivo SDLC sin utilizar un eliminador de módem, utilice un cable DTE y el mandato **set link clocking internal**.
7. Defina la velocidad de enlace (opcional): Si utiliza una sincronización interna, utilice el mandato **set link speed** para elegir la velocidad de reloj correspondiente a esta línea.

   **Nota:** Si utiliza SDLC para establecer conexión desde un PC, también debe definir la codificación (NRZ/NRZI) y el sistema dúplex (full/half) para que coincidan con los de la configuración del PC.
8. Defina el cable de enlace como RS-232, X.21, V.35 o V.36.
9. Compruebe la configuración de SDLC: Utilice el mandato **list link** para comprobar la configuración de la interfaz SDLC.

## Configuración de interfaces X.25

Configure la interfaz X.25 si tiene intención de utilizar el soporte de DLSw para dispositivos QLLC. Siga los pasos siguientes:

1. Defina la interfaz como X.25. En el indicador `Config>`, utilice el mandato **set data-link X25** para definir el tipo de interfaz serie. Se le solicitará un número de interfaz.
2. Entre en el proceso de configuración de X.25, mediante el mandato **net** desde el indicador `Config>`. Se le solicitará un número de interfaz y a partir de este momento entrará los mandatos en el indicador `X.25 Config>`.
3. Utilice el mandato **set address** para definir la dirección DTE del direccionador en esta interfaz.
4. Utilice los mandatos **set pvc** y **set svc** para definir el rango de números de canal lógico a utilizar para los PVC y disponibles para que los utilicen los SVC. Los PVC que defina en la configuración de DLSw deben tener números de canal que pertenezcan al rango de PVC que defina aquí. Para los SVC, debe asegurarse de que el número de canales disponibles para llamadas de entrada y de salida es suficiente para el número de llamadas simultáneas que espera que DLSw pueda colocar o responder.
5. Utilice el mandato **add protocol** para añadir "dls" como un protocolo que funcione sobre X.25 en esta interfaz. X.25 comprende que esto implica soporte de QLLC y le solicita una serie de parámetros operativos de QLLC cuyos valores se aplicarán a todos los circuitos virtuales DLSw de esta interfaz.
6. Utilice el mandato **add pvc** para asociar un determinado número de canal lógico PVC con el protocolo DLSw. Debe hacerlo para cada PVC de esta interfaz que DLSw está configurado para utilizar (es decir, cada PVC para el que ha emitido un mandato **add qllc station** en la configuración de DLSw).

Este número de canal lógico es la clave que comparará la configuración de DLSw correspondiente a esta estación con esta definición de PVC de X.25.

7. Utilice el mandato **add address** para crear una lista de direcciones DTE de X.25 para todos los PVC y SVC definidos en la configuración de DLSw. Observe que DLSw no utiliza direcciones DTE para los PVC, pero se necesitan dentro de la configuración X.25. No es necesario añadir las direcciones DTE de estaciones finales QLLC que pueden realizar llamadas dinámicas a DLSw y no están configuradas en DLSw.
8. Defina las características de capa física o personalidad nacional necesarias para la conexión con la red X.25. Para ver una descripción de los parámetros de X.25 que se pueden configurar, consulte el capítulo sobre cómo configurar la interfaz de red X.25 en el manual *Guía del usuario de software*

## Configuración de DLSw

Antes de configurar DLSw, entre el mandato **list device** en el indicador `Config>` para listar los números de interfaz de diversos dispositivos.

Para configurar el protocolo DLSw:

1. En el indicador `Config>`, entre el mandato **protocol dls**. Aparecerá el indicador `DLSw config>`.
2. En el indicador `DLSw config>`, entre el mandato **enable dls** para activar DLSw en el direccionador.
3. Entre el mandato **set srb** para designar el número de segmento SRB (direccionamiento de rutas de origen) correspondiente al direccionador DLS.

   Este número de segmento SRB debe ser igual para todos los direccionadores DLSw conectados a la misma LAN y debe ser exclusivo en el dominio del puente de rutas de origen. El puente utiliza este número en el Campo de información de direccionamiento (RIF) cuando se envían tramas en la LAN. El número de segmento constituye la clave para evitar bucles.
4. Entre el mandato **open-sap** para cada SAP que desea que conmute DLSw. El direccionador le solicitará números de interfaz. Para abrir los SAP de SNA que se utilizan con más frecuencia (4, 8 y C), especifique SNA. Como mínimo debe abrir los SAP 0 y 4. Para abrir el SAP NetBIOS, especifique NB o F0. Para abrir los SAP de LNM, especifique LNM o, como mínimo, 0 y F4.
5. Utilice el mandato **add tcp** para añadir la dirección IP de cada similar DLSw que desea configurar. Si desea que el direccionador acepte conexiones procedentes de similares no configurados, utilice el mandato **enable-dynamic neighbor**. También se pueden establecer conexiones TCP utilizando OSPF de difusión múltiple y el mandato **join-group**.

   **Nota:** Un direccionador ***sólo*** puede participar en un grupo si su direccionador similar es una plataforma basada en MRS que ejecuta DLSw. Si configura un direccionador DLSw para un grupo, debe activar OSPF y MOSPF en todos los direccionadores DLSw del grupo.
6. Para que la configuración DLSw dé soporte a SDLC, debe añadir una estación de enlace SDLC mediante el mandato **add sdlc**.
7. Para que la configuración DLSw dé soporte a QLLC, añada una estación de enlace QLLC con el mandato**add qllc station**.

O, si desea dar soporte a SVC dinámicos, active interfaces X.25 para entrada de llamadas con el mandato **enable qllc callin** y defina destinos DLSw con el mandato **add qllc destination**.

## Configuración DLSw de ejemplo

En la siguiente configuración DLSw de ejemplo se da por supuesto que el dispositivo no se ha configurado para ningún otro protocolo ni enlace de datos. Por este motivo, el script comienza en el indicador `Config (only)>` en lugar de empezar en el indicador `Config>`.

## Diagrama de ejemplo

El ejemplo se basa en la información que se muestra en la Figura 48 en la página 553.

El direccionador DLSw que se está configurando (R1 en el diagrama) da soporte a una conexión LLC y a una SDLC en su similar DLSw (R2). La conexión TCP entre los dos direccionadores se realiza sobre una línea serie.

Para configurar R1 para DLSw se necesita toda la información que se muestra. Esta información incluye:

- Dirección IP interna de R1 y R2
- Dirección IP de cada puerto que se utiliza para mantener la conexión TCP entre los direccionadores
- Números de interfaz asignados a los dispositivos de red en anillo y SDLC y que se utilizan para la conexión TCP
- Dirección MAC del dispositivo SDLC conectado
- Dirección MAC del dispositivo QLLC conectado
- Número de segmento de puente de rutas de origen del dispositivo de red en anillo conectado

El ejemplo indica dónde se ofrece esta información en el curso del procedimiento de configuración.

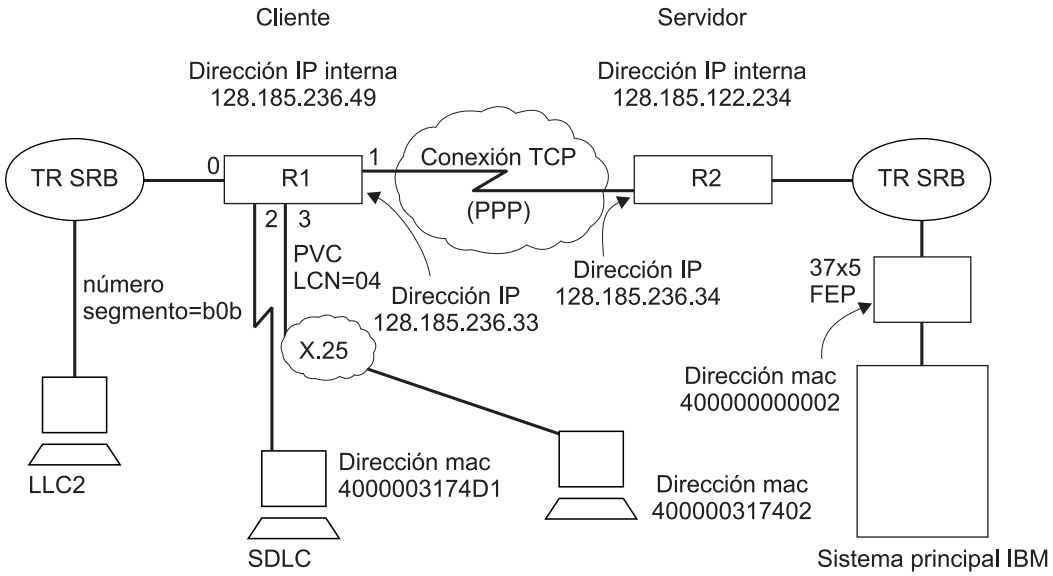



*Figura 48. Diagrama de ejemplo para la configuración DLSw*

## Mandatos de configuración de ejemplo

Esta sección contiene ejemplos de:

- "Paso 1: Adición de dispositivos"
- "Paso 2: Configuración de protocolos" en la página 557
- "Paso 3: Implantación de la función de filtro de protocolos" en la página 561
- "Paso 4: Configuración de DLSw" en la página 562

### Paso 1: Adición de dispositivos

Los dispositivos que añadirá son red en anillo, SDLC o QLLC. También puede añadir Ethernet como un puerto de puente de transporte. Como ilustración, esta configuración DLSw de ejemplo da soporte a SDLC, LLC y QLLC. Sin embargo, en una configuración real sólo es necesario dar soporte a uno de estos enlaces de datos.

En el caso de SDLC y QLLC, debe definir de forma explícita el enlace de datos, puesto que la interfaz también da soporte a otros enlaces de datos como FR, X.25 y SDLC Relay.

```
Config (only)>set data-link sdlc 2
Config (only)>set data-link x25 3
```

Después de añadir dispositivos, puede listarlos para comprobar que se han asignado a las interfaces adecuadas del direccionador.

Entre el mandato **list device** en el indicador `config>` para visualizar una lista de los dispositivos configurados y sus números de interfaz.

```
Config (only)>list device
Ifc 0 Ethernet                      CSR  81600, CSR2  80C00, vector 94
Ifc 1 WAN PPP                       CSR 381620, CSR2 380D00, vector 125
Ifc 2 WAN SDLC                      CSR  81640, CSR2  80E00, vector 92
Ifc 3 WAN X.25                      CSR  81620, CSR2  80D00, vector 93
Ifc 4 WAN Frame Relay               CSR 381640, CSR2 380E00, vector 124
Ifc 5 Token Ring                    CSR 600000, vector 95
```

Observe que este mandato **list** muestra que se ha asignado un dispositivo de red en anillo a la interfaz 5.

1. ***Añada un dispositivo de red en anillo***:

   Configure la red en anillo. Se suelen utilizar 16 Mbps con cables UTP, así que esto es lo que se utilizará en este ejemplo. El mandato **list** que se muestra en estos procedimientos no es necesario ni en este punto ni en ningún otro momento de la configuración del direccionador.

```
Config (only)> network 5
Token-Ring interface configuration

TKR config>speed 16
TKR config>media utp

TKR config>list

Token-Ring configuration:
Packet size (INFO field): 2052
Speed:                    16 Mb/sec
Media:                    Unshielded
RIF Aging Timer:          120
Source Routing:           Enabled
MAC Address:              000000000000
IPX interface configuration record missing

TKR config>exit
```

   *Configuración de la interfaz de WAN*. El primer puerto (interfaz 1) se utiliza para el enlace de WAN (TCP/IP). El enlace de datos seleccionado para la WAN es PPP. Esta es la opción por omisión para el enlace de datos. Las otras posibilidades son frame-relay y X.25.

```
Config (only)>network 1
Point-to-Point user configuration
PPP Config>list hdlc
Mode: Synchronous
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable type: RS-232 DTE
Speed (bps): 0

Transmit Delay Counter: 0
Lower DTR: Disabled
```

   También tiene que definir el tipo de cable. Para PPP el tipo de cable se define mediante el mandato **set hdlc cable**.

   A continuación, defina la velocidad de línea y el tipo de sincronización para la interfaz serie, si es necesario.

```
PPP Config>set hdlc clock internal
Must also the line speed to a valid value
Line speed (2400 to 2048000) [0]? 56000
```

   Después de definir la velocidad de línea y el tipo de sincronización, puede comprobar la configuración con el mandato **list hdlc** tal como se muestra.

```
PPP Config>list hdlc
Mode: synchronous
Encoding: NRZ
Idle State: Flag
Clocking: Internal
Cable type: RS-232 DTE
Speed (bps): 56000

Transmit Delay Counter: 0
Lower DTR: Disabled

PPP Config>exit
```

2. ***Añada un dispositivo SDLC***

Si está configurando DLSw para que dé soporte a SDLC, el siguiente paso consiste en configurar SDLC. La mayoría de los elementos que se pueden configurar no se tienen que modificar.

Para acceder a la configuración de SDLC, utilice el mandato **network** y el número de interfaz a la que se ha asignado un dispositivo SDLC (en este caso, 2).

```
Config>network 2
SDLC user configuration
```

La mayor parte de la información que añade al configurar SDLC está relacionada con el hardware.

El ejemplo comienza con un mandato **list link**. El mandato **list** no modifica la configuración, pero le muestra los valores que están actualmente asociados con el enlace SDLC.

Si está configurando un 2210:

```
SDLC 2 Config>list link
Link configuration for: LINK_2   (ENABLED)

Role:         PRIMARY          Type:        POINT-TO-POINT
Duplex:       FULL             Modulo:      8
Idle state:   FLAG             Encoding:    NRZ
Clocking:     EXTERNAL         Frame Size:  2048
Speed:        0                Group Poll:  00
Cable:        RS-232 DTE

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:  4
           SNRM retry:      6
           Poll retry:      10
```

Del mismo modo que hemos configurado un dispositivo de red en anillo, se deben modificar el tipo de sincronización y la velocidad de línea correspondientes al dispositivo SDLC. Si utiliza un eliminador de módem externo, este paso no es necesario.

```
SDLC 2 Config>set link clock internal
Must also set the line speed to a valid value
Line speed (2400 to 2048000) [0]? 9600
SDLC 2 Config>exit
```

3. ***Añada un dispositivo QLLC***

   A fin de dar soporte a la estación QLLC mostrada en la Figura 48 en la página 553, debe configurar la interfaz 3 para que sea X.25 y tenga soporte de QLLC para DLSw en el PVC indicado. El siguiente ejemplo comienza a partir de cero con una interfaz serie que no es X.25.La siguiente configuración de ejemplo muestra el soporte de QLLC para DLSw en un PVC. Debe:

   a. Utilizar el mandato list device para obtener una lista de las interfaces configuradas.

   b. Seleccionar la interfaz serie en la que desea configurar X.25.

   c. Anotar este número de interfaz y utilizarlo en el mandato set data-link para configurar X.25 en la interfaz.

   En el ejemplo, X.25 se ha configurado en la interfaz 1.

```
Config>net
Network number [0]? 1
X.25 User Configuration

X.25 Config>li sum

X.25 Configuration Summary

Node Address:       <none>
Max Calls Out:           4
Inter-Frame Delay:       0    Encoding:  NRZ
Speed:           56000        Clocking:  Internal
MTU:              2048        Cable:     RS-232 DTE
Lower DTR:   Disabled
Default Window:     2         SVC idle:  30 seconds
National Personality: GTE Telenet (DTE)
PVC              low: 0    high: 0
Inbound          low: 0    high: 0
Two-Way          low: 1    high: 64
Outbound         low: 0    high: 0
Throughput Class in bps Inbound:  2400
Throughput Class in bps Outbound: 2400

X.25 Config>set addr
address [ ]? 3721111
X.25 Config>set pvc low 1
X.25 Config>set pvc high 4
X.25 Config>set svc low-two 5
X.25 Config>set svc high-two 64


X.25 Config>li sum

X.25 Configuration Summary

Node Address:       3721111
Max Calls Out:           4
Inter-Frame Delay:       0    Encoding:  NRZ
Speed:           56000        Clocking:  Internal
MTU:              2048        Cable:     RS-232 DTE
Lower DTR:   Disabled
Default Window:     2         SVC idle:  30 seconds
National Personality: GTE Telenet (DTE)
PVC              low: 1    high: 4
Inbound          low: 0    high: 0
Two-Way          low: 5    high: 64
Outbound         low: 0    high: 0
Throughput Class in bps Inbound:  2400
Throughput Class in bps Outbound: 2400

X.25 Config>li prot

X.25 protocol configuration

No protocols defined
X.25 Config>add prot
Protocol [IP]? dls
Idle timer [20]?
QLLC response timer [20]?
QLLC response count [10]?
Accept Reverse Charges [N]?
Request Reverse Charges [N]?
Station Type (1) PRI  (2) SEC  (3) (PEER) [3]?
Non standard packet size [32]?
Packet window size [128]?
Max message size [256]?
Call User Data (in HEX) [0000000000000000]?
```

```
X.25 Config> li prot

X.25 protocol configuration

Prot         Window      Packet-size        Idle     Max     Station
Number       Size      Default Maximum      Time     VCs      Type
26 -> DLS     128        32      256         20       4       PEER

X.25 Config> li pvc

X.25 PVC configuration

No PVCs defined
X.25 Config>add pvc
Protocol [IP]? dls
Packet Channel [1]? 4
Destination X.25 Address [ ]? 4444
Window Size [2]?
Packet Size [128]?

X.25 Config> li pvc

X.25 PVC configuration

Prtcl        X.25_address     Window    Pkt_len   Pkt_chan
26 -> DLS    4444             2         128       4

X.25 Config> li add

X.25 address translation configuration

No address translations defined

X.25 Config> add addr
Protocol [IP]? dls
Enter an DLS address identifier (upto 12 chars) [ ]? Chicago
X.25 Address [ ]? 4444
X.25 Config> li addr

X.25 address translation configuration

IF #    Prot #       Protocol address -> X.25 address
1       26 -> DLS    Chicago          -> 4444
```

**Nota:** DLSw no utiliza la dirección DTE “4444” utilizada para el PVC con el número de canal lógico “4”; sólo la utiliza X.25 para correlacionar información de configuración. Paralelamente, la dirección de protocolo de DLSw (“Chicago” en este ejemplo), no tiene ningún significado para DLSw; se ofrece para facilitar la consulta de varias direcciones DTE que puede utilizar DLSw. A diferencia de otros protocolos que se ejecutan en X.25, la conversión de direcciones de DLSw está definida como parte de la configuración DLSw y no está definida en la configuración X.25.

## Paso 2: Configuración de protocolos

Una vez finalizada la configuración de dispositivos, debe configurar los protocolos necesarios. Para que se ejecuten sobre DLSw debe configurar IP, OSPF (o RIP), ASRT y el protocolo DLSw.

1. ***Configure IP***

   Este ejemplo comienza con la configuración IP:

   ```
   Config>protocol ip
   Internet protocol user configuration
   ```

   El mandato **list all** muestra la configuración IP por omisión.

```
IP config>list all
Interface addresses
IP addresses for each interface:
   intf  0   192.1.1.3        255.255.255.0    Local wire broadcast, fill 1
   intf  1                                     IP disabled on this interface
   intf  2                                     IP disabled on this interface

Routing

Protocols
BOOTP forwarding: disabled
IP Time-to-live: 64
Source Routing: enabled
Echo Reply: enabled
Directed broadcasts: enabled
ARP subnet routing: disabled
ARP network routing: disabled
Per-packet-multipath: disabled
OSPF: enabled
BGP: disabled
RIP: enabled
RIP default origination: disabled
  Per-interface address flags:
     intf  0   192.1.1.3        Send net, subnet, static and default routes
                                Received RIP packets are ignored.
     intf  1                    IP & RIP are disabled on this interface
     intf  2                    IP & RIP are disabled on this interface

Accept RIP updates always for:
     [NONE]
```

Este ejemplo muestra la creación de una configuración IP mínima. Para obtener más información sobre este importante protocolo, consulte el tema “Utilización de IP” en la página 241.

- Lo primero que hay que hacer es añadir una dirección internet y asignarla a una interfaz sobre la que tiene intención de ejecutar tráfico IP:

  ```
  IP config>add address
  Which net is this address for [0]? 1
  New address [0.0.0.0]? 128.185.236.33
  Address mask [255.255.0.0]? 255.255.255.0
  ```

- Defina la Dirección IP interna. Es la dirección que utilizan los direccionadores DLSw remotos para conectarse al direccionador que está configurando. Si RIP es el protocolo de direccionamiento seleccionado para IP, la dirección IP interna debe coincidir con la dirección IP configurada para una interfaz.

  ```
  IP config>set internal-ip-address 128.185.236.49
  ```

- Las siguientes veces que utilice el mandato **list** se mostrará la información que acaba de añadir.

```
IP config>list all
Interface addresses
IP addresses for each interface:
   intf  0   192.1.1.3        255.255.255.0    Local wire broadcast, fill 1

   intf  1   128.185.236.33   255.255.0.0      Local wire broadcast, fill 1

   intf  2                                     IP disabled on this interface
Internal IP address: 128.185.236.49

Routing

Protocols
BOOTP forwarding: disabled
IP Time-to-live: 64
Source Routing: enabled
Echo Reply: enabled
Directed broadcasts: enabled
ARP subnet routing: disabled
ARP network routing: disabled
Per-packet-multipath: disabled
OSPF: enabled
BGP: disabled
RIP: enabled
RIP default origination: disabled
  Per-interface address flags:
     intf  0   192.1.1.3        Send net, subnet, static and default routes
                                Received RIP packets are ignored.
     intf  1   128.185.236.33   Send net, subnet, static and default routes
                                Received RIP packets are ignored.
     intf  2                    IP & RIP are disabled on this interface

Accept RIP updates always for:
[NONE]

IP config>exit
```

2. ***Configure OSPF o RIP***

   En esta configuración, se utiliza OSPF en lugar de RIP. Puede utilizar cualquiera de estos protocolos de direccionamiento. Sin embargo, si elige RIP, no podrá utilizar la función de grupos de DLSw.

   Primero, entre un mandato **list**. El mandato muestra la configuración OSPF por omisión. Debe modificar esta configuración para que ejecute DLSw.

```
Config>protocol ospf
Open SPF-Based Routing Protocol configuration console
OSPF Config>list all

             --Global configuration--
          OSPF Protocol:          Enabled
          # AS ext. routes:       1000
          Estimated # routers:    50
          External comparison:    Type 2
          AS boundary capability: Disabled
          Multicast forwarding:   Disabled

                  --Area configuration--
Area ID       AuType     Stub?   Default-cost Import-summaries?
0.0.0.0       0=None     No      N/A           N/A
```

   - Ahora, active OSPF y haga una estimación de las rutas y direccionadores OSPF externos.

```
OSPF Config>enable ospf
Estimated # external routes [0]? 100
Estimated # OSPF routers [0]? 25
```

   - Puesto que este ejemplo implementa la Función de grupos de DLSw, debe activar OSPF de difusión múltiple, tal como se muestra a continuación:

```
OSPF Config>enable multicast
Inter-area multicasting enabled? [No]:
```

   - Emita el mandato **set interface** para cada interfaz IP física que vaya a utilizar OSPF. En este ejemplo se da por supuesto que la red troncal es el área OSPF (0.0.0.0). En este momento, solo se ha definido una interfaz IP.

```
OSPF Config>set interface 128.185.236.33
Attaches to area [0.0.0.0]?
Retransmission Interval (in seconds) [5]?
Transmission Delay (in seconds) [1]?
Router Priority [1]?
Hello Interval (in seconds) [10]?
Dead Router Interval (in seconds) [40]?
Type Of Service 0 cost [1]?
Authentication Key [ ]?
Retype Auth. Key [ ]?
Forward multicast datagrams? [Yes]:
Forward as data-link unicasts? [No]:
IGMP polling interval (in seconds) [60]?
IGMP timeout (in seconds) [180]?
OSPF Config>
```

- El siguiente ejemplo muestra la pantalla de OSPF después de que se haya configurado. Para ver lo que ha cambiado en la configuración, compare esta pantalla con la pantalla de la configuración OSPF por omisión mostrada anteriormente.

```
OSPF Config>list all

       --Global configuration--
OSPF Protocol:          Enabled
# AS ext. routes:       100
Estimated # routers:    25
External comparison:    Type 2
AS boundary capability: Disabled
Multicast forwarding:   Enabled
Inter-area multicast:   Disabled

                    --Area configuration--
Area ID      AuType       Stub? Default-cost Import-summaries?
0.0.0.0      0=None       No         N/A           N/A

                    --Interface configuration--
IP address       Area     Cost  Rtrns  TrnsDly  Pri  Hello  Dead
192.1.1.3        0.0.0.0     1      5       1     1     10    40
128.185.236.33   0.0.0.0     1      5       1     1     10    40

                                 Multicast parameters
IP address    MCForward    DLUnicast    IGMPPoll    IGMPtimeout
192.1.1.3         On           Off          60           180
128.185.236.33    On           Off          60           180

OSPF Config>exit
```

3. ***Configure ASRT***

   Configure el direccionador para el direccionamiento de rutas de origen y active el puerto tal como se muestra a continuación:

```
Config (only)>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge
```

- El mandato **list port** muestra que el valor por omisión del puerto es la conexión por puente transparente. La conexión por puente transparente es lo recomendable si el dispositivo conectado es Ethernet, pero no funcionará si el dispositivo es de red en anillo. Observe que el número de puerto 1 equivale al puerto 1 de la interfaz 0. Es decir, el puerto 1 es el puerto de puente lógico para la interfaz física configurada para la red en anillo (consulte la Figura 48 en la página 553).

```
ASRT config>list port
Port Id (dec)    : 128:01, (hex): 80-01
Port State       : Enabled
STP Participation: Enabled
Port Supports    : Transparent Bridging Only
Assoc Interface  : 0
Path Cost        : 0
++++++++++++++++++++++++++++++++++++++++++++
```

- Para poderse ejecutar sobre un enlace de datos LLC (como red en anillo), DLSw necesita SRB (conexión por puente de rutas de origen). En este caso, lo primero que hay que hacer es desactivar la conexión por puente transparente en el puerto.

```
ASRT config>disable transparent
Port Number [1]?

ASRT config>enable source-routing
```

- Ahora, asigne un número de segmento para el puerto. Solo tiene que asignar números de segmento al configurar un dispositivo de puente de rutas de origen, como red en anillo. En este ejemplo, (consulte la Figura 48 en la página 553) **b0b** es el número hexadecimal asignado al dispositivo de red en anillo.

```
Port Number [1]?
Segment Number for the port in hex(1 - FFF) [1]? b0b
Bridge number in hex (1 - 9, A - F) [1]?
```

  Luego active DLSw en el puerto del puente.

```
ASRT config>enable dls
```

Después de llevar a cabo estos pasos, active DLSw tal como se muestra. Puede listar la configuración del puente para confirmar que ha configurado ASRT correctamente.

```
ASRT config>list bridge

          Source Routing Transparent Bridge Configuration
          ===============================================
Bridge:                  Enabled                 Bridge Behavior:
Unknown
                   +----------------------------+
------------------| SOURCE ROUTING INFORMATION |-----------------------------
                   +----------------------------+
Bridge Number:           01                      Segments:  1
Max ARE Hop Cnt:         14                      Max STE Hop cnt: 14
1;N SRB:           Not Active              Internal Segment: 0x000
LF-bit interpret:        Extended

                   +-------------------+
------------------| SR-TB INFORMATION |-------------------------------------
                   +-------------------+
SR-TB Conversion:        Disabled
TB-Virtual Segment:  0x000                       MTU of TB-Domain:  0

                   +-----------------------------------+
------------------| SPANNING TREE PROTOCOL INFORMATION |---------------------
                   +-----------------------------------+
Bridge Address:          Default                 Bridge Priority: 32768/0x8000
STP Participation:       IEEE802.1d

                   +-------------------------+
------------------| TRANSLATION INFORMATION |--------------------------------
                    +-------------------------+
FA<=>GA Conversion:      Enabled                    UB-Encapsulation: Disabled
DLS for the bridge:      Enabled

                   +------------------+
------------------| PORT INFORMATION |-------------------------------------
                   +------------------+
Number of ports added: 1
Port:   1      Interface:       0      Behavior:    SRB Only   STP: Enabled
```

## Paso 3: Implantación de la función de filtro de protocolos

Este es un paso importante que se suele olvidar al configurar DLSw.

Puesto que se utilizará DLSw, en lugar de la conexión por puente, para reenviar tráfico a los SAP (puntos de acceso de servicio) 04, 08, 0C, debemos añadir un filtro de protocolo especial a la configuración de la conexión por puente.

**Nota:** Sólo tiene que implantar el filtro que aquí se describe si se ha configurado una conexión por puente, además de DLSw, a través de los enlaces de la WAN. No es el caso de este ejemplo. En este ejemplo, el procedimiento para crear un filtro SAP se ofrece solo a modo de consulta.

El objetivo del filtro consiste en evitar que el puente reenvíe, a otros puertos, paquetes que sólo debe manejar DLSw. No es conveniente que DLSw y la función de conexión por puente reenvíen los mismos paquetes. Cuando esto sucede, se desarrollan condiciones de contención que degradan el rendimiento de la red.

Este mandato crea un filtro que funciona en todos los paquetes cuyo SAP de destino SAP es 4. El mandato **list** que se emite a continuación muestra las características del filtro.

```
ASRT config>add prot-filter dsap 4
Filter packets arriving on all ports?? [No]: yes

ASRT config>list prot-f dsap
Protocol Class: DSAP
Protocol Type : 04
Protocol State: FILTERED
Port Map      : 1
==========================
No ETHER type Filter Records Associated
No SNAP Filter Records Associated
```

Una vez colocado en su lugar el filtro que necesita, salta de la configuración ASRT.

```
ASRT config>exit
```

## Paso 4: Configuración de DLSw

El último paso consiste en configurar el protocolo DLSw. El siguiente mandato **list** muestra los valores por omisión.

```
Config>protocol dls
DLSw protocol user configuration

DLSw config>list dls
DLSw is                                DISABLED
LLC2 send Disconnect is                ENABLED
Dynamic Neighbors is                   ENABLED
SRB Segment number                     000
MAC <-> IP mapping cache size          128
Max DLSw sessions                      1000
DLSw global memory allotment           141312
LLC per-session memory allotment       8192
SDLC per-session memory allotment      4096
QLLC per-session memory allotment      4096
NetBIOS UI-frame memory allotment      40960

Dynamic Neighbor Transmit Buffer Size  5120
Dynamic Neighbor Receive Buffer Size   5120
Dynamic Neighbor Maximum Segment Size  1024
Dynamic Neighbor Keep Alive            DISABLED
Dynamic Neighbor SessionAlive Spoofing DISABLED
Dynamic Neighbor Priority              MEDIUM

QLLC base source MAC address           40514C430000
QLLC maximum dynamic addresses         64
Type of local MAC list                 NON-EXCLUSIVE
Use of local MAC list is               ENABLED
Use of remote MAC list is              ENABLED
SNA explorer limit                     100
NetBIOS explorer limit                 100
```

Debe activar DLSw y definir el número de segmento SRB. El número de segmento se refiere al dispositivo de red en anillo, tal como se muestra en la Figura 48 en la página 553.

```
DLSw config>enable dls
DLSw config>set srb 020
```

***Configuración de grupos DLSw y sesiones estáticas:*** Este ejemplo define tanto un grupo como una sesión TCP configurada. Esto no es necesario para configurar DLSw. Sin embargo, debe definir uno u otro (un grupo DLSw o una sesión TCP) para las conexiones de salida con un direccionador DLSw contiguo. Si desea que puedan establecer conexiones de entrada direccionadores no configurados, emita el mandato **enable dynamic-neighbors**.

***El mandato join-group:*** El mandato **join-group** sirve para crear un grupo DLSw. Debe designar cada miembro del grupo como Client/Server o Peer. Peer es el valor por omisión.

Aquí, el mandato **join-group** se ejecuta para R1 (consulte la Figura 48 en la página 553), y designa este direccionador DLSw como un Client del grupo 1. Para unir este grupo, R2 se debería añadir como Server y se debería emitir el mandato **join-group** en R2.

```
DLSw config>join
Configure group member (G) or specific multicast address (M) -  [G]?
Group ID (1-64 Decimal) [1]?
Client/Server or Peer Group Member(C/S/P)- [P]? c
Connectivity Setup Type (a/p) [p]?
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]?
Enable/Disable NetBIOS SessionAlive Spoofing (E/D) [D]?
Neighbor Priority (H/M/L) [M]?

DLSw config>list group

   Group#                 Xmit    Rcv      Max      Keep-    SessAlive
Mcast IP Addr Role    CST Bufsize Bufsize  Segsize  alive    Spoofing  Priority
------------- ------- --- ------- -------- -------- -------- --------- --------
Group  1      CLIENT   p    5120    5120     1024   DISABLED DISABLED  MEDIUM
```

***El mandato add TCP:*** El mandato **add TCP** sirve para definir de forma explícita direccionadores contiguos DLSw configurados. La dirección IP del direccionador contiguo DLSw es la dirección IP interna del direccionador DLSw similar (denominado R2 en la Figura 48 en la página 553). También puede configurar R2 con la dirección IP de direccionador contiguo de R1, o bien puede configurar R2 para que acepte direccionadores contiguos dinámicos.

```
DLSw config>add tcp
Enter the DLSw neighbor IP Address [0.0.0.0]? 128.185.122.234
Connectivity Setup Type (a/p) [p]?
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]?
Enable/Disable  NetBIOS SessionAlive Spoofing (E/D)[D]?
Neighbor Priority (H/M/L) [M]?

DLSw config>list tcp
                     Xmit    Rcv     Max      Keep-    SesAlive
Neighbor        CST  Bufsize Bufsize Segsize  Alive    Spoofing Priority
--------------- ---  ------- ------- -------  -------- -------- ---------
128.185.122.234  p     5120    5120    1024   DISABLED DISABLED MEDIUM
```

***Defina cada estación de enlace SDLC:*** Debe definir cada estación de enlace SDLC.

```
DLSw config>add sdlc
Interface # [0]? 2
SDLC Address or 'sw' (switched dial-in) [C1]?
Source MAC address [4000112402C1]? 4000003174d1
Source SAP in hex [4]?
Destination MAC address [000000000000]? 400000000002
Destination SAP in hex [0]? 4
PU type (1/2/4/5) [2]?
XID0 block num in hex (0-0xfff) [0]? 017
XID0 id num in hex (0-0xfffff) [0]? 00001
Poll with TEST (T) or SNRM (S) [T]?

DLSw config>li sdlc all
Net Addr   Status    Source SAP/MAC   Dest SAP/MAC      PU  Blk/Idnum  PollFrame
 2   C1    Enabled   04 4000003174D1  04 400000000002   2   017/00001  TEST
```

***Defina cada estación de enlace QLLC:*** Defina la correlación de direcciones para cada PVC y SVC configurado. En la configuración de ejemplo, hay un dispositivo QLLC conectado a un PVC.

```
DLSw config> add qllc sta
Interface # [0]? 3
PVC or SVC [PVC]?
Logical channel number (1-4095) [0]? 4
Source MAC address [400000310101]? 400000317402
Source SAP in hex [4]?
Destination MAC address [000000000000]? 400000000002
Destination SAP in hex [0]? 4
PU type (2/4/5) [2]?
XID0 block num in hex (0-0xfff) [0]? 017
XID0 id num in hex (0-0xfffff) [0]? 00001
New QLLC station record added

DLSw config> li q st
If  P/S  LCN/DTE addr   E/D Source SAP/MAC   Dest SAP/MAC    PU Blk/IdNum
 3  PVC  4               E  04 400000317402  04 400000000002  2 017/00001
```

***Abra puntos de acceso de servicio (SAP):*** El siguiente paso consiste en abrir puntos de acceso de servicio (SAP) en cada una de las interfaces de conexión por puente.

Los números de SAP 0, 4, 8 y C son los SAP SNA que se utilizan con más frecuencia. Para abrir todos estos SAP, utilice la opción SNA con el mandato **open-sap** tal como se muestra. Para abrir SAP para NetBIOS, elija la opción NB. Si lo prefiere, puede entrar los SAP de forma individual, especificando un número hexadecimal.

```
DLSw config> open-sap
Interface #[1]?
Enter SAP in hex (range 0–FE), or one of the following:
   'SNA', 'NB', or LNM [4]? sna
SAP(s) 0 4 8 C opened on interface 1
DLSw config>
```

A continuación se muestra la pantalla de DLSw que aparece tras la configuración.

```
DLSw config>list dls
DLSw is                                 ENABLED
LLC2 send Disconnect is                 ENABLED
Dynamic Neighbors is                    ENABLED
SRB Segment number                      020
MAC <-> IP mapping cache size           128
Max DLSw sessions                       1000
DLSw global memory allotment            141312
LLC per-session memory allotment        8192
SDLC per-session memory allotment       4096
QLLC per-session memory allotment       4096
NetBIOS UI-frame memory allotment       40960

Dynamic Neighbor Transmit Buffer Size   5120
Dynamic Neighbor Receive Buffer Size    5120
Dynamic Neighbor Maximum Segment Size   1024
Dynamic Neighbor Keep Alive             DISABLED
Dynamic Neighbor SessionAlive Spoofing  DISABLED
Dynamic Neighbor Priority               MEDIUM

QLLC base source MAC address            40514C430000
QLLC maximum dynamic addresses          64
Type of local MAC list                  NON-EXCLUSIVE
Use of local MAC list is                ENABLED
Use of remote MAC list is               ENABLED
SNA explorer limit                      100
NetBIOS explorer limit                  100
```

Cuando haya terminado de configurar DLSw, salga de la configuración DLSw y vuelva a arrancar el direccionador.

```
DLSw config>exit
Config (only)>restart
Are you sure you want to restart the gateway? (Yes or [No]): yes
```

# Configuración y supervisión de DLSw

Este capítulo describe cómo configurar y supervisar el protocolo Data Link Switching. Incluye las siguientes secciones:



## Cómo acceder al entorno de configuración de DLSw

Utilice el proceso CONFIG para modificar la configuración del direccionador. La nueva configuración entra en vigor cuando el dispositivo se vuelve a arrancar.

Para entrar en el proceso de configuración, entre **talk 6** (o **t 6**), en el indicador OPCON (*). Aparecerá el indicador `CONFIG>`, tal como se muestra en el siguiente ejemplo:

```
MOS Operator Console

For help using the Command Line Interface, press ESCAPE, then '?'

* talk 6
Gateway user configuration

CONFIG>
```

Si el indicador `CONFIG>` no aparece inmediatamente, pulse de nuevo la tecla **Intro**.

Todos los mandatos de configuración de DLSw se entran en el indicador `DLS config>`. Para acceder a este indicador, entre el mandato **protocol DLSw** tal como se muestra:

```
Config>protocol dls
DLSw protocol user configuration
DLSw config>
```

## Requisitos previos a la configuración

Antes de empezar ningún procedimiento de configuración, utilice el mandato **list device** desde el indicador **config** para listar los números de interfaz de los distintos dispositivos. Si necesita más explicaciones sobre los mandatos de configuración, consulte los mandatos de configuración que se describen en este capítulo.

**Consideraciones a tener en cuenta**

Para el IBM 2210 con 4 MB de DRAM que ejecuta DLSw:

- El número máximo de almacenamientos intermedios globales debe definirse en 50. Esto asegurará que DLSw tiene la memoria necesaria para que se ejecute de forma eficiente.
- Puede utilizar el mandato **set global-buffers** desde el indicador `Config>` principal para definir el número máximo de almacenamientos intermedios globales.

## Mandatos de configuración de DLSw

Esta sección resume y explica los mandatos de configuración de DLSw. Los mandatos de configuración de DLSw le permite crear o modificar una configuración DLSw. La Tabla 36 contiene un breve resumen de cada mandato. Entre todos los mandatos de configuración de DLSw después del indicador `DLSw Config>`. Los valores por omisión correspondientes a los mandatos y sus parámetros aparecen entre corchetes inmediatamente después del indicador.

Los cambios efectuados en la configuración del direccionador no entran en vigor de forma inmediata, sino que pasan a formar parte de la configuración de SRAM del direccionador cuando este se vuelve a arrancar.

*Tabla 36 (Página 1 de 2). Resumen de mandatos de configuración de DLSw*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Add | Añade una estación de enlace SDLC, una dirección IP de direccionador contiguo TCP, una estación o destino QLLC, entradas de la antememoria, entradas de la lista de direcciones MAC, modificaciones de la prioridad de circuito y modificaciones de exploración de la antememoria MAC. |
| Ban | Permite acceder al indicador de configuración del Nodo límite de acceso (BAN), en el que se pueden entrar mandatos de configuración de BAN. |
| Close-Sap | Cierra un punto de acceso de servicio (SAP) actualmente abierto. DLSw utiliza los SAP para establecer comunicación en interfaces que dan soporte a LLC. |
| Delete | Elimina una estación de enlace SDLC configurada, una conexión TCP, una estación o destino QLLC, entradas de la antememoria, entradas de la lista de direcciones MAC, modificaciones de prioridad de circuito o modificaciones de exploración de la antememoria MAC. |
| Disable | Desactiva el protocolo DLSw, una estación de enlace SDLC, la función de desconexión de LLC, direccionadores contiguos dinámicos, una estación o interfaz QLLC o el uso de la lista de direcciones MAC local o remota. |
| Enable | Activa el protocolo DLSw, una estación de enlace SDLC, la función de desconexión LLC, direccionadores contiguos dinámicos, una estación o interfaz QLLC, el uso de la lista de direcciones MAC local o remota o el valor del bit de precedencia DLSw de IPv4. |
| Join-Group | Permite que los direccionadores contiguos DLSw se busquen de forma dinámica entre sí. |
| Leave-Group | Elimina el direccionador del grupo DLSw especificado. |
| List | Muestra información correspondiente a estaciones de enlace SDLC, SAP, prioridad de circuito, grupos DLSw, información global de DLSw, destinos, estaciones e interfaces QLLC, entradas de la antememoria o entradas de la lista de direcciones MAC. El mandato también ofrece información detallada sobre conexiones TCP. |
| NetBIOS | Ofrece acceso al indicador de configuración de NetBIOS. |
| Open-SAP | Permite a DLSw transmitir datos sobre el SAP especificado. DLSw utiliza los SAP para establecer comunicación en interfaces que dan soporte a LLC. |

| Tabla 36 (Página 2 de 2). Resumen de mandatos de configuración de DLSw | |
|---|---|
| Mandato | Función |
| Set | Configura parámetros de LLC2, el número de sesiones DLSw, el número de segmento SRB, el tamaño del almacenamiento intermedio TCP, asignación de memoria, temporizadores del protocolo, prioridad de circuito, parámetros correspondientes a direccionadores contiguos, parámetros correspondientes al funcionamiento de QLLC y parámetros relacionados con la lista de direcciones MAC. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Add

Utilice el mandato **add** para configurar una estación de enlace SDLC una dirección IP de direccionador contiguo TCP, una estación o destino QLLC, entradas de la antememoria, entradas de la lista de direcciones MAC, modificaciones de prioridad de circuito, y modificaciones de exploración de la antememoria MAC.

**Sintaxis:**

| | |
|---|---|
| a**dd** | cache-entry<br>explorer-override<br>mac-list<br>priority<br>qllc...<br>sdlc<br>tcp |

**cache-entry**

Añade una entrada de la antememoria MAC configurada. Esta entrada de la antememoria correlaciona una determinada dirección MAC con un determinado similar DLSw. Una dirección MAC se puede correlacionar con varios similares DLSw añadiendo varias entradas de la antememoria.

**Ejemplo: `add cache-entry`**

```
Enter MAC Address [400000000000]? 10005a123456
Enter the DLSw neighbor IP Address [0.0.0.0]? 128.185.122.234
          MAC cache entry has been created.
```

**explorer-override**

Añade una entrada de modificación de exploración de la antememoria MAC. Esta modificación permite que una serie de direcciones MAC posean distintas características de antememoria MAC y de flujo de exploración. Cuando se crea una entrada de la antememoria MAC, se efectúa una búsqueda en la lista de modificaciones de exploración en el orden en el que se han configurado. Si se encuentra una coincidencia, se utilizan los parámetros de antememoria MAC y los relacionados con la exploración de la primera modificación de exploración coincidente. Si no se encuentra ninguna coincidencia, se utilizan los valores relacionados con la exploración y de la antememoria MAC global de DLSw.

**Ejemplo:** add explorer-override

```
Enter MAC address value [000000000000]?400031740000
Enter MAC address mask [FFFFFFFFFFFF]?ffffffff0000
Database age timeout (0-1000 secs. Decimal)[0.0]?0
Max wait timer ICANREACH (1-1000 secs. Decimal) [2.0?]
Neighbor priority wait timer (0,0-5.0 secs. Decimal) [2.0]?0
Time to delay sending test response (0.0-5.0 secs. Decimal) [0.0]?
Forwarding explorers (E/L/D) [E]?

Enter position in explorer override list to insert new entry ....
  Record number (0=add at end of list) [0]?
Explorer override record has been created.
```

MAC address value y MAC address mask
: En combinación, estos dos campos representan una serie de direcciones MAC. Para determinar si se debe utilizar un registro de modificación de exploración de antememoria MAC configurada con el valor y máscara especificados para una determinada dirección MAC, se utiliza el siguiente algoritmo:

```
if ((<specific MAC address>AND<override's mask>) == <override's value>)
match on explorer override is found; use override's value
```

Database age timeout
: Especifica el periodo de tiempo que se deben retener las entradas de DLSw no utilizadas. Las entradas de la base de datos correlacionan direcciones MAC de destino con el grupo de similares DLSw que pueden acceder a las mismas.

  Un valor igual a cero indica que las entradas de esta base de datos no deben caducar. Esto puede resultar útil cuando se ejecutan conexiones TCP de direccionadores contiguos sobre interfaces de marcación, pero en general no se recomienda porque desactiva otras funciones de DLSw.

Max wait timer ICANREACH
: Especifica el periodo de tiempo que se debe esperar una respuesta ICANREACH correspondiente a un mensaje CANUREACH transmitido anteriormente.

Neighbor priority wait timer
: Especifica el periodo de tiempo que se debe esperar durante la exploración antes de seleccionar un direccionador contiguo. Esto permite seleccionar un direccionador contiguo de prioridad más alta aunque no sea el primero en responder con un mensaje ICANREACH.

  Un valor igual a cero indica que no se utiliza la característica de prioridad de direccionador contiguo. No habrá información sobre los similares DLSw en antememoria correspondiente a la dirección MAC. Siempre se envía un mensaje CANREACH y se utiliza el primer similar DLSw que envía un mensaje ICANREACH (independientemente de su prioridad).

Delay sending TEST response
: El periodo de tiempo que se debe esperar, una vez finalizada la exploración de una dirección MAC, antes de enviar la respuesta TEST. Esto resulta útil si hay dos 2210 de DLSw en la misma LAN conectada por puente capaces de alcanzar la misma dirección MAC a través de similares DLSw. Si se prefiere un 2210 de DLSw, la respuesta TEST se puede retrasar en el 2210 de DLSw menos adecuado.

Forwarding explorers
: Especifica si los exploradores se deben reenviar a todos los similares DLSw aplicables, se deben reenviar sólo a la conexión TCP local o no se deben reenviar.

Position in explorer override list to insert new entry
: Puesto que se utiliza la primera modificación coincidente de exploración de la antememoria MAC, el orden en que las entradas de modificación de exploración se configuran resulta importante. Este campo especifica en qué lugar de la lista actual de modificaciones se debe insertar esta nueva entrada. Se puede utilizar el mandato **list explorer-override** para ver la lista actual de modificaciones de exploración. Un valor igual a cero para este campo especifica que se debe añadir la nueva entrada al final de la lista actual.

**mac-list** Añade una entrada a la lista de direcciones MAC local. Todas las entradas añadidas a la lista de direcciones MAC local forman la lista de direcciones MAC local. La lista de direcciones MAC local se envía a cada similar DLSw para indicar el grupo de direcciones MAC que se pueden alcanzar utilizando este DLSw.

**Ejemplo: `add mac-list`**

```
Enter MAC Address Value[400000000000]? 10005a000000
Enter MAC Address Mask [ffffff000000]?

MAC list entry has been created.

For the new entry to take effect, you must restart or commit the change using
     't 5': SET MAC LIST
```

Enter MAC Address Value y Enter MAC Address Mask
: Estos dos campos combinados representan un grupo de direcciones MAC a las que se puede alcanzar utilizando este DLSw. Si se recibe una trama en un DLSw similar, se utilizan estos dos campos en el siguiente algoritmo:

```
if ( (<frame's destination MAC address> AND <MAC Address Mask>)
     == <MAC Address Value> )
match on MAC address list found; forward frame to this DLSw
```

**priority** Añade una entrada de modificación de prioridad de circuito. Cuando se establece una sesión DLSw, se efectúa una búsqueda en la lista de modificaciones de prioridad de circuito en el orden en el que están configuradas. Si se encuentra una coincidencia en el rango de SAP de origen, rango de direcciones MAC de origen, rango de SAP de destino y rango de direcciones MAC de destino, se utilizan las prioridades de exploración y la sesión de la entrada coincidente de la modificación de prioridad de circuito. Si no se encuentra ninguna coincidencia con ninguna entrada de modificación de prioridad de circuito, se utilizan los valores por omisión de prioridad de circuito.

**Ejemplo: `add priority`**

```
Enter range of source SAPs .....
  Lower source sap value [0]?
  Upper source sap value [FE]?

Enter range of source MAC addresses .....
  Lower source MAC address [000000000000]?
  Upper source MAC address [FFFFFFFFFFFF]?

Enter range of destination SAPs .....
  Lower destination sap value [0]?
  Upper destination sap value [FE]? c

Enter range of destination MAC addresses .....
  Lower destination MAC address [000000000000]? 10005a000000
  Upper destination MAC address [FFFFFFFFFFFF]? 10005affffff

Enter desired circuit priorities .....
Priority for session traffic (C/H/M/L) [M]? c
Priority for explorer traffic (C/H/M/L) [M]? m

Enter position in circuit priority override list to insert new entry .....
  Record number (0=add at end of list) [0]?
Circuit priority override record has been created.
```

Lower source sap value

Upper source sap value
: Estos dos campos combinados representan el rango de SAP de origen asignado a esta modificación de prioridad de circuito. Si el valor del SAP de origen no tiene importancia, especifique el rango completo de valores de SAP de origen (lower source value = 0 y upper source value = fe).

Lower source MAC address

Upper source MAC address
: Estos dos campos combinados representan el rango de direcciones MAC de origen asignado a esta modificación de prioridad de circuito. Si el valor de la dirección MAC de origen no tiene importancia, especifique el rango completo de valores de direcciones MAC de origen (lower source MAC address = 000000000000 y upper source MAC address = ffffffffffff).

Lower destination sap value

Upper destination sap value
: Estos dos campos combinados representan el rango de SAP de destino asignado a esta modificación de prioridad de circuito. Si el valor del SAP de destino no tiene importancia, especifique el rango completo de valores de SAP de destino (lower destination sap value = 0 y upper destination sap value = fe)

Lower destination MAC address

Upper destination MAC address
: Estos dos campos combinados representan el rango de direcciones MAC de destino asignado a esta modificación de prioridad de circuito. Si el valor de la dirección MAC de destino no tiene importancia, especifique el rango completo de valores de direcciones MAC de destino (lower destination MAC address = 000000000000 y upper destination MAC address = ffffffffffff).

Priority for session traffic
: La prioridad de circuito a asignar a todo el tráfico de sesión que coincida con el rango de SAP de origen, direcciones MAC de origen, SAP de destino y direcciones MAC de destino de esta entrada de modificación de prioridad de circuito.

Priority for explorer traffic
: La prioridad de circuito a asignar a todo el tráfico de exploración que coincida con el rango de SAP de origen, direcciones MAC de origen, SAP de destino y direcciones MAC de destino de esta entrada de modificación de prioridad de circuito.

Position in circuit priority override list to insert new entry
: Puesto que se utiliza la primera modificación coincidente de prioridad de circuito, el orden en que se configuran las entradas de modificación de prioridad de circuito resulta importante. Este campo especifica en qué lugar de la lista actual de modificaciones de prioridad de circuito se debe insertar esta nueva entrada. Se puede utilizar el mandato **list priority** para ver la lista actual de modificaciones de prioridad de circuito. Un valor igual a cero para este campo especifica que se debe añadir la nueva entrada al final de la lista actual.

**qllc** Añade soporte para una estación QLLC en una red X.25 o para un destino DLSw para estaciones QLLC. Una estación QLLC es la estación de enlace lógico que representa un dispositivo QLLC conectado al direccionador a través de una interfaz X.25. Un destino QLLC es una correlación de direcciones que apunta a un dispositivo de la red DLSw. Este dispositivo está conectado a un direccionador contiguo DLSw a través de cualquiera de sus tipos DLC soportados y normalmente no se trata de un dispositivo QLLC.

**Sintaxis:**

| | |
|---|---|
| a**ddqllc** | destination<br>station |

**Ejemplo: `add qllc destination`**

```
Enter the connection id (1-8 alphanumeric chars) [ ]? conn1
Destination MAC address [000000000000]? 400031740000
Destination SAP in hex [4]?
QLLC destination record added/updated
```

Connection id
: Serie de caracteres alfanuméricos cuyos bytes 4-11 se comparan con los datos de usuario de llamada de los paquetes Call_Request de entrada. En muchos productos QLLC, este valor se configura como una contraseña.

  **PRECAUCIÓN:**
  **Si se configura un registro de destino QLLC con el valor "ANYCALL", DLSw acepta todas las llamadas (independientemente de la dirección DTE o del id de conexión). Tenga en cuenta la seguridad si decide aceptar todas las llamadas de entrada.**

Destination MAC address
: La dirección MAC a utilizar como destino para sesiones iniciadas por una llamada QLLC de entrada, donde el paquete Call_Request coincide con el id de conexión anterior.

Destination SAP
: El SAP de destino a utilizar para el mismo tipo de sesión.

**Ejemplo: `add qllc station`**

```
Interface # [0]? 1
PVC or SVC [PVC]?
Logical channel number (1-4095) [0]? 2
Source MAC address [400000310104]?
Source SAP in hex [4]?
Destination MAC address [000000000000]? 400011112323
Destination SAP in hex [0]? 4
PU type (2/4/5) [2]?
XID0 block num in hex (0-0xfff) [0]?
XID0 id num in hex (0-0xfffff) [0]?
New QLLC station record added
```

Interface #
: El número de la interfaz X.25 por la que el dispositivo QLLC se conecta al direccionador.

PVC or SVC
: El tipo de circuito virtual (permanente o conmutado) por el que se va a conectar el dispositivo QLLC.

Logical channel number
: Para los PVC, el número de canal X.25 al que está suscrita la estación QLLC. Este campo no se aplica a los SVC, los cuales utilizan números de canal asignados de forma dinámica.

DTE address
: Para los SVC, el "número de teléfono" por el que se conoce la estación QLLC en su red X.25. Es la dirección del partícipe llamado para las llamadas que emite este direccionador y la dirección del partícipe que emite la llamada para llamadas procedentes de la estación QLLC. Este campo no se aplica a los PVC, los cuales se pueden identificar de forma exclusiva por un número de canal lógico fijo.

Source MAC address
: La dirección de Control de acceso al medio que representa esta estación QLLC ante el resto de la red DLSw. Es la dirección de origen para sesiones DLSw iniciadas por la estación QLLC y la dirección de destino para sesiones iniciadas por otros dispositivos de la red DLSw.

  Esta dirección es necesaria para cada estación y debe ser exclusiva entre todas las direcciones MAC de origen correspondientes a dispositivos QLLC y SDLC configurados en el direccionador. Para conseguir un funcionamiento fiable, también debe ser exclusiva entre todas las direcciones MAC de estaciones finales de la red DLSw. El valor por omisión se crea de modo que sea muy probable que sea exclusivo dentro de la red. Esta y todas las direcciones MAC de DLSw están en formato de orden de bits no canónico (red en anillo).

Source SAP
: La dirección del Punto de acceso de servicio emparejado con la dirección MAC de origen. Se utiliza del mismo modo.

Destination MAC address
: La dirección del Control de acceso al medio que representa una estación de la red DLSw a la que está conectado el dispositivo QLLC. Para los PVC, DLSw intenta iniciar una sesión con esta dirección de destino en cuanto se establece un contacto satisfactorio con el dispositivo QLLC. Para los SVC, DLSw intenta iniciar

una sesión con esta dirección de destino en cuanto el dispositivo QLLC coloca una llamada de entrada.

Esta dirección no es obligatoria. Si no la configura, la estación QLLC sólo puede ser el destino de una sesión DLSw, no el origen.

Destination SAP
: La dirección del Punto de acceso de servicio emparejado con la dirección MAC de destino. Se utiliza del mismo modo. Tanto la dirección MAC de destino como el SAP de destino deben ser distintos de cero para que DLSw los pueda utilizar como destino de una sesión DLSw.

PU type
: El tipo de Unidad física SNA de la estación QLLC. Puede tener uno de los siguientes valores:

  2 Un nodo PU 2.0 o T2.1. También puede representar dispositivos que envían mensajes XID_1 en respuesta a un sondeo XID_null.

  4 Un controlador SNA intermedio que realiza funciones de direccionamiento SNA de subárea. Estos suelen ejecutar software NCP de IBM en una modalidad de nodo de red intermedio (INN) ante otro NCP, y *no* es para conexiones de función límite NCP con dispositivos PU 2.

  5 Un sistema principal o sistema principal con un procesador de componente frontal (por ejemplo, 37xx con NCP) que realiza una conexión de función de límite con un dispositivo PU 2.0 de la red DLSw. Si el sistema principal realiza una conexión con un dispositivo T2.1 de la red DLSw, es preferible, aunque no obligatorio, configurar el sistema principal como un dispositivo T2.1 (es decir, Pu type=2, XID0 block/id num=0).

XID0 block num
: El campo de número de bloque XID que utilizará el direccionador al crear un XID_0 en nombre de la estación QLLC. Este campo sólo se aplica (y se solicita) cuando el tipo de PU es 2. Para dispositivos T2.1 y cualquier dispositivo PU 2.0 que pueda responder por sí mismo a un sondeo XID_null, este campo es opcional y se debe dejar con valor cero. Si no está seguro, es más seguro rellenarlo para todos los dispositivos QLLC PU2.0 y dejar el valor cero para todos los dispositivos T2.1. Si se especifica un valor distinto de cero, debe coincidir con el campo de dirección PU correspondiente de la configuración de nodo principal conmutado NCP de IBM correspondiente a la estación de enlace.

XID0 id num
: El campo de número de identificador XID que va junto al campo de número de bloque XID0. Se utiliza con el mismo objetivo y es necesario en las mismas situaciones.

**sdlc** Añade información SDLC específica para añadir una estación de enlace SDLC a la configuración de una determinada interfaz serie SDLC. El mandato **sdlc** se debe utilizar una vez para cada estación secundaria de la línea SDLC.

**Ejemplo:** `add sdlc`

```
DLSw config>add sdlc
Interface # [0]? 2
SDLC Address or 'sw' (switched call-in) [C1]?
Source MAC address [4000112402C1]? 4000003174d1
Source SAP in hex [4]?
Destination MAC address [000000000000]? 400000000002
Destination SAP in hex [0]? 4
PU type (1/2/4/5) [2]?
XID0 block num in hex (0-0xfff) [0]? 017
XID0 id num in hex (0-0xfffff) [0]? 00001
Poll with TEST (T), SNRM (S), or DELAYED SNRM (D) [T]?
```

Interface #
: El número de la interfaz SDLC por la que el dispositivo SDLC se conecta al direccionador.

SDLC Address
: La dirección SDLC de la estación de enlace que está conectado, entre 01–FE o “sw”. “Sw” indica que se trata de un circuito conmutado de entrada de llamadas SDLC.

Source MAC address
: La dirección MAC de esta PU SDLC. Este valor identifica la estación SDLC conectada dentro del dominio DLSw. Debe ser exclusivo entre las estaciones SDLC y QLLC conectadas a este direccionador y debe ser exclusivo entre todos los SDLC, QLLC y LAN.

Source SAP in hex
: Junto con la dirección MAC de origen, representa la estación final SDLC dentro del dominio DLSw.

Destination MAC Address
: La dirección MAC de la estación de enlace remota a la que se conecta. La dirección MAC está en formato de orden de bits no canónico (red en anillo). Esto es cierto aunque la estación final remota esté en Ethernet. En este caso, utilice el mandato **flip** de supervisión de ASRT para ayudar a alternar la dirección MAC.

  **Nota:** La dirección de destino no puede tener el valor 0 si se trata de un circuito conmutado de entrada de llamadas SDLC (indicado por “sw” como la dirección SDLC).

Destination SAP in hex
: Define el SAP a utilizar cuando se intente una conexión de forma automática cuando se active la estación de enlace. Si este SAP es 0, la estación de enlace está en modalidad pasiva y no inicia el establecimiento de línea. En este caso, la dirección MAC de destino se pasa por alto.

  **Nota:** El SAP de destino no puede tener el valor 0 si se trata de un circuito conmutado de entrada de llamadas SDLC (indicado pro “sw” como la dirección SDLC).

PU type
: El tipo de Unidad física SNA de la estación SDLC. Puede tener uno de los siguientes valores:

  1 Un nodo PU1. Si un nodo PU1 conectado a SDLC se comunica con un dispositivo conectado a SDLC que da soporte a dispositivos PU1, configure el tipo de PU como 1 y el id/número de bloque XIDO como cero. Si un nodo PU1 conectado a SDLC se comunica con un dispositivo conectado a la

LAN que da soporte a dispositivos PU1, configure el tipo de PU como 1 y el id/número de bloque XIDO como un valor distinto de cero.

2 Un nodo PU 2.0 o T2.1.

4 Un controlador SNA intermedio que realiza funciones de direccionamiento SNA de subárea. Estos suelen ejecutar software NCP de IBM en una modalidad de nodo de red intermedio (INN) ante otro NCP, y *no* es para conexiones de función límite NCP con dispositivos PU 2.

5 Un sistema principal, con o sin procesador de componente frontal (por ejemplo, un 37xx con NCP), que realiza una conexión de función de límite con un dispositivo PU 2.0 de la red DLSw. Si el dispositivo realiza una conexión con un dispositivo T2.1 de la red DLSw, debe configurar el sistema principal como un dispositivo T2.1 (es decir, PU type=2, XID0 block/id num=0).

**Nota:** No puede definir esta parámetro para un circuito conmutado de entrada de llamadas SDLC. Se adopta un tipo de PU de 2.0.

XID0 block num

El campo de número de bloque XID que utilizará el direccionador al crear un XID_0 en nombre de la estación SDLC. Este campo sólo se aplica y se solicita cuando el tipo de PU es 1 ó 2. Es opcional y se debe dejar como cero para dispositivos T2.1 y cualquier dispositivo PU 2.0 que pueda responder por sí mismo a un sondeo XID_null. Si no está seguro, es más seguro rellenarlo para todos los dispositivos SDLC PU2.0 y dejar el valor cero para todos los dispositivos T2.1. También se debe dejar el valor cero para los dispositivos PU1 que se comunican con dispositivos conectados a SDLC que dan soporte a dispositivos PU1. Si se especifica un valor distinto de cero, debe coincidir con el campo de dirección PU correspondiente de la configuración de nodo principal conmutado NCP de IBM correspondiente a la estación de enlace.

**Nota:** Si define para este parámetro un valor distinto de cero para un circuito conmutado de entrada de llamadas SDLC, la información configurada se coloca en XID_0. Para un circuito conmutado de entrada de llamadas SDLC, el número de bloque XID_0 configurado se utiliza de otro modo. El software da por supuesto que la estación de entrada de llamadas creará siempre su propio XID_0. Si para este parámetro se define un valor distinto de cero, el valor XID_0 de la estación se modifica con el valor configurado. Si para este parámetro se define el valor cero, el XID_0 de la estación no se modifica.

XID0 id num

El campo de número de identificador XID que va junto al campo de número de bloque XID0. Se utiliza con el mismo objetivo y es necesario en las mismas situaciones.

Poll type

Define cómo y cuando se debe sondear el dispositivo SDLC:

**TEST** Sondear el dispositivo SDLC con una trama TEST cuando la interfaz pase a estar activa.

**SNRM** Sondear el dispositivo SDLC con una trama SNRM cuando la interfaz pase a estar activa.

**DELAYED SNRM**
Sondear el dispositivo SDLC con una trama SNRM cuando se haya establecido la sesión DLSW y la interfaz esté activa.

**tcp** Añade la dirección interna de un similar DLSw con el que este DLSw puede realizar una conexión.

**Ejemplo: `add tcp`**

```
Enter the DLSw neighbor IP Address [0.0.0.0]? 128.185.14.1
Connectivity setup type (a/p) [p]?
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal)  [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive? (E/D) - [D]?
Enable/Disable NetBIOS SessionAlive Spoofing (E/D) [D]?
Neighbor Priority (H/M/L) [M]?
```

Enter the DLSw neighbor IP Address
Indica la dirección IP del similar DLSw remoto de la red IP con el que desea establecer una conexión.

Connectivity setup type
Indica si la conexión TCP con este DLSw se debe realizar en el momento de arrancar el direccionador (Active) o cuando se necesite (Passive). Para ver un a visión general de estas opciones, consulte el tema “Conexiones TCP, descubrimiento de direccionadores contiguos y exploración de difusión múltiple” en la página 528.

Transmit Buffer Size
El tamaño del almacenamiento intermedio de transmisión de paquetes, comprendido entre 1024 y 32768. El valor por omisión es 5120.

Receive Buffer Size
El tamaño del almacenamiento intermedio de recepción de paquetes, comprendido entre 1024 y 32768. El tamaño por omisión es 5120.

Maximum Segment Size
El tamaño máximo del segmento TCP, comprendido entre 64 y 16384. El valor por omisión es 1024.

Enable/Disable Keepalive (E/D)
Indica si desea que DLSw envíe mensajes Keepalive de conexión TCP. El valor por omisión es D (Desactivado).

Enable/Disable NetBIOS SessionAlive Spoofing (E/D)
Indica si desea eliminar las tramas-I SessionAlive de NetBIOS (que no se reenvíen al asociado DLSw). El valor por omisión es D (Desactivado), lo que significa no eliminar tramas.

Neighbor Priority
Le permite especificar la prioridad del direccionador contiguo, que puede ser High, Medium o Low. Si se puede alcanzar una estación de destino a través de varios direccionadores contiguos con distintas prioridades, DLSw intenta establecer circuitos con dicha

estación a través del direccionador contiguo que tenga la prioridad más alta.

## BAN

Utilice el mandato **ban** para acceder al indicador de configuración de Nodo límite de acceso (BAN). Los mandatos BAN se entran en el indicador de configuración de BAN (`BAN config>`). Consulte el tema “BAN” en la página 92 para ver una explicación de cada uno de estos mandatos.

**Sintaxis:**

b**an**

## Close-Sap

Utilice el mandato **close-sap** para desactivar la conmutación DLSw para el punto de acceso de servicio (SAP) especificado. LCC utiliza estos SAP para la configuración en la red.

**Sintaxis:**

c**lose-sap**

**Ejemplo: `close-sap`**

```
Interface #[1]?
Enter SAP in hex (range 0–FE), or one of the following:
   'SNA', 'NB', or LNM [0]? sna
SAP(s) 0 4 8 C closed on interface 1
```

**Interface #**

El número de interfaz que utiliza el SAP abierto.

**Enter SAP**

Puede entrar SAP individuales en hexadecimal o bien puede entrar SNA, NB (NetBIOS) o LNM (LAN Network Manager).

Si entra los SAP en hexadecimal, el rango es el comprendido entre 0 y FE y el SAP debe ser un número par.

Si entra SNA, los SAP 0, 4, 8 y C se cierran.

Si entra NB, el SAP F0 se cierra.

Si entra LNM, los SAP 0, 2, D4, F2, F4, F8 y FC se cierran.

## Delete

Utilice el mandato **delete** para eliminar una estación de enlace SDLC, una dirección IP de direccionador contiguo TCP, una estación o destino QLLC, entradas de la antememoria, entradas de direcciones MAC, modificaciones de prioridad de circuito y modificaciones de exploración de la antememoria MAC de la configuración DLSw.

**Sintaxis:**

| | |
|---|---|
| del**ete** | cache-entry |
| | explorer-override |
| | mac-list |
| | priority |

qllc...
sdlc
tcp

**cache-entry**
Elimina una entrada de la antememoria MAC configurada.

**Ejemplo: `delete cache-entry`**

```
Enter mac cache record number [1]? 1
MAC cache entry has been deleted
```

**mac cache record number**
El número de registro de la entrada de la antememoria MAC a suprimir. El número de registro se puede determinar mediante el mandato de configuración **list cache all**.

**explorer-override**
Elimina una entrada de modificación de exploración de la antememoria MAC.

**Ejemplo: `delete explorer-override`**

```
Enter explorer override record number [1]?
Explorer override record has been deleted.
```

**Explorer override record number**
El número de registro de la entrada de modificación de exploración de la antememoria MAC a suprimir. El número de registro se puede determinar mediante el mandato **list explorer-override** desde *talk 6*.

**mac-list** Elimina una entrada de la lista local de direcciones MAC.

**Ejemplo: `delete mac-list`**

```
Enter mac list record number [1]? 1
Local MAC list entry 10005A000000 / FFFFFF000000 has been deleted.

For the deletion to take effect, commit the change using
  't 5': SET MAC-LIST.
```

**mac list record number**
El número de registro de la entrada de la lista MAC a suprimir. El número de registro se puede determinar mediante un mandato de configuración **list mac-list all**.

**priority** Elimina una entrada de modificación de prioridad de circuito.

**Ejemplo: `delete priority`**

```
Enter circuit priority override record number [1]? 1
Circuit priority override record has been deleted.
```

**Circuit priority override record number**
El número de registro de la entrada de modificación de prioridad de circuito a suprimir. El número de registro se puede determinar mediante el parámetro de configuración **list priority**.

**qllc** Elimina soporte para una estación QLLC en una red X.25 o para un destino DLSw para estaciones QLLC.

**Sintaxis:**

del**ete** q**llc** destination
station

**Ejemplo: `del q destination`**

```
DLSw config>del qllc dest
Enter the connection id (1-8 alphanumeric chars) [ ]? conn1
QLLC Destination record deleted
```

**Ejemplo: `del q station`**

```
DLSw config>del qllc st
Interface # [0]? 2
PVC or SVC [PVC]?
Logical channel number (1-4095) [0]? 4
QLLC station record deleted
```

**sdlc** Elimina la estación de enlace SDLC especificada de la lista de estaciones a las que DLSw puede ofrecer servicios cuando se vuelva a arrancar el direccionador.

**Sintaxis:**

del**ete** s**dlc**

**Ejemplo: `delete sdlc`**

```
Interface #[0]? 1
SDLC Address or 'sw' (switched dial-in) [C1]?
Record deleted
```

**Interface #**
El número de interfaz del direccionador que se conecta a la estación de enlace SDLC.

**SDLC Address**
La dirección SDLC de la estación de enlace remota que está suprimiendo. Los valores son los comprendidos entre 01 y FE o “sw” para un circuito conmutado de entrada de llamadas SDLC.

**tcp** Elimina la dirección IP (*dirección_ip*) del similar DLSw con el que puede establecer una conexión TCP.

**Sintaxis:**

del**ete** t**cp** *dirección_ip*

**Ejemplo: `delete tcp`**

```
IP Address [0.0.0.0]? 128.185.14.1
```

## Disable

Utilice el mandato **disable** para desactivar el protocolo DLSw, una estación de enlace SDLC, la función de desconexión de LLC direccionadores contiguos dinámicos, una interfaz o estación QLLC o el uso de listas de direcciones MAC locales y remotas.

**Sintaxis:**

d**isable** dls
dynamic-neighbors
llc
mac-list
qllc...
sdlc

**dls** Evita que el direccionador de conexión por puente realice funciones de DLSw sobre todas las interfaces configuradas DLSw.

**Ejemplo: `disable dls`**

**dynamic-neighbors**
Evita que el direccionador acepte conexiones TCP DLSw de entrada procedentes de direcciones IP *que no sean* las de los direccionadores contiguos DLSw configurados mediante el mandato **add tcp**.

**Ejemplo: `disable dy`**

**llc** Evita que el direccionador termine de forma activa una conexión LLC emitiendo una trama LLC DISC. En su lugar, termina las conexiones LLC de forma pasiva. Esto hace que la conexión LLC de la estación final detecte la terminación del enlace. El sistema principal IBM responde de forma diferente ante desconexiones activas y pasivas.

Este mandato no afecta a la función de conmutación correspondiente a LLC de DLSw. Utilice el mandato **close-sap** para detener la función de conmutación LLC.

**Ejemplo: `disable llc`**

**mac-list** Desactiva el uso de listas de direcciones MAC locales o remotas.

**Sintaxis:**

**mac-list** local
remote

**Ejemplo: `disable mac-list local`**

```
Use of local MAC list is  DISABLED

For the change to take effect, restart or commit the change using
  't 5' : 'SET MAC-LIST'.
```

**Ejemplo: `disable mac-list remote`**

```
Use of remote MAC list is  DISABLED

For the change to take effect, restart or commit the change using
  't 5' : 'SET MAC-LIST'.
```

**qllc** Si especifica “callin” evita que DLSw acepte llamadas QLLC de entrada en la interfaz X.25 especificada. Este es el estado por omisión; una interfaz se debe activar de forma específica para que permita llamadas de entrada a DLSw.

Si especifica “station” evita que una estación QLLC configurada sea el origen o el destino de sesiones DLSw.

**Sintaxis:**

**qllc** callin
station

**Ejemplo: `dis q callin`**

```
Select the interface to be disabled for incoming QLLC calls:
Interface # [0]? 1
Interface 1 is now disabled for incoming QLLC calls
```

**Ejemplo: `dis q station`**

```
Interface # [0]? 1
PVC or SVC [PVC]?
Logical channel number (1–4095) [0] 2
This QLLC station has been marked disabled
```

**sdlc** Evita conexiones DLSw con la estación de enlace SDLC especificada.

**Ejemplo: `disable sdlc`**

```
Interface #[0]? 1
SDLC Address or 'sw' (switched dial-in) [C1]?
Record updated
```

## Enable

Utilice el mandato **enable** para activar el protocolo DLSw, una estación de enlace SDLC, la función de desconexión de LLC, direccionadores contiguos dinámicos, una interfaz o estación QLLC o el uso de listas de direcciones MAC locales o remotas.

**Sintaxis:**

**enable** dls
dynamic-neighbors
ipv4 dlsw precedence
llc
mac-list
qllc...
sdlc

**dls** Activa el funcionamiento de DLSw en el direccionador.

**Ejemplo: `enable dls`**

**dynamic-neighbors**
Define el direccionador para que acepte conexiones TCP DLSw de entrada procedentes de direcciones IP *que no sean* las de los direccionadores contiguos configurados mediante el mandato **add tcp**. Este es el estado por omisión.

**ipv4 dlsw precedence**
Define el direccionador para que defina los bits de precedencia IP correspondientes a IP versión 4. La característica BRS del direccionador lee estos bits de precedencia para establecer prioridades en el tráfico DLSw.

**Ejemplo:**

```
enable IPv4 DLSw Precedence
IPv4 Precedence is now enabled.
```

**llc** Permite al direccionador terminar una conexión LLC tras la pérdida de la conexión TCP.

**mac-list** Desactiva el uso de listas de direcciones MAC locales o remotas.

**Sintaxis:**

**mac-list** local
remote

**Ejemplo: enable mac-list local**

```
Use of local MAC list is  ENABLED

For the change to take effect, restart or commit the change using
  't 5' : 'SET MAC-LIST'.
```

**Ejemplo: enable mac-list remote**

```
Use of remote MAC list is  ENABLED

For the change to take effect, restart or commit the change using
  't 5' : 'SET MAC-LIST'.
```

**qllc** Si especifica “callin” hace que DLSw reciba llamadas QLLC de entrada en la interfaz X.25 especificada.

Si especifica “station” permite que una estación QLLC configurada sea el origen o el destino de sesiones DLSw. Este es el estado por omisión de cada estación QLLC configurada.

**Sintaxis:**

**qllc** callin
station

**Ejemplo: `en q callin`**

```
Select the X.25 interface to be enabled for incoming QLLC calls:
Interface # [0]? 1
Interface 1 now enabled for incoming QLLC calls
```

**Ejemplo: `en q station`**

```
Interface # [0]? 1
PVC or SVC [PVC]?
Logical channel number (1-4095) [0]? 2
This QLLC station has been marked enabled
```

**sdlc** Permite conexiones DLSw con la estación de enlace SDLC especificada.

**Ejemplo: `enable sdlc`**

```
Interface #[0]? 1
SDLC Address or 'sw' (switched dial-in) [C1]?
Record updated
```

## Join-Group

Utilice el mandato **join-group** para permitir que los direccionadores contiguos DLSw busquen de forma dinámica y creen sesiones TCP entre sí y para permitir la exploración de difusión múltiple y el reenvío de tramas. Para ver una visión general de estas funciones, consulte el tema “Conexiones TCP, descubrimiento de direccionadores contiguos y exploración de difusión múltiple” en la página 528. Para utilizar este mandato, la internet IP que se utilice debe dar soporte al direccionamiento de difusión múltiple y debe configurar OSPF y MOSPF desde el indicador `OSPF Config>`.

Al añadir un direccionador DLSw a un grupo, debe seleccionar si desea utilizar el modelo de ID de grupo de identificación de grupo (según el que el direccionador crea las direcciones de difusión múltiple correspondientes) o si desea especificar las direcciones de difusión múltiple. El modelo de ID de grupo es más fácil de configurar, pero debe especificar las direcciones de difusión múltiple si desea tener conectividad de difusión múltiple con productos que no son IBM DLSw Versión 2. Un direccionador puede ser miembro de ambos estilos de grupos simultáneamente.

Puede unir un máximo de 64 grupos mediante el modelo de ID de grupo. Cuando asigna un direccionador DLSw a un grupo, el protocolo DLSw añade de forma automática una de dos direcciones al número de grupo para formar una dirección de difusión múltiple. El direccionador transmite la dirección de difusión múltiple para identificarse ante los otros miembros del grupo y para transmitir paquetes a dichos miembros. Las dos direcciones que se añaden al número de grupo son 225.0.1.0 para similares y clientes DLSw y 225.0.1.64 para servidores DLSw. Por

ejemplo, la dirección de difusión múltiple correspondiente a un cliente del grupo 2 sería 225.0.1.2.

**Sintaxis:**

jo**in-group**

**Ejemplo:**

El siguiente ejemplo corresponde al valor por omisión [G]. Las descripciones que siguen al ejemplo contienen información sobre (G) y (M).

```
DLSw config>join
Configure group member (G) or specific multicast address (M) -  [G]?
Group ID (1-64 Decimal) [1]? 2
Client/Server or Peer Group Member(C/S/P)- [P]? c
Connectivity Setup Type (A/P/) [P]?
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]?
Enable/Disable NetBIOS SessionAlive Spoofing (E/D) [D]?
Neighbor Priority (H/M/L) [M]?
```

**Group member or specific multicast address**
Selecciona si desea que el direccionador cree direcciones de difusión múltiple y si desea especificar dichas direcciones usted mismo.

**Multicast IP address**
La dirección IP de difusión múltiple es una dirección IP de difusión múltiple compatible con DLSw Versión 2 y dentro del rango 224.0.10.0 a 224.0.10.191 que sirve para enviar y/o recibir tráfico de exploración DLSw.

**Read Only , Write Only  or Read Write**
Este parámetro indica si la dirección IP de difusión múltiple configurada se debe utilizar sólo para recibir tráfico de exploración (Read Only), sólo para enviar tráfico de exploración (Send Only), o tanto para enviar como para recibir tráfico de exploración (Read Write).

**Group ID** El número del grupo al que desea unir este direccionador.

**Client/Server or Peer Group Member**
El papel que debe asumir este direccionador dentro del grupo: C para cliente, S para servidor o P para similar.

**Connectivity setup type**
Indica si el direccionador se debe unir al grupo como miembro Activo o Pasivo. Esto controla el momento en que se establecen conexiones TCP con otros miembros del grupo, tal como se describe en el tema “Conexiones TCP, descubrimiento de direccionadores contiguos y exploración de difusión múltiple” en la página 528.

**Transmit Buffer Size**
El tamaño del almacenamiento intermedio de transmisión de paquetes, comprendido entre 1024 y 32768. El valor por omisión es 5120.

**Receive Buffer Size**
El tamaño del almacenamiento intermedio de recepción de paquetes, comprendido entre 1024 y 32768. El tamaño por omisión es 5120.

**Maximum Segment Size**

El tamaño máximo del segmento TCP, comprendido entre 64 y 16384. El valor por omisión es 1024.

**Enable/Disable Keepalive**

Indica si desea que DLSw envíe mensajes Keepalive de TCP a las conexiones activas dentro de este grupo. El valor por omisión es D (Desactivado).

**Enable/Disable NetBIOS SessionAlive Spoofing (E/D)**

Indica si desea eliminar las tramas-I SessionAlive de NetBIOS (que no se reenvíen a los asociados DLSw relacionados con este grupo). El valor por omisión es D (Disable), lo que significa que las tramas no se eliminan.

**Neighbor Priority (H/M/L) [M]?**

Le permite especificar la prioridad del direccionador contiguo, que puede ser High, Medium o Low. Si se puede alcanzar una estación final de destino a través de varios direccionadores contiguos con distintas prioridades, DLSw intenta establecer circuitos con dicha estación final a través del direccionador contiguo que tenga la prioridad más alta.

## Leave-Group

Utilice el mandato **leave-group** para eliminar el direccionador de un grupo configurado mediante el mandato **join-group** o para dejar de utilizar una dirección de difusión múltiple configurada.

**Leave-group** no afecta a las conexiones TCP existentes pertenecientes al grupo especificado.

**Sintaxis:**

l**eave-group**

**Ejemplo: leave-group**

```
Configure group member (G) or specific multicast address (M) -  [G]?
Group ID (1-64 Decimal) [1]? 2
```

## List

Utilice el mandato **list** para visualizar información de DLSw sobre estaciones de enlace SDLC, prioridad de circuito, SAP, direccionadores contiguos TCP, grupos, direccionadores contiguos dinámicos, destinos, interfaces, estaciones QLLC, entradas de la antememoria, entradas de la lista de direcciones MAC, modificaciones de prioridad de circuito y modificaciones de exploración de la antememoria MAC.

**Sintaxis:**

| | |
|---|---|
| l**ist** | cache |
| | dls |
| | explorer-override |
| | groups |
| | llc2 |
| | mac-list |
| | open |

priority
gllc...
sdlc
tcp
timers

**cache** Lista las entradas configuradas de la antememoria de direcciones MAC.

**Sintaxis:**

cache all
entry-number

**cache all**

**Ejemplo: `cache all`**

```
Entry  Mac Address   IP Address
-----  ------------  ---------------
    1  10005A123456  128.185.236.49
    2  10005A789ABC  128.185.236.49
```

**cache entry-number**

**Ejemplo: `cache entry-number`**

```
Enter mac cache record number [1]?

Entry  Mac Address   IP Address
-----  ------------  ---------------
    1  10005A123456  128.185.236.49
```

**dls** Muestra la información que se ha configurado con los mandatos **enable** y **set**.

**Ejemplo: `list dls`**

(La salida del mandato **list dls** es igual a la salida del mandato **list dls global**. Consulte la página 605 para ver un ejemplo de esta salida.)

**explorer-override**
Muestra las modificaciones configuradas de exploración de la antememoria MAC.

**Ejemplo: `list explorer-override`**

```
    Explorer      Explorer      DB Age    Wait ICR  Nbr Pri   TESTrsp  Forwarding
ID  MAC Value     MAC Mask      Timeout   Timeout   Timeout   Delay    Explorers
--  ------------  ------------  --------  --------  --------  -------  ---------
 1  400031740000  FFFFFFFF0000  DISABLED    20      DISABLED  0.0      AllPartners
 2  10005A000000  FFFFFF000000   1200       20      2.0       0.0      NoPartner
```

**groups** Muestra información de grupo correspondiente a este similar DLSw que se ha configurado con el mandato **groups config**. Consulte el tema “List” en la página 604 para obtener más información.)

**llc2** Muestra los parámetros de LLC2 que se han configurado con el mandato **set llc2**. (Para ver una explicación completa de estos parámetros, consulte el mandato **set llc2** en la página 593.) Estos parámetros se definen para cada interfaz. Si no se han efectuado cambios en los parámetros de LLC2 mediante el mandato **set llc2**, no se generará ninguna salida.

**Ejemplo: `list llc2`**

```
SAP     t1   t2   ti   n2   n3   tw   rw   nw   acc
 0       1    1   30    8    1    2    2    1    0
```

**SAP** Número de SAP.

**t1** Temporizador de respuestas.

**t2** Temporizador de acuses de recibo.

**ti** Temporizador de inactividad.

**n2** Valor máximo de reintentos.

**n3** Número de tramas-I recibidas antes de enviar ACK.

**tw** Ventana de transmisión.

**rw** Ventana de recepción.

**nw** ACK necesarios para aumentar Ww.

**acc** La implantación actual de LLC2 no utiliza prioridad de acceso. Como resultado, el valor por omisión de este parámetro siempre es 0.

**mac-list** lista las entradas configuradas de la lista de direcciones MAC.

**Syntax:**

**mac** all
entry-number

**mac-list all**

**Ejemplo: `list mac-list all`**

```
Entry  Mac Value     Mac Mask
-----  ------------  ------------
    1  10005A000000  FFFFFF000000
    2  400031740000  FFFFFFFF0000
```

**mac-list entry-number**

**Ejemplo: `list mac-list entry-number`**

```
Enter mac list record number [1]?

Entry  Mac Value     Mac Mask
-----  ------------  ------------
    1  10005A000000  FFFFFF000000
```

**open** Muestra todos los SAP abiertos y sus interfaces asociadas.

**Ejemplo: `list open`**

```
Interface    SAP(s)
    0         0  4
    1         0  4  8  C
```

**priority** Lista las prioridades de circuito seleccionadas para circuitos SNA y NetBIOS, las proporciones de transmisión entre las distintas prioridades de circuito y el tamaño de trama mayor configurado para NetBIOS.

```
DLSw config> list priority
Default priority for SNA DLSw session traffic is          MEDIUM
Default priority for NetBIOS DLSw session traffic is      MEDIUM
Default priority for SNA DLSw explorer traffic is         MEDIUM
Default priority for NetBIOS DLSw explorer traffic is     MEDIUM


Message allocation by C/H/M/L priority is   4/3/2/1
Maximum frame size for NetBIOS is           2052


    Source/  SAP      MAC Address                  Session   Explorer
ID  Dest     Range    Range                        Priority  Priority
--  -------  -------  ---------------------------  --------  --------
 1  Source:  00 - FE  000000000000 - FFFFFFFFFFFF  CRITICAL  MEDIUM
    Dest  :  00 - 0C  10005A000000 - 10005AFFFFFF
 2  Source:  04 - 04  400031740000 - 40003174FFFF  CRITICAL  MEDIUM
    Dest  :  00 - FE  000000000000 - FFFFFFFFFFFF
```

Las prioridades de circuito son Critical, High, Medium o Low. El direccionador utiliza el valor de prioridad que el usuario asigna para limitar de forma selectiva la longitud de ráfaga de distintos tipos de tráfico. Por ejemplo, si asigna al tráfico SNA el valor de prioridad Critical y al tráfico de sesión NetBIOS el valor de prioridad Medium, con una asignación de mensajes de 4/3/2/1, el direccionador procesa 4 tramas de sesión SNA antes de procesar 2 tramas NetBIOS, y así sucesivamente. En este ejemplo, dos tercios del ancho de banda disponible se dedica al tráfico SNA. Cuando el direccionador asigna ancho de banda utilizando las propiedades especificadas, *cuenta tramas en lugar de bytes*.

**qllc...** Lista estaciones, destinos o interfaces QLLC.

**Sintaxis:**

| | |
|---|---|
| q**llc** | callin<br>destination<br>station |

**Ejemplo: `li q callin`**

```
Interfaces enabled for incoming QLLC calls to DLSw:
    1
```

**Ejemplo: `li q destination`**

```
Connection ID   Dest  SAP/MAC
   CHICAGO       04   400000112323
```

Para ver una descripción de los parámetros, consulte el mandato **add qllc destination** en la página 573.

**Ejemplo: `li q station`**

```
1f  P/S  LCN/DTE addr  E/D Source SAO/MAC   Dest Sap/MAC     PU Blk/IdNum
 1  PVC  2             E  04 400000310104  04 400011112323   2 000/00000
 1  PVC  4             E  04 400000317402  04 400000000002   2 017/00001
 1  SVC  3721111       E  04 400000310103  00 000000000000   2 000/00000
```

Los parámetros que se listan aquí están descritos en la página 573. “E/D” indica si la estación se ha desactivado mediante el mandato **disable qllc station**.

**sdlc** Muestra información sobre la estación de enlace SDLC configurada con el mandato **add sdlc link station**.

**Nota:** Los circuitos conmutados de entrada de llamadas SDLC se indican con “FF(sw)” en el campo de dirección.

**Ejemplo: `list sdlc all`**

```
Net  Addr    Status    Source SAP/MAC    Dest SAP/MAC     PU Blk/IdNum  PollType
2    C1      Enabled   04 4000003174D1   00 400000000002  2  000/00000  TEST
2    C2      Enabled   04 4000103D01C2   00 000000000000  4
2    C3      Enabled   04 4000103D01C2   00 000000000000  2  017/00001  SNRM
3    FF(sw)  Enabled   04 4000103d01d2   04 400000000003  2  017/00002
```

**Net** El número de ID de la interfaz que conecta la estación de enlace SDLC.

**Addr** La dirección SDLC, comprendida entre 01 y FE o “FF(sw)” para un circuito conmutado de entrada de llamadas SDLC, de la estación de enlace que se conecta.

**Status** El estado, activada (enabled) o desactivada (disabled), de la estación de enlace.

**Source SAP/MAC**
El SAP LLC y las direcciones MAC que representan la estación SDLC conectada al dominio DLSw.

**Dest SAP/MAC**
El SAP LLC y las direcciones MAC de una estación final remota con la que la estación SDLC conectada iniciará un establecimiento de circuito cuando la estación SDLC se active.

**PU** El tipo de PU SNA del dispositivo SDLC conectado, que puede ser:

2 Un nodo PU 2.0 ó T2.1

4 Una PU 4 realizando funciones de direccionamiento de subárea INN con otra PU 4 (es decir, NCP-a-NCP)

5 Un sistema principal o sistema principal con un procesador de componente frontal (por ejemplo, 37xx con NCP) que realiza una conexión de función de límite con un dispositivo PU 2.0 de la red DLSw

**Blk/IdNum**
El número de bloque XID0 y el número de Id que utiliza el direccionador para generar un XID0 en nombre del dispositivo SDLC conectado. Este campo sólo se muestra para los dispositivos PU tipo 2.

**PollType** El tipo de trama SDLC que utiliza el direccionador para realizar el contacto inicial con la estación SDLC, que puede ser una trama TEST, una trama SNRM o una trama SNRM retrasada (una trama SNRM que sólo se envía después de que se haya establecido la sesión DLSw). Este campo sólo se muestra para los dispositivos PU tipo 2.

**tcp** Muestra los direccionadores contiguos TCP DLSw configurados. Los direccionadores contiguos se han configurado con el mandato **add tcp**.

**Ejemplo: `list tcp`**

```
                    Xmit    Rcv     Max     Keep-    SesAlive
Neighbor        CST Bufsize Bufsize Segsize Alive    Spoofing Priority
--------------- --- ------- ------- ------- -------- -------- --------
128.185.122.234  p    5120    5120    1024  DISABLED DISABLED MEDIUM
128.185.14.1     p    5120    5120    1024  DISABLED DISABLED MEDIUM
```

**Neighbor** La dirección IP del direccionador contiguo TCP

**CST** Tipo de configuración de conectividad, cuyos valores pueden ser Active o Passive.

**Xmit Bufsize**
El tamaño del almacenamiento intermedio de transmisión de paquetes, comprendido entre 1024 y 32768. El valor por omisión es 5120.

**Rcv Bufsize**
El tamaño del almacenamiento intermedio de recepción de paquetes, comprendido entre 1024 y 32768. El valor por omisión es 5120.

**Max Segsize**
El tamaño máximo del segmento TCP, comprendido entre 64 y 16384. El valor por omisión es 1024.

**Keepalive**
El estado de la función Keepalive, cuyos valores pueden ser enabled o disabled.

**SesAlive Spoofing**
El estado de la función de simulación SesAlive de NetBIOS, cuyos valores pueden ser enabled o disabled.

**Priority** La prioridad del direccionador contiguo en el proceso de selección. La prioridad del direccionador contiguo puede ser High, Medium o Low.

**timers** El tiempo, especificado por el usuario, durante el que se esperan diversas actividades.

**Ejemplo: `list timers`**

```
Database age timer                 1200  seconds
Max wait timer for ICANREACH       20    seconds
Wait timer for LLC test response   15    seconds
Wait timer for SDLC test response  15    seconds
QLLC session retry timer           20    seconds
Join Group Interval                900   seconds
Neighbor priority wait timer       2.0   seconds
Neighbor Inactivity Timer            5   minutes
Time to delay sending test resp.   0.0   seconds
```

Para obtener más información, consulte el mandato **list timers**.

## NetBIOS

Muestra el indicador de configuración de NetBIOS.

Para ver una descripción de los mandatos de NetBIOS, consulte el tema “Mandatos de NetBIOS” en la página 178.

**Sintaxis:**

n**etbios**

## Open-Sap

Emita el mandato **open-sap** para todos los SAP que desea que utilice DLSw, como origen o como destino de circuitos DLSw. Los valores de SAP de SNA que se utilizan con más frecuencia son 00, 04, 08 y 0C; todos estos SAP se pueden abrir conjuntamente utilizando el nemónico “SNA”. El SAP de NetBIOS es F0 y se hace referencia al mismo como “NB”. A los SAP relacionados con la función LAN

Network Manager se hace referencia como “LNM”. Abra los SAP correspondientes a los protocolos que ha seleccionado, en las interfaces a través de las cuales DLSw alcanza las estaciones finales SNA o NetBIOS, LNM o los puentes que gestiona LNM.

**Sintaxis:**

open-sap

**Ejemplo: `open-sap`**

```
Interface #[1]?
Enter SAP in hex (range 0–FE), or one of the following:
  'SNA', 'NB', or LNM [4]? sna
SAP(s) 0 4 8 C opened on interface 1
```

**Interface #**
: El número de la interfaz sobre la que desea abrir el SAP.

**Enter SAP in hex**
: Puede entrar SAP individuales en hexadecimal o puede entrar los valores SNA, NB (para NetBIOS) o LNM (para LAN Network Manager).

  Si entra los SAP en hexadecimal, el rango es el comprendido entre 0 y FE y el SAP debe ser un número par. Si entra SAP 4, 8 o C sin haber abierto anteriormente el SAP 0 en la misma interfaz, el SAP 0 se abrirá automáticamente.

  Si entra SNA, se abren los SAP 0, 4, 8 y C.

  Si entra NB, se abre el SAP F0.

  Si entra LNM, se abren los SAP 0, 2, D4, F2, F4, F8 y FC.

## Set

Utilice el mandato **set** para configurar el tamaño de la antememoria de correlación entre direcciones MAC y direcciones IP, los parámetros de LLC2, el número máximo de sesiones DLSw, el número de segmento SRB, los temporizadores de protocolo, el tamaño de los almacenamientos intermedios de recepción TCP direccionadores contiguos dinámicos TCP, parámetros correspondientes al funcionamiento de QLLC, parámetros relacionados con la lista de direcciones MAC y modificaciones de prioridad de circuito.

**Sintaxis:**

**set**
: cache
  dynamic-tcp
  explorer-limit
  llc2
  mac-list
  maximum
  memory
  priority
  qllc
  srb
  timers

**cache**
: El mandato **set cache** le permite especificar el tamaño de la antememoria de correlación entre direcciones MAC y direcciones IP.

  DLSw utiliza información guardada en esta antememoria para descubrir

rutas a estaciones remotas. Cuanto mayor es la antememoria, más probabilidades tiene DLSw de encontrar una estación remota deseada sin enviar tramas CANUREACH a todos los direccionadores contiguos TCP/IP conocidos.

Sin embargo, no debe definir un tamaño de esta antememoria excesivo. Si lo hace, el direccionador utilizará más memoria, lo que dejará menos memoria disponible para las sesiones DLSw reales. El efecto será una reducción del número de sesiones DLSw que el direccionador puede manejar.

**Ejemplo: `set cache`**

```
MAC  IP cache size (4 - 65535) [128]?
```

**dynamic-tcp**

Le permite especificar diversos parámetros de TCP para conexiones TCP de direccionadores contiguos dinámicos (es decir, aquellos que reciben conexiones de entrada procedentes de direccionadores contiguos no definidos mediante el mandato **add tcp**). DLSw solo utiliza estos valores si los direccionadores contiguos dinámicos están activados.

**Ejemplo: `set dyn`**

```
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]?
Enable/Disable NetBIOS SessionAlive Spoofing (E/D) [D]?
Neighbor Priority (H/M/L) [M]?
```

Para ver una descripción de estos parámetros consulte el mandato **add tcp** en la página 578.

**explorer-limit**

Le permite especificar límites en el número de tramas exploradoras SNA y NetBIOS que se pueden colocar en cola simultáneamente para ser enviadas a un asociado DLSw.

**Ejemplo: `set explorer-limit`**

```
Max SNA explorers per transport queue (0-1000)[100]?
Max NB explorers per transport queue (0-1000)[100]?
DLSW explorer limit values have been set.
```

**Max SNA explorers per transport queue**

El número máximo de tramas exploradoras SNA que se pueden colocar simultáneamente en cola para ser enviadas a un determinando asociado DLSw.

**Max NB explorers per transport queue**

El número máximo de tramas exploradoras NetBIOS que se pueden colocar simultáneamente en cola para ser enviadas a un determinado asociado DLSw.

**llc2** Le permite configurara atributos de LLC2 específicos para un determinado SAP.

**Ejemplo: `set llc2`**

```
Enter SAP in hex (range 0-F0)  [0]?  04
Reply timer (T1) in sec. [1]?
Receive Ack timer (T2) in 100 millisec. [1]?
Inactivity Timer (Ti) in sec. [30]?
Transmit Window (Tw), 1-127, 0=default [2]?
Receive Window (Rw), 127 Max [2]?
Acks needed to increment Ww (Nw) [1]?
Max Retry value (N2) [8]?
Number I-frames received before sending ACK (N3) [1]?
```

**Enter SAP in hex**

El número de SAP que desea ajustar. Los valores válidos son los comprendidos entre 0 y FE.

**Reply timer (T1)**

Este temporizador caduca cuando el similar LLC2 no recibe un acuse de recibo o respuesta necesarios procedentes de otro similar LLC2.

**Receive Ack timer (T2)**

El retraso que se produce al enviar un acuse de recibe correspondiente a una trama en formato-I en milisegundos.

**Inactivity Timer (Ti)**

Este temporizador caduca cuando el LLC no recibe una trama durante un periodo de tiempo especificado. Cuando el temporizador caduca, el similar LLC2 transmite un RR hasta que el similar LLC2 responde o se supera el número de reintentos N2. El valor por omisión es 30 segundos.

**Transmit Window (Tw)**

El número máximo de tramas-I que se pueden enviar antes de recibir un RR. Los valores válidos son los comprendidos entre 1 y 127. 0 define Tw con su valor por omisión. El valor por omisión es 2.

**Receive Window (Rw)**

El número máximo de tramas-I numeradas secuencialmente sin acuse de recibo que puede recibir un similar LLC2 desde un sistema principal remoto.

**Acks needed to increment Ww (Nw)**

Este parámetro afecta al modo en que funciona el algoritmo dinámico de colocación en ventana. Especifica el número de acuses de recibo después de una condición de error. El valor por omisión es 1. La ventana de trabajo (Ww) es una duplicación que cambia de forma dinámica de la ventana de transmisión (Tw). Cuando se detecta un error LLC, la ventana de trabajo (Ww) se restablece a 1. El valor de 'Acks needed to increment Ww' especifica el número de acuses de recibo que debe recibir la estación antes de incrementar Ww en 1. El valor de Ww continuará aumentando de este modo hasta que Ww = Tw.

**Max Retry value (N2)**

El número máximo de veces que el similar LLC2 transmite un RR sin recibir un acuse de recibo cuando caduca el temporizador de inactividad (Ti).

**Number I-frames received before sending ACK (N3)**

Este valor se utiliza con el temporizador T2 para reducir el tráfico de acuses de recibo correspondientes a tramas-I reci-

bidas. Para este contador se define un valor especificado que va decreciendo cada vez que se recibe una trama-I. Cuando este contador alcanza el valor 0 o el temporizador T2 caduca, se envía un acuse de recibo.

Para asegurar un buen rendimiento, defina para N3 un valor menor que el valor de Tw de LLC remoto. El valor por omisión es 1.

**mac-list** modifica la exclusividad de la lista de direcciones MAC local.

**Ejemplo: `set mac-list`**

```
Local MAC list exclusivity (E=exclusive, N=non-exclusive) [N]? e

MAC list parameter set.

For the change to take effect, restart or commit the change using
  't 5' : 'SET MAC-LIST'.
```

**Local MAC list exclusivity**

Indica si la lista de MAC local es de tipo exclusive (representa que se puede acceder a todas las direcciones MAC a través de este DLSw) o de tipo no exclusive (representa que se puede acceder a un grupo de direcciones MAC a través de este DLSw).

**maximum**

Define el número máximo de sesiones DLSw a las que puede dar soporte el protocolo DLSw. Esto incluye sesiones SNA y NetBIOS (circuitos).

**Ejemplo: `set maximum`**

```
Maximum number of DLSw sessions (1-60000) [1000]?
```

**memory** Le permite especificar la cantidad máxima de memoria disponible para DLSw y la cantidad de memoria disponible para cada sesión DLSw y para las tramas-UI de NetBIOS. El direccionador utiliza valores de trama-UI y valores por sesión para definir los límites en los que los algoritmos de control de flujo comenzarán/dejarán de aplicar presión de retroceso sobre las fuentes de datos y comenzarán/dejarán de eliminar tráfico de tramas-UI.

El direccionador actualmente no utilizar el valor de asignación DLSw general, así que se puede dejar su valor por omisión. Los mensajes DLS.161 que hacen referencia a los sondeos de transmisión y recepción global (no el sondeo de tramas-UI de NetBIOS) se pueden pasar por alto. En lugar de utilizar estos sondeos lógicos, los algoritmos de ritmo de DLSw utilizan el estado de la memoria física para determinar los tamaños de ventanas a anunciar.

Los valores de asignación de sesiones LLC, SDLC y QLLC ofrecen límites por circuito (par estación final) en la colocación en almacenamiento intermedio de datos que fluyen de dispositivos conectados a LLC, SDLC y QLLC respectivamente a TCP. Cuando el direccionador alcanza estos límites, envía RNR/RR a las estaciones finales adecuadas. El estado de sondeos por sesión se puede consultar mediante el mandato **list dlsw memory** de supervisión de DLSw como parte de la lista de sesiones activas.

**Ejemplo: `set memory`**

```
Number of bytes to allocate for DLSw (at least 2638)[140800]?
Number of bytes to allocate per LLC session [8192]?
Number of bytes to allocate per SDLC session [4096]?
Number of bytes to allocate per QLLC session [4096]?
Number of bytes to allocate for NetBIOS UI-frames [40960]?
```

La asignación de tramas-UI de NetBIOS controla el número de tramas-UI (incluye NetBIOS DATAGRAM, NAME_QUERY, ADD_NAME_QUERY, etc.) que DLSw puede colocar en almacenamiento intermedio en cualquier momento. Cuando se encuentra al límite, DLSw elimina tramas-UI de NetBIOS recibidas, que deben volver a transmitir las estaciones finales que las han originado. Si se define un límite demasiado bajo se pueden producir errores intermitentes de intentos de establecimiento de circuitos NetBIOS. El direccionador notifica una condición de eliminación de trama mediante el mensaje de ELS DLS.161 (que hace referencia al sondeo global de tramas-UI de NetBIOS).

**priority**

Le permite especificar las prioridades de circuito a utilizar para circuitos SNA y circuitos NetBIOS, así como una proporción de tráfico *entre* estas prioridades. Puede utilizar el mandato **set priority** para especificar como prioridad de circuito los valores Critical, High, Medium o Low (en orden descendente, de Critical a Low). El direccionador utiliza los valores de prioridad que asigne para limitar de forma selectiva la longitud de ráfaga de determinados tipos de tráfico que transmite a sus direccionadores contiguos.

Esta función sólo está activa durante periodos de congestión, cuando los mensajes DLSw hacen cola antes de ser enviados a TCP. Por ejemplo, puede asignar al tráfico SNA una prioridad de sesión y de exploración de Critical, lo que corresponde por omisión a un valor de asignación de mensajes de 4. Si luego asigna al tráfico de exploración y de sesión NetBIOS una prioridad de Medium, que corresponde a una asignación de mensajes de 2, el direccionador transmite 4 tramas SNA antes de transmitir 2 tramas NetBIOS. Cuando el direccionador procesa 2 tramas NetBIOS, luego procesa de nuevo 4 tramas SNA, y así sucesivamente. Al asignar ancho de banda utilizando las prioridades asignadas, el direccionador cuenta tramas en lugar de bytes. Además, se negocia una determinada prioridad de circuito con el direccionador contiguo en el momento de activación del circuito; por lo tanto, el direccionador contiguo puede establecer una nueva prioridad de circuito utilizando una política que no sea la basada en los valores de configuración especificados para este direccionador. También puede desear asignar distintas prioridades a su tráfico de exploración y de sesiones SNA y NetBIOS.

También puede utilizar el mandato **set priority** para definir un tamaño máximo de trama para todos los circuitos NetBIOS que pasan a través de este direccionador. Las estaciones finales NetBIOS tienen tendencia a generar tramas con el tamaño mayor posible, lo que hace que una sola trama en un enlace de baja velocidad ocupe dicho enlace durante varios segundos, lo que afecta negativamente al tráfico SNA interactivo. Para reducir este efecto, puede definir un valor menor para el tamaño máximo de trama que el direccionador señala a estaciones finales NetBIOS utilizando mecanismos estándares de conexión por puente de

rutas de origen. Si ha conectado por puente de forma transparente (TB) segmentos en la red que ejecutan NetBIOS, defina como tamaño máximo de trama NetBIOS un valor mínimo de 1470.

**Ejemplo: `set priority`**

```
Default priority for SNA DLSw session traffic (C/H/M/L) [M]?
Default priority for NetBIOS DLSw session traffic (C/H/M/L) [M]?
Default priority for SNA DLSw explorer traffic (C/H/M/L) [M]?
Default priority for NetBIOS DLSw explorer traffic (C/H/M/L) [M]?
Message allocation by C/H/M/L priority (4 digits) [4/3/2/1]?
Maximum NetBIOS frame size (516, 1470, 2052, or 4399) [2052]? 516
```

**qllc** Le permite especificar un rango de direcciones MAC asignadas de forma dinámica que se utilizan como dirección MAC de origen para llamadas QLLC dinámicas de entrada.

Para especificar el rango, especifique una dirección MAC base de “X” para el rango y un número máximo “N” de direcciones dinámicas. DLSw elige direcciones MAC comprendidas entre X y X+(N–1).

**Ejemplo: `set qllc`**

```
QLLC base MAC address [40514C430000]?
Maximum QLLC dynamic addresses (0-max sess) [64]?
```

**srb** Define el número de segmento de Puente de direccionamiento de origen (SRB) que identifica DLSw en redes en anillo. Especifique el número de segmento como un valor hexadecimal de tres dígitos.

**Ejemplo: `set srb`**

```
Enter segment number hex (1-FFF) [5]?
```

**timers** Define los temporizadores del protocolo DLSw.

**Ejemplo: `set timers`**

```
DLSw config>set timers
Database age timeout (0-10000 secs. Decimal) [1200]? 480
Max wait timer ICANREACH (1-1000 secs. Decimal) [20]?
Wait timer LLC test response (1-1000 secs. Decimal) [15]?
Wait timer SDLC test response (1-1000 secs. Decimal) [15]?
QLLC session retry timer (1-1000 secs. Decimal) [20]?
Group join timer interval (1-60000 secs. Decimal) [900]? 180
Neighbor priority wait timer (0, 1.0-5.0 secs. Decimal) [2.0]?
Neighbor Inactivity Termination Timer (0-255 minutes) [5]?
Time to delay sending test response (0.0-5.0 secs. Decimal) [0.0]?
DLSw timer values have been set.
```

**Database age timeout**
: Especifica el periodo de tiempo que se deben retener las entradas de DLSw no utilizadas. Las entradas de la base de datos correlacionan direcciones MAC de destino con el grupo de similares DLSw que pueden acceder a las mismas.

  Un valor igual a cero indica que las entradas de esta base de datos no deben caducar. Esto puede resultar útil cuando se ejecutan conexiones TCP de direccionadores contiguos sobre interfaces de marcación, pero en general no se recomienda porque desactiva otras funciones de DLSw.

**Max wait timer**
: Especifica el periodo de tiempo que se debe esperar una respuesta ICANREACH correspondiente a un mensaje CANUREACH transmitido anteriormente.

**Wait timer LLC test response**
: Especifica el periodo de tiempo que se debe esperar una respuesta TEST de LLC antes de abandonar.

**Wait timer SDLC test response**
Especifica el periodo de tiempo que se debe esperar una respuesta TEST de SDLC antes de abandonar.

**QLLC session retry timer**
El tiempo que espera el direccionador antes de volver a intentar establecer contacto con una estación QLLC para iniciar una sesión DLSw.

**Group join timer interval**
El periodo de tiempo que el direccionador espera antes de realizar difusiones generales de grupos de mensajes de anuncio de grupo. Esto puede afectar el periodo de tiempo que tardan las funciones DLSw basadas en grupos en recuperarse de un error del direccionador intermedio y puede afectar a la cantidad de actividad general necesaria para que funcione la función de difusión múltiple. Este valor no se utiliza si configura conexiones TCP en lugar de utilizar las características de difusión múltiple IP de DLSw.

**Neighbor priority wait timer**
Periodo de tiempo que se debe esperar durante la exploración antes de seleccionar un direccionador contiguo. Esto permite seleccionar un direccionador contiguo de prioridad más alta aunque no sea el primero en responder con un mensaje ICANREACH.

Un valor igual a cero indica que no se utiliza la característica de prioridad de direccionador contiguo. No habrá información sobre los similares DLSw en antememoria correspondiente a cada dirección MAC. Siempre se envía un mensaje CANUREACH y se utiliza el primer similar DLSw que envía un mensaje ICANREACH (independientemente de su prioridad).

**Inactive neighbor termination timer**
El tiempo que espera DLSw antes de desactivar una conexión TCP pasiva inactiva (cero sesiones).

**Delay sending TEST response**
El periodo de tiempo que se debe esperar, una vez finalizada la exploración de una dirección MAC, antes de enviar la respuesta TEST. Esto resulta útil si hay dos 2210 de DLSw en la misma LAN conectada por puente capaces de alcanzar la misma dirección MAC a través de similares DLSw. Si se prefiere un 2210 de DLSw, la respuesta TEST se puede retrasar en el 2210 menos adecuado.

## Mandatos de supervisión de DLSw

Esta sección describe los mandatos de supervisión de DLSw. Estos mandatos entran en vigor de forma inmediata pero no pasan a formar parte de la configuración de SRAM del direccionador. Por lo tanto, aunque los mandatos de supervisión le permiten realizar cambios en tiempo real en la configuración del direccionador, estos cambios quedan anulados por la configuración de SRAM cuando se vuelve a arrancar el direccionador. La supervisión consiste en las siguientes acciones:

- Supervisión de los protocolos e interfaces de red que actualmente utiliza el direccionador.
- Visualización de mensajes ELS (Sistema de registro cronológico de sucesos) relacionados con el rendimiento y la actividad del direccionador.
- Realización de cambios en tiempo real en la configuración DLSw sin que ello afecte de forma permanente a la configuración de SRAM.

## Cómo acceder al entorno de supervisión de DLSw

Para entrar en el entorno de supervisión de DLSw (proceso GWCON), entre **talk 5** (o **t 5**) en el indicador OPCON (*) y **protocol dls** en el indicador GWCON (+), tal como se muestra en el siguiente ejemplo:

```
MOS Operator Console

For help using the Command Line Interface, press ESCAPE, then '?'

* talk 5
+ protocol dls
DLS>
```

## Mandatos de supervisión de DLSw

Esta sección describe los mandatos de supervisión de DLSw que aparecen en la Tabla 37. Utilice estos mandatos para obtener información de la base de datos.

*Tabla 37 (Página 1 de 2). Resumen de mandatos de supervisión de DLSw*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Add | Añade de forma dinámica una estación de enlace SDLC, una dirección IP de direccionador contiguo TCP, una estación o destino QLLC, entradas de la antememoria, entradas de la lista de direcciones MAC, modificaciones de la prioridad de circuito o modificaciones de exploración de la antememoria MAC de la configuración actual. |
| BAN | Le permite acceder al indicador de consola del Nodo límite de acceso (BAN) para entrar mandatos específicos de la consola BAN. Consulte el tema “Utilización de la característica Nodo límite de acceso (BAN)” en la página 63 para obtener más información. |
| Close-Sap | Cierra de forma dinámica un SAP LLC actualmente abierto. Las interfaces LLC utilizan SAP para establecer comunicación en la red. |
| Delete | Elimina de forma dinámica una estación de enlace SDLC, una sesión DLSw, una dirección IP de direccionador contiguo TCP, una estación o destino QLLC, entradas de la antememoria, entradas de la lista de direcciones MAC, modificaciones de la prioridad de circuito y modificaciones de exploración de la antememoria MAC. |
| Disable | Desactiva de forma dinámica la función de conmutación de LLC, una estación de enlace SDLC, direccionadores contiguos dinámicos, una interfaz o estación QLLC o el uso de listas de direcciones MAC locales y remotas. |
| Enable | Activa de forma dinámica la función de conmutación de LLC, una estación de enlace SDLC, direccionadores contiguos dinámicos, una interfaz o estación QLLC o el uso de listas de direcciones MAC locales y remotas. |

| Tabla 37 (Página 2 de 2). Resumen de mandatos de supervisión de DLSw | |
|---|---|
| Mandato | Función |
| Join-Group | Añade de forma dinámica el direccionador a un grupo DLSw distinto del de la configuración de SRAM. |
| Leave-Group | Elimina de forma dinámica el direccionador del grupo DLSw especificado. |
| List | Muestra información correspondiente a estaciones de enlace SDLC, SAP, prioridad de circuito, grupos DLSw, sesiones DLSw, sesiones para destinos, estaciones e interfaces QLLC, entradas de la antememoria o entradas de la lista de direcciones MAC. El mandato también ofrece información detallada sobre conexiones y funciones TCP. |
| NetBIOS | Ofrece acceso al indicador de soporte de NetBIOS. |
| Open-SAP | Abre de forma dinámica un SAP LLC. |
| Set | Cambia de forma dinámica los parámetros de LLC2, el número máximo de sesiones DLSw, asignación de memoria, temporizadores de protocolos, prioridad de circuito, parámetros de direccionadores contiguos dinámicos, parámetros correspondientes al funcionamiento de QLLC o parámetros relacionados con la lista de direcciones MAC. |
| Test | Compara determinadas direcciones MAC con la antememoria actual de direcciones MAC y las listas de direcciones MAC. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Add

Utilice el mandato **add** para configurar de forma dinámica una estación de enlace SDLC, una dirección IP de direccionador contiguo TCP, una estación o destino QLLC, entradas de la antememoria, entradas de la lista de direcciones MAC, modificaciones de prioridad de circuito y modificaciones de exploración de antememoria MAC sin que ello afecte a la configuración de SRAM.

**Sintaxis:**

| | |
|---|---|
| a**dd** | cache-entry<br>explorer-override<br>mac-list<br>priority<br>qllc...<br>sdlc<br>tcp |

Para ver ejemplos y descripciones de los campos, consulte el mandato **add** en el capítulo sobre configuración del tema “Add” en la página 569.

## BAN

Utilice el mandato **ban** para acceder al indicador de supervisión de BAN (Nodo límite de acceso). Entre el mandato **ban** en el indicador DLS>.

**Sintaxis:**

b**an**

Una vez haya accedido al indicador de supervisión de BAN, puede empezar a entrar mandatos específicos de supervisión. Consulte el tema “Utilización de la característica Nodo límite de acceso (BAN)” en la página 63 para ver una explicación de los mandatos de supervisión de BAN.

Para volver al indicador DLSw> en cualquier momento, entre el mandato **exit**.

## Close-SAP

Utilice el mandato **close-sap** para desactivar de forma dinámica el uso que hace DLSw del SAP especificado sin que ello afecte a la configuración de SRAM de DLSw.

**Sintaxis:**

c**lose-sap**

**Ejemplo: `close-sap`**

```
Interface #[1]?
Enter SAP in hex (range 0-FE), or one of the following:
  'SNA', 'NB', or LNM [0]? 04
SAP(s) 4 closed on interface 1
```

(Encontrará una explicación de los parámetros de **close-sap** en la página 579.)

## Delete

Utilice el mandato **delete** para eliminar de forma dinámica una estación de enlace SDLC, una sesión DLSw una dirección IP de direccionador contiguo TCP, una estación o destino QLLC, entradas de la antememoria, entradas de la lista de direcciones MAC, modificaciones de prioridad de circuito o modificaciones de exploración de la antememoria MAC sin que ello afecte a la configuración de SRAM de DLSw. Este mandato también interrumpe cualquier sesión existente.

**Sintaxis:**

**delete**
- cache-entry
- dls
- explorer-override
- mac-list
- priority
- qllc...
- sdlc
- tcp

**cache-entry**

Suprime la entrada especificada de la antememoria

**Ejemplo: `delete cache-entry`**

```
Enter MAC Address [400000000000]? 10005a123456
MAC 10005A123456 / IP address 128.185.122.234 configured cache entry deleted.
```

**dls** Elimina una sesión DLSw actualmente activa.

**Ejemplo: `delete dls`**

```
Session identifier [1]?
```

**explorer-override**

Elimina la entrada especificada de modificación de exploración de la antememoria MAC.

### Ejemplo: delete explorer-override

```
Enter explorer override record number [1]?
Explorer override record has been deleted.
```

**mac-list** Suprime la entrada especificada de la lista de direcciones MAC.

### Ejemplo: `delete mac-list`

```
Enter mac list record number [1]?

Local MAC list entry 10005A000000 / FFFFFF000000 has been deleted.
```

**priority** Suprime la entrada especificada de modificación de prioridad de circuito.

### Ejemplo: `delete priority`

```
Enter circuit priority override record number [1]?
Circuit priority override record has been deleted.
```

**qllc** Elimina el soporte de una estación o destino QLLC. Si suprime una estación que está activa actualmente, DLSw comprueba que realmente desea desactivar la conexión antes de hacerlo. La supresión de un destino no afecta a las conexiones existentes.

### Sintaxis:

**qllc** destination
station

### Ejemplo: `del q destination`

```
Enter the connection id (1-8 alphanumeric chars) [ ]? conn1
QLLC Destination record deleted
```

### Example: `del q station`

```
Interface # [0]? 2
PVC or SVC [PVC]?
Logical channel number (1-4095) [0]? 4
QLLC station record deleted
```

**sdlc** Cierra el enlace SDLC actualmente activo sin que ello afecte a la información de configuración de la estación de enlace SDLC.

### Ejemplo: `delete sdlc`

```
Interface #[0]? 1
SDLC Address or 'sw' (switched dial-in) [C1]?
Link closed
```

**Interface #**
El número de interfaz del direccionador que se conecta a la estación de enlace SDLC.

**SDLC Address**
La dirección SDLC de la estación de enlace remota que está suprimiendo, comprendida entre 01 y FE o “sw” para un circuito conmutado de entrada de llamadas SDLC.

**tcp** Elimina la dirección IP (*dirección_ip*) del similar DLSw con el que se ha efectuado la conexión TCP. La conexión TCP se cierra.

### Ejemplo: `delete tcp`

```
IP Address [0.0.0.0]? 128.185.14.1
```

## Disable

Utilice el mandato **disable** para desactivar de forma dinámica la función de desconexión de LLC, el protocolo DLSw, una estación de enlace SDLC, direccionadores contiguos dinámicos, una interfaz o estación QLLC o el uso de listas de direcciones MAC locales o remotas sin que ello afecte a la configuración de DRAM de DLSw. No se da soporte a la desactivación de la función DLSw ***entera*** desde el indicador de supervisión.

**Sintaxis:**

| | |
|---|---|
| di**sable** | dynamic-neighbors<br>llc<br>mac-list<br>qllc...<br>sdlc |

(Encontrará ejemplos sobre la utilización de los parámetros del mandato **disable** en la página 582.)

## Enable

Utilice el mandato **enable** para activar de forma dinámica la función de desconexión de LLC, una estación de enlace SDLC, direccionadores contiguos dinámicos, una interfaz o estación QLLC o el uso de listas de direcciones locales y remotas sin que ello afecte a la configuración de SRAM de DLSw.

**Sintaxis:**

| | |
|---|---|
| en**able** | dynamic-neighbors<br>llc<br>mac-list<br>qllc...<br>sdlc |

(Encontrará ejemplos sobre la utilización de los parámetros del mandato **enable** en la página 583.)

## Join-Group

Utilice el mandato **join-group** para hacer que DLSw comience el descubrimiento de direccionadores contiguos, la exploración de difusiones múltiples y las funciones de reenvío de tramas de difusión múltiple.

Para encontrar información adicional y un ejemplo, consulte el tema “Utilización de DLSw” en la página 525.

**Sintaxis:**

jo**in-group**

## Leave-Group

Utilice el mandato **leave-group** para que DLSw deje de realizar funciones de descubrimiento de direccionadores contiguos, exploración de difusión múltiple y reenvío de tramas de difusión múltiple en el grupo especificado o utilizando la dirección de difusión múltiple especificada. Este cambio ser realiza sin que afecte a la configuración de SRAM de DLSw. **Leave-group** interrumpe las conexiones TCP existentes activadas bajo el grupo o dirección de difusión múltiple especificados. Para encontrar información adicional y un ejemplo, consulte el tema “Utilización de DLSw” en la página 525.

**Sintaxis:**

le**ave-group**

**Ejemplo:**

```
Configure group member (G) or specific multicast address (M) -  [G]?
Group ID (1-64 Decimal) [1]? 2
```

## List

Utilice el mandato **list** para visualizar información de DLSw sobre estaciones de enlace SDLC, prioridad de circuito, SAP, direccionadores contiguos TCP, grupos, direccionadores contiguos dinámicos, estaciones, destinos e interfaces QLLC, entradas configuradas de la antememoria, entradas de la lista de direcciones MAC y modificaciones de exploración de la antememoria MAC.

**Sintaxis:**

li**st** dls...
explorer-override
groups...
llc2...
mac-list
priority...
qllc...
sdlc...
tcp...
timers

**dls** Muestra información perteneciente al protocolo DLSw. Las opciones (global, memory, sessions y cache) correspondientes a los parámetros de DLSw se describen a continuación y en las páginas siguientes.

**Global** Muestra los valores operativos de los parámetros generales configurados de DLSw.

**Memory** Muestra información sobre la memoria DLS configurada y el uso actual de la memoria.

**Sessions** Muestra información actual sobre sesiones DLS que incluye origen, destino, estado, indicadores, dirección IP de destino e ID de sesión.

**cache** Lista las direcciones de la antememoria de direcciones MAC de DLSw.

**dls global**

Muestra información global de parámetros de DLS.

**Ejemplo: `list dls global`**

```
DLSw is                                ENABLED
LLC2 send Disconnect is                ENABLED
Dynamic Neighbors is                   ENABLED
SRB Segment number                     020
MAC <-> IP mapping cache size          128
Max DLSw sessions                      1000
DLSw global memory allotment           141312
LLC per-session memory allotment       8192
SDLC per-session memory allotment      4096
QLLC per-session memory allotment      4096
NetBIOS UI-frame memory allotment      40960
Dynamic Neighbor Transmit Buffer Size  5120
Dynamic Neighbor Receive Buffer Size   5120
Dynamic Neighbor Maximum Segment Size  1024
Dynamic Neighbor Keep Alive            DISABLED
Dynamic Neighbor SessionAlive Spoofing DISABLED
Dynamic Neighbor Priority              MEDIUM
QLLC base source MAC address           40514C430000
QLLC maximum dynamic addresses         64
Type of local MAC list                 NON-EXCLUSIVE
Use of local MAC list is               ENABLED
Use of remote MAC list is              ENABLED
SNA explorer limit                     100
NetBIOS explorer limit                 100
```

**DLSw is** Estado del protocolo DLSw, cuyos valores pueden ser enabled o disabled.

**LLC2 send disconnect is**
Estado de evitar que el direccionador interrumpa una conexión LLC2 tras la pérdida de la conexión TCP. Los valores válidos son enabled o disabled.

**Dynamic Neighbors**
Indica si DLSw acepta intentos de conexiones TCP de entrada procedentes de direcciones DLSw que no están configurados (es decir, mediante el mandato **add tcp**).

**SRB Segment number**
El segmento SRB que identifica DLSw en el RIF.

**MAC<->IP mapping cache size**
Especifica el tamaño de la antememoria de correlación MAC-IP.

**Max DLSw Sessions**
El número máximo de sesiones DLSw a las que el protocolo DLSw puede dar soporte (tanto sesiones SNA como NetBIOS).

**DLSw global memory allotment**
La cantidad máxima de memoria que puede utilizar DLSw.

**LLC per-session memory allotment**
La cantidad máxima de memoria que pueden utilizar las sesiones DLSw de LLC.

**SDLC per-session memory allotment**
La cantidad máxima de memoria que puede utilizar cada sesión DLSw de SDLC.

**QLLC per-session memory allotment**
La cantidad máxima de memoria que puede utilizar cada sesión DLSw de QLLC.

**NetBIOS UI-frame memory allotment**
La cantidad máxima de memoria que pueden utilizar todas las tramas-UI de NetBIOS que reenvía DLSw.

**Dynamic Neighbor Transmit Buffer Size**
El tamaño del almacenamiento intermedio de transmisión TCP para conexiones TCP dinámicas.

**Dynamic Neighbor Receive Buffer Size**
El tamaño del almacenamiento intermedio de recepción TCP para conexiones TCP dinámicas.

**Dynamic Neighbor Maximum Segment Size**
El tamaño máximo de segmento TCP para conexiones TCP dinámicas.

**Dynamic Neighbor Keep Alive**
Si se van a enviar o no mensajes Keep alive de TCP en la nuevas conexiones TCP dinámicas.

**Dynamic Neighbor NetBIOS SessionAlive Spoofing**
Si se van a reenviar o no tramas-I SessionAlive de NetBIOS a los similares DLSw establecidos en nuevas conexiones TCP dinámicas.

**Dynamic Neighbor Priority**
La prioridad de direccionador contiguo a utilizar para todas las nuevas conexiones TCP dinámicas.

**QLLC base source MAC address**
La dirección MAC más baja del rango utilizado como direcciones MAC de origen para llamadas dinámicas de entrada QLLC (SVC).

**QLLC maximum dynamic addresses**
El número máximo de direcciones MAC dinámicas de origen que se pueden utilizar en cualquier momento para llamadas dinámicas QLLC de entrada.

**dls sessions all**
Muestra información sobre las sesiones dls actuales.

**Ejemplo: `list dls session all`**

```
      Source           Destination        State       Flags  Dest. IP Addr   Id
  1. 400000000003 04  500000000003 04   Connected           128.185.236.51   2
```

**Source** La dirección MAC de origen y SAP de la sesión. Para sesiones con un origen SDLC, QLLC o APPN, la dirección MAC se sustituye por las siguientes series de caracteres de modo que se pueda identificar fácilmente dichas sesiones:

```
DLC Type        Characters      Content
  SDLC            1-5           "SDLC "
                  6-7           Interface number
                  8             "-"
                  9-10          SDLC station address
                  11-12         "  "
  QLLC            1-5           "QLLC "
                  6-7           Interface number
                  8             "P" for PVC, or "S" for SVC
                  9-12          LCN for PVC, or last 4 bytes of
                                     DTE address for SVC
  APPN            1-4           "APPN"
                  5-12          "        "
```

**Destination**
La dirección MAC de destino de la sesión.

**State** El estado de la sesión. Se pueden visualizar los siguientes estados:

**DISCONECT**
Indica el estado inicial sin ningún circuito ni conexión establecidos.

**RSLV_PEND**
Indica que el DLSw de destino está esperando una indicación SSP_STARTED o va después de una petición SSP_START.

**CIRC_PEND**
Indica que el DLSw de destino está esperando una respuesta SSP_REACHACK a un mensaje SSP_ICANREACH.

**CIRC_EST**
Indica que se ha establecido el circuito de extremo a extremo.

**CIR_RSTRT**
Indica que el DLSw que ha originado el restablecimiento está esperando que se vuelva a arrancar el enlace de datos y una respuesta SSP_RESTARTED a un mensaje SSP_RESTART.

**CONN_PEND**
Indica que el DLSw de origen está esperando una respuesta SSP_CONTACTED a un mensaje SSP_CONTACT.

**CONT_PEND**
Indica que el DLSw de destino está esperando una confirmación SSP_CONTACTED a un mensaje SSP_CONTACT.

**CONNECTED**
Indica que el circuito está completamente activo para la transferencia de datos orientada a conexión.

**DISC_PEND**
Indica que el DLSw que ha originado la desconexión está esperando una respuesta SSP_HALTED a un mensaje SSP_HALT.

**HALT_PEND**
Indica que el DLSw remoto está esperando una indicación SSP_HALTED después de una petición SSP_HALT.

**REST_PEND**
Indica que el DLSw local ha recibido un RESTART_DL pero aún no ha devuelto un DL_RESTARTED.

**CIRC_STRT**
Indica que el DLSw local ha enviado un CANUREACH_cs pero aún no ha recibido un ICANREACH_cs.

**HLT_NOACK**
Indica que el DLSw local ha recibido un HALT_DL_NOACK pero aún no ha terminado de cerrar la estación de enlace.

**Flags** Los distintivos pueden ser uno de los siguientes:

A - MENSAJE DE CONTACTO PENDIENTE

B - RESOLUCIÓN DE SAP PENDIENTE

C - SE ESPERA SALIDA OCUPADA

D - TCP OCUPADO

E - SUPRESIÓN PENDIENTE

F - CIRCUITO INACTIVO

**Dest. IP Addr**
La dirección IP del similar DLSw remoto.

**Id** El número utilizado para identificar la sesión. Utilice este número en cualquier mandato que necesite el ID de sesión.

**dls sessions appn**
Muestra información sobre sesiones dls que tienen APPN en este direccionador como punto final.

**Ejemplo: `list dls sess appn`**

```
Source            Destination      State      Flags    Dest IP Addr    Id
--------------    --------------   ---------  -------  --------------  ----
1 APPN         04  400000000011 04  CONNECTED          187.7.239.11    0
2 APPN         04  400000000014 04  CONNECTED          142.7.245.14    1
```

**dls sessions ban**
Muestra información actual sobre sesiones BAN

**Ejemplo: `list dls session ban`**

```
BAN port number (user 0 for all ports) [0]?
No active sessions
```

**dls sessions dest**
Muestra información sobre sesiones dls por dirección MAC de destino.

**Ejemplo: `list dls session dest`**

```
Destination MAC Address [40000000001]? 50000000003

Source              Destination       State       Flags  Dest. IP Addr  Id
1. 400000000003 04  500000000003 04   Connected          128.185.236.51  2
2. 400000000002 04  500000000003 04   Connected          128.185.236.52  3
```

**dls sessions detail**
Muestra información detallada sobre sesiones dls.

**Ejemplo: `list dls session detail`**

```
                    Session Identifier [1]?

Source           Destination         State       Dest. IP Addr    Id
1. 400000000003 04  500000000003 04     Connected   128.185.236.512  2

                     Personality:      TARGET
                     XIDs sent:        2
                     XIDs rcvd:        0
                     Datagrams sent:   0
                     Datagrams rcvd:   0
                     Info frames sent: 15
                     Info frames rcvd: 0
                     RIF:              0620 0202 B0B 0
                     Local CID:        0136AF74:7E000021
                     Remote CID:       014AB030:7E000003
                     Priority:         MEDIUM
```

**Personality**
El ORIGEN (iniciador) o DESTINO (receptor) de la conexión.

**XIDs sent XIDs rcvd**
El número total de XID que este similar DLSw ha enviado y ha recibido del similar DLSw remoto.

**Datagrams sent Datagrams rcvd**
El número total de datagramas que este similar DLSw ha enviado y recibido del similar DLSw remoto.

**Info frames sent Info frames rcvd**
El número de tramas-I que este similar DLSw ha enviado y recibido del similar DLSw remoto.

**RIF** La información que se incluye en el RIF de la trama de prueba de LLC.

**Local CID**
El ID de circuito DLSw asignado por este direccionador.

**Remote CID**
El ID de circuito DLSw asignado por el direccionador contiguo.

**Priority** La prioridad de circuito DLSw establecida para este circuito cuando se inició.

**dls sessions ip**
Muestra sesiones dls con un determinado direccionador contiguo conectado a TCP.

**Ejemplo: `list dls session ip`**

```
Enter the DLS neighbor IP address [0.0.0.0]? 128.185.236.512

      Source        Destination      State      Dest. IP Addr     Id
1. 400000000003 04  500000000003 04  Connected  128.185.236.512   2
```

**dls sessions nb**
Lista información sobre los circuitos actualmente activos que dan soporte a NetBIOS.

**Ejemplo: `list dls sessions nb`**

```
      Source        Destination      State      Dest. IP Addr     Id
1. 400000000003 F0  500000000003 F0  Connected  128.185.236.512   2
```

**dls sessions range**
El rango de sesiones dls que desea visualizara. Este número se encuentra a la izquierda de la dirección MAC de origen.

**Ejemplo: `list dls session range`**

```
Start [1]?
Stop  [1]?

   Source           Destination      State       Dest.  IP Addr    Id
1. 400000000003 04  500000000003 04  Connected   128.185.236.512   2
```

**dls sessions src**
Muestra toda la información sobre sesiones dls por dirección MAC de origen.

**Ejemplo: `list dls session src`**

```
        Source MAC Address [400000000001]?

   Source        Destination      State       Flags Dest. IP Addr  Id
1. SDLC 04   400000000002 04      Connected     10.1.49.401        1
```

**Nota:** En este ejemplo, la dirección MAC de origen 400000000001 se correlaciona con el nombre “SDLC 04”. Si no sabe la dirección MAC de origen necesaria como parámetro de este mandato, entre el mandato **list SDLC config all** para obtener esta información.

### dls sessions state

Muestra todas las sesiones dls con un determinado estado.

**Ejemplo: `list dls session state`**

```
        DISCONECT = 0,  RSLV_PEND = 1
        CIRC_PEND = 2,  CIRC_EST  = 3
        CIR_RSTRT = 4,  CONN_PEND = 5
        CONT_PEND = 6,  CONNECTED = 7
        DISC_PEND = 8,  HALT_PEND = 9
        REST_PEND = 10  WT_HALTNA = 11
        CIRC_STRT = 12  HLT_NOACK = 13

        Enter state value (0-10) [7]?

    Source            Destination      State       Flags  Dest. IP Addr Id
1. 400000000003 04  10005AF181A4 04  Connected          128.185.236.84  0
2. 400000000002 04  400000000088 04  Connected          128.185.236.84  1
```

### list dls cache all

El mandato **list dls cache all** lista las entradas de la antememoria de direcciones MAC de DLSw. Esta antememoria contiene una base de datos de las conversiones de dirección MAC a direccionador contiguo IP más recientes. Ofrece la dirección MAC, el tiempo de permanencia (en segundos) en la antememoria y la dirección IP del direccionador.

**Ejemplo: `list dls cache all`**

```
    Mac Address   Entry Type  Secs to live      IP Address(es)   LFSize
1.  10005A123456  PERMANENT   (not being timed) 128.185.236.84   0
2.  10005A789ABC  STATIC      (not being timed) 128.185.236.84   0
3.  10005AF1809B  DYNAMIC        810            128.185.236.84   2052
4.  10005AF181A4  DYNAMIC        1170           128.185.236.84   2052
5.  400000000088  DYNAMIC        1170           128.185.236.84   2052
```

### dls cache config

Muestra entradas configuradas de la antememoria MAC de DLSw.

**Ejemplo: `list dls cache config`**

```
Mac Address   IP Address       Source     Last Mod
------------  ---------------  ---------  ---------
10005A123456  128.185.236.84   PERMANENT  UNCHANGED
10005A789ABC  128.185.236.84   STATIC     ADDED
```

### list dls cache range

Muestra información correspondiente a un determinado rango de entradas de la antememoria.

**Ejemplo: `list dls cache range`**

```
Start [1]?
Stop ]1]? 20
       Mac Address   Entry Type  Secs to live      IP Address(es)   LFSize
   1.  10005A123456  PERMANENT   (not being timed) 128.185.236.84   0
   2.  10005A789ABC  STATIC      (not being timed) 128.185.236.84   0
   3.  10005AF1809B  DYNAMIC        810            128.185.236.84   2052
   4.  10005AF181A4  DYNAMIC        1170           128.185.236.84   2052
   5.  400000000088  DYNAMIC        1170           128.185.236.84   2052
```

### dls memory

Este mandato lista todas las sesiones DLSw existentes y la cantidad de memoria que utiliza cada sesión.

**Ejemplo: `list dls memory`**

```
Total DLSw bytes requested:             153600
Global receive pool bytes granted:       92160
 Currently in use:                          0
Global transmit pool bytes granted:      61440
 Currently in use:                         232

NetBIOS UI-frame pool total bytes:       40960
 Currently in use:                          0


                                      Session    Initial  Current  Congest  DLC Xmits
Id Source            Destination        State      alloc   alloc    State     Queued
5. SDLC 04C1     04  400000000003  04  Connected   16384   16384    READY       0
6. 400000000003  04  0000c9001119  04  Connected   16384   16384    READY       0
```

El campo “Currently in use” muestra la cantidad total de memoria actualmente asignada por DLS. Esto incluye todas las asignaciones de sesiones y los mensajes de control.

El campo “Congest State” contiene información sobre el control de flujo y puede tener los siguientes valores:

**Ready** Indica que la sesión no está congestionada.

**Session** Indica que la sesión ha utilizado la mayoría de sus asignaciones de sesiones y probablemente tiene flujo controlado por el enlace de datos.

**Global** Indica que la sesión está congestionada debido a falta de memoria en el direccionador.

**Ses/gbl** Indica que la sesión está congestionada debido a una combinación de falta de memoria global y de sesiones.

El campo “DLC Xmits Queued” muestra el número total de tramas en cola para ser transmitidas en DLS a LLC o SDLC, más el número en cola dentro de DLC en espera de acuse de recibo de la estación final conectada.

**explorer-override**

Lista las modificaciones configuradas de exploración de la antememoria MAC.

**Ejemplo: list explorer-override**

```
    Explorer      Explorer      DB Age    Wait ICR  Nbr Pri   TESTrsp  Forwarding
ID  MAC Value     MAC Mask      Timeout   Timeout   Timeout   Delay    Explorers
--  ------------  ------------  --------  --------  --------  -------  ---------
 1  400031740000  FFFFFFFF0000  DISABLED    20      DISABLED  0.0      AllPartners
 2  10005A000000  FFFFFF000000   1200       20      2.0       0.0      NoPartner
```

**mac-list all**

Muestra todas las entradas de la lista de direcciones MAC locales y remotas.

**Ejemplo: `list mac-list all`**

```
MAC Value     MAC Mask      IP Address
------------  ------------  ---------------
10005AF17F23  FFFFFFFFFFFF  Local
10005AF1809B  FFFFFFFFFFFF  128.185.236.84
4000189E2000  FFFFFFFFF000  128.185.236.84
4000189E3000  FFFFFFFFF000  Local
```

**mac-list config**

Muestra todas las entradas de la lista de direcciones MAC configuradas de forma local.

**Ejemplo: `list mac-list config`**

```
Entry  Mac Value     MAC Mask      Source     Last Mod
-----  ------------  ------------  ---------  ---------
    1  10005AF17F23  FFFFFFFFFFFF  STATIC     UNCHANGED
    2  4000189E3000  FFFFFFFFF000  STATIC     UNCHANGED
```

**mac-list local**

Muestra todas las entradas activas de la lista de direcciones MAC local.

**Ejemplo: `list mac-list local`**

```
LOCAL MAC List
Type of MAC List (active) ....... EXCLUSIVE
Type of MAC List (pending) ...... EXCLUSIVE


MAC Value     MAC Mask
------------  ------------
10005AF17F23  FFFFFFFFFFFF
4000189E3000  FFFFFFFFF000
```

**mac-list remote**

Muestra TODAS las entradas activas de la lista de direcciones MAC remotas correspondientes a un determinado similar DLSw.

**Ejemplo: `list mac-list remote`**

```
Enter the DLSw neighbor IP Address [0.0.0.0]? 128.185.236.84
 Partner IP Address .............. 128.185.236.84
Type of MAC List ................ EXCLUSIVE
Use of remote MAC lists ......... ENABLED


MAC Value     MAC Mask
------------  ------------
10005AF1809B  FFFFFFFFFFFF
4000189E2000  FFFFFFFFF000
```

**groups config**

Muestra información de grupo correspondiente a este similar DLSw que se ha configurado con el mandato **join-group**.

**Ejemplo: `list groups config`**

```
   Group#                     Xmit    Rcv     Max     Keep-    SesAlive
Mcast IP Addr   Role      CST Bufsize Bufsize Segsize Alive    Spoofing Priority
--------------- --------- --- ------- ------- ------- -------- -------- --------
224.0.10.0      READWRITE  p    5120    5120    1024  DISABLED DISABLED MEDIUM
Group  2        PEER       p    5120    5120    1024  DISABLED DISABLED MEDIUM
```

**Group # / Mcast IP Addr**

Para grupos cliente/servidor/similar, el número del grupo. Para grupos DLSw Versión 2, la dirección de difusión múltiple de la que debe leer o en la que debe grabar.

**Role** Para grupos de cliente/servidor/similar, el papel que asumirá este direccionador dentro del grupo, según su configuración. Para grupos DLSw Versión 2, el papel de lectura/grabación de la dirección de difusión múltiple configurada; los valores posibles son read-only, write-only o read-write.

**CST** El tipo de configuración de conectividad que utilizará este direccionador, según su configuración, dentro del grupo; los valores posibles son Active (a) o Passive (p).

**Xmit Bufsize**

El tamaño del almacenamiento intermedio de transmisión de paquetes, comprendido entre 1024 y 32768. El valor por omisión es 5120.

**Rcv Bufsize**
El tamaño del almacenamiento intermedio de recepción de paquetes, comprendido entre 1024 y 32768. El valor por omisión es 5120.

**Max Segsize**
El tamaño máximo del segmento TCP, comprendido entre 64 y 16384. El valor por omisión es 1024.

**Keepalive**
Muestra el estado de la función Keepalive, cuyos valores pueden ser enabled o disabled.

**SesAlive Spoofing**
Muestra el estado de la función de simulación SessionAlive de NetBIOS, cuyos valores posibles son enabled o disabled.

**Priority** Muestra la prioridad del direccionador contiguo en el proceso de selección. La prioridad del direccionador contiguo puede ser High, Medium o Low.

**groups statistics**
Muestra estadísticas sobre el uso de grupos DLSw para el tráfico de exploración desde la última vez que se volvió a arrancar el direccionador o desde que se creó el grupo.

**Ejemplo: `list groups stat`**

```
Group number    Data pkts   Data Bytes   Ctrl pkts   CURex pkts   NQex pkts
    or              Sent         Sent        Sent         Sent        Sent
Multicast IP@       Rcvd         Rcvd        Rcvd         Rcvd        Rcvd
-------------   ---------   ---------   ----------   ----------   ---------
Group 1                 0           0          116           24          10
                        0           0           25           10           2
224.0.10.0              0           0          224           33           0
                        0           0           21            8           0
```

**llc2 open**
Muestra información correspondiente a todos los SAP abiertos actualmente en interfaces entre similares LLC2.

**Ejemplo: `list llc2 open`**

```
Interface   SAP(s)
    0        0  4
    1        0  4  8  C
```

**llc2 SAP parameters**
Muestra información sobre la configuración de parámetros de LLC2. Sólo se mostrarán las configuraciones que se han modificado. Si no se ha utilizado el mandato **set llc2**, no se generará ninguna salida.

**Ejemplo: `list llc2 sap parameters`**

```
SAP             t1    t2    ti    n2    n3    tw    rw    nw    acc
---             --    --    --    --    --    --    --    --    ---
 0               1     1    30     8     1     2     2     1     0
```

**llc2 sessions all**
Muestra información actual sobre todas las sesiones LLC2.

**Ejemplo: `list llc2 sessions all`**

```
   SAP   Int.   Remote Addr    Local Addr    State      RIF
1. 04    6     400000000003   500000000003  CONTACTED  0620 0202 B0B0
```

**State** El estado de la sesión llc. Se pueden visualizar los siguientes estados:

**DISCONNECTED**

Indica que la estructura de control de enlace de datos existe pero no se ha establecido ningún enlace de datos.

**CONNECT_PEND**

Se entra en el estado de pendiente de conexión cuando se recibe una trama de mandato TEST en un SAP NULL o cuando se recibe un mandato DLC_START_DL procedente del DLS.

**RESOLVE_PEND**

Se entra en el estado de pendiente de resolución cuando se ha enviado un mandato DLC_RESOLVE_C a DLS.

**CONNECTED**

Este es el estado fijo en el que los servicios de nivel LLC Tipo 1 están disponibles a través de la nube de DLS. Se entra en este estado cuando se recibe un mandato DLC_RESOLVE_R procedente de DLS o cuando se recibe una trama de respuesta TEST procedente de la red.

**CONTACT_PEND**

Se entra en este estado siempre que hay pendiente una respuesta a un SABME transmitido o recibido.

**CONTACTED**

Este es el estado fijo en el que se entra cuando se ha recibido una respuesta UA correspondiente a un SABME transmitido o se ha transmitido un UA previamente correspondiente a un SABME recibido. En este estado, se intercambian tramas de información LLC2 sobre la nube de DLS.

**DISCONNECT_PENDING**

Se entra en este estado cuando se ha transmitido o recibido un mandato DISC o cuando se ha recibido un DLC_HALT procedente de DLS.

**llc2 sessions ban**

Muestra información actual correspondiente a sesiones LLC2 que intervienen en la función BAN.

**llc2 sessions nb**

Muestra información actual correspondiente a sesiones LLC2 que transportan tráfico del protocolo NetBIOS.

**llc2 sessions range**

Muestra información actual correspondiente al rango seleccionado de sesiones LLC2.

**Ejemplo: `list llc2 sessions range`**

```
Start[1]?
Stop[1]?
              SAP   Int.   Remote Addr   Local Addr    State      RIF
            1. 04    6     400000000003  500000000003  Contacted  0620 0202 B0B0
```

**priority** Muestra información sobre la prioridad de circuito DLSw.

**Ejemplo: `list priority`**

```
Default priority for SNA DLSw session traffic is          HIGH
Default priority for NetBIOS DLSw session traffic is      MEDIUM
Default priority for SNA DLSw explorer traffic is         MEDIUM
Default priority for NetBIOS DLSw explorer traffic is     LOW

Message allocation by C/H/M/L priority is   4/3/2/1
Maximum frame size for NetBIOS is           516

    Source/  SAP      MAC Address                  Session   Explorer
ID  Dest     Range    Range                        Priority  Priority
--  -------  -------  ---------------------------  --------  --------
 1  Source:  00 - FE  000000000000 - FFFFFFFFFFFF  CRITICAL  MEDIUM
    Dest  :  00 - 0C  10005A000000 - 10005AFFFFFF
 2  Source:  04 - 04  400031740000 - 40003174FFFF  CRITICAL  MEDIUM
    Dest  :  00 - FE  000000000000 - FFFFFFFFFFFF
```

**qllc...** Lista interfaces, destinos o estaciones QLLC que están activados.

**Sintaxis:**

**qllc**
- callin
- destinations
- sessions
- stations

**Ejemplo: `li qllc callin`**

```
Interfaces enabled for incoming QLLC calls to DLSw:
    1
```

**Ejemplo: `li qllc dest`**

```
Connection ID   Dest  SAP/MAC           Hits
  CHICAGO       04   400000112323         0
```

Para ver una descripción de los campos de la pantalla que puede configurar, consulte el mandato **add qllc** en el tema “Utilización de DLSw” en la página 525. El campo *Hits* indica el número de veces que DLSw ha utilizado una coincidencia entre el id de conexión de un paquete Call_Request de QLLC de entrada y este id de conexión.

**Ejemplo: `li qllc sess`**

```
If  P/S  LCN/DTE addr    Source SAP/MAC   Dest SAP/MAC      Type   State
 4  PVC  4               04 400000310401  00 000000000000   PERM   NET_DOWN
 4  SVC  3721111         04 400000310402  00 000000000000   STAT   NET_DOWN
     2 Circuits    1 PVC   1 SVC       1 Permanent   1 Static   0 Dynamic
```

Para ver una descripción de los campos de la pantalla que puede configurar, consulte el mandato **add qllc** en el tema “Utilización de DLSw” en la página 525.

El campo *Type* tiene los siguientes valores:

**PERM (Permanente)**
Esta definición de estación formaba parte de la configuración del direccionador la última vez que se arrancó el direccionador.

**STAT (Estático)**
Esta definición de estación la ha añadido el usuario bajo la función de supervisión de DLSw después de que se arrancara por última vez el direccionador.

**DYNM (Dinámico)**
DLSw ha creado de forma dinámica esta definición de estación como resultado de una llamada de entrada o debido a la necesidad de colocar varias llamadas de salida en una sola dirección DTE remota.

La línea de resumen que aparece en la parte inferior de la lista de sesiones muestra el número de sesiones de cada tipo que existen actualmente.

El campo *State* indica el estado de la conexión DLSw desde un punto de vista de QLLC. Estos estados difieren de los estados de DLS que se visualizan bajo los mandatos **list dls sess** y añaden información sobre lo que pasa en la interfaz QLLC. Los valores posibles son:

**NET_DOWN**
La interfaz X.25 está actualmente inactiva.

**PLC_DOWN**
La capa de paquetes X.25 está actualmente inactiva.

**DISCONNECTED**
Para este y todos los siguientes estados, la interfaz X.25 y las capas de paquetes están activas. En este estado, DLSw espera que una estación final inicie un establecimiento de conexión.

**XID_POLL**
DLSw está sondeando la estación final QLLC con un QXID (XID_null) en un intento de contactar inicialmente con el dispositivo o de recuperar una conexión perdida.

**SETMODE_POLL**
DLSw está sondeando la estación final QMS en un intento de contactar inicialmente con el dispositivo o de recuperar una conexión perdida.

**SENT_EX**
DLSw ha escuchado una estación final QLLC y está explorando el destino adecuado en la red DLSw.

**CS_PEND**
La exploración de DLSw ha sido satisfecha y ha iniciado una petición de arranque de circuito (ha enviado CUR_cs).

**CALL_REQ_PEND**
DLSw ha colocado una petición de llamada de salida a una estación final QLLC y está esperando a ver si se responde a la llamada satisfactoriamente.

**ESTABLISHED**
El circuito DLSw está en estado de “circuito establecido”; está disponible para enviar y recibir XID SNA.

**CONTACT_PEND**
DLSw ha enviado QSM a la estación final QLLC y está esperando QUA.

**CONNECTED**
El circuito DLSw está completamente activo y transporta datos de usuario final de tramas-I.

**DISC_PEND**
DLSw ha solicitado una desconexión de circuito a la estación QLLC y está esperando un acuse de recibo.

**RESET_PEND**

DLSw ha solicitado una llamada de restauración de PVC o de borrado de SVC a la estación QLLC y está esperando un acuse de recibo.

**Ejemplo: `li qllc sta`**

```
If  P/S  LCN/DTE addr   E/D Source SAP/MAC   Dest SAP/MAC    PU Blk/IdNum  Type
 1  PVC  2               E  04 400000310104  04 400011112323  2 000/00000  PERM
 1  SVC  3721111         E  04 400000310103  00 000000000000  2 000/00000  PERM
 1  PVC  4               E  04 400000317402  04 400000000002  2 017/00001  PERM
```

Para ver una descripción de los campos de la pantalla que puede configurar, consulte el mandato **add qllc** en el tema “Utilización de DLSw” en la página 525. El campo “E/D” indica si la estación está actualmente activada. El campo “Type” tiene los mismos valores que se han descrito para el mandato **list qllc sessions**.

**sdlc config**

Muestra parámetros configurados para la PU conectada a SDLC.

**Ejemplo: `list sdlc config`**

```
    Interface #, or 'ALL' [0]? all

Net  Addr    Status    Source SAP/MAC    Dest SAP/MAC      PU  Blk/Idnum  PollType
1    C1      Enabled   04 4000103D01C1   00000000000000    2   000/00000  TEST
1    C2      Enabled   04 4000103D01C2   00000000000000    2   000/00000  SNRM
3    FF(sw)  Enabled   04 4000103D01D2   04 400000000003   2   000/00000  TEST
```

**sdlc sessions**

Muestra información sobre todas las sesiones DLS SDLC dentro del direccionador.

**Ejemplo: `list sdlc sessions`**

```
    Net  Address   Source SAP/MAC    Dest SAP/MAC     PU    OutQ   State
1.   1    C1       04 4000103D01C1   00 000000000000  2      0    NET_DOWN
2.   1    C2       04 4000103D01C2   00 000000000000  2      0    NET_DOWN
```

Puesto que DLSw y SDLC tienen capacidad para llevar a cabo una negociación completa de XID, es posible que la estación de enlace SDLC conectada defina el enlace con una dirección de estación SDLC diferente a la configurada en el direccionador. Cuando esto sucede, las dos direcciones de estación SDLC se muestran bajo la columna “Addr” de la pantalla, con el formato `xx(yy)`. En este formato, `xx` es la dirección de estación configurada en este direccionador y se sigue utilizando en todos los mandatos de configuración y de supervisión para hacer referencia a esta estación de enlace. La dirección operativa actual que ha definido el dispositivo SDLC conectado es el valor `yy` que aparece entre paréntesis a la derecha.

**tcp capabilities**

Muestra la información recibida de un direccionador DLSw asociado en su mensaje de intercambio de funciones.

**Ejemplo: `list tcp capabilities`**

```
Enter the DLSw neighbor IP Address [0.0.0.0]? 128.185.236.84
Vendor ID:                10005A
Vendor product version:   IBM 2210 Nways MRS 5765-B86 Feature 5045 V3 R2
Initial pacing window:    12
Preferred TCP connections: 1
Supported SAPs:           00 04 08 0C F0
MAC List Exclusivity:     Complete List
MAC List:                 08005ACEEA1C [FFFFFFFFFFFF]
                          4000189E2000 [FFFFFFFFF000]
NetBIOS Exclusivity:      (not supplied)
NetBIOS Name List:        (none supplied)
Multicast Version:        01
IBM CST:                  Passive Transport
IBM Multicast:            Available
IBM Capex Correlator:     19660
```

**Vendor ID**

El Identificador exclusivo organizacional (OUI) de IEEE del proveedor del DLSw contiguo. El OUI de IBM es X'10005A'.

**Vendor version**

Una serie de texto que ha enviado el DLSw contiguo para describirse a sí mismo. “(not available)” indica que la implantación del direccionador contiguo no ha enviado dicha serie de texto.

**Initial pacing window**

El número de mensajes SSP de ritmo que puede enviar este DLSw al DLSw contiguo tras recibir la otorgación inicial de ritmo para cada nuevo circuito.

**Preferred TCP connections**

El número de conexiones TCP (1 ó 2) que desea tener este direccionador contiguo. El IBM 2210 se ajusta al número solicitado y sólo tendrá una conexión TCP dúplex completo con los direccionadores contiguos que lo soliciten.

**Supported SAPs**

La lista de SAP que el DLSw contiguo ha abierto o abrirá de forma automática en cualquiera de sus interfaces de LAN o representando sus estaciones SDLC conectadas.

**MAC List Exclusivity**

Indica si la lista de direcciones MAC enviada por este direccionador contiguo se debe considerar como una lista completa o parcial de direcciones MAC locales con respecto a este direccionador contiguo. La respuesta “(not supplied)” indica que este direccionador contiguo no ha enviado ninguna lista de direcciones MAC como parte de sus funciones.

**MAC List** Muestra todos los valores y máscaras de la lista MAC que este direccionador contiguo ha enviado en su lista de direcciones MAC. La respuesta “(none supplied)” indica que este direccionador contiguo no ha enviado ninguna lista de direcciones MAC como parte de sus funciones.

**NetBIOS Exclusivity**

Indica si la lista de nombres NetBIOS que ha enviado este direccionador contiguo se debe considerar como una lista completa o parcial de los nombres NetBIOS locales con respecto a este direccionador contiguo. La respuesta “(not supplied)” indica que este direccionador contiguo no ha

enviado ninguna lista de nombres NetBIOS como parte de sus funciones.

**NetBIOS Name List**
Muestra todos los calificadores de nombres NetBIOS que ha enviado este direccionador contiguo en su lista de nombres NetBIOS. La respuesta “(none supplied)” indica que este direccionador contiguo no ha enviado ninguna lista de nombres NetBIOS como parte de sus funciones.

**Multicast Version**
Indica a qué versión de difusión múltiple da soporte este direccionador contiguo, según lo definido en el estándar AIW. La respuesta *not supplied* indica que este direccionador contiguo no ha enviado ninguna versión de difusión múltiple como parte de sus funciones.

**IBM CST** Indica qué tipo de configuración de conectividad (CDT) de IBM ha configurado este direccionador contiguo. La respuesta *not supplied* indica que este direccionador contiguo no ha enviado ningún CST de IBM como parte de sus funciones.

**IBM Multicast**
Indica si las funciones de difusión múltiple específicas de IBM están o no disponibles en este direccionador contiguo. La respuesta *not supplied* indica que este direccionador contiguo no ha enviado ninguna difusión múltiple de IBM como parte de sus funciones.

**IBM Capex Correlator**
Indica el valor del último correlacionador IBM Capex recibido de este direccionador contiguo. La respuesta *not supplied* indica que este direccionador contiguo no ha enviado ningún correlacionador IBM Capex como parte de sus funciones.

**tcp config**
Muestra los parámetros de configuración correspondientes a todas las conexiones TCP configuradas a direccionadores DLSw similares.

**Ejemplo: `list tcp config`**

```
                    Xmit    Rcv     Max     Keep-    SesAlive
Neighbor        CST Bufsize Bufsize Segsize Alive    Spoofing Priority
--------------- --- ------- ------- ------- -------- -------- --------
128.185.236.84   p    5120    5120    1024  DISABLED DISABLED MEDIUM
```

**tcp sessions**
Muestra el estado de todas las sesiones TCP conocidas a direccionadores DLSw similares.

**Ejemplo: `list tcp sessions`**

```
   Group   IP Address      Conn State     CST  Version  Active Sess Sess Creates
   ------- --------------- -------------- ---  -------- ----------- ------------
1          128.185.236.49  ESTABLISHED     p   AIW V1R0      2           4
```

**Group** El grupo a través del que se ha descubierto el direccionador contiguo, si es aplicable

**IP Address**
La dirección IP del direccionador contiguo utilizada para DLSw

**Conn State**

El estado de la conexión de transporte (que puede consistir en 1 ó 2 conexiones TCP) a este direccionador contiguo. Los estados válidos son:

**DOWN** No se ha establecido la sesión TCP; no se intercambian funciones (sólo asociados pasivos).

**CAPEX FAILED**
Ha fallado un intento de intercambiar funciones; la sesión TCP está inactiva.

**Unicasting**
No se ha establecido la sesión TCP; las funciones se han intercambiado satisfactoriamente (sólo asociados pasivos) (lista para tráfico de exploración DLSw)

**PENDING R/W**
Este 2210 ha intentado establecer una sesión TCP con el direccionador contiguo.

**RD EST/WR PEND**
La sesión TCP entre el direccionador contiguo y este 2210 está activa, pero la sesión TCP entre este 2210 y el direccionador contiguo no está activa.

**RD EST/WR PEND**
La sesión TCP entre este 2210 y el direccionador contiguo está activa, pero la sesión TCP entre el direccionador contiguo y este 2210 no está activa.

**CAPEX PENDING**
La sesión TCP se ha establecido; está en proceso de intercambiar funciones.

**ESTABLISHED**
La sesión TCP se ha establecido; se han intercambiado funciones (lista para utilizarse para sesiones DLSw).

**CLOSING**
Desactivando la sesión TCP.

**RECONNECT WAIT**
La sesión TCP no se ha establecido; en espera de que expire el temporizador a fin de intentar volver a establecer la sesión TCP.

**CST** Tipo actual de configuración de conectividad, que puede ser:

```
a - Configurada localmente como activa
p - Configurada localmente como pasiva
A - Configurada localmente como pasiva, pero funcionando en modalidad activa
    debido a los requisitos del direccionador contiguo
D - No configurada localmente, pero una conexión TCP dinámica de direccionador contiguo
```

**Version** El nivel del protocolo DLSw del direccionador contiguo. Puede ser uno de los direccionadores compatibles con AIW VnRm para AIW, implantación RFC1434+ para pre-AIW V1R0 o UNKNOWN.

**Active Sess**

El número actual de sesiones DLSw (circuitos) activas (en cualquier estado) en esta conexión de transporte

**Sess Creates**

El número total de sesiones DLSw (circuitos) que han entrado en el estado CIRC_EST desde la última vez que se ha arrancado el direccionador o se ha emitido el mandato “add tcp” de esta conexión de transporte.

**tcp statistics**

Muestra estadísticas sobre el uso de conexiones de transporte TCP desde la última vez que se ha arrancado el direccionador o se ha emitido el mandato “add tcp” de esta conexión de transporte.

**Ejemplo: `list tcp statistics`**

```
Enter the DLSw neighbor IP Address -0.0.0.0-? 192.1.1.3
                                    Transmitted           Received
                                    -----------           -----------
 Data Messages                           214                  231
 Data Bytes                            372997               413259
 Control Messages                         16                   34

 CanYouReach Explorer Messages             0                    0
 ICanReach Explorer Messages               0                    0
 NameQuery Explorer Messages               1                    2
 NameRecognized Explorer Messages          2                    1
```

**timers** El tiempo, especificado por el usuario, durante el que se esperan diversas actividades.

**Ejemplo: `list timers`**

```
Database age timer                1200  seconds
Max wait timer for ICANREACH      20    seconds
Wait timer for LLC test response  15    seconds
Wait timer for SDLC test response 15    seconds
QLLC session retry timer          20    seconds
Join Group Interval               900   seconds
Neighbor priority wait timer      2.0   seconds
Neighbor Inactivity Timer           5   minutes
Time to delay sending test resp.  0.0   seconds
```

**Database age timer**

El tiempo en que se deben conservar entradas de la base de datos de direcciones de dirección MAC a dirección IP sin referencia. Cero indica que las entradas de esta base de datos no caducan.

**Max wait timer for ICANREACH**

El tiempo en que el direccionador espera una respuesta a un mensaje CANUREACH antes de decidir que la sesión no se va a activar.

**Wait timer for LLC test response**

El tiempo en que el direccionador espera una respuesta TEST de LLC antes de volver a transmitir la trama TEST de LLC.

**Wait timer for SDLC test response**

El tiempo que espera el direccionador antes de volver a intentar establecer contacto con una estación SDLC para iniciar una sesión DLSw.

**QLLC session retry timer**
El tiempo que espera el direccionador antes de volver a intentar establecer contacto con una estación QLLC para iniciar una sesión DLSw.

**Join Group Interval**
El tiempo que transcurre entre difusiones generales de anuncio de grupos DLSw.

**Neighbor priority wait timer**
El tiempo en que DLSw espera antes de seleccionar un direccionador contiguo durante un determinado intento de establecer una sesión.

**Neighbor Inactivity Timer**
El tiempo que espera DLSw antes de desactivar una conexión TCP pasiva inactiva (cero sesiones).

**Delay sending TEST response**
El periodo de tiempo que se debe esperar, una vez finalizada la exploración de una dirección MAC, antes de enviar la respuesta TEST

## NetBIOS

Muestra el indicador de supervisión de NetBIOS.

**Sintaxis:**

n**etbios**

**Ejemplo:** `netbios`

```
NetBIOS Support User Configuration
NetBIOS config>
```

Para ver una descripción de los mandatos de NetBIOS, consulte el tema “Configuración y supervisión de NetBIOS” en la página 175.

## Open-Sap

Utilice el mandato **open-sap** para activar de forma dinámica la conmutación DLSw correspondiente al punto de acceso de servicio (SAP) especificado sin que ello afecte a la configuración de SRAM de DLSw.

**Sintaxis:**

op**en-sap**

**Ejemplo:** `open-sap`

Consulte el tema “Open-Sap” en la página 591 para obtener más información sobre los parámetros de **open-sap**.

## Set

Utilice el mandato **set** para cambiar de forma dinámica los parámetros de LLC2, el número máximo de sesiones DLSw, los temporizadores de protocolo, direccionadores contiguos dinámicos TCP, parámetros para el funcionamiento de QLLC,parámetros relacionados con la lista de direcciones MAC y parámetros de prioridad de circuito sin que ello afecte a la configuración de SRAM de DLSw.

**Sintaxis:**

| | |
|---|---|
| se**t** | dynamic-tcp<br>explorer-limit<br>llc2<br>mac-list<br>memory<br>priority<br>qllc<br>timers |

**dynamic-tcp**

Le permite especificar diversos parámetros de TCP para conexiones TCP de direccionadores contiguos dinámicos (es decir, aquellos que reciben conexiones de entrada procedentes de direccionadores contiguos no definidos mediante el mandato **add tcp**). DLSw solo utiliza estos valores si los direccionadores contiguos dinámicos están activados.

**Sintaxis:** dynamic-tcp

**Ejemplo: `set dyn`**

```
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]?
Enable/Disable NetBIOS SessionAlive Spoofing (E/D) [D]?
Neighbor Priority (H/M/L) [M]?
```

Para ver una descripción de estos parámetros, consulte el mandato **add tcp** en el tema “Utilización de DLSw” en la página 525.

**explorer-limit**

Le permite especificar límites en el número de tramas exploradoras SNA y NetBIOS que se pueden colocar en cola simultáneamente para ser enviadas a un asociado DLSw.

**Ejemplo: `set explorer-limit`**

```
Max SNA explorers per transport queue (0-1000)[100]?
Max NB explorers per transport queue (0-1000)[100]?
DLSw explorer limit values have been set.
```

**Max SNA explorers per transport queue**

El número máximo de tramas exploradoras SNA que se pueden colocar simultáneamente en cola para enviarlas a un determinando asociado DLSw.

**Max NB explorers per transport queue**

El número máximo de tramas exploradoras NetBIOS que se pueden colocar simultáneamente en cola para enviarlas a un determinado asociado DLSw.

**llc2** Le permite configurara atributos de LLC2 específicos para un determinado SAP.

**Ejemplo: `set llc2`**

(Encontrará un ejemplo del mandato **set llc2** en la página 593).

**mac-list** Le permite definir la exclusividad local de direcciones MAC. Este mandato también le permite confirmar todos los cambios efectuados previamente mediante los siguientes mandatos de supervisión:

- enable mac-list local
- enable mac-list remote
- disable mac-list local
- disable mac-list remote
- add mac-list
- delete mac-list
- set mac-list

Como resultado de este mandato, se enviarán nuevas funciones de ejecución a todos los similares DLSw para que comuniquen la nueva información.

**Sintaxis:** mac-list

**Ejemplo: `set mac-list`**

```
Local MAC list exclusivity (E=exclusive, N=non-exclusive) [N]? e

MAC list parameter set.

For the change to take effect, commit the change (next question).

The next question allows you to commit
any of the following changes (permanent and temporary):
  - changes made using ENABLE MAC-LIST LOCAL
  - changes made using ENABLE MAC-LIST REMOTE
  - changes made using DISABLE MAC-LIST LOCAL
  - changes made using DISABLE MAC-LIST REMOTE
  - changes made using ADD MAC-LIST
  - changes made using DELETE MAC-LIST
  - changes made using SET MAC-LIST

Would you like to commit the MAC list changes? [No]: y

Use of local MAC list remains    ENABLED.
Use of remote MAC list remains    ENABLED.
Type of local MAC list has changed from NON-EXCLUSIVE to EXCLUSIVE    .
Entry added temporarily:   08005ACEE5D9 / FFFFFFFFFFFF.
Entry added temporarily:   4000189E3000 / FFFFFFFFF000.
Would you still like to commit the MAC list changes? [No]: y


MAC address list changes have been committed.
```

**memory** Este mandato le permite especificar de forma dinámica la cantidad total de memoria asignada a DLSw y la cantidad de memoria a asignar a cada sesión DLSw.

**Ejemplo: `set memory`**

Encontrará un ejemplo del uso del mandato **set memory** en la página 595.

**priority** Le permite especificar prioridades de circuito a utilizar para circuitos SNA y circuitos NetBIOS. Puede configurar las prioridades de circuito Critical, High, Medium o Low (en orden descendente de Critical a Low).

Este mandato también le permite configurar la proporción de transmisiones de transporte para cada prioridad de circuito y definir el tamaño máximo de trama a utilizar para NetBIOS. Si su red contiene algún segmento conectado por puente de forma transparente (TB), utilice un tamaño máximo de trama NetBIOS de al menos 1470.

**Ejemplo: `set priority`**

Para obtener más información sobre el mandato **set priority**, consulte la página 596.

**qllc** Le permite especificar un rango de direcciones MAC asignadas de forma dinámica que se utilizan como dirección MAC de origen para sesiones DLSw resultantes de llamadas QLLC dinámicas de entrada.

Para especificar el rango, especifique una dirección MAC base de “X” para el rango y un número máximo “N” de direcciones dinámicas. DLSw elige direcciones MAC comprendidas entre X y X+(N–1).

**Sintaxis:**

q**llc**

**Ejemplo: `set qllc`**

```
DLSw config>set qllc
QLLC base MAC address [40514C430000]?
Maximum QLLC dynamic addresses (0-max sess) [64]?
```

**timers** Define los temporizadores del protocolo DLSw.

**Ejemplo: `set timers`**

Encontrará un ejemplo del mandato **set timers** en la página 597.

## Test

Utilice el mandato **test** para realizar pruebas sobre la antememoria de direcciones MAC y la lista de direcciones MAC actualmente activas.

**Sintaxis:**

**test** cache
mac-list

**cache** Le permite determinar el modo en que una trama destinada a una determinada dirección MAC se reenviará en función de la antememoria actual y la información de similares DLSw.

**Sintaxis:** cache

### Ejemplo: `test cache`

```
MAC address to be tested [000000000000]? 10005af1809b
 Enter largest frame size to perform test against [2052]?

Destination MAC address being tested .... 10005AF1809B

MAC cache entry found:
  Entry type = DYNAMIC

Handling of SNA explorer SSP messages ....
  Explorer SSP message not sent (information found locally).

Handling of SNA circuit setup SSP messages ....
  Circuit Setup SSP message would be forwarded to 128.185.236.84

Handling of NetBIOS explorer SSP messages ....
  Explorer SSP message would be broadcast.
  How explorer destined for this MAC address is forwarded to DLSw partners
.....
    Send to all partners with non-exclusive mac address lists.
  There are currently no DLSw partners to forward the explorer to.

Handling of NetBIOS circuit setup SSP messages ....
  No currently known transport that can support circuit setup for given lfsize.
```

**mac-list** Le permite comparar una determinada dirección MAC con todas las entradas actualmente activas de la lista de direcciones MAC (locales y remotas). Esto resulta útil para resolver problemas de conflicto de listas de direcciones MAC.

**Sintaxis:** mac-list

### Ejemplo: `test mac-list`

```
MAC address to be tested [000000000000]? 10005af1809b

Destination MAC address being tested .... 10005AF1809B


MAC address value  MAC address mask   IP Address
-----------------  -----------------  ---------------
10005AF1809B       FFFFFFFFFFFF       128.185.236.84
```

# Utilización de ARP

Este capítulo describe cómo utilizar los protocolos Address Resolution Protocol (ARP) e Inverse Address Resolution Protocol (Inverse ARP) en el direccionador. Incluye las siguientes secciones:



**Nota:** Si la carga del software del dispositivo no contiene Asynchronous Transfer Mode (ATM), los mandatos relacionados con ATM no serán válidos ni se visualizarán en los indicadores de configuración y consola de ARP.

## Visión general de ARP

El protocolo ARP es un protocolo de nivel bajo que correlaciona dinámicamente direcciones de capa de red con direcciones ATM o direcciones del control del acceso al medio (MAC) físicas. Dada únicamente la dirección de capa de red del sistema de destino, ARP ubica la dirección ATM o la dirección del MAC del sistema principal de destino dentro del mismo segmento de red.

Por ejemplo, un direccionador recibe un paquete IP destinado a un sistema principal conectado a una de sus LAN. El paquete sólo contiene una dirección de destino IP de 32 bits. Para crear la cabecera de capa de enlace de datos, un direccionador consigue la dirección del MAC física del sistema principal de destino. A continuación, el direccionador correlaciona esta dirección con la dirección IP de 32 bits. Esta función se denomina *resolución de direcciones*. La Figura 49 en la página 628 ilustra cómo funciona ARP.

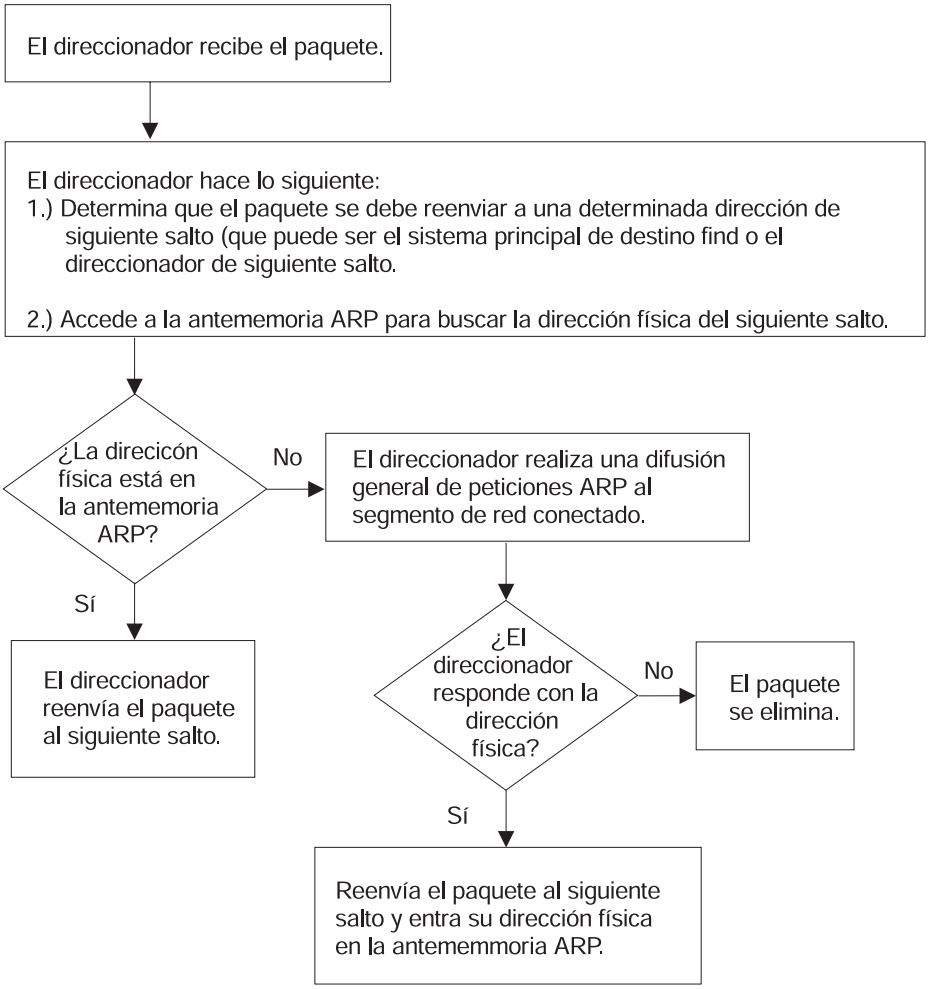



*Figura 49. Difusión para la resolución de direcciones de ARP*

Cuando un direccionador convierte una dirección de capa de red en una dirección física, el direccionador accede a la antememoria de ARP (conversión). La antememoria de ARP contiene la dirección del MAC física que corresponde a esta dirección de capa de red. Si falta la dirección, el direccionador difunde una petición ARP a todos los sistemas principales del segmento de red conectado para ubicar la dirección del MAC física correcta. El nodo con la dirección del MAC física correcta responde al direccionador. A continuación, el direccionador envía el paquete al nodo y entra la dirección del MAC física en la antememoria de conversión para usos futuros.

RFC 1577, IP clásico y ARP sobre ATM, extiende el protocolo ARP con un formato de paquete diferente y con la adición de una entidad conocida como Servidor ARP tal como se describe en “Componentes de IP clásico” en la página 631.

## Visión general de Inverse ARP

Inverse ARP, descrito en RFC 1293/2390, se ha creado para las redes Frame Relay. Este protocolo define un método para que los direccionadores de una red Frame Relay aprendan las direcciones de protocolo de otros direccionadores con un sistema que reduce el tráfico de una manera muy eficiente eliminando la necesidad de utilizar paquetes ARP difundidos para la resolución de direcciones.

Inverse ARP descubre una dirección de protocolo enviando paquetes de petición Inverse ARP a la dirección de hardware (para los circuitos Frame Relay, el identificador de circuito es el equivalente de Frame Relay de una dirección de hardware; para ATM, una dirección ATM se intercambia) tan pronto como se activa el circuito. El direccionador remoto responde con su dirección de protocolo y la correlación resultante se almacena en la antememoria de ARP.

En ATM, el paquete Inverse ARP se ha hecho extensivo al manejo de las direcciones ATM de tamaño variable del origen y destino. Las direcciones aprendidas por Inverse ARP se ajustan a una duración del mismo modo que las aprendidas por ARP.

Las entradas de dirección de protocolo con dirección de hardware aprendidas por Inverse ARP no sobrepasan un tiempo de espera excedido cuando caduca el temporizador de renovación de ARP. Las correlaciones no caducan en absoluto excepto cuando se desactiva el circuito Frame Relay. Esto significa que el direccionador no tiene necesidad de transmitir ninguna difusión de ARP para actualizar la antememoria de ARP. No obstante, el direccionador permite actualizaciones de una entrada cuando el otro direccionador (remoto) cambia su dirección de protocolo.

El soporte para ARP e Inverse ARP mejora en gran medida la interoperatividad del direccionador con direccionadores de otros proveedores sobre Frame Relay para la correlación dinámica de direcciones de protocolo y de hardware. Si los otros direccionadores conectados a Frame Relay dan soporte a Inverse ARP, las correlaciones se aprenden dinámicamente tal como se ha descrito anteriormente. Si los direccionadores conectados no dan soporte a Inverse ARP, sino que dan soporte al ARP “tradicional” sobre Frame Relay, las correlaciones pueden aprenderse también dinámicamente por medio de intercambios de ARP (vea la Figura 49 en la página 628).

Si es necesario, puede configurar manualmente las direcciones de protocolo de otros direccionadores utilizando el mandato de configuración de Frame Relay **add protocol-address**. Para obtener información adicional, consulte el capítulo Configuring and Monitoring Frame Relay Interfaces del manual *Guía del usuario de software*.

## IP clásico y ARP sobre ATM (RFC 1577)

Internet Engineering Task Force (IETF) ha normalizado su solución para enviar tráfico de IP sobre una interfaz ATM en RFC 1577, “Classical IP & ARP over ATM” (IP clásico y ARP sobre ATM). Este documento, creado por el grupo de trabajo de IP sobre ATM de IETF, tiene por objetivo que la infraestructura de ATM se mantenga transparente para IP. La mayoría de las aplicaciones que se ejecutan hoy en día en un entorno de LAN o WAN no contemplarán ninguna diferencia en las funciones; no obstante, su aumento de rendimiento y productividad puede ser importante, tal como se describe en la sección “Ventajas de IP clásico” en la página 630.

RFC 2225 es una extensión de RFC 1577 que cambia el mecanismo de registro del cliente y permite diversos servidores ATM ARP. El 2210 da soporte tanto al comportamiento definido en RFC 1577 como al comportamiento definido en 2225.

Para obtener información adicional sobre IP clásico y ARP sobre ATM, así como para ver ilustraciones que muestren configuraciones de redes lógicas y físicas, consulte el manual *Guía del usuario del programa de configuración para productos Nways Multiprotocol and Access Services*.

## Subredes IP lógicas (LIS) en IP clásico (CIP)

En IP clásico (CIP), las estaciones IP se agrupan en subredes IP lógicas (LIS). Los servidores y clientes IP clásico están definidos para dar soporte a estas subredes de una manera similar a la definición de los servidores y clientes LAN Emulation para los servicios LAN Emulation Services descritos en el capítulo “Using and Configuring LAN Emulation Services (LES)” del manual *Guía del usuario de software*.

En el caso de muchos mandatos de configuración, se le solicitará que responda a preguntas que son idénticas a las relacionadas con los clientes LAN Emulation Client y servidores LAN Emulation Server. Por ejemplo, las preguntas que requieren ESI y selectores de dirección ATM se realizarán de igual manera tanto si configura IP clásico como LAN Emulation.

Cada una de estas preguntas de configuración está basada en la definición de cliente. Un cliente se define como un número de interfaz (sólo ATM) y una dirección IP.

En su formato más sencillo, el cliente IP no tiene servidor y sólo puede comunicarse con los que se ponen en contacto con su dirección ATM asignada *automáticamente*. Si se han asignado PVC, serán operativos.

Para obtener una descripción más detallada de ATM, consulte el capítulo “Using, Configuring, and Monitoring ATM” del manual *Guía del usuario de software*.

## Ventajas de IP clásico

IP clásico tiene varias ventajas sobre con el protocolo IP convencional:

- Velocidades mayores de línea proporcionadas por ATM
- Utilización más eficiente del ancho de banda disponible

  IP clásico necesita menos bytes de trama que, por ejemplo, las LAN (que contienen direcciones del MAC de origen y de destino), por lo que se utiliza menos ancho de banda para la actividad general y más para los datos.
- No es necesario tráfico difundido para la resolución de las tramas ARP

  En un entorno de difusión, el tráfico de ARP puede afectar, contrariamente, a todas las estaciones. En IP clásico, el tráfico de ARP sólo afecta al Servidor ARP y al cliente que solicita la información. Ninguna de las otras estaciones de la subred queda afectada por este tráfico.
- Canales de conversación independientes

  Cuando se utiliza IP sobre un medio compartido, como, por ejemplo, Red en Anillo o Ethernet, las tramas transmitidas entre dos estaciones excluyen el envío de mensajes de otras estaciones de la misma red física. Esto es así aunque no se difunda el tráfico. En IP clásico, se establecen canales independientes entre los sistemas principales que sostienen la conversación. Estos canales pueden establecerse con parámetros de tráfico que protejan la conversación de interferencias de otras conversaciones.

- Un método más sencillo para añadir, suprimir, trasladar o cambiar estaciones

  Las mismas ventajas de los traslados, adiciones, supresiones, etc. que se describen para LAN Emulation sobre ATM se aplican asimismo a la subred IP lógica (LIS) en CIP. Consulte el capítulo “Using, Configuring, and Monitoring ATM” del manual *Guía del usuario de software*.

  La pertenencia a un grupo en una LIS no está basada en la ubicación física. Pueden agruparse en la misma LIS estaciones relacionadas lógicamente. La facilidad con la que un cliente puede registrarse con el Servidor ARP hace que las adiciones y los cambios sean simples. La supresión se producirá de forma natural dado que el Servidor ARP impone una duración a sus entradas.

  Mientras que todos los miembros de una LIS deben dar soporte al modelo IP clásico, el 2210 puede direccionar con facilidad entre las subredes IP lógicas (LIS) de CIP y las subredes LAN emuladas. Es posible que algunos equipos funcionen mejor con CIP, a la vez que otros equipos funcionan mejor con LAN Emulation. La flexibilidad del 2210 le permite colocar este equipo donde sea más efectivo.

## Componentes de IP clásico

La subred IP lógica contiene todas las propiedades de una subred IP normal, sea Ethernet, Red en Anillo o Frame Relay. No obstante, puesto que ATM es una red de acceso múltiple sin difusión (NBMA), el método de difusión existente para la resolución de direcciones no puede llevarse a cabo. Para solucionar el problema del sistema de direccionamiento, RFC 1577 describe un procedimiento de registro/petición además de aportar la noción de un Servidor ARP y clientes ARP.

Se define un servicio de ARP por LIS. El servicio de ARP puede ser un Servidor ARP o varios Servidores ARP distribuidos por LIS. El servicio mantiene la conversión de direcciones IP en direcciones ATM. Permite que los Clientes CIP se registren con la recepción de VCC de entrada y la realización de consultas al cliente sobre la información correspondiente. El servicio de ARP también responde a peticiones ATMARP en relación con direcciones ATM correspondientes a direcciones IP solicitadas por el cliente. Finalmente, el servicio de ARP gestiona y actualiza sus tablas imponiendo una duración a las entradas de ARP y gestionando las VCC de entrada.

El cliente es la entidad que siempre coloca llamadas. Un cliente, al realizar una acción de IML, colocará una llamada en un Servidor ARP y se registrará con el mismo. La llamada colocada por el cliente en el servidor se denomina canal de control. Cuando el cliente tiene tráfico para transmitir a otro cliente de la LIS, el cliente envía una petición ARP al Servidor de ARP con la dirección IP de destino. El servidor devuelve una respuesta (si el servidor tiene la información en su tabla) o un mensaje NAK (si no hay información disponible). El cliente utiliza esta dirección ATM para colocar una llamada en el cliente de destino (esta llamada se denomina canal de datos). Una vez establecida la llamada, pueden pasar por el enlace datagramas de IP en cualquier momento.

Dentro del modelo CIP, existen dos formas de peticiones/respuestas: las peticiones/respuestas ATM ARP (denominadas las ARP) y las peticiones/respuestas InATMARP. Las InATMARP pueden considerarse una reunión de información de primera mano. Es decir, la InATMARP se utiliza para consultar al otro extremo de una VCC su dirección IP y dirección ATM. La InATMARP también informa al otro extremo de quién es (su dirección IP y direc-

ción ATM). La ATMARP puede considerarse información para la subrogación. Un cliente CIP envía una ATMARP al Servidor ARP para encontrar la dirección ATM correspondiente a la dirección IP especificada. El Servidor responde con la información solicitada, o bien con un mensaje NAK si la información no está disponible. No obstante, RFC requiere que todos los clientes y servidores respondan a las ARP e InATMARP con la respuesta adecuada.

Los clientes RFC 2225 se registran con el Servidor ARP enviando una petición ARP en que las direcciones de protocolo de origen y destino están establecidas en el mismo valor. El proceso de registro se completa satisfactoriamente cuando los clientes reciben una respuesta ARP a esta petición.

Para cada LIS, el dispositivo puede aparecer únicamente como cliente o bien puede aparecer como cliente y Servidor ARP en esta LIS. El dispositivo no da soporte únicamente a un Servidor ARP porque esto infringe la recomendación de RFC 1577 consistente en que cada Servidor ARP debe contener una dirección IP.

Consulte el manual *Guía del usuario de software* para obtener información adicional sobre las interfaces virtuales ATM.

## Tiempos de espera excedidos y renovación

Tanto el cliente CIP como el Servidor ARP imponen una duración a sus entradas de ARP. Una vez que caduque el temporizador para una entrada de ARP, se suprimirá esta entrada. Si fluye tráfico cuando una entrada de ARP se vuelve obsoleta, este tráfico cesará durante un período hasta que se cree una nueva entrada de ARP. Para evitar cualquier interrupción en el servicio, el dispositivo proporciona una opción de renovación automática. Esta opción permite que el cliente transmita una petición ARP al Servidor ARP o una respuesta InATMARP positiva únicamente al cliente de destino un tiempo antes de que caduque la entrada de ARP. Si el destino responde, se restablece el temporizador de la entrada de ARP. Si el destino no responde, se suprime la entrada. El Servidor ARP emite automáticamente un mensaje InATMARP antes de que caduque una entrada de su tabla. El cliente y los Servidores ARP toman por omisión períodos de duración de 5 minutos y 20 minutos respectivamente. Estos períodos de tiempo son configurables para cada LIS (cliente o par cliente/servidor).

**Notas:**

1. Las entradas de ARP siempre se renuevan si se recibe una ARP o InARP de ese cliente.
2. **Auto-refresh** toma por omisión el valor de *No* para un cliente y *Yes* para un servidor.

Es necesario que los clientes RFC 2225 se vuelvan a registrar con el Servidor ARP cada 15 minutos enviando una petición ARP de su propia dirección IP. El período de tiempo para la renovación es configurable, pero RFC 2225 especifica que 15 minutos es el intervalo para volverse a registrar.

No es necesario que los servidores RFC 2225 renueven las entradas de cliente utilizando las InARP. Volverse a registrar es responsabilidad del cliente. El valor por omisión de **auto-refresh** del servidor permanece en *Yes* para que el servidor sea compatible con los clientes RFC 1577. Si la LIS sólo tiene clientes RFC 2225, **auto-refresh** puede establecerse en *No* en los servidores.

## Direcciones IP y los componentes de CIP

Las direcciones IP son clave para el direccionamiento de IP. Cuando se configura el dispositivo, la acción de añadir una dirección IP a una interfaz (puerto ATM) crea automáticamente un cliente CIP. El cliente se define con más detalle si se añade información de cliente ATM ARP, pero es la adición de la dirección IP lo que crea el cliente.

Cada servidor, puesto que contiene una dirección IP, de manera implícita contiene un cliente asimismo. Cuando configure el servidor, debe configurar una dirección IP, lo que creará automáticamente un cliente. A continuación, se crean las bases de datos necesarias y se mantienen para servir a las peticiones de entrada.

La dirección IP configurada no implica necesariamente que el dispositivo vaya a actuar como direccionador. Para que actúe como direccionador, debe configurarse un protocolo de direccionamiento de nivel superior, como, por ejemplo, OSPF. No obstante, si el dispositivo está conectado a diversas subredes y se le envían paquetes desde una subred destinados a una estación de una de las otras subredes conectadas, el dispositivo reenviará ese paquete sin tener configurado ningún protocolo de direccionamiento. Además, si se envía un paquete al dispositivo pero el destino del paquete no es el dispositivo y el destino está en la misma subred que el origen, el dispositivo enviará un mensaje de redireccionamiento de ICMP al originador y reenviará el paquete al sistema principal correspondiente.

## Direcciones ATM de los componentes de CIP

Cada cliente recibe una dirección ATM exclusiva. Como se ha descrito anteriormente, sólo se da soporte a las direcciones NSAP. La persona que configura puede elegir el identificador de sistema final (ESI) y el selector o bien éstos pueden generarse automáticamente durante la inicialización. Si un dispositivo se configura como sólo cliente en una LIS, no es necesario configurar el ESI ni el selector (es recomendable utilizar la generación automática). Si un dispositivo se configura como un par cliente/servidor, es muy recomendable que el usuario especifique su propio selector y, si es necesario, el ESI. (Tenga en cuenta que el ESI tomará por omisión un valor incorporado de 6 bytes que será exclusivo.) El usuario deseará especificar esta información con el fin de que cada vez se active la dirección ATM específica para este Servidor. Los clientes que deseen conectarse con este servidor pueden confiar en el hecho de que la dirección ATM del Servidor no cambiará.

Si se configura un par servidor/cliente para una LIS específica, tanto el uno como el otro utilizarán la misma dirección ATM. Las direcciones ATM (combinación de ESI/Selector) para cada cliente CIP deben ser exclusivas.

## Conexión de canal virtual (VCC)

Una conexión de canal virtual (VCC) es el denominador común inferior para la transmisión de datos. Puede crearse dinámicamente, en cuyo caso una VCC es un circuito virtual conmutado (SVC), o puede configurarse en las estaciones de conmutación y las estaciones finales ATM como circuito virtual permanente (PVC).

Los SVC requieren que un protocolo de señalización o configuración con llamada establezca la conexión. Configurar un SVC es parecido a colocar una llamada telefónica. El usuario marca un número telefónico y espera a que se responda al teléfono para comunicarse con la parte que responda. Si cualquier extremo cuelga el teléfono, el llamador debe volver a marcar el número para comunicarse otra vez.

Lo mismo sucede con los SVC ATM. El sistema principal emite un mensaje de configuración con una dirección ATM de 20 bytes (similar a un número telefónico) y espera a que el otro extremo se conecte. Cualquier sistema principal puede colgar el canal.

Los PVC, por otra parte, no requieren un protocolo de señalización. Tampoco requieren niveles de comparación de UNI. Son estáticos y están disponibles para el sistema principal desde la inicialización hasta el apagado. El sistema principal no necesita realizar ninguna acción para “configurar” la conexión. Como tales, los PVC son más simples y, en general, más fiables que los SVC.

La implementación de IP clásico del dispositivo da soporte tanto a PVC como a SVC. Los SVC pueden generarse automáticamente a través del proceso de resolución de direcciones y de la configuración con llamada subsiguiente que efectúe el código de IP clásico o bien el usuario puede configurar explícitamente un SVC. El subsistema ARP activa y desmantela los SVC automáticos según lo que sea necesario para el envío de tráfico de IP. Un SVC configurado se activa durante la inicialización y se mantiene de forma indefinida. Si el SVC configurado no se conecta, el dispositivo continúa reintentando la conexión periódicamente hasta que se apaga la alimentación.

Los PVC y los SVC configurados no requieren definición de Servidor ARP. Es decir, una LIS puede constar de sistemas principales que estén interconectados sólo por información configurada. Opcionalmente, la dirección IP de destino de un PVC o SVC configurado puede configurarse asimismo. Si no se configura la dirección IP, se utilizan los paquetes InATMARP para determinar qué dirección IP se encuentra en el extremo opuesto de una VCC. Para una red de cualquier tamaño, la cantidad de configuración manual se convertiría en prohibitiva. Los SVC generados automáticamente reducen de manera drástica la cantidad de información configurada y proporcionan la flexibilidad máxima para añadir y trasladar sistemas principales.

Las VCC generadas automáticamente sólo pueden existir con la ayuda de un Servidor ARP. Cada cliente debe configurarse con la dirección ATM del Servidor ARP. Inmediatamente después de la inicialización, el cliente intentará conectarse con el servidor ARP. Esta conexión viene referida como canal de control. La utilización principal de un canal de control es para enviar peticiones y respuestas ATMARP e InATMARP, aunque, si el Servidor ARP también es un cliente, el canal de control también puede utilizarse para enviar datos IP. Las VCC automáticas generadas para enviar datos de un sistema principal a otro vienen referidas como canales de datos.

Los atributos de los canales de control y de datos pueden adaptarse a las necesidades del usuario. La configuración de CIP del dispositivo permite la configuración de la velocidad punta de célula, la velocidad sostenida de célula, los tamaños máximos de SDU y otras características de los canales de control y de datos configuradas por el dispositivo. Un usuario también puede elegir limitar las velocidades de célula de las llamadas de entrada para evitar los problemas causados por las discrepancias en los anchos de banda de las diversas conexiones ATM.

## Parámetros de configuración clave para IP clásico

La simplicidad de CIP radica en que se necesitan muy pocos parámetros de configuración. Para un dispositivo sólo cliente, son necesarios tres elementos informativos:

1. La dirección IP y la máscara de subred. (**add address**)
2. La(s) dirección (direcciones) ATM del Servidor ARP (o Servidores ARP distribuidos). (**add arp-server**)
3. Configure el cliente ARP y responda *No* a la pregunta de si el cliente también es un servidor.

La dirección IP y la máscara de subred son necesarias para proporcionar al cliente su identidad de IP exclusiva con el fin de que pueda enviar y recibir datagramas de IP. También define la subred a la que pertenece este cliente CIP. El cliente utiliza la dirección ATM del Servidor ARP durante la inicialización para establecer un canal de control con el Servidor ARP.

Pueden definirse diversos Servidores ARP para una LIS determinada con el fin de servir de reserva. Si se desactiva el Servidor ARP primario, el cliente puede conmutar a un Servidor ARP de reserva para evitar un punto de anomalía individual. El cliente podrá conmutar de nuevo al Servidor ARP primario tan pronto como éste último reanude el servicio. La primera dirección ATM de Servidor ARP configurada se elegirá como Servidor ARP primario por omisión para una LIS determinada. Puede cambiar el Servidor ARP primario utilizando el mandato **reorder** desde el indicador de mandatos `ARP Config>`.

La configuración del servidor es igualmente simple. Básicamente, el servidor tiene que definirse con una dirección ATM fija y conocida, y tiene que saber a qué LIS va a servir. La configuración del servidor necesita lo siguiente:

1. La dirección IP y la máscara de subred. (**add address**)
2. La respuesta de “Yes” a la pregunta sobre si este cliente también es un servidor. (**add atm-arp-client-configuration**)
3. La especificación de un selector explícito para la dirección ATM del servidor (la respuesta de “no” a la pregunta de si el usuario desea utilizar el selector asignado internamente). (**add atm-arp-client-configuration**)

La dirección IP y la máscara de subred indican al servidor a qué LIS va a servir. La dirección IP también proporciona acceso de IP al servidor y a la función de direccionamiento si se desea (mediante el cliente implícito). Se realizan las preguntas 2 y 3, entre otras, en “add atm-client-configuration”. La pregunta 2 es necesaria para habilitar la función de servidor en esta LIS. La pregunta 3 se utiliza para proporcionar al servidor una dirección ATM previsible.

## Cómo entrar direcciones

Las direcciones se entran de dos maneras, según si la dirección representa (1) una dirección IP o bien (2) una dirección ATM, una dirección del MAC o un descriptor de ruta, tal como se indica a continuación:

1. Dirección IP

   Las direcciones IP se entran siguiendo el formato decimal con puntos, un campo de cuatro bytes representado por cuatro números decimales (del 0 al 255) que están separados por un punto (.).

2. Dirección ATM o del MAC o descriptor de ruta

Las direcciones ATM, las direcciones del MAC y los descriptores de ruta se entran como series de caracteres hexadecimales con o sin caracteres separadores opcionales entre los bytes. Los caracteres separadores válidos son guiones (–), puntos (.) o signos de dos puntos (:).

Esto se aplica a las direcciones entradas para ATM, para LAN Emulation así como para IP clásico y ARP sobre ATM.

**Ejemplo de dirección IP:**

**01.255.01.00**

**Ejemplos de dirección ATM, dirección del MAC o descriptor de ruta:**

**A1FF010203**

o bien

**A1–FF–01–02–03**

o bien

**A1.FF.01.02.03**

o bien

**39.84.0F.00.00.00.00.00.00.00.00.00.03.10.00.5A.00.DE.AD.C8**

o bien

**A1:FF:01:02:03**

o incluso

**A1–FF.01:0203**

## Visión general de la redundancia de IP clásico

La redundancia en el Servidor ARP tiene dos dispositivos. Uno funciona como servidor ARP primario y el otro funciona como reserva para el primario. La redundancia de IP clásico le permite especificar en la configuración qué dispositivo actuará como servidor primario y qué dispositivo actuará como servidor secundario (servidor de reserva). En este tipo de redundancia, el servidor primario se configura para el servicio y direccionamiento relativos a una LIS determinada. Cuando falla el primario, el de reserva efectúa el registro utilizando la dirección ATM del primario y toma posesión como Servidor ARP. También puede actuar como pasarela IP por omisión redundante, con lo cual tomará posesión como servidor y direccionador para esta LIS. Por lo tanto, cuando todo es operativo, el primario tiene dos direcciones IP en la LIS (una dirección IP de cliente y una dirección IP de pasarela) y el de reserva sólo tiene una dirección IP de cliente en la LIS. Cuando falle el primario, obviamente éste ya no aparecerá de ninguna manera en la LIS y el de reserva tendrá dos direcciones IP en la LIS (su dirección IP de cliente original y su dirección de pasarela IP por omisión de redundancia recién obtenida). El de reserva también asumirá el papel del Servidor ARP para esta LIS (tomando posesión de la dirección ATM del primario).

La configuración de la redundancia en el Servidor ARP proporcionará la posibilidad de controlar qué dispositivo actuará como primario y qué dispositivo actuará como secundario. Esto permite que el usuario equilibre de manera efectiva la carga en los Servidores ARP mientras proporciona una reserva. Por ejemplo, es posible que

desee que un dispositivo sea el Servidor ARP primario para seis LIS y el secundario para otras seis LIS. Y puede que desee que un segundo dispositivo sea el secundario para las seis primeras LIS y el primario para las otras seis LIS. La configuración resultante tendrá 12 LIS, seis a las que sirve un dispositivo y seis a las que sirve el otro. Si se desactiva uno de los dispositivos, el otro tomará posesión del papel de servidor para las 12 LIS en total.

Debe tenerse en cuenta que habrá dos direcciones ATM asociadas con el punto final ATM. Una dirección ATM será la dirección ATM real y la otra será una dirección ATM especial de redundancia, denominada dirección de redundancia. La dirección de redundancia siempre se registra. El canal de redundancia se establece entre las direcciones del primario y secundario de redundancia. Las direcciones de redundancia sólo se utilizan para la actividad de redundancia. Las direcciones reales se utilizan para el intercambio de información de IP.

En la redundancia de Servidor ARP, cuando se configura como primario, la entidad primaria *siempre* intentará registrar su dirección ATM real hasta que obtenga un resultado satisfactorio. El primario también intentará colocar una llamada para el canal de redundancia dirigida al secundario.

**Notas:**

1. La redundancia de Servidor ARP requiere que los clientes de la LIS puedan asociar más de una dirección IP con una sola VCC.
2. El primario y el de reserva deben estar conectados al mismo conmutador ATM.

Los pasos siguientes describen el proceso de configuración de la redundancia de Servidor ARP para una LIS con Servidor ARP no distribuido:

1. Configure un par Cliente/Servidor ARP en un dispositivo. Éste será el Servidor ARP primario.
2. Configure sólo un Cliente ARP en el otro dispositivo. Éste proporcionará la función de Servidor ARP de reserva.
3. Utilice direcciones ATM diferentes y direcciones IP diferentes para el par Cliente/Servidor ARP primario y el Cliente ARP que proporciona la función de Servidor ARP de reserva (ambas direcciones IP deben estar en la misma LIS).

**Nota:** Consulte la configuración de muestra proporcionada en la sección “Configuraciones de ARP de muestra” en la página 668 para obtener información más detallada.

La redundancia de Servidor ARP proporciona la posibilidad de un servidor de reserva para los clientes 1577. Los clientes 2225 no necesitan la redundancia de Servidor ARP porque pueden conmutar a un Servidor ARP de reserva.

## Visión general del Servidor ARP distribuido

El Servidor ARP distribuido le permite mantener la conectividad con una LIS en el caso de una anomalía de Servidor ARP. Puede definir tantos servidores distribuidos como necesite por LIS (normalmente, basta con tres o cuatro). Los servidores distribuidos pueden ubicarse en cualquier parte de la red ATM. No es necesario que estén entramados, pero debe existir alguna vía de acceso de comunicación del uno al otro.

Una ventaja adicional del Servidor ARP distribuido es que puede distribuirse la carga del Servicio de ATM ARP entre muchos dispositivos, lo que permite que se manejen grandes LIS de una manera más eficiente.

Los Servidores ARP distribuidos de la misma LIS deben estar configurados con:

- El mismo ID del grupo de servidores (SGID)
- Un par ESI/selector que se utilizará para formar la dirección ATM que los otros servidores pueden utilizar para ponerse en contacto con este servidor con el fin de intercambiar información de base de datos ARP.
- Las direcciones ATM de los Servidores conectados directamente (DCS) con los que el Servidor ARP distribuido intenta sincronizarse.

El Servidor ARP distribuido se ajusta al borrador de IETF "Server Cache Synchronization Protocol (SCSP) – NBMA". SCSP es el protocolo de fines generales para la distribución de bases de datos de servidor sobre las redes ATM.

Los clientes ARP ATM deben ser capaces de reconocer cuándo no es operativa su conexión con el Servidor ARP y deben poder conmutar a un servidor alternativo. Los clientes que se ajustan a RFC 2225 satisfacen este requisito.

## Ejemplos de Servidores ARP distribuidos

En la Figura 50, están definidos dos Servidores ARP en una LIS. Estos Servidores ARP están configurados de manera que uno tiene un duplicado de la base de datos de ARP del otro. El protocolo SCSP de cada dispositivo está configurado con la dirección SCSP ATM del otro Servidor ARP. Los Servidores ARP establecen una sesión privada con el fin de intercambiar información de base de datos. Los protocolos SCSP, en el dispositivo, interactúan con el Servidor ARP del mismo dispositivo para obtener los cambios de la antememoria y para informar de este tipo de cambios.

El cliente ARP ATM está configurado de manera que tiene dos Servidores ARP, uno como servidor primario y el otro como servidor de reserva en el caso de que se produzca una anomalía. Si el cliente pierde el contacto con el primario, se registrará con el de reserva. El de reserva tendrá la base de datos de resolución de ARP completa y proporcionará el servicio de resolución de ARP al cliente.

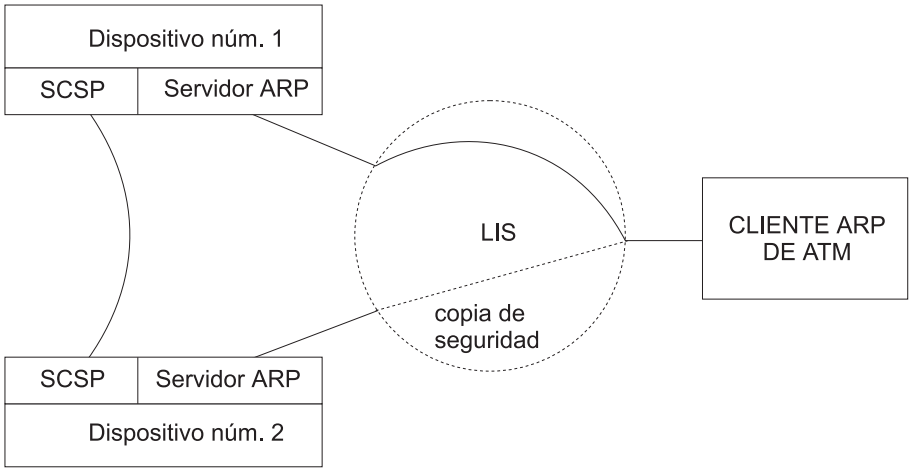



*Figura 50. Configuración simple de Servidor ARP distribuido*

En la Figura 51 en la página 639, están configurados tres Servidores ARP en una LIS. El Dispositivo 1 está configurado con un Servidor conectado directamente (DCS), el Dispositivo 2 está configurado con dos DCS, y el Dispositivo 3 está configurado con un DCS.

El Cliente 1 está configurado con el Dispositivo 1 como su Servidor ARP. El Cliente 2 está configurado con el Dispositivo 3 como su servidor primario y el Dispositivo 2 como su servidor de reserva. Con esta configuración, el Cliente 1 puede obtener la dirección del Cliente 2 a partir del Dispositivo 1 aunque el Cliente 2 esté registrado con el Dispositivo 3. Igualmente, el Cliente 2 puede obtener la dirección del Cliente 1 a partir del Dispositivo 3.

Si falla el Dispositivo 3, el Cliente 2 puede conmutar al Dispositivo 2 para el servicio de ARP sin pérdida de conectividad. Si falla el Dispositivo 1, el Cliente 1 perderá finalmente la conectividad con la LIS porque no tiene configurado un Servidor ARP de reserva. Si falla el Dispositivo 2, se pierde la redundancia. Para que esta configuración retuviese la redundancia al completo, los dispositivos tendrían que estar entramados en una malla completa.

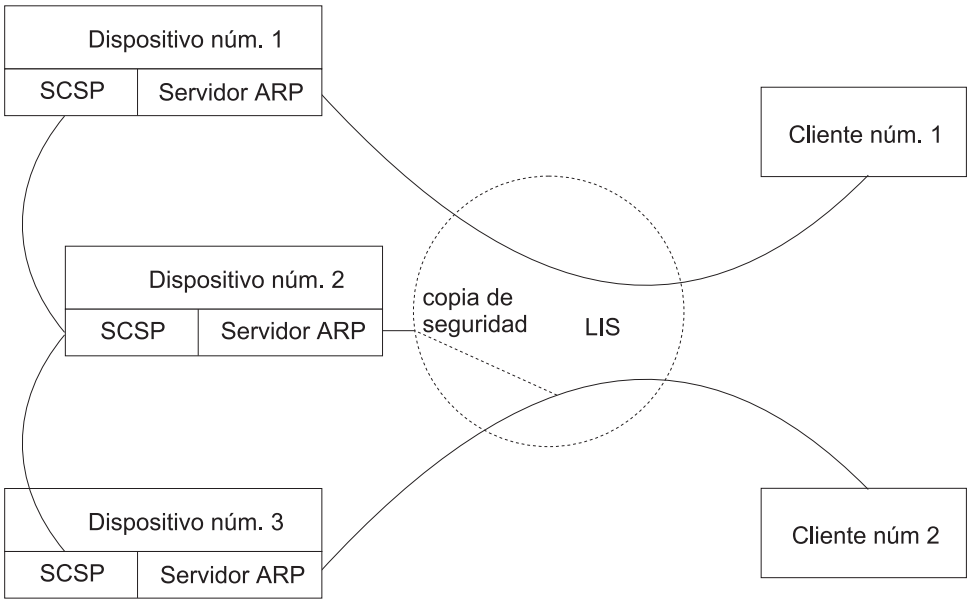



*Figura 51. Configuración distribuida con tres Servidores ARP*

## Redundancia de similar

El Servidor ARP distribuido le permite proporcionar soporte de servidor ARP alternativo a los clientes RFC 2225. La redundancia de Servidor ARP le permite definir un servidor ARP de reserva para los clientes RFC 1577. La función de redundancia y la función de Servidor ARP distribuido pueden estar definidas en el mismo dispositivo. En esta configuración, tanto el primario como el de reserva se definen como servidores con el protocolo SCSP habilitado. Cuando ambos están operativos, actúan como servidores ARP con la base de datos de ARP completa disponible. Cuando falla el primario, el de reserva toma posesión de la dirección ATM del primario (y también mantiene la suya propia). Además, si falla el de reserva, el primario puede tomar posesión de la dirección ATM del de reserva y, por lo tanto, dar soporte a sus clientes 1577.

**Nota:** Tanto el primario como el de reserva deben estar conectados al mismo conmutador ATM.

.

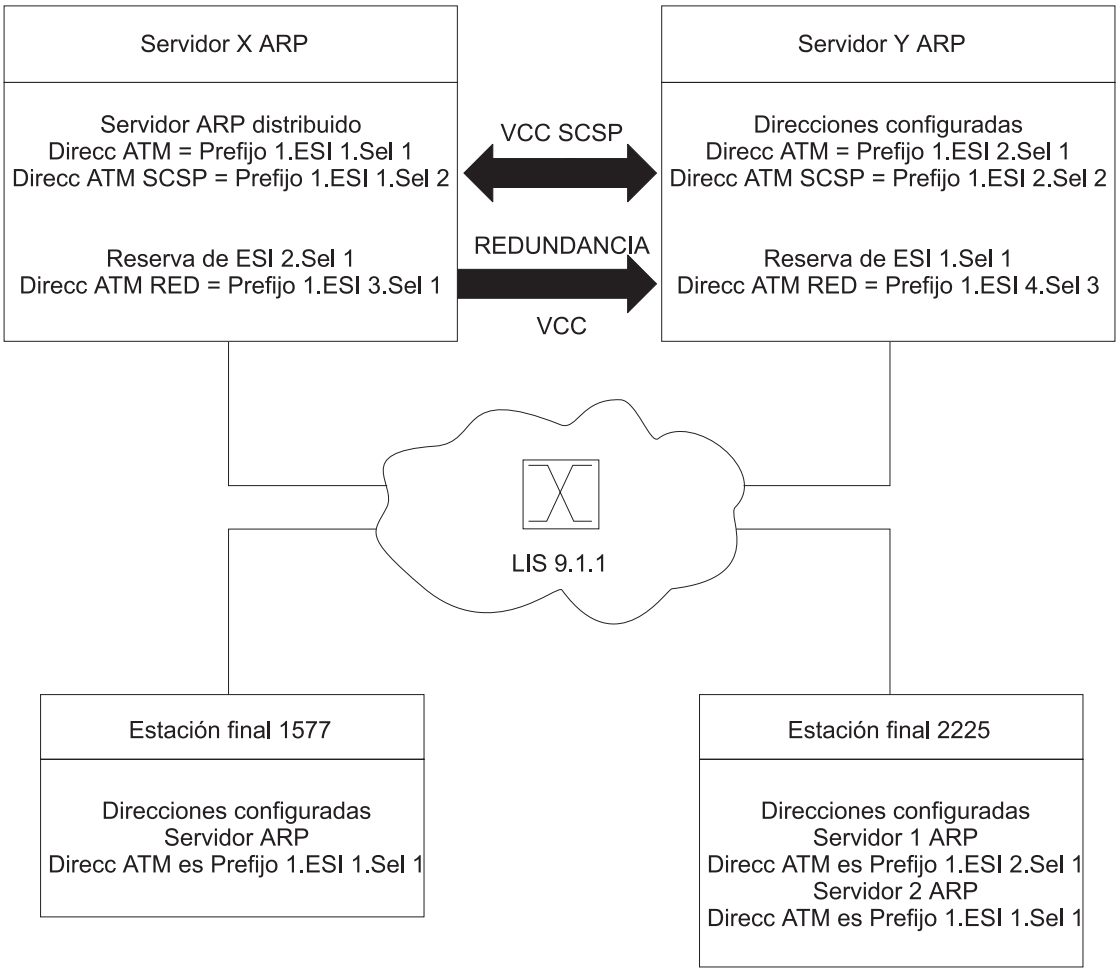



*Figura 52. Configuración de Servidor ARP con clientes RFC 1577 y 2225*

Un servidor puede configurarse como servidor redundante y servidor distribuido. En la Figura 52, se utilizan servidores ATMARP distribuidos para la LIS 9.1.1. Los Servidores X e Y sirven de forma activa a conjuntos diferentes de clientes ATMARP en la LIS 9.1.1. El Servidor X sirve al cliente que se ajusta a RFC 1577 y el Servidor Y es la primera elección del cliente 2225. Las bases de datos de los dos Servidores ARP están sincronizadas por medio del protocolo SCSP. Si el Servidor Y llegase a fallar, el cliente 2225 utilizaría la siguiente entrada de su lista de direcciones ATM de Servidor ATMARP y se conectaría con el Servidor X.

Con el fin de proporcionar la redundancia de Servidor ARP para el cliente que se ajusta a 1577, el Servidor X está designado como Servidor ARP primario para la dirección ATM Prefijo 1.ESI 1.Sel 1 y el Servidor Y está designado como Servidor ARP de reserva para la dirección ATM Prefijo 1.ESI 1.Sel 1. Los Servidores ARP primario y de reserva proporcionan soporte de redundancia. Si falla el Servidor X y toma posesión el Servidor Y, el Servidor Y registrará la dirección ATM Prefijo 1.ESI 1.Sel 1 además de sus otras direcciones ATM. Así, el Servidor Y representará simultáneamente a la dirección ATM Prefijo 1.ESI 1.Sel 1 y a la dirección ATM Prefijo 1.ESI 2.Sel 1. Si el Servidor X se recupera a continuación y restablece la

VCC de redundancia con el Servidor Y, éste desregistrará la dirección ATM Prefijo 1.ESI 1.Sel 1 para que el Servidor X pueda reanudar su papel como uno de los Servidores ARP activos de la LIS.

La redundancia de similar depende de la existencia del canal de redundancia entre el par de Servidores ARP distribuidos que se han configurado para la redundancia. El cliente o servidor ATM con el ESI de redundancia *mayor* iniciará el canal de redundancia con el asociado. En este ejemplo, ESI 3 es superior a ESI 4, por lo que el Servidor X iniciará la llamada para el canal de redundancia con el Servidor Y.

## Configuración de la redundancia de similar

Cuando se crea una nueva configuración para la redundancia de Servidor ARP, se habilita automáticamente la redundancia de similar si el cliente ATM IP clásico está configurado como Servidor ARP distribuido.

Cuando se utiliza una configuración existente de un release anterior, no se habilita automáticamente la redundancia de similar. En este caso, con el fin de habilitar la redundancia de similar, utilice el mandato **change redundancy** para proporcionar el ESI y el selector de servidor asociado a cada uno de los Servidores ARP distribuidos y grabar la configuración en el dispositivo. A continuación, se habilitará la redundancia de similar siempre y cuando los Servidores ARP de redundancia sean Servidores ARP distribuidos.

Cuando se inhabilite el Servicio de ARP distribuido para un cliente cambiando la configuración del cliente para una dirección IP determinada y exista una configuración de redundancia, se inhabilitará la redundancia de similar. Se le solicitará que verifique la configuración de la redundancia para realizar la corrección cuando se inhabilite el servicio de ARP distribuido.

## Visión general de IPX y ARP sobre ATM (RFC 1483)

El 2210 utiliza la encapsulación LLC/SNAP especificada por RFC 1483 para transportar tráfico de IPX sobre ATM. Los 2210 (y otros direccionadores que dan soporte a la encapsulación LLC/SNAP de RFC 1483 en ATM) se pueden interconectar en mallas completas o parciales mediante conexiones RFC 1483 configuradas de forma manual. Tanto los PVC como los SVC configurados reciben soporte. Sin embargo, los SVC con direccionadores IPX deben estar dedicados a IPX; no se pueden compartir con otros protocolos, como IP.

Al igual que en IP clásico, se pueden especificar características de Calidad de servidor configurando parámetros de tráfico de VCC, como velocidades punta y sostenida, y se pueden configurar varios circuitos en una sola interfaz ATM.

El 2210 da soporte a una sola red IPX por interfaz ATM. Esto significa que sólo hay un cliente ATM ARP por interfaz para IPX, el cual se debe configurar de forma explícita. Por lo tanto, todos los direccionadores interconectados de la interfaz ATM deben formar parte de la misma red IPX.

Las direcciones ATM de IPX deben ser exclusivas entre todos los componentes que utilizan la encapsulación de RFC 1483, incluidos los componentes de IP clásico. Las partes de ESI y selector de las direcciones ATM de IPX se configuran del mismo modo que las direcciones ATM de IP clásico. Si el 2210 no va a iniciar

el SVC, al menos el selector se debería especificar de forma explícita en la configuración actual para proporcionar una dirección fija que se pueda configurar en el direccionador que emite la llamada.

Las direcciones de protocolo IPX tienen dos partes:

- Un número de red de 4 bytes, y
- Un número de sistema principal de 6 bytes (o ID de sistema principal)

Los números de red deben ser exclusivos dentro de los dominios de direccionamiento IPX, y los números de sistema principal deben ser exclusivos dentro de una determinada red. El número de sistema principal IPX se establece (por medio del 2210) en el componente ESI de la dirección ATM asociada. El ESI toma por omisión la dirección del MAC incorporada en el hardware de la interfaz ATM en el caso de que el usuario no lo configure explícitamente.

Los números de sistema principal IPX de destino pueden especificarse durante la configuración de la VCC o aprenderse dinámicamente mediante la InATMARP. Debe configurar de forma manual los números de sistema principal IPX de los direccionadores de destino que no dan soporte a la InATMARP. La InATMARP también se utiliza para renovar periódicamente el conocimiento del 2210 del número de sistema principal IPX de un direccionador conectado.

Los direccionadores que están interconectados en una malla parcial y ofrecen direccionamiento intermedio entre direccionadores de la misma interfaz ATM deberían inhabilitar el horizonte de división IPX de la interfaz ATM. De este modo se asegura que RIP y SAP informan correctamente a los direccionadores interconectados sobre todas las rutas y servicios disponibles. Los direccionadores interconectados en una malla completa no necesitan inhabilitar el horizonte de división.

Utilizando el recurso de la interfaz virtual ATM, IPX deja de estar limitado a una sola dirección por interfaz ATM física. Pueden definirse diversas interfaces virtuales ATM en una interfaz ATM física y puede configurarse una dirección IPX en cada interfaz virtual ATM.

Consulte el manual *Guía del usuario de software* para obtener información adicional sobre las interfaces virtuales ATM.

## Visión general de la función de puente sobre ATM (RFC 1483)

Aunque la función de puente no se sirve del soporte de ARP, la implementación de la función de puente sobre ATM nativo comparte algunas estructuras internas con ARP. En esta relación, los registros de cliente y canal ATM para los puertos de puente pueden visualizarse y modificarse (sólo el registro de cliente). Tenga en cuenta que la adición y la supresión de estos registros se realiza automáticamente cuando se añade o se suprime un puerto de puente en una interfaz ATM.

Si desea obtener información más detallada sobre el soporte de RFC 1483 para la función de puente sobre ATM, consulte “Soporte RFC 1483 para la conexión por puente” en la página 57.

# Configuración y supervisión de ARP

Este capítulo describe cómo configurar y supervisar la actividad del protocolo ARP y cómo utilizar los mandatos de supervisión de ARP. Incluye las siguientes secciones:



## Acceso al entorno de configuración de ARP

Para obtener información sobre cómo acceder al entorno de configuración de ARP, consulte "Getting Started" en el manual *Guía del usuario de software*.

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

1. En el indicador de OPCON, entre **talk 6**. (Para obtener información más detallada sobre este mandato, consulte "The OPCON Process and Commands" en el manual *Guía del usuario de software*.) Por ejemplo:

   ```
   * talk 6
   Config>
   ```

   Después de que entre el mandato **talk 6**, se visualizará el indicador CONFIG (`Config>`) en el terminal. Si no aparece el indicador la primera vez que entre la configuración, pulse **Intro** de nuevo.

2. En el indicador CONFIG, entre el mandato **prot arp** para obtener el indicador `ARP Config>`.

## Mandatos de configuración de ARP e Inverse ARP

Esta sección describe los mandatos de configuración de ARP para redes que no son ATM. La Tabla 38 en la página 644 lista los mandatos de configuración de ARP. Puede acceder a los mandatos de configuración de ARP en el indicador `ARP config>`.

**Nota:** Estos mandatos no se utilizan para la configuración de ARP en relación con IP clásico, IPX y la función de puente sobre interfaces ATM. Sin embargo, pueden utilizarse para la configuración de ARP en relación con clientes ATM LAN Emulation.

*Tabla 38. Resumen de los mandatos de configuración de ARP para redes que no son ATM*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Add Entry | Añade una entrada de conversión en dirección del MAC. |
| Change Entry | Cambia una entrada de conversión en dirección del MAC. |
| Delete Entry | Suprime una entrada de conversión en dirección del MAC. |
| Disable Auto-refresh | Inhabilita la auto renovación de ARP. |
| Enable Auto-refresh | Habilita la auto renovación de ARP. |
| List | Lista los datos de configuración de ARP de la SRAM. |
| Set | Establece los valores de tiempo de espera excedido de uso y renovaciones. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Add Entry

Utilice el mandato **add entry** para añadir una entrada de “correlación de dirección de protocolo con dirección de hardware estática”. Actualmente, este mandato sólo está soportado para las direcciones IP.

**Sintaxis:**

a**dd** e**ntry** *ifz# tipo-prot dir-prot dir-MAC*

**ifz#** **Valores válidos**: Cualquier interfaz definida

**Valor por omisión**: 0

**tipo-prot** **Valores válidos**: Cualquier protocolo al que dé soporte ARP.

**Valor por omisión**: IP

**dir-prot** **Valores válidos**: Cualquier dirección IP válida

**Valor por omisión**: 0

**dir-MAC** **Valores válidos**: Cualquier dirección del MAC válida

**Valor por omisión**: Ninguno

**Ejemplo:** **`add entry`**

```
Interface Number [0]?
Protocol [IP]?
IP Address [0.0.0.0]?
Mac Address []?
```

## Change Entry

Utilice el mandato **change entry** para cambiar una entrada de "correlación de dirección de protocolo con dirección de hardware estática". Actualmente, este mandato sólo está soportado para las direcciones IP. El parámetro de dirección de hardware (dir-MAC) debe ser la dirección del nodo que se cambia.

**Sintaxis:**

**change entry** *ifz# tipo-prot dir-prot dir-MAC*

**ifz#** **Valores válidos**: Cualquier interfaz definida

**Valor por omisión**: 0

**tipo-prot** **Valores válidos**: Cualquier protocolo al que dé soporte ARP.

**Valor por omisión**: IP

**dir-prot** **Valores válidos**: Cualquier máscara IP válida

**Valor por omisión**: Ninguno

**dir-MAC** **Valores válidos**: Cualquier dirección del MAC válida

**Valor por omisión**: Ninguno

**Ejemplo: `change entry`**

```
Interface Number [0]?
Protocol [IP]?
IP Address [0.0.0.0]?
Mac Address []?
```

## Delete Entry

Utilice el mandato **delete entry** para suprimir una entrada de "correlación de dirección de protocolo con dirección de hardware estática". Actualmente, este mandato sólo está soportado para las direcciones IP.

**Sintaxis:**

**delete entry** *ifz# tipo-prot dir-prot*

**ifz#** **Valores válidos**: Cualquier interfaz definida

**Valor por omisión**: 0

**tipo-prot** **Valores válidos**: *IP* o *IPX*

**Valor por omisión**: IP

**dir-prot** **Valores válidos**: Cualquier dirección IP válida

**Valor por omisión**: 0.0.0.0

**Ejemplo: `delete entry`**

```
Interface Number [0]?
Protocol [IP]?
IP Address [0.0.0.0]?
```

## Disable Auto-Refresh

Utilice el mandato **disable auto-refresh** para inhabilitar la función de auto renovación. La función de auto renovación representa la posibilidad del direccionador de enviar una petición ARP sobre la base de la entrada de la antememoria de conversión antes de que caduque el temporizador de renovación. La petición se envía directamente a la dirección de hardware de la conversión actual en lugar de una difusión. Si se inhabilita la auto renovación, no se efectúa ninguna petición ARP 'preventiva', se permite que caduque el temporizador de renovación y se elimina la conversión de ARP de la tabla. El próximo paquete de protocolo para la dirección de protocolo de destino causará que se difunda una nueva petición ARP sobre la red.

**Sintaxis:**

dis**able** a**uto-refresh**

**Ejemplo:** `disable auto-refresh`

## Enable Auto-Refresh

Utilice el mandato **enable auto-refresh** para habilitar la función de auto renovación. La función de auto renovación representa la posibilidad del direccionador de enviar una petición ARP sobre la base de la entrada de la antememoria de conversión antes de que caduque el temporizador de renovación. La petición se envía directamente a la dirección de hardware de la conversión actual en lugar de una difusión.

La habilitación de la auto renovación puede causar que se retengan entradas en la antememoria sin tener en cuenta su uso. En las redes con un gran número de nodos, esto puede conducir a un número excesivo de entradas de la antememoria, lo que puede afectar negativamente al rendimiento del direccionador. Sin embargo, en las redes con pocos nodos, esta opción ayuda a reducir el tráfico de ARP difundido.

**Sintaxis:**

en**able** a**uto-refresh**

**Ejemplo:** `enable auto-refresh`

## List

Utilice el mandato **list** para visualizar el contenido de la configuración de ARP del direccionador que se ha almacenado en la SRAM. El mandato list visualiza los valores actuales de tiempo de espera excedido para el temporizador de uso y renovación.

**Sintaxis:**

li**st** all / config / entry

**all** Lista la configuración de ARP seguida de todas las entradas de ARP.

**Ejemplo:** `list all`

```
ARP configuration:

Refresh Timeout: 5 minutes
Auto Refresh: disabled

Mac address translation configuration
IF #           Prot #         Protocol --> Mac Address
 0               0           2.2.2.1 --> 0000C90932EF
```

**config** Lista la configuración para los diferentes parámetros de ARP.

**Ejemplo:** **`list config`**

```
ARP configuration:

Refresh Timeout: 5 minutes
Auto refresh: disabled
```

**entry** Lista las entradas de ARP de la SRAM.

**Ejemplo:** **`list entry`**

```
Mac address translation configuration

IF #           Prot #         Protocol --> Mac Address
 0               0           2.2.2.1 --> 0000C90932EF
```

## Set

Utilice el mandato **set** para establecer un parámetro de configuración de ARP.

**Sintaxis:**

**set** refresh-timer

**refresh-timer** *minutos*

Cambia el valor de tiempo de espera excedido para el temporizador de renovación. Si desea cambiar el valor de tiempo de espera excedido para el temporizador de renovación, entre el valor de tiempo de espera excedido en minutos. Un valor de cero (0) desactiva (inhabilita) el temporizador de renovación.

Este temporizador se utiliza para determinar cuándo debe renovarse una entrada de antememoria de conversión de ARP, mientras esté habilitada la auto renovación, o eliminarse, mientras esté inhabilitada la auto renovación. Con la inhabilitación del temporizador, se retienen las entradas hasta que provoca que se eliminen entradas una conversión de dirección aprendida de nuevo, hasta que se borran entradas manualmente con el mandato de supervisión de ARP **clear** o hasta que se reinicia el direccionador.

**Valores válidos**: Un número entero de minutos dentro del rango del 0 al 65535

**Valor por omisión**: 5 minutos

**Ejemplo:** **`set refresh-timer 3`**

# Mandatos de configuración de ARP sobre ATM

Esta sección describe los mandatos de configuración de ARP sobre ATM. Estos mandatos son aplicables a:

- IP clásico y ARP sobre ATM
- IPX sobre ATM
- La función de puente de 1483

Entre los mandatos en el indicador `ARP Config>`.

## Efecto sobre las entradas de tabla de ARP

Estos mandatos sólo se aplican a la interfaz ATM física en que residan las entradas de ARP para ARP sobre ATM. Estos mandatos no tendrán ningún efecto sobre una interfaz que no sea ATM.

*Tabla 39. Resumen de los mandatos de configuración de ARP sobre ATM*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| List | Lo lista todo (la configuración actual de ARP sobre ATM), lista los Servidores ARP (sólo para IP) o lista las entradas de PVC ATM ARP, las entradas de SVC ATM ARP, la configuración de los clientes ATM ARP y la redundancia. |
| Add | Añade un servidor ARP, una configuración de cliente ATM ARP, una entrada de PVC ATM ARP, una entrada de SVC ATM ARP o redundancia. |
| Change | Cambia la configuración de cliente ATM ARP o la redundancia. |
| Delete | Suprime un servidor ARP, una configuración de cliente ATM ARP, una entrada de PVC ATM ARP, una entrada de SVC ATM ARP o la redundancia. |
| Disable | Inhabilita **auto-refresh** para que no se renueven automáticamente entradas de ARP. |
| Enable | Habilita **auto-refresh** para que se renueven automáticamente entradas de ARP. |
| Set | Establece **refresh-timer** para imponer una duración a entradas de ARP. |
| Reorder | Selecciona el Servidor ARP primario entre una lista determinada de Servidores ARP. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Add

Utilice el mandato **add** para añadir un servidor ARP, una configuración de cliente ATM ARP, una entrada de SVC ATM ARP o redundancia.

**Sintaxis:**

add
- arp-server
- atm-arp-client-configuration
- pvc-atm-arp-entry
- svc-atm-arp-entry
- redundancy

**arp-server private-nsapa *dirección-IP-cliente-local dirección-NSAP-privada***
Añade un servidor ARP al cliente especificado o añade un Servidor conectado directamente (DCS) a un Servidor ARP.

Si la dirección IP es un cliente únicamente, la dirección NSAP es la dirección de un servidor remoto. Pueden añadirse diversos servidores remotos por cliente. Durante la inicialización, el cliente CIP especificado colocará una llamada en un Servidor ARP y lo utilizará como mecanismo para resolver direcciones IP con direcciones ATM.

Si la dirección IP es un servidor, la dirección NSAP es la dirección de un DCS para el Servidor ARP distribuido. Esta dirección debe coincidir con la dirección SCSP ATM para el DCS (no la dirección ATM del cliente). Utilice el mandato de supervisión **List Server-Groups** en el indicador de mandatos SCSP> bajo **t 5** para determinar la dirección SCSP ATM de un servidor. Consulte “Supervisión de Server Cache Synchronization Protocol (SCSP)” en la página 685 para obtener más información.

**local-client-IP-address**

Este valor especificará la dirección IP del cliente o servidor.

**Valores válidos**: Cualquier dirección IP válida

**Valor por omisión**: Ninguno

**private-nsap-address**

Este campo es la dirección privada de punto de acceso especificado de red que tiene el formato de sistema de dirección especificado en UNI Versiones 3.0 y 3.1. Cuando se configura un DCS, este valor es la dirección ATM del DCS.

El primer byte de *nsapa* define el formato de sistema de dirección, tal como se indica a continuación:

| *Primer byte* | *Especificación del formato de dirección NSAP* |
|---|---|
| 0x39 | Formato de ATM de DCC |
| 0x47 | Formato de ATM de ICD |
| 0x45 | Formato de ATM de E.164 |

**Nota:** Este valor corresponde al par (dirección IP/número de puerto) de un cliente.

**Valor por omisión**: Ninguno

**Ejemplo**:

```
ARP config> add arp-server private-nsapa
Local Client IP Address [0.0.0.0]? 2.2.3.100
Private NSAP Address: Specify 40 digits
ATM Address []? 39840f000000000000000000410005a3345f3a0
```

**atm-arp-client-configuration**

Añade una configuración de cliente ATM ARP.

Se le solicitará que proporcione información sobre las características de las VCC que se configurarán y se recibirán en este cliente o servidor, los valores de tiempo de espera excedido de renovación y auto renovación, la manera en que se determina la dirección ATM para este cliente, los parámetros del Servicio de ARP distribuido, así como el tamaño de trama que este cliente puede manejar.

**Nota:** Cualquier parámetro de ancho de banda o célula que sea igual a cero recibirá el trato de velocidad de línea de la interfaz ATM.

### Ejemplo para IP:

```
ARP config> add atm-arp-client-configuration
Interface Number [0]?
Protocol [IP]?
Client IP Address [0.0.0.0]? 1.1.1.2
This client is also a server? [Yes] yes
Refresh timeout (in minutes) [20]?
Enable auto-refresh? [Yes]:
Refresh by InAtmArp? [Yes]:
  (  1) Use burned in ESI
  (  2) 111111111111
  (  3) 222222222222
  (  4) 121212121212
  (  5) AAAAAAAAAAAA
Select ESI [1]?2
Use internally assigned selector? [Yes]: no
Selector Only, Page 00..FF [00] ? 11
Validate PCR for best effort VCCs? [No]:
Maximum Reserved Bandwidth for incoming VCCs (Kbps) [0]?
Use Best Effort Server for Control VCCs? [Yes]:
Peak Cell Rate of outbound control VCCs (Kbps) [0]?
Sustained Cell Rate of outbound control VCCs (Kbps) [0]?
Use Best Effort Server for Data VCCs? [Yes]:
Peak Cell Rate of outbound Data VCCs (Kbps) [0]?
Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?
Max SDU size (bytes) [9188]?
Participate in Server Synchronization [No]? yes
Server Group ID [1]?
Do you want to accept sessions from non-configured DCSs [Yes]?
Hello Interval [3]
Dead Factor [3]?
(  1) Use burned in ESI
(  2) 111111111111
(  3) 222222222222
(  4) 121212121212
(  5) AAAAAAAAAAAA
Server Synchronization ESI [2]?
Server Synchronization selector, Range 00..FF [00]? 12
Server Synchronization Max SDU size (bytes) [9188]?
Re-registration time with Arp Server (in minutes) [15]?


To enable or change multicast support,
please issue the ADD or CHANGE MULTICAST-SUPPORT command.
```

### Ejemplo para IPX:

```
ARP config> add atm-arp-client-configuration
Interface Number [0]?
Protocol [IP]? IPX
Refresh timeout (in minutes) [5]?
Enable auto-refresh? [Yes]:
  (  1) Use burned in ESI
Select ESI [1]?
Use internally assigned selector? [Yes]:
Validate PCR for best effort VCCs? [No]:
Maximum Reserved Bandwidth for incoming VCCs (Kbps) [0]?
Use Best Effort Server for Control VCCs? [Yes]:
Peak Cell Rate of outbound control VCCs (Kbps) [0]?
Sustained Cell Rate of outbound control VCCs (Kbps) [0]?
Max SDU size (bytes) [9188]?
```

### Ejemplo para la función de puente:

```
ARP config> add atm-arp-client-configuration
Interface Number [0]?
Protocol [IP]? ASRT
Clients for this protocol can only be changed here.
Additions must be done under ASRT Config by adding a port.
```

### Interface Number

Número de interfaz asignado.

**Valores válidos**: Cualquier interfaz del dispositivo

**Valor por omisión**: 0

**Protocol** **Valores válidos:** *IP*, *IPX* **o** *ASRT*

**Valor por omisión**: IP

**Client IP Address**

Dirección IP de cliente (sólo IP). Debe coincidir con la dirección configurada mediante el mandato **p IP**.

**Nota:** Este valor también se utiliza para el LSID en el protocolo SCSP.

**Valores válidos**: Cualquier dirección IP válida

**Valor por omisión**: 0.0.0.0

**This client is also a server**

Yes o No. Si es que no, el cliente no es un servidor. (Sólo IP)

**Refresh timeout (in minutes)**

Valor de tiempo de espera excedido de renovación en minutos. Caducarán entradas de ARP después de este número de minutos si no se renuevan.

**Valores válidos**: Un número entero de minutos dentro del rango del 0 al 65535

**Valor por omisión**: 5 minutos

**Enable auto-refresh**

YES o NO.

Si es que No, no se renovarán automáticamente entradas de ARP.

**Valor por omisión**: No para un cliente, Yes para un Servidor

**Refresh by InAtmArp**

YES o NO.

Si es YES y se ha habilitado la auto renovación, se transmitirán periódicamente peticiones InAtmArp para confirmar la existencia del sistema principal remoto.

Si es NO y se ha habilitado la auto renovación, se transmitirán peticiones AtmArp al Servidor ARP para volver a confirmar la entrada de ARP.

**Valor por omisión**: No para un cliente, Yes para un Servidor

**Select ESI**

Especifica si debe utilizarse como componente Identificador de sistema final de la dirección ATM una dirección del MAC administrada universalmente o una dirección del MAC configurada bajo la configuración de interfaz ATM. Esta pregunta viene precedida de una lista de ESI válidos entre los que debe realizarse la selección.

**Valores válidos:** Cualquiera de los valores listados en el menú que precede a esta pregunta. 12 dígitos hexadecimales que se hayan definido como dirección ESI por medio del mandato de configuración de red ATM **Add ESI**.

**Valores por omisión:** 1 (burned-in)

**Use internally assigned selector**
Uso del selector asignado internamente.

**Valores válidos**: Yes o No

**Valor por omisión**: Yes

**Selector** Es el último byte de la dirección ATM del cliente.

**Valores válidos**: Cualquier valor de un solo octeto que no se haya utilizado anteriormente y se encuentre dentro del rango definido para el dispositivo.

**Valor por omisión**: 0

**Validate PCR for best effort VCCs**
Puede ser verdadero o falso. Si es verdadero, las VCC Best-Effort se rechazarán si la PCR hacia adelante señalada sobrepasa el ancho de banda reservado máximo o la velocidad del adaptador. Si es falso, las PCR Best-Effort se aceptarán sin tener en cuenta la velocidad punta de célula señalada.

**Maximum Reserved Bandwidth for incoming VCCs (Kbps)**
Define la velocidad sostenida de célula (SCR) máxima aceptable para una VCC de entrada. Si no se especifica la SCR en la llamada de entrada, este parámetro define la velocidad punta de célula (PCR) máxima aceptable. Las llamadas recibidas cuyos parámetros de tráfico especifiquen velocidades mayores se liberarán. Este parámetro se aplica a los parámetros de velocidad de célula hacia adelante y hacia atrás. La restricción impuesta por este parámetro es aplicable a las conexiones Best Effort (si “validate PCR” es yes) y se compara con la PCR de la llamada de entrada.

**Valores válidos**: Un número entero de Kbps dentro del rango del 0 a la velocidad de línea. Si entra 0, el parámetro se establece en la velocidad de línea.

**Valor por omisión**: Ninguno

**Use Best Effort Service for Control VCCs**
Especifica el tipo de características de tráfico a asociar con las VCC de control. El ancho de banda no es Reserved para el tráfico de Best Effort.

**Valores válidos**: *Ancho de banda Best Effort* o *Reserved*

**Valor por omisión**: Best Effort

**Peak Cell Rate of outbound control VCCs (Kbps)**
Especifica el parámetro de tráfico de velocidad punta de célula (PCR) para la VCC de control. Este valor de PCR se utiliza para los valores de PCR hacia adelante y hacia atrás de las VCC de ancho de banda Best Effort y Reserved.

**Valores válidos**: Un número entero de Kbps dentro del rango del 0 a la velocidad de línea del dispositivo ATM. Si entra 0, el parámetro se establece en la velocidad de línea.

**Valor por omisión**:

- En el caso de Best Effort, el valor por omisión es la velocidad de datos máxima
- En el caso de Reserved, no existe un valor por omisión

**Sustained Cell Rate of outbound control VCCs (Kbps)**
Especifica el ancho de banda reservado por todas las VCC en un dispositivo ATM determinado. (La velocidad sostenida de célula puede considerarse relativa al ancho de banda reservado.) Este parámetro sólo es aplicable cuando no se ha seleccionado Best Effort Service para las VCC de control.

**Valores válidos**: Un número entero de Kbps dentro del rango del 0 a la PCR de VCC de control. Si entra 0, el parámetro se establece en la velocidad de línea.

**Valor por omisión**: Ninguno

**Use Best Effort Server for Data VCCs**
Yes o No. Especifica el tipo de características de tráfico a asociar con las VCC de datos. El ancho de banda no es Reserved para el tráfico de Best Effort.

**Peak Cell Rate of outbound Data VCCs (Kbps)**
Especifica el parámetro de tráfico de velocidad punta de célula (PCR) para las VCC de datos. Este valor de PCR se utiliza para los valores de PCR hacia adelante y hacia atrás de las VCC de ancho de banda Best Effort y Reserved.

**Valores válidos**: Un número entero de Kbps dentro del rango del 0 a la PCR de VCC de control. Si entra 0, el parámetro se establece en la velocidad de línea.

**Valor por omisión**: 0

**Sustained Cell Rate of outbound Data VCCs (Kbps)**
Especifica el parámetro de tráfico de velocidad sostenida de célula (SCR) para las VCC de datos. (La velocidad sostenida de célula puede considerarse relativa al ancho de banda reservado.) Este parámetro sólo es aplicable cuando no se ha seleccionado Best Effort Server para las VCC de datos.

**Valores válidos**: Un número entero de Kbps dentro del rango del 0 al valor de PCR para la VCC de datos. Si entra 0, el parámetro se establece en la velocidad de línea.

**Valor por omisión**: Ninguno

**Max SDU size (bytes)**
Especifica el tamaño máximo de SDU que se especificará cuando se coloquen llamadas desde esta dirección de cliente. También se utiliza para verificar las llamadas entrantes. Este parámetro no puede establecerse en un valor superior al tamaño máximo de SDU para la interfaz ATM física (puerto).

**Valores válidos**: Un entero dentro del rango del 72 al tamaño máximo de SDU de la interfaz

**Valor por omisión**: 9188

**Participate in Server Synchronization**
Especifica si la base de datos de ARP para la LIS bajo la que reside este servidor se distribuirá.

**Valores válidos**: Yes o No

**Valor por omisión**: No

**Server Group ID**
Especifica el valor para identificar a este grupo de servidores. Este valor debe ser exclusivo para todos los grupos de servidores (del tipo de protocolo ATMARP) dentro de la red ATM. Debe utilizarse este valor para todos los servidores de este grupo de servidores (de esta LIS).

**Valores válidos**: Del 0 al 65535

**Valor por omisión**: 1

**Accept sessions from non-configured DCS**
Especifica si este Servidor local debe aceptar conexiones de DCS que no estén configurados explícitamente.

**Valores válidos**: Yes o No

**Valor por omisión**: Yes

**Hello Interval**
Especifica el tiempo en segundos entre los envíos de mensajes Hello para este Servidor local.

**Valores válidos**: Del 0 al 65535

**Valor por omisión**: 3

**Dead Factor**
Especifica el múltiplo de los intervalos de Hello después del cual los servidores conectados directamente (DCS) deben considerar que este servidor está inactivo.

**Valores válidos**: Del 0 al 65535

**Valor por omisión**: 3

**SCSP ESI**
Especifica si debe utilizarse como componente Identificador de sistema final de la dirección SCSP ATM una dirección del MAC administrada universalmente o una dirección del MAC configurada bajo la configuración de interfaz ATM. Esta pregunta viene precedida de una lista de ESI válidos entre los que debe realizarse la selección.

**Valores válidos:** Cualquiera de los valores listados en el menú que precede a esta pregunta. 12 dígitos hexadecimales que se hayan definido como dirección ESI por medio del mandato de configuración de red ATM **Add ESI**.

**Valor por omisión:** El ESI del Cliente/Servidor

**SCSP Selector**
Especifica el selector a asociar con este Servidor local SCSP. Si ***SCSP ESI*** toma por omisión el ESI del Servidor

ARP, este valor de selector debe ser diferente del selector del Servidor ARP.

Es el último byte de la dirección ATM de este servidor local.

**Nota:** La dirección SCSP ATM puede compartirse entre los clientes CIP de la misma interfaz. La dirección ATM también puede compartirse con otros protocolos que utilizan el LLC ATM de 1483. Consulte el capítulo titulado “Using and Configuring ATM” del manual *Guía del usuario de software*. La dirección SCSP ATM no puede compartirse con clientes IP, IPX o ASRT.

**Valores válidos**: Cualquier selector válido que no se haya utilizado anteriormente y se encuentre dentro del rango definido para el dispositivo.

**Valor por omisión**: 0

**Re-registration time with Arp Server (in minutes)**

Especifica el intervalo de tiempo entre las peticiones de registro del cliente al Servidor ARP.

**Valores válidos**: Un entero dentro del rango del 0 al 65535

**Valor por omisión**: 15

**pvc-atm-arp-entry**

Añade un PVC y crea opcionalmente una entrada de ARP permanente si se especifica la dirección de protocolo de destino. Para las interfaces ATM virtuales, debe comprobar la configuración de la interfaz ATM real donde está situada la AVI y todas las otras AVI configuradas en la interfaz ATM real. Es necesario un nuevo par VPI/VCI para un nuevo PVC a menos que desee específicamente compartir el tráfico del nuevo PVC con el tráfico de un PVC existente.

**Ejemplo para IP**:

```
ARP config> add pvc-atm-arp-entry
Interface Number [0]?
Protocol [IP]?
Local client IP address [0.0.0.0]? 2.2.3.100
Specify destination protocol address? [Yes]: no
Permanent Virtual Circuit VPI, Range 00..FF [00]?
Permanent Virtual Circuit VCI, Range 0000..FFFF [0000]? 0029
```

**Ejemplo para IPX**:

```
ARP config> add pvc-atm-arp-entry
Interface Number [0]?
Protocol [IP]? IPX
Specify destination protocol address? [Yes]: no
Permanent Virtual Circuit VPI, Range 00..FF [00]?
Permanent Virtual Circuit VCI, Range 0000..FFFF [0000]? 0037
```

**Ejemplo para la función de puente**:

```
ARP config> add pvc-atm-arp-entry
Interface Number [0]?
Protocol [IP]? ASRT
Channels for this protocol must be added under ASRT Config by adding
a port.
```

**interface number**

**Valores válidos**: El número de la interfaz asignada

**Valor por omisión**: 0

**protocol** Valores válidos: *IP*, *IPX*, *ASRT*

**Valor por omisión**: IP

**local client IP address**

Necesario para IP. Esta dirección asocia este PVC con un cliente.

**Valores válidos**: Cualquier dirección IP válida

**Valor por omisión**: 0.0.0.0

**destination protocol address**

**Valores válidos**: Cualquier dirección IP válida. (Para IPX, cualquier número de sistema principal IPX de 6 bytes válido.)

**Valor por omisión**: 0.0.0.0

**permanent virtual circuit VPI**

**Valores válidos**: Cualquier valor válido dentro del rango del 0 al 255

**Valor por omisión**: 0

**permanent virtual circuit VCI**

**Valores válidos**: Cualquier valor dentro del rango del 0 al 65535

**Valor por omisión**: 0

**svc-atm-arp-entry**

Añade un SVC y crea opcionalmente una entrada de ARP permanente.

**Ejemplo para IP**:

```
ARP config> add svc-atm-arp-entry
Interface Number [0]?
Protocol [IP]?
Local client IP address [0.0.0.0]? 2.2.3.100
Specify destination protocol address? [Yes]: no
Destination ATM Address []? 39840f000000000000000000000210005a00dead03
```

**Ejemplo para IPX**:

```
ARP config> add svc-atm-arp-entry
Interface Number [0]?
Protocol [IP]? IPX
Specify destination protocol address? [Yes]: no
Destination ATM Address []? 39840f000000000000000000000210005a00dead03
```

**Ejemplo para la función de puente**:

```
ARP config> add svc-atm-arp-entry
Interface Number [0]?
Protocol [IP]? ASRT
Channels for this protocol must be added under ASRT Config by adding
a port.
```

**interface number**

**Valores válidos**: El número de la interfaz asignada.

**Valor por omisión**: 0

**protocol** **Valores válidos:** *IP*, *IPX* o *ASRT*

**Valor por omisión**: IP

**local client IP address**

Necesario para IP. Esta dirección asocia este SVC con un cliente.

**Valores válidos**: Cualquier dirección IP válida

**Valor por omisión**: 0.0.0.0

**destination protocol address**

**Valores válidos**: Cualquier dirección IP válida. Para IPX, cualquier número de sistema principal IPX de 6 bytes válido.

**Valor por omisión**: 0.0.0.0

**destination ATM address**

**Valores válidos**: Cualquier dirección ATM válida

**Valor por omisión**: Ninguno

## Redundancy

Utilice este mandato para añadir una configuración de redundancia.

### Ejemplo de redundancia de Servidor ARP

```
ARP config>add red
Interface Number [0]?
Protocol [IP]?
Local client IP Address [0.0.0.0]? 1.1.1.1
Note: Local Redundancy ESI must be different from the Primary Server ESI
  (  1) Use burned in ESI
  (  2) 111111111111
  (  3) AAAAAAAAAAA
  (  4) BBBBBBBBBBB
Select Local Redundancy ESI [1]? 3
Local Redundancy selector, Range 00..FF [00]? aa
Partner's (Redundancy) ATM Address, 40 Hex digits
 [0000000000000000000000000000000000000000]?
39840f00000000000000000001bbbbbbbbbbbbbb  1
Redundancy default IP Gateway also ? [No]: yes
If Yes, Redundancy default IP Gateway protocol address [0.0.0.0]? 1.1.1.3
ARP config>

---------- Backup Server (client) -----------------

ARP config>add red
Interface Number [0]?
Protocol [IP]?
Local client IP Address [0.0.0.0]? 1.1.1.2
Note: Local Redundancy ESI must be different from the Primary Server ESI
  (  1) Use burned in ESI
  (  2) 111111111111
  (  3) AAAAAAAAAAA
  (  4) BBBBBBBBBBB
Select Local Redundancy ESI [1]? 4
Local Redundancy selector, Range 00..FF [00]? bb
Partner's (Redundancy) ATM Address, 40 Hex digits
 [0000000000000000000000000000000000000000]?
 39840f00000000000000000001aaaaaaaaaaaaa  1
  (  1) Use burned in ESI
  (  2) 111111111111
  (  3) AAAAAAAAAAA
  (  4) BBBBBBBBBBB
Partner Server ESI [1]? 2
Partner Server selector, Range 00..FF [00]? 11
Redundancy default IP Gateway also ? [No]: yes
If Yes, Redundancy default IP Gateway protocol address [0.0.0.0]? 1.1.1.3
ARP config>exit
Config>
```

**Nota:** 1 Esta entrada debería aparecer en la línea anterior. Se muestra aquí en una línea individual por razones de formato.

**Interface Number**

Número de interfaz asignado

**Protocol** IP

**Local Client IP Address**
Asocia esta configuración de redundancia con un cliente.

**Valores válidos:** Cualquier dirección IP

**Valores por omisión:** 0.0.0.0

**Select Redundancy ESI**
Especifica si debe utilizarse como componente Identificador de sistema final de la dirección CIPC o CIPS ATM la dirección del MAC administrada universalmente o una dirección del MAC configurada bajo la configuración de interfaz ATM. Esta pregunta viene precedida de una lista de ESI válidos entre los que debe realizarse la selección.

**Valores válidos:** El ESI de redundancia debe ser diferente de todos los ESI funcionales del cliente/servidor ARP de tipo primario.

**Valor por omisión:** 1

**Choose Redundancy Selector**
Identifica el byte de selector para la dirección ATM de redundancia.

**Valor válido**: Cualquier valor de un solo octeto que no se haya utilizado anteriormente y se encuentre dentro del rango definido para el dispositivo.

**Valor por omisión:** 00

**Partner's (Redundancy) ATM Address**
Especifica la dirección ATM del Servidor ARP de redundancia.

**Valores válidos:** Sólo son válidas direcciones NSAP privadas. El primer byte (identificador de autorización y formato) debe contener un valor de:

39 — Formato de ATM de Código de datos de país
47 —- Formato de ATM de Designador de código internacional
45 — Formato de ATM de E.164

**Valor por omisión:** Ninguno

**Partner Server ESI**
Especifica el componente ESI de la dirección ATM real del asociado.

**Valores válidos:** Un ESI de servidor válido listado en el menú que precede a esta pregunta.

**Valor por omisión:** 1

**Partner Server Selector**
Especifica el componente selector de la dirección ATM real del asociado.

**Valores válidos:** El valor definido para el selector del servidor

**Valor por omisión:** 00

**Redundancy's default IP gateway also?**
Especifica si esta entidad de ARP participará en la provisión del soporte de la redundancia de la pasarela por omisión para la LIS.

**Valor por omisión:** No

**Redundancy's default IP gateway address**
Especifica la dirección IP de la pasarela por omisión de redundancia para esta LIS. Ésta es la dirección IP configurada en los sistemas principales que utilizan el direccionador como direccionador por omisión.

**Valor por omisión:** 0.0.0.0

## Change

Utilice el mandato **change** para cambiar la configuración de ATM-ARP.

**Sintaxis:**

ch**ange** entry

atm-arp-client-configuration

redundancy

multicast-support

**atm-arp-client-configuration**
Cambia la configuración de cliente ATM ARP.

Consulte la página 649 para obtener una descripción de los parámetros de **Change**.

### Ejemplo para IP:

```
ARP config> change atm-arp-client-configuration
Interface Number [0]?
Protocol [IP]?
Client IP Address [0.0.0.0]? 1.1.1.2
This client is also a server? [Yes] yes
Refresh timeout (in minutes) [20]?
Enable auto-refresh? [Yes]:
Refresh by InAtmArp? [Yes]:
  (  1) Use burned in ESI
  (  2) 111111111111
  (  3) 222222222222
  (  4) 121212121212
  (  5) AAAAAAAAAAAA
Select ESI [1]?2
Use internally assigned selector? [Yes]: no
Selector Only, Page 00..FF [00] ? 11
Validate PCR for best effort VCCs? [No]:
Maximum Reserved Bandwidth for incoming VCCs (Kbps) [0]?
Use Best Effort Server for Control VCCs? [Yes]:
Peak Cell Rate of outbound control VCCs (Kbps) [0]?
Sustained Cell Rate of outbound control VCCs (Kbps) [0]?
Use Best Effort Server for Data VCCs? [Yes]:
Peak Cell Rate of outbound Data VCCs (Kbps) [0]?
Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?
Max SDU size (bytes) [9188]?
Participate in Server Synchronization [No]? yes
Server Group ID [1]?
Do you want to accept sessions from non-configured DCSs [yes]?
Hello Interval [3]
Dead Factor [3]?
(  1) Use burned in ESI
(  2) 111111111111
(  3) 222222222222
(  4) 121212121212
(  5) AAAAAAAAAAAA
Server Synchronization ESI [2]?
Server Synchronization selector, Range 00..FF [00]? 12
Server Synchronization Max SDU size (bytes) [9188]?
Re-registration time with Arp Server (in minutes) [15]?


To enable or change multicast support,

please issue the ADD or CHANGE MULTICAST-SUPPORT command.
```

### Ejemplo para IPX:

```
ARP config> change atm-arp-client-configuration
Interface Number [0]?
Protocol [IP]? IPX
Refresh timeout (in minutes) [5]?
Enable auto-refresh? [Yes]:
  (  1) Use burned in ESI
Select ESI [1]?
Use internally assigned selector? [No]:
Selector Only, Range 00..FF [00]? 20
Validate PCR for best effort VCCs? [No]:
Maximum Reserved Bandwidth for incoming VCCs (Kbps) [0]?
Use Best Effort Server for Data VCCs? [Yes]:
Peak Cell Rate of outbound data VCCs (Kbps) [0]?
Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?
Max SDU size (bytes) [9188]?
```

Puesto que sólo existe un registro de configuración de cliente IPX ATM-ARP para una interfaz ATM, no se le solicita que entre una dirección de protocolo.

**Ejemplo para la función de puente**:

```
ARP config> change atm-arp-client-configuration
Interface Number [0]?
Protocol [IP]? asrt
Client Address (Port Number) [0]? 2    1
  (  1) Use burned in ESI
Select ESI [1]?
Use internally assigned selector? [No]:
Selector Only, Range 00..FF [0A]?
Validate PCR for best effort VCCs? [No]:
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]?
Max SDU size (bytes) [9188]?
```

**Nota:** 1 En el caso de la función de puente, se le solicita un número de puerto en lugar de una dirección de protocolo.

Además, si se va a utilizar soporte de SVC para un puerto en particular, no debe utilizarse un selector asignado internamente para el cliente correspondiente. El usuario debe especificar el selector con el fin de que se conozca definitivamente la dirección ATM de este cliente para la configuración en el otro extremo.

El uso de este mandato sólo es necesario si desea utilizar valores diferentes de los valores por omisión para los parámetros de tráfico.

**redundancy**

Cambia la configuración de la redundancia para un cliente.

Vea la página 657 para obtener una descripción de los parámetros que puede cambiar.

## Delete

Utilice el mandato **delete** para suprimir un servidor ARP, una configuración de cliente ATM ARP, una entrada de PVC ATM ARP o una entrada de SVC ATM ARP.

**Sintaxis:**

| | |
|---|---|
| de**lete** | arp-server |
| | atm-arp-client-configuration |
| | pvc-atm-arp-entry |
| | svc-atm-arp-entry |
| | redundancy |
| | mars-server |

**arp-server**

Suprime un servidor ARP o DCS.

Especifique la dirección del servidor ARP. Esta pregunta viene precedida de una lista de servidores ARP o DCS válidos entre los que debe realizarse la selección.

**Valores válidos**: Cualquiera de los valores listados en el menú que precede a esta pregunta.

**Valor por omisión**: 0

**Ejemplo para IP**:

```
ARP config> del arp-server

ATM Arp Remote Server List:
   IP Address      Number       Address / Sub Address
        1.1.1.1     [ 1]       39.84.0F.00.00.00.00.00.00.00.00.00.02.
                                                  11.11.11.11.11.11.11
        1.1.1.1     [ 2]       39.84.0F.00.00.00.00.00.00.00.00.00.03.
                                                  AA.AA.AA.AA.AA.AA.AA

Number of the IP Address/Arp Server pair to be deleted
Default of 0 will delete nothing [0]? 1
```

**atm-arp-client-configuration**

Suprime una configuración de cliente ATM ARP para un cliente.

Especifique el número de interfaz, el protocolo y la dirección IP de cliente.

**interface number**

**Valores válidos**: Cualquier interfaz definida

**Valor por omisión**: 0

**protocol** **Valores válidos:** *IP*, *IPX* **o** *ASRT*

**Valor por omisión**: IP

**client IP address**

**Valores válidos**: Cualquier dirección IP válida

**Valor por omisión**: 1.1.1.100

**Ejemplo para IP**:

```
ARP config> del atm-arp-client-configuration
Interface Number [0]?
Protocol [IP]?
Client IP Address [1.1.1.100]? 2.2.3.100
ATM ARP Client Config record deleted
```

**Ejemplo para IPX**:

```
ARP config> del atm-arp-client-configuration
Interface Number [0]?
Protocol [IP]? IPX
ATM ARP Client Config record deleted
```

Puesto que sólo existe un registro de configuración de cliente IPX ATM-ARP para una interfaz ATM, no se le solicita que entre una dirección de protocolo.

Respecto a las descripciones de los campos, consulte el ejemplo anterior para IP.

**Ejemplo para la función de puente**:

```
ARP config> del atm-arp-client-configuration
Interface Number [0]?
Protocol [IP]? ASRT
Clients for this protocol can only be changed here.
Deletions must be done under ASRT Config by deleting a port.
```

**pvc-atm-arp entry**

Suprime una entrada de PVC ATM ARP.

Especifique el número de entrada para la entrada de PVC ATM ARP que desee suprimir.

**Ejemplo para IP e IPX**:

```
ARP config> del pvc

ATM Arp Permanent Virtual Circuit Definitions
No. IF# Prot# P/S     Protocol     -> VPI / VCI
1    0    0    P         0.0.0.0   ->  00 / 0029
2    0    7    P 00.00.00.00.00.00 ->  00 / 0037
Which Arp entry do you want to delete [0]? 1
ATM Arp entry 1 being deleted
```

El núm. 1 es un PVC IP y el núm. 2 es un PVC IPX.

**Ejemplo para la función de puente**:

```
ARP config> del pvc
ATM Arp Permanent Virtual Circuit Definitions
No. IF# Prot# P/S     Protocol     -> VPI / VCI    (Client Address)
1    0   23    P                   ->   0 / 87     (Port: 1)
Which Arp entry do you want to delete [0]? 1
Channels for this protocol must be deleted under ASRT Config by
deleting a port.
```

**svc-atm-arp-entry**

Suprime una entrada de SVC ATM ARP.

Especifique el número de entrada para la entrada de SVC ATM ARP que desee suprimir.

**Ejemplo para IP e IPX**:

```
ARP config> del svc

ATM Arp Switched Virtual Circuit Definitions
No. IF# Prot# P/S     Protocol     -> Destination ATM Address
1    0    0    S         0.0.0.0   ->
                39.84.0F.00.00.00.00.00.00.00.00.00.02.10.00.5A.00.DE.AD.03
2    0    7    P 00.00.00.00.00.00 ->
                39.84.0F.00.00.00.00.00.00.00.00.00.02.11.00.B7.38.AA.BB.12

Which Arp entry do you want to delete [0]? 1
ATM Arp entry 1 being deleted
```

El núm. 1 es un SVC IP y el núm. 2 es un SVC IPX.

**Ejemplo para la función de puente**:

```
ARP config>del svc
ATM Arp Switched Virtual Circuit Definitions
No. IF        Prot    P/S     Protocol     -> Destination ATM Address (Client)
2    0   23    S                    -> 39.11.22.33.44.55.66.77.88.99.00.11.22
                                    33.44.55.66.77.88.99 (Port: 2)
Which Arp entry do you want to delete [0]? 2
Channels for this protocol must be deleted under ASRT Config by deleting a port.
```

**redundancy**

Suprime la configuración de la redundancia para un cliente.

## Disable

Utilice el mandato **disable** para inhabilitar la auto renovación de entradas de ARP.

El valor de *auto-refresh* de la configuración queda alterado temporalmente por el valor de *auto-refresh* de la configuración de cliente ATM ARP. Consulte la página 649 para obtener información sobre los parámetros de configuración de cliente ATM ARP.

**Sintaxis:**

| | |
|---|---|
| di**sable** | auto-refresh |

**auto-refresh**

Inhabilita la auto renovación de una entrada de ARP.

**Valores válidos**: Yes o No

**Valor por omisión**: Yes para un cliente, No para un Servidor

## Enable

Utilice el mandato **enable** para habilitar la auto renovación de entradas de ARP.

El valor de *auto-refresh* de la configuración queda alterado temporalmente por el valor de *auto-refresh* de la configuración de cliente ATM ARP. Consulte la página 649 para obtener información sobre los parámetros de configuración de cliente ATM ARP.

**Sintaxis:**

**enable** auto-refresh

**auto-refresh**

Habilita la auto renovación de una entrada de ARP.

**Valores válidos**: Yes o No

**Valor por omisión**: No para un cliente, Yes para un Servidor

## List

Utilice el mandato **list** para visualizar el contenido de la configuración de ARP del direccionador que se ha almacenado en la SRAM. El mandato list también visualiza los valores actuales para el temporizador de uso y renovación.

**Sintaxis:**

**list** entry
all
arp-servers
atm-arp-client-configuration
pvc-atm-arp-entry
svc-atm-arp-entry
redundancy
mars-servers

**all** Lista la configuración de ARP seguida de todas las entradas de ARP.

**Ejemplo:** `list all`

```
ARP config> list all
ARP configuration:

Refresh timeout: 5 minutes
Auto refresh: disabled

Mac address translation configuration

No arp entries defined

ATM Arp Server List:
  IP Address      Number       Address / Sub Address
 1.1.1.1     [ 1]       39.84.0F.00.00.00.00.00.00.00.00.00.02.
                                     11.11.11.11.11.11.11
 1.1.1.1     [ 2]       39.84.0F.00.00.00.00.00.00.00.00.00.03.
                                     AA.AA.AA.AA.AA.AA.AA
```

### arp-servers

Lista los servidores ARP. Si es una configuración de sólo cliente, esta salida lista los Servidores ARP configurados. Si es una configuración de Servidor ARP distribuido, se listan los Servidores conectados directamente que se hayan configurado. Consulte la sección “Visión general del Servidor ARP distribuido” en la página 637 para obtener una explicación de la comunicación entre los Servidores ARP distribuidos.

```
ARP config> list arp-servers

ATM Arp Remote Server List:
   IP Address      Number       Address / Sub Address
        1.1.1.1     [ 1]       39.84.0F.00.00.00.00.00.00.00.00.00.02.
                                        11.11.11.11.11.11.11
        1.1.1.1     [ 2]       39.84.0F.00.00.00.00.00.00.00.00.00.03.
                                        AA.AA.AA.AA.AA.AA.AA
```

### atm-arp-client-configuration

Lista la configuración de los clientes ATM ARP.

```
ARP config> list atm

ATM Arp Clients:

-----------------------------------------------------

If: 0  Prot: 0  Addr: 1.1.1.2          ESI: 11.11.11.11.11.11  Sel: 11
Server: yes  Refresh T/O: 20   AutoRefr: yes   By InArp: yes  Validate PCR: no
Use Best Effort: yes/yes  (Control/Data)   Max B/W(kbps):      0
Cell Rate(kbps):  Peak:      0/     0      Sustained:      0/     0
Max SDU(bytes):   9188
Server Synchronization: yes  SGID: 1       Secure DCSs: no
Hello Interval: 3    Dead Factor: 3
Server Synchronization ESI: 11.11.11.11.11.11   Selector: 12
Server Synchronization Max SDU(bytes):   9188
Arp Server Re-registration time in (minutes): 15
Multicast Support: no    Broadcast Support: no
```

Consulte la página 649 para las descripciones de los campos.

### redundancy

Lista las configuraciones de la redundancia y el estado de la pasarela.

```
ARP config>list red


ATMARP Clients with Redundancy Configured
-----------------------------------------

If:  0    Prot: IP    Addr: 1.1.1.2
Red. ESI: bb.bb.bb.bb.bb.bb   Red. SEL: bb   Pri/Secy: Secondary
Partner's (Red.) ATM Address:  39.84.0F.00.00.00.00.00.00.00.00.01.aa.aa.aa.aa.aa.aa.aa
Partner Server ESI: BB.BB.BB.BB.BB.BB Partner Server SEL: AA
Redundancy Default IP Gateway Address: 1.1.1.3
-----------------------------------------
```

```
ARP config>list red


ATMARP Clients with Redundancy Configured
-----------------------------------------

If:  0    Prot: IP    Addr: 2.2.2.2
Red. ESI: aa.aa.aa.aa.aa.aa  Red. SEL: aa   Pri/Secy: Primary
Partner's (Red.) ATM Address:  39.84.0F.00.00.00.00.00.00.00.00.01.bb.bb.bb.bb.bb.bb.bb
Partner Server ESI: BB.BB.BB.BB.BB.BB Partner Server SEL: AA
Redundancy Default IP Gateway Address: 1.1.1.3
-----------------------------------------
```

**If:** Número de interfaz

**Prot:** IP

**Addr:** Dirección IP

**Red. ESI:** Identifica la parte de ESI de la dirección ATM de redundancia:

Incorporado - Especifica que debe utilizarse la dirección del MAC administrada universalmente del adaptador de ATM como la parte de Identificador de sistema final (ESI) de la dirección ATM de redundancia.
Administrado localmente - Identifica un Identificador de sistema final administrado localmente que debe utilizarse como componente ESI de la dirección ATM de redundancia.

**Red. SEL:**
Identifica la parte de Selector de la dirección ATM de redundancia.

**Peer Redundancy/Primary/Secondary**
Identifica el papel del cliente/servidor.

Si es primario, el cliente/servidor colocará una llamada desde su dirección ATM de redundancia a la dirección ATM de redundancia del secundario.

Si es secundario, este cliente/servidor estará desocupado mientras esté establecida la VCC de redundancia.

Si es similar, coloca la llamada el servidor con la dirección ATM de redundancia mayor.

**Partner's (Red.) ATM Address:**
Especifica la dirección ATM de redundancia del cliente/servidor asociado.

**Partner Server ESI:**
Identifica un ESI administrado localmente que debe utilizarse como componente ESI de la dirección ATM del Servidor ARP asociado cuando falle el Servidor ARP.

**Partner Server SEL:**
Identifica la parte de Selector del ESI y selector de servidor asociado que está configurada en el direccionador asociado.

**Redundancy Default IP Gateway Address:**
Especifica la dirección de pasarela IP por omisión. Es la dirección de pasarela por omisión configurada en los clientes a los que sirve este Servidor ARP. La definición de esta dirección permite que el Servidor ARP proporcione la función de direccionamiento desde una subred a otra.

**pvc-atm-arp-entry**

Lista los PVC ARP.

```
ARP config> list pvc

ATM Arp Permanent Virtual Circuit Definitions


No. IF# Prot# P/S    Protocol   -> VPI / VCI
1    0    0    P      0.0.0.0   ->  00 / 0029   2    0   23    P ->  00 / 0068
```

**No.** Número de VCC

**IF#** Número de interfaz

**Prot#** Número de protocolo (Prot# 0 = IP, 7 = IPX, 23=ASRT)

**P/S:** P para PVC, S para SVC

**Protocol** Dirección IP (número de sistema principal IPX si el protocolo es IPX)

**VPI/VCI** El valor decimal del canal definido.

**svc-atm-arp-entry**

Lista los SVC ARP.

```
ARP config> list svc

ATM Arp Switched Virtual Circuit Definitions


No. IF# Prot# P/S     Protocol     -> Destination ATM Address
2    0    0    S         0.0.0.0   ->
                    39.84.0F.00.00.00.00.00.00.00.00.02.10.00.5A.00.DE.AD.03
```

**No** Número de VCC

**IF#** Número de interfaz

**Prot#** Número de protocolo (Prot# 0 = IP, 7 = IPX, 23=ASRT)

**P/S:** P para PVC, S para SVC

**Protocol** Dirección IP (número de sistema principal IPX si el protocolo es IPX)

**Destination ATM Address**

Dirección ATM de destino

## Reorder

Utilice el mandato **reorder** para seleccionar el Servidor ARP primario entre una lista de Servidores ARP. Este mandato es útil para los que son clientes solamente.

**Sintaxis:**

**reorder arp**

**Ejemplo: `reorder arp`**

```
    ATM Arp Remote Server List:
       IP Address      Number       Address / Sub Address
            1.1.1.1     [ 1]       39.84.0F.00.00.00.00.00.00.00.00.02.
                                                 11.11.11.11.11.11.11
            1.1.1.1     [ 2]       39.84.0F.00.00.00.00.00.00.00.00.03.
                                                 AA.AA.AA.AA.AA.AA.AA
Number of the IP Address/Arp Server ATM Address pair to be made Primary
Default of 1 will change nothing [1]?
```

## Set

Utilice el mandato **Set** para establecer el valor de temporizador de renovación (en minutos). Caducarán entradas de ARP después de este número de minutos si no se renuevan.

**Sintaxis:**

**set** refresh-timer

**refresh-timer**

Especifica el valor para el temporizador de duración de entradas de ARP.

**Valores válidos**: Un número entero de minutos dentro del rango del 0 al 65535

**Valor por omisión**: 5

---

# Configuraciones de ARP de muestra

Las configuraciones de muestra muestran la secuencia completa de sucesos para esa configuración.

## Configuración de la redundancia de Servidor ARP en una LIS con Servidor ARP no distribuido

**Configuración de un asociado**

La muestra siguiente facilita la configuración de un Servidor ARP para la redundancia de Servidor ARP.

Notas:

1. Añadir el dispositivo ATM físico
2. Añadir los ESI administrados localmente
3. Añadir la dirección IP a utilizar para el servidor
4. Empezar la configuración de ARP
5. Definir un cliente ATM ARP
6. Definir el Servidor ARP
7. Utilizar el ESI administrado localmente
8. Empezar la configuración de la redundancia para la dirección IP 1.1.1.1

```
Config (only)>add device atm        1
Device Slot #(0-3) [0]?
Adding CHARM ATM Adapter device in slot 0  port 1 as interface #0
Use "net 0" to configure CHARM ATM Adapter parameters
Config (only)>net
Network number [0]?
ATM user configuration
ATM Config>int
ATM interface configuration
ATM Interface Config>add esi   2
ESI in 00.00.00.00.00.00 form []? 11.11.11.11.11.11
ATM Interface Config>add esi
ESI in 00.00.00.00.00.00 form []? aa.aa.aa.aa.aa.aa
ATM Interface Config>exit
ATM Config>exit
Config (only)>p ip
Internet protocol user configuration
IP config>add addr    3
Which net is this address for [0]?
New address [0.0.0.0]? 1.1.1.1
Address mask [255.0.0.0]?
IP config>exit

Config (only)>p arp   4 .
ARP user configuration
ARP config>add atm   5
Interface Number [0]?
Protocol [IP]?
Client IP Address [0.0.0.0]? 1.1.1.1
This client is also a server? [No]: yes   6
Refresh timeout (in minutes) [20]?
Enable auto-refresh? [Yes]:
Refresh by InAtmArp? [Yes]:
  (  1) Use burned in ESI
  (  2) 111111111111
  (  3) AAAAAAAAAAAA
Select ESI [1]? 2      7
Use internally assigned selector? [Yes]: n
Selector Only, Range 00..FF [00]? 11
Validate PCR for best effort VCCs? [No]:
Maximum Reserved Bandwidth for incoming VCCs (Kbps) [0]?
Use Best Effort Server for Control VCCs? [Yes]:
Peak Cell Rate of outbound control VCCs (Kbps) [0]?
Sustained Cell Rate of outbound control VCCs (Kbps) [0]?
Use Best Effort Server for Data VCCs? [Yes]:
Peak Cell Rate of outbound Data VCCs (Kbps) [0]?
Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?
Max SDU size (bytes) [9188]?
Participate in Server Synchronization [N]?
Re-registration time with Arp Server (in minutes) [15]?
ARP config>add red      8
Interface Number [0]?
Protocol [IP]?
Local client IP Address [0.0.0.0]? 1.1.1.1
Note: Local Redundancy ESI must be different from the Primary Server ESI
  (  1) Use burned in ESI
  (  2) 111111111111
  (  3) AAAAAAAAAAAA
Select Local Redundancy ESI [1]? 3
Local Redundancy selector, Range 00..FF [00]? aa
Partner's (Redundancy) ATM Address, 40 Hex digits
[0000000000000000000000000000000000000000]?
39.84.0F.00.00.00.00.00.00.00.00.01.bb.bb.bb.bb.bb.bb.bb

Redundancy default IP Gateway also ? [Yes]:
If Yes, Redundancy default IP Gateway protocol address [0.0.0.0]? 1.1.1.3
ARP config>exit
Config (only)>reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
  EXIT, reload requested
```

### Configuración del Asociado

La muestra siguiente facilita la configuración del asociado para la redundancia de Servidor ARP.

Notas:

1. Añadir el dispositivo ATM físico
2. Añadir los ESI administrados localmente
3. Empezar la configuración de ARP
4. Ésta es la definición de cliente
5. Cuando es secundario, definir como sólo cliente (si no, es una LIS con Servidor ARP distribuido). Si es un Servidor ARP distribuido, el asociado puede definirse como LIS con Servidor ARP distribuido.
6. Utilizar el ESI administrado localmente
7. Definir el Servidor ARP
8. Empezar la configuración de la redundancia para la dirección IP 1.1.1.2
9. Definir el secundario

```
Config (only)>add device atm  1
Device Slot #(0-3) [0]?
Adding CHARM ATM Adapter device in slot 0  port 1 as interface #0
Use "net 0" to configure CHARM ATM Adapter parameters
Config (only)>net
Network number [0]?
ATM user configuration
ATM Config>int
ATM interface configuration
ATM Interface Config>add esi
ESI in 00.00.00.00.00.00 form []? 11.11.11.11.11.11
ATM Interface Config>add esi  2
ESI in 00.00.00.00.00.00 form []? bb.bb.bb.bb.bb.bb
ATM Interface Config>exit
ATM Config>exit
Config (only)>p ip
Internet protocol user configuration
IP config>add addr
Which net is this address for [0]?
New address [0.0.0.0]? 1.1.1.2
Address mask [255.0.0.0]?
IP config>exit
```

```
Config (only)>p arp  3
ARP user configuration
ARP config>add atm   4
Interface Number [0]?
Protocol [IP]?
Client IP Address [0.0.0.0]? 1.1.1.2
This client is also a server? [No]: no   5
Refresh timeout (in minutes) [5]?
Enable auto-refresh? [no]:
Refresh by InAtmArp? [no]:
  (  1) Use burned in ESI
  (  2) 111111111111
  (  3) BBBBBBBBBBB
Select ESI [1]? 1   6
Use internally assigned selector? [Yes]: y
Validate PCR for best effort VCCs? [No]:
Maximum Reserved Bandwidth for incoming VCCs (Kbps) [0]?
Use Best Effort Server for Control VCCs? [Yes]:
Peak Cell Rate of outbound control VCCs (Kbps) [0]?
Sustained Cell Rate of outbound control VCCs (Kbps) [0]?
Use Best Effort Server for Data VCCs? [Yes]:
Peak Cell Rate of outbound Data VCCs (Kbps) [0]?
Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?
Participate in Server Synchronization  (Y or N) [N]?    N
Max SDU size (bytes) [9188]?
Re-registration time with Arp Server (in minutes) [15]?
ARP config> add arp-server private-nsapa 7
Local Client IP Address [0.0.0.0]? 1.1.1.2
Private NSAP Address: Specify 40 digits
ATM Address []? 39840F0000000000000000000111111111111111
ARP config>add red   8
Interface Number [0]?
Protocol [IP]?
Local client IP Address [0.0.0.0]? 1.1.1.2
Note: Local Redundancy ESI must be different from the Primary Server ESI
  (  1) Use burned in ESI
  (  2) 111111111111
  (  3) BBBBBBBBBBB
Select Local Redundancy ESI [1]? 3
Local Redundancy selector, Range 00..FF [00]? bb
Partner's (Redundancy) ATM Address, 40 Hex digits
[0000000000000000000000000000000000000000]?
39.84.0F.00.00.00.00.00.00.00.00.01.aa.aa.aa.aa.aa.aa.aa    9
  (  1) Use burned in ESI
  (  2) 111111111111
  (  3) BBBBBBBBBBB
Select Partner Server ESI [1]? 2
Partner selector, Range 00..FF [00]? 11
Redundancy default IP Gateway also ? Yes
If Yes, Redundancy default IP Gateway protocol address [0.0.0.0]? 1.1.1.3
ARP config>exit
Config (only)>reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
  EXIT, reload requested
```

**Notas:**

1. En una LIS con Servidor ARP distribuido, ambos asociados son Servidores ARP distribuidos.
2. La configuración de la redundancia de Servidor ARP es el mismo proceso tanto en el caso del Servidor ARP distribuido como en el caso del Servidor ARP no distribuido.

## Acceso al entorno de supervisión de ARP

Utilice el procedimiento siguiente para acceder a los mandatos de supervisión de ARP. Este proceso le proporciona acceso al proceso de *supervisión* de ARP.

1. En el indicador de OPCON, entre **talk 5**. (Para obtener información más detallada sobre este mandato, consulte “The OPCON Process” en el manual *Guía del usuario de software*.)Por ejemplo:

   ```
   * talk 5
   +
   ```

   Después de que entre el mandato **talk 5**, se visualizará el indicador de GWCON (+) en el terminal. Si no aparece el indicador la primera vez que entre la configuración, pulse **Intro** de nuevo.

2. En el indicador +, entre el mandato **protocol arp** para obtener el indicador ARP>.

   **Ejemplo:**

   ```
   + prot arp
   ARP>
   ```

## Mandatos de supervisión de ARP para redes que no son ATM

Esta sección describe los mandatos de supervisión de ARP para redes que no son ATM. Puede acceder a los mandatos de supervisión de ARP en el indicador ARP>.

**Nota:** Si la carga del software del dispositivo no contiene Asynchronous Transfer Mode (ATM), los mandatos relacionados con ATM no serán válidos ni se visualizarán en los indicadores de configuración y supervisión de ARP.

La Tabla 40 muestra los mandatos.

*Tabla 40. Resumen de los mandatos de supervisión de ARPpara redes que no son ATM*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Clear | Borra la antememoria en relación con una interfaz especificada. |
| Dump | Visualiza la antememoria para una interfaz especificada. |
| Hardware | Lista cada red configurada con ARP. |
| Ping | Verifica la conectividad entre el dispositivo y la estación final especificada. |
| Protocol | Lista cada protocolo configurado con ARP. |
| Statistics | Visualiza la información de ARP. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Clear

Utilice el mandato **clear** si desea vaciar la antememoria de ARP en relación con una interfaz de red determinada. El mandato **clear** puede utilizarse para forzar la supresión de transacciones incorrectas.

Para borrar una interfaz en particular, entre el número de interfaz o red como parte del mandato. Para obtener el número de interfaz, utilice el mandato de CONFIG **list devices**.

**Sintaxis:**

c**lear** *núm. interfaz*

**Ejemplo:** `clear 1`

## Dump

Utilice el mandato **dump** si desea visualizar la antememoria de ARP para una combinación de red/protocolo determinada. Con el fin de visualizar la antememoria de ARP para una interfaz en particular, entre el número de interfaz o red como parte del mandato. Para obtener el número de interfaz, utilice el mandato de CONFIG **list devices**.

Si hay más de un protocolo en esta red, también debe facilitarse el número de protocolo. Ello hace que la supervisión visualice las correlaciones de dirección de hardware con protocolo almacenadas en esta base de datos. Si solamente un protocolo utiliza ARP en la interfaz especificada, el número de protocolo es opcional. Para obtener el número de protocolo, utilice el mandato de CONFIG **protocol**.

La visualización del mandato **dump** muestra la dirección de hardware, la dirección de protocolo y el parámetro de temporizador de renovación para cada correlación.

**Sintaxis:**

d**ump** *núm. interfaz núm. protocolo*

**Ejemplo:** `dump 2 ip`

```
Hardware Address    IP Address      Refresh
02-07-01-00-00-01   192.9.1.2       Permanent
a1-b2-c3-4d-5e-6f   128.185.214.36  5
100                 128.185.123.51  Not Aging
16                  128.185.214.38  Not Aging
```

Los parámetros válidos de temporizador de renovación son:

**Permanent**
: Una correlación entre dirección de hardware y dirección de protocolo configurada estáticamente (entrada mediante el mandato de ARP **add entry** o el mandato de frame-relay **add protocol** o el mandato de X25 **add address**). Estas entradas no caducan ni se sobregraban con correlaciones aprendidas dinámicamente.

**minutes to expire**
: El número de minutos hasta que esta correlación caduque por la duración o hasta que se renueve (si está habilitada la auto renovación). Este parámetro se expresa como valor numérico.

**Not Aging**

Una correlación de SVC o PVC fija aprendida por medio de Inverse ARP. Sólo empieza a tener duración cuando se desactiva el circuito. La correlación puede sobregrabarse con una dirección aprendida de nuevo y puede borrarse mediante el mandato de supervisión de ARP **clear**.

## Hardware

Utilice el mandato **hardware** para visualizar las redes registradas con ARP. El mandato **hardware** lista cada red registrada con ARP y visualiza el espacio de direcciones de hardware (AS de hardware) además de la dirección de hardware local de cada red.

**Sintaxis:**

**hardware**

**Ejemplo:** **hardware**

```
Network       Hardware AS    Hardware Address

1 FR/0          000F            1023
5 TKR/0         0006            00:00:C9:09:32:EF
8 Eth/0         0001            AA-00-04-00-26-14
9 IPPN/0        2048            128.185.214.38
10 BDG/0        0001            00-00-93-90-4C-F7
```

**Nota:** La entrada de IPPN hace referencia a la función de túnel de IP en que el campo de dirección de hardware indica la dirección IP del túnel de IP.

## Ping

Utilice el mandato **ping** para que el direccionador envíe peticiones de eco ICMP a un determinado destino. Para obtener más información sobre el mandato **ping**, consulte el tema “Ping” en la página 350.

## Protocol

Utilice el mandato **protocol** para visualizar (por red) los protocolos que tienen direcciones registradas con ARP. Este mandato visualiza la red, el nombre de protocolo, el número de protocolo, el espacio de direcciones de protocolo (en hexadecimal) y las direcciones de protocolo locales.

**Sintaxis:**

p**rotocol**

**Ejemplo:** **protocol**

```
Network  Protocol (num)  AS    Protocol Address(es)
5 TKR/0  IP       (00)   800    128.185.209.38
6 TKR/1  IP       (00)   800    10.1.181.38
8 Eth/0  IP       (00)   800    128.185.221.38
8 Eth/0  AP2      (22)   80F3   221/38
```

**Nota:** Las entradas de SR hacen referencia al direccionamiento de origen - la dirección de protocolo se utiliza para indicar la dirección del MAC. Utilice el mandato de Red en Anillo **dump** para ver las entradas de los RIF reales.

## Statistics

Utilice el mandato **statistics** para visualizar una variedad de estadísticas sobre el funcionamiento del módulo ARP.

**Sintaxis:**

**statistics**

**Ejemplo:** **statistics**

```
ARP input packet overflows
Net   Count
 PPP/0  0
 PPP/1  0
 TKR/0  0
IPPN/0  0
 BDG/0  0

ARP cache meters
Net Prot  Max Cur Cnt    Alloc  Refresh: Tot  Failure  TMOs: Refresh
0   0     1   1   1       17             0        0               13
0  22     1   0   0        6             0        0                6
1   0     1   1   2       27             0        0               25
1  16     3   3   7      291             0        0                0
2   0     1   0   0        2             0        0                2
2  16     1   0   0        1             0        0                0
8   0     1   1   1       11             0        0               10
```

| | |
|---|---|
| ARP input packet overflows | Visualiza los contadores que representan el número de paquetes ARP desechados en entrada porque la capa de ARP estaba demasiado ocupada. Las cuentas se muestran por interfaz de red. |
| ARP cache meters | Consta de una variedad de medidores relativos al funcionamiento de la antememoria de ARP. Todas las cuentas se muestran por protocolo y por interfaz. |
| Net | Visualiza los números de interfaz. |
| Prot | Visualiza los números de protocolo. |
| Max | Visualiza la longitud máxima permanente de la cadena de totales de control. |
| Cur | Visualiza la longitud máxima actual de la cadena de totales de control. |
| Cnt | Visualiza la cuenta de entradas que actualmente están activas. |
| Alloc | Visualiza la cuenta de entradas creadas. |
| Rfrsh:Tot | Visualiza el número de peticiones de renovación enviadas para esta interfaz de red y este protocolo. |
| Fail | Visualiza el número de anomalías producidas en intentos de auto renovación debido a la falta de disponibilidad de los recursos internos. Esta cuenta no hace referencia a si una entrada se ha renovado o no. |
| TMOs:Rfrsh | Visualiza la cuenta de entradas suprimidas debido a un tiempo de espera excedido del temporizador de renovación. |

# Mandatos de supervisión de ARP sobre ATM

Esta sección describe los mandatos de supervisión de ARP sobre ATM (CIP). Describe los mandatos de supervisión para:

- IP clásico y ARP sobre ATM
- IPX sobre ATM
- La función de puente de 1483

Los mandatos de supervisión relativos a IPX sobre ATM son básicamente los mismos que los relativos a IP clásico y ARP. La diferencia principal es el formato de las direcciones de protocolo:

- Las direcciones de protocolo para IP se especifican como campos de 4 bytes en notación decimal con puntos.
- Las direcciones de protocolo para IPX se especifican como campos de 6 bytes en caracteres hexadecimales.

**Nota:** El mandato **ping** para IPX sobre ATM es diferente del utilizado para IP clásico y ARP. La versión del mandato **ping** de IPX está disponible en la supervisión de IPX. Puede acceder a los mandatos de supervisión de ARP en el indicador `ARP>`. La Tabla 41 muestra los mandatos.

Para obtener más información, consulte “IP clásico y ARP sobre ATM (RFC 1577)” en la página 629 y “Visión general de IPX y ARP sobre ATM (RFC 1483)” en la página 641. Para conseguir información adicional sobre ARP sobre ATM e ilustraciones que muestren configuraciones de redes lógicas y físicas, consulte el manual *Guía del usuario del programa de configuración para productos Nways Multiprotocol and Access Services*.

Puesto que la función de puente no utiliza ARP, la supervisión sólo puede utilizarse para comprobar el estado de un canal asociado con un puerto de puente. Además, dado que la función de puente no utiliza direcciones de protocolo, sólo se visualiza con un canal el número de puerto para el puerto asociado (local).

*Tabla 41. Resumen de los mandatos de supervisión de ARP sobre ATM*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Delete | Desactiva inmediatamente un canal activo. Puede activarse o no un nuevo canal para sustituir el antiguo según las condiciones. |
| Display | Visualiza todos los canales (VCC) asociados con una interfaz ATM individual. |
| Dump | Muestra qué canales ATM deben utilizarse para enviar datagramas y muestra sus direcciones IP correspondientes. |
| Hardware | Lista cada red configurada con ARP. |
| Ping | Verifica la conectividad entre el dispositivo y la estación final especificada. |
| Protocol | Lista cada protocolo configurado con ARP. |
| Redundancy-State | Visualiza los clientes IP configurados con redundancia. |
| Statistics | Visualiza las estadísticas del código de ARP sobre todas las interfaces de red. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Activate

Utilice el mandato **activate** para activar los PVC o los SVC configurados de IP clásico y de IPX sobre RFC 1483 sin tener que rearrancar el dispositivo.

**Sintaxis:**

ac**tivate** channel

pvc

svc

**channel** Activa los PVC y los SVC.

*all* Utilice *all* para indicar que el mandato se aplica a todas las interfaces.

*specific* Activa los canales del número de interfaz de red que se proporcione.

**pvc** Sólo activa los PVC.

*all* Utilice *all* para indicar que el mandato se aplica a todas las interfaces.

*specific* Activa los PVC del número de interfaz de red que se proporcione.

**svc** Sólo activa los SVC.

*all* Utilice *all* para indicar que el mandato se aplica a todas las interfaces.

*specific* Activa los SVC del número de interfaz de red que se proporcione.

**Ejemplo:**

```
ARP>  activate chan spec 0
ATM Arp PVC/SVC(s) Activated:

No. IF# Prot# P/S Protocol  -> VPI/VCI or Dest ATM Addr (Client Addr)
 2   0    0    P  4.2.11.2  -> 00/924
 3   0    0    S            ->39.84.0F.00.00.00.00.00.00.00.00.00.01.10.00.5A.00.AB.CD.C8(Ip 4.2.2.0)
```

**No** Especifica el número de VCC.

**IF#** Especifica el número de interfaz.

**PROT#** Especifica el número de protocolo:

- IP = 0
- IPX = 7

**P/S** P indica PVC. S indica SVC.

**Protocol** Especifica la dirección IP de destino o el número de sistema principal IPX.

**VPI/VCI or Dest ATM Addr** Especifica el par VPI/VCI del PVC definido o bien la dirección ATM de destino del SVC.

## Delete

Utilice el mandato **delete** para desactivar inmediatamente un canal activo. Puede activarse o no un nuevo canal para sustituir el antiguo según las condiciones.

Suprima un canal específico de la lista de canales activos. Debe ir con mucha precaución cuando invoque esta opción. Se suprime el canal especificado por el par VPI/VCI si se encuentra en la lista de canales activos. Antes de la supresión, se libera el canal con un código de causa de suspensión normal. También se suprimen todas las entradas de ARP dependientes de este canal en particular.

**Sintaxis:**

de**lete**

**Ejemplo: `delete`**

```
ARP> del 0
VPI, Range 00..FF [00]?
VCI, Range 0000..FFFF [0000]? 0020
Channel found and deleted
```

## Display

Utilice el mandato **display** para visualizar todos los canales (VCC) asociados con una interfaz ATM individual.

**Sintaxis:**

di**splay**

**Ejemplo: `display`**

```
ARP> display 0
Active Channel List : Net 0
   P/S FLAGS LIST  VPI/VCI    FwdPcr    FwdScr     MaxSDUsz Control P2P
  0) S   80    01   00/0020  155000000 155000000      9188      T     T
        Tgt Addr. 39.84.0F.00.00.00.00.00.00.00.00.02.10.00.5A.00.DE.AD.02
        Client Address (owner): 1.1.1.100
        Target Protocol Addresses: 1.1.1.2
New Channel List : Net 0
PVC Channel List : Net 0
   P/S FLAGS LIST  VPI/VCI    FwdPcr    FwdScr     MaxSDUsz Control P2P
  1) P   80    03   00/0085  155000000 155000000      9188      F     T
        Tgt Addr:
        Client Address (owner): 3.5.5.5
        Target Protocol Addresses: 3.4.4.4
```

**P/S** P significa que este canal es un PVC. S significa que este canal es un SVC.

**List** Para el uso interno.

**Flags** Para el uso interno.

**VPI/VCI** El identificador de vía de acceso virtual y el identificador de canal virtual del canal en uso.

**FwdPcr** La velocidad punta de célula en bits por segundo.

**FwdScr** La velocidad sostenida de célula en bits por segundo.

**MaxSDUsz**
El tamaño máximo de SDU para este canal. Todos los paquetes transmitidos o recibidos sobre esta interfaz deben tener un tamaño inferior o

igual a este tamaño menos el prefijo de cabecera de 8 bytes utilizado por RFC 1483.

**Control** T si es un canal de control (canal para el servidor ARP). F si es un canal de datos (canal para otro cliente).

**P2P** T si este canal es punto a punto. F si este canal es punto a multipunto.

**Active Channel List**
Estos canales son conexiones verdaderas con la parte remota. Pueden fluir datos sobre estas conexiones con los parámetros de tráfico mostrados.

**New Channel List**
Estos canales están en proceso de conectarse con el otro extremo. No pueden fluir datos sobre los mismos hasta que se trasladen a la lista de activos.

**PVC Channel List**
Son canales que se han configurado específicamente como PVC. Toman las características de cliente para los canales de datos definidos en la configuración de cliente.

**Client Address**
Es la dirección de protocolo del cliente local conectado a esta VCC.

**Target Protocol Address**
Es la dirección de protocolo del cliente remoto conectado a esta VCC.

## Dump

Utilice el mandato **dump** para mostrar qué canales ATM deben utilizarse al enviar datagramas y para mostrar sus direcciones IP de destino correspondientes.

Esta tabla representa toda la tabla de ARP para una red ATM física que ejecuta IP clásico. La dirección de hardware es el identificador de VCC resultante (VPI/VCI) para un canal activo. Es decir, todo el tráfico que deba enviarse a la dirección IP se transmitirá sobre el canal asociado (listado bajo Hardware Address).

**Nota:** Si el sistema principal del otro extremo del canal envía una petición o una respuesta con su propia dirección, el tiempo de renovación se restablecerá automáticamente en su valor máximo.

**Sintaxis:**

du**mp**

**Ejemplo:** **dump**

```
 ARP>du 0
Hardware Address  IP Address          Refresh      Origin Srvrid   Seq number
  0/0               1.1.1.1           19               1.1.1.1      868997267
  0/0               1.1.1.2           permanent        1.1.1.2      868997028
  0/0               1.1.1.3           permanent        1.1.1.2      868997028
  0/35              1.1.1.5           20               1.1.1.2      868997042
```

Bajo Refresh, el tiempo especificado es el tiempo aproximado antes de que la entrada de ARP caduque (en minutos). Si se activa la auto renovación, se emitirá una petición ARP o una petición InATMARP 30 segundos antes de la caducidad. Si se recibe una respuesta antes de la caducidad, se restablece el tiempo de Refresh y la entrada de ARP permanece. Si no se recibe respuesta o si se desactiva la

auto renovación, la entrada de ARP se suprimirá cuando caduque. Volverá a crearse cuando se necesite.

A continuación, se indican estados válidos para Refresh:

**Hardware Address**
Especifica las direcciones de hardware registradas con ARP. Si aparece “0/0” bajo Hardware Address, significa que no existe un canal abierto para esta entrada de ARP.

**Estados para Refresh**

- 
- Si aparece “resolve only” bajo Refresh, significa que esta entrada de ARP sólo existe para resolver la dirección ATM de la dirección IP determinada. Estas entradas se utilizan para el registro con el servidor ARP (registro de 2225).
- Si aparece “not aging” bajo Refresh, la entrada permanecerá un tiempo indefinido.

**Origin Server Id**
El ID de DCS (dirección IP para los productos de IBM) del servidor que ha originado esta entrada de antememoria. Es posible que, si un cliente se registra con diversos servidores, haya más de una entrada de antememoria para la dirección IP de este cliente. Habrá una entrada para cada servidor con el que se registre el cliente, pero cada una tendrá un Origin ID diferente.

**Seq. Number**
El número de secuencia actual de la entrada de antememoria de SCSP correspondiente (en decimal). Este número debe coincidir en todos los servidores del grupo de servidores para esta entrada de antememoria en particular.

## Hardware

Utilice el mandato **hardware** para listar todas las direcciones ATM asociadas con cada cliente IP configurado.

**Sintaxis:**

h**ardware**

**Ejemplo:** **`hardware`**

```
ARP> hardware
    Network         Hardware AS     Hardware Address
    0 ATM/0         0013            39.84.0F.00.00.00.00.00.00.00.00.00.01.
                                    10.00.5A.00.DE.AD.C8  (IP 1.1.1.100)
    1 IPPN/0        0800            1.1.1.100
```

**Network:** El número de red física.

**Hardware AS:**
El tipo de hardware utilizado en los paquetes ARP para clasificar esta red. Para ARP sobre ATM, el tipo de AS es 0x13 (decimal 19).

**Hardware Address:**
La dirección de hardware. Normalmente, esta dirección es una dirección del MAC para otras redes, pero para ATM es la dirección ATM asociada

con un cliente específico. En el ejemplo, se accede al cliente IP, 1.1.1.100, llamando a la dirección ATM correspondiente 39.84.0F.00.00.00.00.00.00.00.00.00.01.10.00.5A.00.DE.AD.C8.

## Ping

Utilice el mandato **ping** para verificar la conectividad entre el dispositivo y la estación final especificada.

Ping funciona exactamente igual que en cualquiera de las otras redes. Emite una petición de eco ICMP cada segundo y visualiza las estadísticas de las respuestas correspondientes. Tenga en cuenta que la dirección de origen de la petición contendrá la dirección del cliente que coincida más con la subred del destino.

**Sintaxis:**

pi**ng**

**Ejemplo: `ping`**

```
ARP> ping 1.1.1.2
PING 1.1.1.100 -> 1.1.1.2: 56 data bytes, ttl=64, every 1 sec.
56 data bytes from 1.1.1.2: icmp_seq=0. ttl=64. time=19. ms
56 data bytes from 1.1.1.2: icmp_seq=1. ttl=64. time=11. ms

----1.1.1.2 PING Statistics----
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 11/15/19 ms
```

## Protocol

Utilice el mandato **protocol** para listar todas las direcciones de cliente de cada una de las interfaces de red. Es exactamente igual que en el caso de las otras interfaces. Para una interfaz ATM, la lista de direcciones de protocolo significa todos los clientes CIP configurados en esta interfaz.

**Sintaxis:**

pr**otocol**

**Ejemplo: `protocol`**

```
ARP> protocol
Network  Protocol (num)  AS     Protocol Address(es)
0 ATM/0  IP       ( 0)   0800   1.1.1.100
```

## Redundancy-State

Utilice el mandato **redundancy-state** para visualizar (por red) los clientes IP que se han configurado con redundancia.

**Sintaxis:**

red**undancy-state**

El ejemplo siguiente muestra la sección de supervisión de la redundancia relativa al Servidor ARP primario cuando el canal de redundancia se encuentra inactivo.

```
CGW Operator monitoring
+p arp
ARP>red
Network number  [0]?
Protocol [IP]
If: 0 Prot: IP  Clients configured with Redundancy
-----------------------------------------------------------
Addr: 1.1.1.1   Place Redundancy Call: Yes  Real Esi: Up  Red. Esi: Up  Red. Chnl: Down
                    FLAGS: Real Client: C8  Red. Client: C8 RedFlags: C0
                    Red. Channel: 0/0
                     Red. Channel: Source ATM address
 39.84.0F.00.00.00.00.00.00.00.00.00.01.AA.AA.AA.AA.AA.AA.AA
                     Red. Channel: Target ATM address
39.84.0F.00.00.00.00.00.00.00.00.00.01.BB.BB.BB.BB.BB.BB.BB
                     Redundancy Status: Active
 Redundancy default IP Gateway protocol address: 1.1.1.3
```

El ejemplo siguiente muestra la sección de supervisión de la redundancia relativa al Servidor primario cuando el canal de redundancia se encuentra activo.

```
CGW Operator monitoring
+p arp
 ARP>red
 Network number  [0]?
 Protocol [IP]?
 If: 0 Prot: IP  Clients configured with Redundancy
 -----------------------------------------------------------
 Addr: 1.1.1.1   Place Redundancy Call: Yes  Real Esi: Up  Red. Esi: Up  Red. Chnl: Up
                     FLAGS: Real Client: C8  Red. Client: C8 RedFlags: D0
                     Red. Channel: (VPI/VCI)  0/32
                     Red. Channel: Source ATM address
 39.84.0F.00.00.00.00.00.00.00.00.00.01.AA.AA.AA.AA.AA.AA.AA
                     Red. Channel: Target ATM address
 39.84.0F.00.00.00.00.00.00.00.00.00.01.BB.BB.BB.BB.BB.BB.BB
                     Redundancy Status: Active
 Redundancy default IP Gateway protocol address: 1.1.1.3
 -----------------------------------------------------------
```

El ejemplo siguiente muestra la sección de supervisión de la redundancia relativa al asociado cuando el canal de redundancia se encuentra inactivo y el asociado actúa como Servidor Arp de reserva.

```
ARP>red
 Network number  [0]?
 Protocol [IP]?
 If: 0 Prot: IP  Clients configured with Redundancy
 -----------------------------------------------------------
 Addr: 1.1.1.2   Place Redundancy Call: No  Real Esi: Up  Red. Esi: Up  Red. Chnl: Down
                     FLAGS: Real Client: C8  Red. Client: C8 RedFlags: 80
                     Red. Channel: 0/0
                    Red. Channel: Source ATM address
 39.84.0F.00.00.00.00.00.00.00.00.00.01.BB.BB.BB.BB.BB.BB.BB
                     Red. Channel: Target ATM address
 39.84.0F.00.00.00.00.00.00.00.00.00.01.AA.AA.AA.AA.AA.AA.AA
                     Redundancy Status: Active
 Partner Server ESI: 11.11.11.11.11.11, Partner Server SEL: 11, In backup Server mode
 Redundancy default IP Gateway Protocol address: 1.1.1.3
 -------------------------------------------
```

El ejemplo siguiente muestra la sección de supervisión de la redundancia relativa al secundario cuando el canal de redundancia se encuentra activo y el secundario actúa como cliente y no en modalidad de Servidor ARP de reserva (porque el servidor ARP primario se encuentra activo).

```
ARP>red
Network number  [0]?
 Protocol [IP]?
 If: 0 Prot: IP  Clients configured with Redundancy
 ------------------------------------------------------
Addr: 1.1.1.2   Place Redundancy Call: No  Real Esi: Down  Red. Esi: Up  Red. Chnl: Up
                     FLAGS: Real Client: C0  Red. Client: C8 RedFlags: 90
                     Red. Channel: (VPI/VCI)  0/32
                     Red. Channel: Source ATM address
 39.84.0F.00.00.00.00.00.00.00.00.00.01.BB.BB.BB.BB.BB.BB.BB
                    Red. Channel: Target ATM address
 39.84.0F.00.00.00.00.00.00.00.00.00.01.AA.AA.AA.AA.AA.AA.AA
                     Redundancy Status: Inactive, not trying ...
 Partner Server ESI: 11.11.11.11.11.11, Partner Server SEL: 11, Acting as a Client
 Redundancy default IP Gateway Protocol address: 1.1.1.3
 ------------------------------------------
 ARP>exit
```

Se visualizan los campos siguientes en la supervisión de la redundancia:

**If:** Especifica el número de interfaz.

**Prot:** Especifica el protocolo.

**Addr:** Especifica la dirección IP del cliente.

**Place Redundancy Call**
Indica si el cliente iniciará la llamada de redundancia. Vea la página 641.

**Real ESI:** Indica el estado del ESI real. Si el estado es Up, significa que la dirección ATM del cliente se ha registrado satisfactoriamente con el conmutador. Si el estado es Down, significa que el intento del cliente de registrar su dirección ATM con el conmutador no ha sido satisfactorio.

**Red. ESI:** Indica el estado del ESI de redundancia. Si el estado es Up, significa que la dirección ATM del canal de redundancia se ha registrado satisfactoriamente con el conmutador. Si el estado es Down, significa que la dirección ATM del canal de redundancia no se ha registrado satisfactoriamente con el conmutador.

**Red. Chnl:**
Indica el estado del canal de redundancia. Si el estado es Up, significa que se ha configurado el canal de redundancia entre el primario y el secundario. Si el estado es Down, significa que no se ha configurado el canal de redundancia entre el primario y el secundario.

**Red Channel**
Proporciona el par VPI/VCI del canal de redundancia.

**Red. Channel Source ATM address:**
Identifica la dirección ATM del canal de redundancia de origen.

**Red. Channel Target ATM address:**
Identifica la dirección ATM del canal de redundancia de destino.

**Redundancy Status:**
Identifica el estado de la redundancia.

**Active** Proporciona Servicios de ARP.

**Inactive** No proporciona Servicios de ARP.

**Partner Server ESI:**

Identifica un ESI administrado localmente que debe utilizarse como componente ESI de la dirección ATM del Servidor ARP asociado cuando falle el Servidor ARP asociado.

**Partner Server SEL:**

Identifica la parte de Selector del ESI y selector que está configurada en el dispositivo asociado. Este campo sólo se visualiza para el Servidor ARP de reserva o similar.

**Redundancy Default IP Gateway Address:**

Especifica la dirección de pasarela IP por omisión. Es la dirección de pasarela por omisión configurada en los clientes a los que sirve este Servidor ARP. Esta dirección permite que el Servidor ARP proporcione la función de direccionamiento desde una subred a otra.

## Statistics

Utilice el mandato **statistics** para visualizar las estadísticas del código de ARP sobre todas las interfaces de red. Estas estadísticas son como las estadísticas del código de ARP sobre cualquiera de las otras interfaces según describe la sección “Statistics” en la página 675.

**Sintaxis:**

**statistics**

**Ejemplo: `statistics`**

```
ARP> statistics

    ARP input packet overflows
        Net   Count
       ATM/0  0
      IPPN/0  0
       BDG/0  0

    ARP cache meters
    Net Prot  Max Cur Cnt    Alloc  Refresh: Tot  Failure  TMOs: Refresh
      0   0     1   1   1        1             0        0              0
```

# Supervisión de Server Cache Synchronization Protocol (SCSP)

Utilice la función de supervisión de SCSP para supervisar el estado de la sincronización de los servidores.

## Acceso al entorno de supervisión de SCSP

Utilice el procedimiento siguiente para acceder a los mandatos de supervisión de SCSP. Este proceso le proporciona acceso al proceso de *supervisión* de SCSP.

1. En el indicador de OPCON, entre **talk 5**. (Para obtener información más detallada sobre este mandato, consulte "The OPCON Process and Commands" en el manual *Guía del usuario de software*.) Por ejemplo:

   ```
   * talk 5
   +
   ```

   Después de que entre el mandato **talk 5**, se visualizará el indicador de GWCON (+) en el terminal. Si no aparece el indicador la primera vez que entre la configuración, pulse **Intro** de nuevo.

2. En el indicador +, entre el mandato **protocol scsp** para obtener el indicador `SCSP`.

   **Ejemplo:**

   ```
   + prot scsp
   SCSP>
   ```

## Mandatos de supervisión de SCSP

Esta sección describe los mandatos de supervisión de SCSP. Puede acceder a los mandatos de supervisión de SCSP en el indicador `SCSP>`. La Tabla 42 muestra los mandatos.

*Tabla 42. Resumen de los mandatos de supervisión de SCSP*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxxi. |
| List | Lista información sobre la supervisión de SCSP. |
| Statistics | Visualiza estadísticas de SCSP para un Servidor conectado directamente. |
| Dump | Vuelca la antememoria de SCSP en relación con un grupo de servidores. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxii. |

## List

Utilice el mandato **List** para visualizar información sobre el estado de la sincronización de los servidores. Puede entrar también el signo ? después de un nombre de mandato específico si desea listar las opciones del mismo.

**Sintaxis:**

**list** dcs . . .
server-groups . . .

**dcs** *interfaz sgid*

Lista todos los DCS de un grupo de servidores.

interfaz — Especifica el número de interfaz bajo el que se ha definido el DCS.

sgid — Especifica el identificador de grupo de servidores de este DCS.

**Ejemplo:**

```
SCSP>li dcs
Network number [0]?
Server Group ID [0]?
      DCS Id      HFSM State  CAFSM State  M/S  CRL Len  ReTran Len
 03.04.02.00   Bidirectional      Aligned   S         0           0
```

DCS Id — El identificador hexadecimal del DCS (del otro extremo de la VCC).

HFSM State — El estado de la Máquina de estado finito de Hello para esta sesión de DCS. Los estados son:

- Down_Inop — El canal para el DCS está inactivo.
- Down — El canal para el DCS está inactivo, pero está en proceso una apertura.
- Waiting — El Servidor local (LS) ha enviado un mensaje Hello al DCS y está esperando una respuesta.
- Unidirectional — El LS ha recibido un mensaje Hello del DCS, pero todavía no se ha reconocido este Servidor local.
- Bidirectional — El LS y el Servidor conectado directamente se reconocen mutuamente. Éste es el estado normal.

CAFSM State — El estado de la Máquina de estado finito de alineación de antememoria para esta sesión de DCS. Los estados son:

- Down — Todavía no ha empezado la alineación de antememoria.
- MS_Neg — El LS y el DCS están negociando respecto al estado de Maestro/Esclavo.
- Summarize — El LS y el DCS están intercambiando información de resumen de antememoria.

| | | |
|---|---|---|
| | Update | El LS y el DCS están intercambiando la información de antememoria al completo. |
| | Aligned | El LS y el DCS están sincronizados. Éste es el estado normal. |
| M/S | | Indica el estado de Maestro (M) o Secundario (S) de este LS. Sólo es significativo si el estado de CAFSM es Summarize, Update o Aligned. |
| CRL Len | | La longitud de la lista de peticiones de longitud de antememoria. Es el número de registros de actualización de antememoria que quedan para enviar durante el estado Update. |
| ReTran Len | | La longitud de la lista de retransmisiones. Es el número de registros de actualización de antememoria que quedan para el acuse de recibo del DCS. |

**server-groups** *interfaz*

Lista información sobre todos los grupos de servidores.

**interfaz** Número de interfaz de red

**Ejemplo:**

```
SCSP config> list ser
Network number [0]?
       SGID  Protocol      LSID  DCSs  ATM Addr
          1    ATMARP  04040100     0  39.84.0F.00.00.00.00.00.00.00.00.00.01.
                                       11.11.11.11.11.11.01
          0    ATMARP  03040100     1  39.84.0F.00.00.00.00.00.00.00.00.00.01.
                                       11.11.11.11.11.11.01
```

**sgid** Identificador de grupo de servidores. Es el identificador configurado para los servidores de este grupo de servidores (LIS).

**Protocol** El tipo de base de datos a intercambiar.

**lsid** Valor hexadecimal del identificador de servidor local. Identifica a este Servidor dentro del grupo de servidores. Para ATMARP, es la dirección IP del cliente.

**DCSs** El número de Servidores conectados directamente que están asociados con este Servidor local.

**ATM address** La dirección ATM de este Servidor local. Los DCS deben utilizarla para configurar conexiones con este Servidor local.

## Statistics

Utilice este mandato si desea mostrar estadísticas para un Servidor conectado directamente.

Utilice el mandato **Statistics** para visualizar información sobre el estado de la sincronización de los servidores. Puede entrar también el signo ? después de un nombre de mandato específico si desea listar las opciones del mismo.

**Sintaxis:**

**statistics** *interfaz grupo-servidores id-dcs*

**interfaz** Especifica el número de interfaz bajo el que se ha definido el DCS.

**Valores válidos**: Cualquier interfaz definida

**Valor por omisión**: 0

**grupo-servidores**
Especifica el grupo de servidores de este DCS.

**Valores válidos**: 0 - 65535

**Valor por omisión**: 0

**id-dcs** Especifica el identificador hexadecimal del DCS (del otro extremo de la VCC).

**Valores válidos**:

**Valor por omisión**: 0

**Ejemplo:**

```
SCSP>stat 0 0
DCS ID (hex) [0]?
DCS with that ID not found, listing all DCS's.
-------------------------------------------
DCS ID: 03.04.02.00
HFSM State: Bidirectional   DCS Hello Interval(sec): 3   DCS Dead Factor: 3
CAFSM State: Aligned  Master/Slave: S   CA seq: 33D35204   CSUS seq: 33D351F1
Cache Summary List sent?: yes   Cache Summary List ACKed?: yes
Cache Request List Size: 0   Cache ReTransmit List Size: 0   Age(sec): 302
ATM Addr: 39.84.0F.00.00.00.00.00.00.00.00.04.12.12.12.12.12.12.01
VPI: 0  VCI: 32  Missed Hello Msgs: 0   RID doesn't match LSID: 0
Short Messages: 0   Sequence Mismatches: 0
```

**DCS Id** Vea la página 686.

**HFSM State**
Vea la página 686.

**CAFSM State**
Vea la página 686.

**Hello Interval**
El intervalo en segundos para que el DCS emita mensajes Hello.

**DCS Dead Factor**
El número de intervalos de Hello que deben pasar sin que se reciba un mensaje Hello después de los cuales este DCS se considerará inactivo.

**Master/Slave**
Vea la página 686.

**CA Seq** El número de secuencia del mensaje de alineación de antememoria actual.

**CSUS Seq**
El número de secuencia del mensaje de petición de actualización de estado de antememoria actual.

**Cache Summary List Sent?**
Yes si se ha transmitido completamente la lista de resumen de la antememoria al DCS (durante el estado de alineación de antememoria).

**Cache Summary List Acked?**
Yes si se ha reconocido toda la lista de resumen de la antememoria (durante el estado de alineación de antememoria).

**Cache Request List size**
Vea la página 686.

**Cache ReTransmit List size**
Vea la página 686.

**Age** El número de segundos desde que se ha inicializado este DCS.

**VPI, VCI** El identificador de vía de acceso virtual y el identificador de canal virtual de la VCC con el DCS.

**Missed Hello Msgs**
El número de mensajes Hello perdidos durante el estado bidireccional.

**RID doesn't match LSID**
El número de mensajes recibidos en que el ID de receptor del mensaje no coincide con el LSID del LS.

**Short Messages**
El número de mensajes SCSP formados incorrectamente (demasiado cortos).

**Sequence Mismatches**
El número de violaciones de protocolo relativas al número de secuencia.

## Dump

Utilice el mandato **Dump** si desea volcar la antememoria de SCSP en relación con un grupo de servidores.

**Sintaxis:**

d**ump** *interfaz grupo-servidores*

**interfaz** Especifica el número de interfaz bajo el que se ha definido el DCS.

**Valores válidos**: Cualquier interfaz definida

**Valor por omisión**: 0

**grupo-servidores**
Especifica el grupo de servidores de este DCS.

**Valores válidos**: 0 - 65535

**Valor por omisión**: 0

**Ejemplo:**

```
SCSP> dump 0 0
Next key to assign = 33D351F1
Key           Origin ID              Seq. No.   Age   Paddr
03.04.02.00   03.04.02.00           869487085     0   03.04.02.00
03.04.01.00   03.04.01.00           869487090     0   03.04.01.00
SCSP>
```

**Key** El valor de clave de antememoria hexadecimal para esta entrada de antememoria. Para ATM ARP, corresponde a la dirección IP del servidor (en hexadecimal).

**Origin ID** El ID de DCS hexadecimal del servidor que ha originado esta entrada de antememoria. Para ATM ARP, corresponde a la dirección IP del servidor (en hexadecimal).

**Age** El número de minutos durante los que ha existido esta entrada sin una entrada de antememoria de servidor coincidente. Una vez alcanzados los 20 minutos, esta entrada caduca.

**Paddr** La dirección de protocolo correspondiente de esta entrada de antememoria. Si está en blanco, significa que no hay una entrada de antememoria de servidor correspondiente (por ejemplo, una entrada de antememoria de ATM ARP).

# Utilización de IPX

Este capítulo describe cómo utilizar el protocolo IPX en el 2210. Incluye las siguientes secciones:



## Visión general de IPX

La implementación de IPX por parte de IBM permite que el direccionador funcione como direccionador interredes Novell NetWare. Tiene estas características:

- Compatibilidad con todos los entornos de las versiones anteriores de Novell NetWare.
- Compatibilidad con la función de puente de un servidor de archivos NetWare más un puente de NetWare autónomo.
- Soporte para el emulador de Novell NetBIOS.

## Sistema de dirección IPX

Las secciones siguientes describen el sistema de dirección IPX.

### Números de red

Un número de red IPX especifica la ubicación de una red determinada en una internet. Puede utilizar direcciones de diversas partes como la dirección ciudad-calle-casa que se utiliza para correos. Por ejemplo, IPX hace referencia a números de red (ciudad), números de sistema principal (calle) y números de socket (casa). Estas direcciones permiten la comunicación entre dos entidades de redes diferentes.

### Números de sistema principal

Cada circuito IPX necesita un número de sistema principal (nodo) de 6 bytes.

Los circuitos Red en Anillo y Ethernet utilizan la dirección del MAC de hardware como número de sistema principal y no pueden cambiarse.

Puesto que las líneas serie no tienen direcciones del MAC de hardware, debe especificar un número de sistema principal exclusivo. IPXWAN utiliza el identificador de nodo configurado y, a continuación, x'0000'.

Los circuitos ATM utilizan el identificador de sistema final (ESI) como número de sistema principal. Se utilizará el ESI incorporado si no se ha configurado ninguno.

## Circuitos IPX

El software de direccionamiento IPX modela las interfaces de red como un solo circuito de difusión IPX, como uno o más circuitos punto a punto IPXWAN o como una combinación de ambos tipos de circuitos. El tipo de encapsulación, sistema de dirección IPX y protocolos de direccionamiento que se utilicen en el circuito dependen del DLC subyacente y de si el circuito IPX está configurado como circuito de difusión o punto a punto IPXWAN.

Los circuitos de difusión IPX tienen las características siguientes:

- Se utilizan en interfaces LAN
- Se utilizan en interfaces WAN cuando no se ha configurado IPXWAN
- Se limitan a un solo circuito de difusión IPX por interfaz
- Se les debe asignar un número de red IPX distinto de cero
- Para las LAN, se utiliza la dirección del MAC de la interfaz de red como número de nodo IPX del circuito
- Para las WAN, se utiliza el número de sistema principal IPX configurado como número de nodo IPX del circuito
- Se permite el uso simultáneo de RIP/SAP y rutas y servicios estáticos.

Los circuitos punto a punto IPXWAN tienen las características siguientes:

- Sólo pueden utilizarse en interfaces WAN
- Es posible que no se limiten a un solo circuito punto a punto IPXWAN por interfaz
- Se utiliza IPXWAN para negociar parámetros
- Es posible que no necesiten un número de red IPX
- Se utiliza un ID de nodo IPXWAN seguido de 0000 como número de nodo IPX del circuito
- Se limitan a un solo tipo de direccionamiento negociado.

Las secciones siguientes describen cómo se modelan los tipos de interfaces de red soportadas.

## LAN (Red en Anillo, Ethernet, ATM LAN Emulation)

El software de direccionamiento IPX modela una interfaz LAN como un solo circuito de difusión IPX.

Debe asignarse al circuito un número de red IPX exclusivo y distinto de cero.

La dirección del MAC de la interfaz de red sirve de número de nodo IPX del circuito.

Se utiliza la dirección de todas las estaciones LAN (x'FFFFFFFFFFFF') para recibir y transmitir los paquetes difundidos, como, por ejemplo, las actualizaciones de RIP y SAP.

Se da soporte a los tipos normales de encapsulación para el tipo de interfaz LAN correspondiente.

El tamaño máximo de paquete IPX deriva de la MTU configurada para la interfaz.

Respecto a las interfaces Red en Anillo, puede habilitarse el direccionamiento de origen en la interfaz para permitir que el reenviador IPX llegue a las estaciones finales (y a otros direccionadores) a través de los puentes de ruta de origen.

En el circuito pueden utilizarse todos los tipos de direccionamiento siguientes o cualquiera de ellos:

- Rutas/servicios estáticos
- RIP/SAP (con número)

## ATM nativa

El software de direccionamiento IPX modela una interfaz ATM como un solo circuito de difusión IPX. Como tal, los PVC y SVC ATM subyacentes definidos por el usuario para interconectar direccionadores en la red ATM son transparentes para el software de direccionamiento IPX.

Debe asignarse al circuito un número de red IPX exclusivo y distinto de cero.

Se utiliza el componente ESI de la dirección ATM como número de nodo IPX del circuito. Se utilizará el ESI incorporado si no se ha configurado un ESI en el cliente IPX ATM ARP asociado con la interfaz ATM.

La dirección de todas las estaciones LAN (x'FFFFFFFFFFFF') sirve de dirección de difusión IPX. Los paquetes dirigidos a la dirección de difusión se transmiten sobre todos los VC de la interfaz por medio del DLC ATM subyacente.

El tamaño máximo de paquete IPX deriva de la MTU configurada para la interfaz.

El DLC ATM subyacente utiliza la ATM InARP para correlacionar las direcciones de nodo IPX de destino con el VC ATM correspondiente. Opcionalmente, las direcciones de nodo IPX de destino pueden configurarse de manera estática en el caso de los VC conectados a los direccionadores que no dan soporte a la ATM InArp.

Para dar soporte a topologías ATM de malla no completa, puede inhabilitarse el horizonte de división en el circuito. Esto permite que RIP y SAP propaguen información por todos los VC de la interfaz para que pueda producirse el direccionamiento intermedio entre los VC de la misma interfaz.

Las topologías ATM de malla completa no necesitan la inhabilitación del horizonte de división.

En el circuito pueden utilizarse todos los tipos de direccionamiento siguientes o cualquiera de ellos:

- Rutas/servicios estáticos
- RIP/SAP (con número)

## Point-to-Point Protocol (PPP)

El software de direccionamiento IPX modela una interfaz PPP como un solo circuito de difusión IPX o como un solo circuito punto a punto IPXWAN.

El tamaño máximo de paquete IPX deriva de la MTU negociada por el DLC PPP subyacente.

***Circuito de difusión IPX:*** Cuando se configura como circuito de difusión, debe asignarse al circuito un número de red exclusivo y distinto de cero.

Puesto que no existe una dirección del MAC asociada con una interfaz PPP, se utiliza un número de sistema principal configurado como número de nodo IPX del circuito.

En el circuito pueden utilizarse todos los tipos de direccionamiento siguientes o cualquiera de ellos:

- Rutas/servicios estáticos
- RIP/SAP (con número)

***Circuito punto a punto IPXWAN:*** Cuando se configura como circuito punto a punto IPXWAN, utiliza IPXWAN para negociar los parámetros de direccionamiento.

El tipo de direccionamiento RIP con número de IPXWAN requiere que se asigne al circuito un número de red exclusivo y distinto de cero. Los otros tipos de direccionamiento de IPXWAN (RIP sin número, direccionamiento estático) no requieren un número de red (valor 0).

Puesto que no existe una dirección del MAC asociada con la interfaz PPP, se utiliza el identificador de nodo IPXWAN seguido de 0000 como número de nodo IPX del circuito.

Puede configurarse el tipo de direccionamiento a negociar en el circuito. Si se habilita el direccionamiento estático, no se negociará ningún otro tipo de direccionamiento. Puede habilitar cualquiera de los tipos restantes que siguen o todos ellos y se negociarán en favor de un solo tipo de direccionamiento por orden de preferencia descendente:

- RIP/SAP sin número
- RIP/SAP con número

## Frame Relay

El software de direccionamiento IPX modela una interfaz Frame Relay como:

- un solo circuito de difusión IPX o
- un conjunto de uno o más circuitos punto a punto IPXWAN o
- una combinación de ambos.

El tamaño máximo de paquete IPX deriva de la MTU configurada para la interfaz.

El DLC Frame Relay subyacente utiliza la InARP para correlacionar las direcciones de nodo IPX de destino con el circuito virtual Frame Relay correspondiente. Opcionalmente, las direcciones de nodo IPX de destino pueden configurarse de manera estática en el caso de los VC conectados a los direccionadores que no dan soporte a la InArp.

***Circuito de difusión IPX:*** Todos los circuitos virtuales de la interfaz Frame Relay que no están configurados como circuitos punto a punto IPXWAN están agrupados juntos y modelados como un solo circuito de difusión IPX al que debe asignarse un número de red exclusivo y distinto de cero. Como tal, los circuitos virtuales subyacentes definidos por el usuario para interconectar direccionadores en la red Frame Relay son transparentes para el software de direccionamiento IPX.

Puesto que no existe una dirección del MAC asociada con una interfaz Frame Relay, se utiliza un número de sistema principal configurado como número de nodo IPX del circuito.

La dirección de todas las estaciones LAN (x'FFFFFFFFFFFF') sirve de dirección de difusión IPX del circuito. Los paquetes dirigidos a la dirección de difusión se transmiten sobre todos los VC del circuito de difusión IPX por medio del DLC Frame Relay subyacente. Esta función de difusión de protocolo Frame Relay se activa habilitando las siguientes opciones de configuración de Frame Relay:

- Difusión de protocolo
- Emulación con vertimiento múltiple

Para dar soporte a topologías Frame Relay de malla no completa, puede inhabilitarse el horizonte de división en el circuito de difusión IPX. Esto permite que RIP y SAP propaguen información por todos los circuitos virtuales del circuito de difusión IPX para que pueda producirse el direccionamiento intermedio entre los circuitos virtuales del mismo circuito de difusión IPX.

Las topologías Frame Relay de malla completa no necesitan la inhabilitación del horizonte de división.

En el circuito pueden utilizarse todos los tipos de direccionamiento siguientes o cualquiera de ellos:

- Rutas/servicios estáticos
- RIP/SAP (con número)

***Circuito punto a punto IPXWAN:*** IPX puede configurarse de manera que funcione como circuitos punto a punto IPXWAN sobre PVC y SVC Frame Relay individuales. Se utiliza IPXWAN para negociar los parámetros de direccionamiento.

El tipo de direccionamiento RIP con número de IPXWAN requiere que se asigne al circuito un número de red exclusivo y distinto de cero. Los otros tipos de direccionamiento de IPXWAN (RIP sin número, direccionamiento estático) no requieren un número de red (valor de 0).

Puesto que no existe una dirección del MAC asociada con la interfaz Frame Relay, se utiliza el identificador de nodo IPXWAN seguido de 0000 como número de nodo IPX del circuito.

Puede configurarse el tipo de direccionamiento a negociar en el circuito. Si se habilita el direccionamiento estático, no se negociará ningún otro tipo de direccionamiento. Puede habilitar cualquiera de los tipos restantes que siguen o todos ellos y se negociarán en favor de un solo tipo de direccionamiento por orden de preferencia descendente:

- RIP/SAP sin número
- RIP/SAP con número

## X.25

El software de direccionamiento IPX modela una interfaz X.25 como un solo circuito de difusión IPX. Como tal, los VC subyacentes definidos por el usuario para interconectar direccionadores en la red X.25 son transparentes para el software de direccionamiento IPX.

Debe asignarse al circuito un número de red IPX exclusivo y distinto de cero.

Puesto que no existe una dirección del MAC asociada con una interfaz X.25, se utiliza un número de sistema principal configurado como número de nodo IPX del circuito.

La dirección de todas las estaciones LAN (x'FFFFFFFFFFFF') sirve de dirección de difusión IPX del circuito. Los paquetes dirigidos a la dirección de difusión se transmiten a todas las direcciones X.25 de destino del circuito de difusión IPX por medio del DLC X.25 subyacente.

El tamaño máximo de paquete IPX deriva de la MTU configurada para la interfaz.

Para dar soporte a topologías X.25 de malla no completa, puede inhabilitarse el horizonte de división en el circuito de difusión IPX. Esto permite que RIP y SAP propaguen información por todas las direcciones X.25 de destino del circuito de difusión IPX para que pueda producirse el direccionamiento intermedio entre los VC del mismo circuito de difusión IPX.

Las topologías X.25 de malla completa no necesitan la inhabilitación del horizonte de división.

En el circuito pueden utilizarse todos los tipos de direccionamiento siguientes o cualquiera de ellos:

- Rutas/servicios estáticos
- RIP/SAP (con número)

Las direcciones de nodo IPX de destino deben configurarse estáticamente en el caso de todas las direcciones X.25 de destino porque el DLC X.25 no da soporte a la InArp.

## Configuración de IPX

Esta sección describe cómo configurar IPX inicialmente. Las secciones siguientes describen parámetros opcionales que puede establecer.

1. Visualice el indicador de configuración de IPX tal como se muestra aquí:

```
* talk 6
Config> protocol ipx
IPX protocol user configuration
IPX config>
```

2. Habilite IPX globalmente.

```
IPX config> enable ipx
```

3. Añada un circuito de difusión sobre WAN o LAN o bien un circuito IPXWAN sobre WAN.

```
IPX Config>add broadcast-circuit
Which interface [0]? 1
IPX circuit number[3]? 5
IPX network number in hex
('0' is only allowed on IPXWAN unnumbered circuits) [1]? 01

IPX Config>add ipxwan-circuit
Which interface [0]? 2
IPX circuit number[4]? 6
IPX network number in hex
('0' is only allowed on IPXWAN unnumbered circuits) [1]? 40
Use Frame Relay PVC ? no
Frame Relay SVC circuit name ? Indianapolis
```

**Nota:** El número de red IPX 0 sólo es válido en RIP o circuitos de direccionamiento estático sin número IPXWAN. El número de red IPX FFFFFFFF no es un número de red IPX válido. El número de red IPX FFFFFFFE está reservado para la Ruta por omisión de IPX y no puede utilizarse como número de red IPX.

4. Si ha habilitado IPX de manera que se ejecute sobre un circuito serie, asigne un número de sistema principal exclusivo al direccionador.

```
IPX config>set host-number
Host number for serial lines (in hex) []? 2
```

5. Opcionalmente, cambie el tipo de trama para Ethernet, Red en Anillo o ATM LAN Emulation Client. No es necesario establecer el tipo de trama en el caso de los circuitos que no son Ethernet, Red en Anillo o ATM LAN Emulation Client. Consulte la sección “Frame” en la página 729 para obtener una descripción de los tipos de tramas disponibles.

   Los formatos de encapsulación por omisión son:

   - Ethernet - Ethernet_8023
   - Red en Anillo - MSB de Red en Anillo

   Utilice el mandato **frame** tal como se muestra aquí:

```
IPX config> frame ethernet_8023
IPX circuit number [1]? 2
```

6. Opcionalmente, cambie los parámetros de IPXWAN para los que no desee utilizar los valores por omisión.

```
IPX config> set ipxwan
IPX circuit number [1]? 3
Routing type ('u'=Unnumbered, 'r'=RIP, 'b'=Both, 's'=Static) [u] r
Connection Timeout (in sec) [60]? 90
Retry timer (in sec) [60]? 45
```

## Tareas de configuración opcionales

En las secciones siguientes se describen valores opcionales que puede ajustar.

## Especificación del tamaño de la tabla de redes IPX de RIP

La tabla de redes IPX de RIP contiene información sobre cada red IPX. El tamaño por omisión de la tabla es 32. Puede configurar el tamaño de la tabla dentro del rango del 1 al 2048; sin embargo, es posible que en el direccionador existan limitaciones de memoria que pueden impedir que se utilice el tamaño de tabla máximo.

```
IPX config>set maximum networks
New Network table size [32]? 32
```

## Especificación del intervalo de actualización de RIP

IPX utiliza RIP para mantener rutas en las tablas de direccionamiento. Una ruta indica la vía de acceso que un paquete sigue. El intervalo de actualización de RIP determina la frecuencia con la que el direccionador difunde sus tablas de información de direccionamiento a sus circuitos. También determina durante cuánto tiempo permanece una entrada de RIP antes de que caduque.

En las tablas de direccionamiento permanecen entradas válidas durante un período de tres múltiplos del intervalo de actualización de RIP y el direccionador difunde sus tablas de RIP una vez cada intervalo de actualización.

Por ejemplo, el intervalo por omisión es de 1 minuto, lo que permite que una entrada válida permanezca en la tabla durante 3 minutos. Después de este tiempo, si una entrada no se ha renovado mediante una actualización de RIP, la ruta se marca con una cuenta de saltos de infinito (16) y luego se suprime. Cada 60 segundos, el direccionador difunde sus tablas de RIP a los circuitos correspondientes.

Puede configurar el intervalo de RIP dentro del rango de 1 a 1440 minutos (24 horas). Si se aumenta el intervalo de RIP, se reduce el tráfico en las líneas WAN y circuitos dial. También evita que los circuitos dial-on-demand efectúen la marcación a menudo.

**Nota:** Mientras que los anuncios de RIP completos están controlados por el intervalo, el direccionador propaga los cambios de la topología de red tan pronto como los aprende.

El intervalo de RIP no puede configurarse en el servidor de archivos Novell.

```
IPX config>set rip-update-interval
IPX circuit number [1]? 2
RIP timer value(minutes) [1]? 2
```

## Especificación del tamaño de la tabla de servicios de SAP de IPX

La tabla de servicios de Service Advertising Protocol (SAP) de IPX es una base de datos distribuida que se utiliza para encontrar servicios de NetWare, como, por ejemplo, servidores de archivos. Los servicios se identifican de manera exclusiva mediante un tipo numérico de 2 bytes y un nombre de 47 caracteres. Cada suministrador de servicios anuncia sus servicios especificando el tipo de servicios, el nombre y la dirección. El direccionador acumula esta información en una tabla y la envía a otros direccionadores. El tamaño por omisión de la tabla es 32.

Puede configurar el tamaño de la tabla dentro del rango del 1 al 2048; es posible que restricciones de memoria del direccionador impidan que se utilice el tamaño de tabla máximo.

```
IPX config>set maximum services
New Service table size [32]? 32
```

## Especificación del intervalo de actualización de SAP

El intervalo de Service Advertising Protocol (SAP) de IPX le permite configurar el tiempo entre las actualizaciones de SAP en IPX por circuito. Todos los circuitos del direccionador que pertenezcan a la misma red deben utilizar el mismo intervalo de SAP. Este intervalo determina el tiempo de duración de la información de la tabla y el intervalo entre las difusiones a circuitos del direccionador.

En la tabla de servicios de SAP permanecen entradas válidas durante un período de tres múltiplos del intervalo de actualización de SAP y el direccionador difunde su información de tabla de servicios de SAP una vez cada intervalo de actualización.

Puede configurar el intervalo de SAP dentro del rango de 1 a 1440 minutos (24 horas). Si se aumenta el intervalo de SAP, se reduce el tráfico en las líneas WAN y circuitos dial. También evita que los circuitos dial-on-demand efectúen la marcación a menudo.

**Nota:** Mientras que los anuncios de SAP completos están controlados por este intervalo, el direccionador propaga los cambios de la topología de red tan pronto como los aprende.

El intervalo de SAP no puede configurarse en el servidor de archivos Novell.

```
IPX config>set sap-update
IPX circuit number [1]? 2
SAP timer value(minutes) [1]? 4
```

## Filtración de paquetes de serialización y Keepalive de IPX

Puede configurar IPX de manera que impida que los paquetes de serialización y Keepalive activen continuamente un enlace dial-on-demand o de manera que minimice el tráfico sobre un enlace dial-on-demand.

En la Figura 53 en la página 700, por ejemplo, si el Cliente Novell inicia la sesión del Servidor Novell y, a continuación, permanece desocupado, el servidor envía peticiones Keepalive periódicas al cliente y éste responde con respuestas Keepalive. La filtración de Keepalive hace que los direccionadores entren la primera respuesta Keepalive en sus tablas de Keepalive y, a continuación, reenvíen la respuesta. Después de esto, los direccionadores no reenvían tráfico Keepalive para esta conexión cliente-servidor sobre el enlace WAN. En lugar de ello, el Direccionador A responde a las peticiones Keepalive que recibe del servidor y el Direccionador B envía las peticiones Keepalive al Cliente Novell.

La filtración de Keepalive también impide que los direccionadores reenvíen paquetes de serialización de NetWare sobre el enlace WAN.

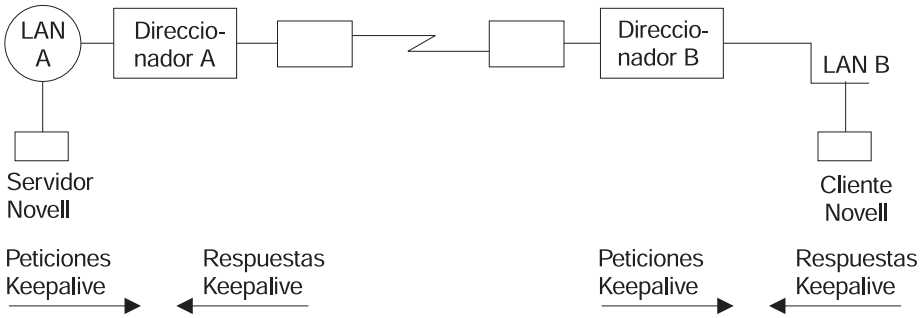



*Figura 53. Filtración de Keepalive*

Para configurar la filtración de Keepalive, habilítela en los circuitos dial.

```
IPX Config> enable keepalive-filtering
IPX circuit number [1]? 5
```

## Configuración de diversas rutas

Puede configurar IPX de manera que mantenga más de una entrada de tabla de direccionamiento para la misma red de destino. La ventaja de esta función es que, si se desactiva una ruta, se utiliza inmediatamente la ruta alternativa. El direccionador no tiene que esperar una difusión de RIP, que puede tardar desde unos segundos a un minuto, para aprender una nueva ruta. El direccionador sólo almacena vías de acceso de igual coste en la tabla de direccionamiento.

Utilice el mandato siguiente si desea configurar el número máximo de rutas que se almacenarán en la tabla de direccionamiento para cada destino. El rango es del 1 al 64. El valor por omisión es 1.

```
IPX config>set maximum routes-per-destination
New maximum number of routes per destination net [1]? 4
```

Utilice el mandato siguiente para establecer el número total de entradas mantenidas en la tabla de direccionamiento. El rango es del 1 al 4096. El valor por omisión es 32. Establezca el número de entradas en el mismo tamaño que la tabla de redes de RIP como mínimo. (Configure el tamaño de la tabla de redes de RIP utilizando el mandato **set maximum networks** explicado en este capítulo.)

```
IPX config> set maximum total-route-entries
New route table size [32]? 40
```

Sobre la base de un circuito IPX, puede configurar el coste de circuito de RIP (en ciclos). El coste de circuito se toma en consideración al calcular el coste de ruta total en los anuncios de las rutas. Si existen diversas rutas hacia el mismo destino, puede influir en la selección de ruta asignando a un circuito IPX un coste de ruta superior al de otro circuito. Utilice el mandato siguiente con el fin de establecer el coste de circuito para una ruta conectada directamente específica.

```
IPX config> set rip-ticks
IPX circuit number [1]? 2
RIP ticks value (in 55msec ticks [0]? 3
```

## Configuración de rutas estáticas

Pueden configurarse rutas estáticas por número de red de destino. Cada ruta estática se asocia con un circuito y se instala en la tabla de direccionamiento cuando se activa IPX en el circuito. La ruta estática se elimina de la tabla de direccionamiento cuando se desactiva IPX en el circuito, cuando se desactiva el circuito en sí o cuando se aprende una ruta aprendida dinámicamente hacia la red de destino. Las rutas aprendidas dinámicamente (mediante RIP) siempre alteran temporalmente rutas estáticas. La ruta estática se reinstalará en la tabla de direccionamiento cuando se reactive IPX en el circuito, cuando se reactive el circuito en sí o cuando se hayan perdido todas las rutas de RIP hacia la red de destino.

Las rutas estáticas son especialmente útiles sobre los circuitos dial-on-demand en que se ha inhabilitado RIP y las rutas hacia las redes de destino se han configurado estáticamente sobre el circuito dial-on-demand.

El direccionamiento estático puede utilizarse en un circuito solo o en combinación con RIP. La única excepción para ello es cuando se habilita el direccionamiento estático en un circuito IPXWAN. En este caso, el direccionamiento estático es el único tipo de direccionamiento negociado por IPXWAN.

RIP anunciará las rutas estáticas con sujeción al horizonte de división y a los filtros aplicables.

Cuando se configuran diversas rutas estáticas por red de destino, se utilizan las mismas normas utilizadas para elegir rutas de RIP a la hora de determinar qué rutas estáticas se instalan en la tabla de direccionamiento. Se instalarán diversas rutas estáticas hacia la misma red de destino en la tabla de direccionamiento si tienen igual coste. Puede almacenar simultáneamente el máximo de rutas que ha configurado por destino en la tabla de direccionamiento.

El ejemplo siguiente muestra cómo configurar una ruta estática de IPX.

```
IPX Config> disable rip
IPX circuit number [1]? 2

IPX Config> enable route-static

IPX Config> add route-static
IPX net address: (1-fffffffe) [1]? 30
IPX circuit number [1]? 2
Next-hop address, in hex [] ? 400000003000
Ticks: (0-30000) [0]? 4
Hops: (0-14) [0]? 4
```

## Configuración de servicios estáticos

Pueden configurarse servicios estáticos por par consistente en nombre o tipo de servicio. Cada servicio estático se asocia con un circuito y se instala en la tabla de servicios de SAP cuando se activa IPX en el circuito y se conoce una ruta hacia la red del servicio (mediante anuncio de RIP o ruta estática). El servicio estático se elimina de la tabla de SAP cuando se desactiva IPX en el circuito, cuando se desactiva el circuito en sí, cuando se pierde la ruta hacia la red del servidor o cuando se aprende dinámicamente el mismo servicio. Mientras se conozca una ruta hacia la red del servidor, el servicio estático se reinstalará en la tabla de servicios cuando se reactive IPX en el circuito, cuando se reactive el circuito en sí o cuando se pierda el servicio aprendido por medio de SAP. Los servicios aprendidos dinámicamente (utilizando SAP) siempre alteran temporalmente servicios estáticos.

Los servicios estáticos son especialmente útiles sobre los circuitos dial-on-demand en que se ha inhabilitado SAP y los servicios se han configurado estáticamente sobre el circuito dial-on-demand.

Los servicios estáticos pueden utilizarse en un circuito solos o en combinación con RIP/SAP. La única excepción para ello es cuando se habilita el direccionamiento estático en un circuito IPXWAN. En este caso, el direccionamiento estático es el único tipo de direccionamiento negociado por IPXWAN.

SAP anunciará los servicios estáticos con sujeción al horizonte de división y a los filtros aplicables.

Cuando se configuran diversos servicios estáticos por nombre o tipo, se utilizan las mismas normas utilizadas para elegir servicios de SAP a la hora de determinar qué servicio estático se instala en la tabla de direccionamiento. Tenga en cuenta que, si hay configurados servicios estáticos de igual coste, se instalará en la tabla de servicios el definido en el mismo circuito que la ruta actual hacia la red del servidor.

El ejemplo siguiente muestra cómo configurar un servicio estático de IPX.

```
IPX Config> disable sap
IPX circuit number [1]? 2

IPX Config> enable sap-static

IPX Config> add sap-static
Sap type: (0-ffff) [4]?
Sap name: []? FILE_SERVER01
IPX circuit number [1]? 2
IPX net address: (1-fffffffe) [1]? 30
IPX node address, in hex: []? 400000202000
IPX socket: (0-ffff) [451]?
Hops: (0-14) [0]? 4
```

## Configuración de la ruta por omisión de RIP

La ruta por omisión es un caso especial de ruta estática. Se utiliza en calidad de último recurso como siguiente salto para redes de destino desconocidas.

La ruta por omisión es especialmente útil en los circuitos dial-on-demand cuando se ha inhabilitado RIP. La configuración de la ruta por omisión en el circuito dial-on-demand permite que los clientes soliciten rutas y envíen paquetes a las redes de destino de la otra parte del circuito sin que se tenga que configurar una ruta estática para cada destino.

### Manejo de RIP

Para los direccionadores que utilizan RIP, el número de red FFFFFFFE designa la ruta por omisión.

Cuando se anuncien las rutas de RIP, se anunciará la ruta por omisión (como cualquier otra ruta estática) después del sometimiento a los filtros de RIP y al horizonte de división.

A la hora de responder a una petición RIP relativa a una red de destino desconocida, el direccionador sólo contesta si tiene una ruta por omisión en la tabla de direccionamiento.

A la hora de reenviar paquetes, si la ruta hacia la red de destino es desconocida, el reenviador reenviará el paquete al direccionador de siguiente salto que anuncie la ruta por omisión (o al direccionador de siguiente salto indicado por la definición de ruta por omisión estática local en el caso del direccionamiento estático).

El ejemplo siguiente muestra cómo configurar una ruta por omisión de RIP.

```
IPX Config> enable route-static

IPX Config> add route-static
IPX net address: (1-fffffffe) [1]? fffffffe
IPX circuit number [1]? 2
Next-hop address, in hex: []? 400000003030
Ticks: (0-30000) [0§? 4
Hops: (0-14) [0]? 4
```

### Interacción con SAP

Generalmente, los anuncios de SAP sólo se aceptan si se conoce una ruta hacia la red del servidor. Si no se conoce la ruta hacia la red del servidor pero sí una ruta por omisión, también se acepta el anuncio (después del sometimiento a los filtros de SAP).

Los anuncios de SAP que se acepten en virtud de la existencia de la ruta por omisión se anunciarán en todos los circuitos IPX que no sean aquél del que se ha aceptado el anuncio de SAP (horizonte de división). Por supuesto, el anuncio se someterá a los filtros de SAP antes de anunciarse. Se aplican las mismas normas a las respuestas a peticiones SAP.

## Configuración de filtros de IPX globales (controles del acceso de IPX)

Los filtros de IPX globales se aplican a todos los circuitos IPX. Pueden utilizarse para impedir que el direccionador reenvíe paquetes sobre la base de direcciones IPX (red/sistema principal/socket). Puede utilizar los filtros de IPX globales para proporcionar seguridad o para detener el reenvío de paquetes de aplicaciones de “propagación” más allá del área de interés.

Los filtros de IPX globales se basan en la dirección de origen IPX inicial y la dirección IPX de destino final. Las direcciones de salto intermedias no son importantes.

Una dirección IPX (de origen o de destino) para un filtro global consta de un número de red IPX, un número de sistema principal IPX y un rango de números de socket IPX que se especifican en hexadecimal. El número de red y el número de sistema principal pueden especificarse como 0, que es un comodín que coincide con todos los números de red y de sistema principal, respectivamente. Un rango del 0 al FFFF es un comodín para los sockets.

La lista de filtros globales es una lista de entradas con un orden. Cada entrada de filtro global puede configurarse como inclusiva o exclusiva. El direccionador compara los paquetes que recibe con la lista de filtros globales.

- Si un paquete coincide con una entrada inclusiva, el direccionador reenvía el paquete.
- Si un paquete coincide con una entrada exclusiva, el direccionador elimina el paquete.
- Si el direccionador llega al final de la lista sin que el paquete coincida con una entrada, el direccionador elimina el paquete. (Esto es equivalente a tener una entrada exclusiva con comodín al final de la lista.)

Al crear listas de filtros globales, tome en consideración las advertencias siguientes sobre IPX:

- En primer lugar, no bloquee nunca los sockets RIP y SAP (X'0453' y X'0452'). RIP y SAP son necesarios para reenviar paquetes IPX correctamente.
- Recuerde que la lista de filtros globales se aplica a todos los circuitos. Tendrá que utilizar números de red de origen y/o de destino en los filtros globales para representar los controles direccionales.
- Sepa dónde se ubican los servicios que intenta proteger. En el indicador `IPX>`, entre el mandato **slist** para determinar la dirección de un servicio.

  **Nota:** Todos los servicios de un servidor de archivos Novell (versión 3.0 ó superior) están en la red interna del servidor, normalmente en el sistema principal 000000000001. Puesto que el número de red interna es único en toda una red IPX, puede protegerlo bloqueando todos los paquetes para el rango de sockets de red interna 0–FFFF. Para bloquear solamente el servidor de archivos, utilice el rango de sockets de 0451–0451.
- Al extraer números de socket de **slist** para crear una lista de filtros globales, recuerde que algunos servicios tienen números de socket fijos y algunos tienen números de socket dinámicos (temporales). Puesto que los sockets del rango 4000–7FFF son dinámicos, no hay garantía de que el servicio tenga el mismo número de socket la próxima vez que se rearranque el servidor de archivos. Sin embargo, los números de socket del rango 8000–FFFF están asignados por Novell, y generalmente permanecerán constantes.

**Nota:** Los filtros globales y los filtros de circuito se excluyen mutuamente. Si se habilita la filtración de SAP global, no pueden habilitarse los filtros de SAP de circuito (y viceversa). Si se habilita la filtración de IPX global (*controles del acceso*), no pueden habilitarse los filtros de IPX de circuito (y viceversa).

El direccionador examina cada trama IPX para ver si coincide con una entrada de la lista de filtros globales. Aplica la primera coincidencia, por lo tanto el orden de los filtros globales es importante. El direccionador examina los paquetes IPX teniendo en cuenta los criterios siguientes:

1. Tipo de filtro global (dos tipos):
   a. Inclusivo, que indica que, si el paquete coincide con los criterios siguientes, se reenvía
   b. Exclusivo, que indica que, si el paquete coincide con los criterios siguientes, se desecha
2. Red de destino - se toma directamente del campo de red de destino IPX del paquete.
3. Sistema principal de destino - se toma directamente del campo de sistema principal de destino IPX del paquete.
4. Socket de destino inicial/final - se toman directamente del campo de socket de destino IPX del paquete (no del campo de sistema principal). (El número de socket es la ubicación, dentro del protocolo, que enlaza lógicamente el paquete con un servicio de aplicación.)

5. Red de origen - se toma directamente del campo de red de origen IPX del paquete.
6. Sistema principal de origen - se toma directamente del campo de sistema principal de origen IPX del paquete.
7. Socket de origen inicial/final - se toman directamente del campo de socket de origen IPX del paquete.

El resultado del ejemplo siguiente será reenviar solamente los paquetes IPX de cualquier cliente existente en la red IPX 1871 que estén destinados a la aplicación NCP, del Servidor de archivos Novell 0000 C93A 0912, situado en la red 18730. Todo el tráfico restante se eliminará.

```
IPX config>add access control
Enter type [E]? I
Destination network number (in hex) [ ]? 18730
Destination host number (in hex) [ ]? 0000C93A0912
Starting destination socket number (in hex) [ ]? 0451
Ending destination socket number (in hex) [ ]? 0451
Source network number (in hex) [ ]? 1871
Source host number (in hex) [ ]? 0
Starting source socket number (in hex) [ ]? 4000
Ending source socket number (in hex) [ ]? 7FFF
```

## Filtros de SAP globales

Los filtros de SAP globales se aplican a todos los circuitos. Pueden utilizarse para impedir que se propague información de anuncios de servicios por medio del direccionador. Las razones principales para utilizar los filtros de SAP globales son cuatro:

- Desea utilizar servidores con tamaños pequeños de enlace lógico (por ejemplo, NetWare Versión 2.15 ó inferior) y debe limitar la cantidad de información en la base de datos de SAP.
- No desea anunciar determinados servicios fuera del área local porque el acceso remoto a los mismos sería inadecuado.
- Desea eliminar la información que llena desordenadamente la tabla de SAP.
- Desea reducir la presencia de anuncios de SAP innecesarios en los enlaces WAN porque los anuncios de SAP pueden consumir una cantidad considerable de ancho de banda de WAN.

**Nota:** Ninguna de estas razones menciona explícitamente la seguridad. Los filtros de SAP globales no pueden proteger un servicio. Todo lo que hace SAP es proporcionar una conversión de nombre en dirección para los servicios. Si un intruso potencial conoce la dirección del servicio, el bloqueo de su anuncio mediante los filtros de SAP globales no protegerá el servicio. Sólo los controles del acceso pueden proporcionar seguridad.

El filtro de SAP global se basa en el establecimiento de una cuenta máxima de saltos para un servicio en particular o un grupo de servicios. En la tabla de SAP se acepta cualquier anuncio de servicio coincidente recibido con la cuenta de saltos especificada (o inferior). Los otros se ignoran. Sólo se reanuncian o se utilizan para responder a consultas los servicios de la base de datos de SAP.

**Nota:** El direccionador sólo le permite entrar nombres de servicio en ASCII de 7 bits. Algunos nombres de servicio utilizan datos binarios, lo que supone una

violación de las especificaciones relativas a SAP de Novell. No podrá hacer que se filtren estos servicios por el nombre.

Un filtro de SAP global puede aplicarse a todos los servicios de un tipo. Novell asigna números de tipo hexadecimales de 4 dígitos para cada tipo de servicio. Como alternativa, un filtro de SAP global puede aplicarse a un servicio determinado de un tipo. Esto se realiza especificando el nombre del servicio.

Puede haber varios servidores con el mismo tipo de servicio, cada uno con un nombre de servicio único. En este caso, puede configurar diversos filtros de SAP globales con el mismo tipo de servicio de manera que se filtren nombres de servicio únicos o bien puede configurar un solo filtro de SAP de manera que se filtre el tipo de servicio para todos los nombres de servicio (filtro con comodín).

## Creación de filtros de SAP globales

Para configurar los filtros de SAP globales:

1. Entre **add filter** en el indicador `IPX Config>`. Debe especificar varias entradas clave que normalmente se encuentran en las difusiones de SAP:
   a. Número de saltos. Esta entrada indica la cuenta de saltos permitida para una entrada de SAP (si es superior, se desecha).
   b. Tipo de servicio
   c. Nombre de servicio
2. Entre **set filter on** en el indicador `IPX Config>` para habilitar el filtro.

El ejemplo siguiente muestra la creación de un filtro de SAP global en relación con un servidor de impresión específico.

```
IPX config> add filter
Maximum number of hops allowed [1]? 2
Service type [4]? 0047
Optional service name [ ]? rem-ptr1
IPX config> set filter on
```

Este filtro de SAP global hace que el direccionador ignore los anuncios de SAP de cualquier servidor de impresión (tipo de servicio 0047) denominado **rem-ptr1** que esté alejado más de dos saltos. El filtro impide que el direccionador propague los anuncios que coincidan con estos criterios.

## Determinación del tipo de servicio para un filtro de SAP global

Con el fin de determinar el tipo de SAP para un filtro que desee establecer, siga estos pasos:

1. En el indicador *, entre **talk 5**. A continuación, en el indicador +, entre **protocol ipx**.

   En el indicador `IPX>`, entre **slist**. Anote la entrada para los servicios que desee que se filtren.
2. En el indicador `*`, entre **talk 6**. A continuación, en el indicador `Config>`, entre **protocol ipx**. Añada el filtro de SAP global correspondiente y la cuenta de saltos correspondiente para el servicio que desee que se filtre.
3. Después de crear el filtro, reinicie el direccionador.
4. Si se ha filtrado un servicio satisfactoriamente, ya no debe aparecer listado. Compruebe si el servicio ya no aparece listado entrando **slist** en el indicador `IPX>`.

# Filtros de circuito IPX - Visión general

La función de direccionamiento IPX da soporte a cuatro tipos de filtros basados en circuito: DIRECCIONADOR, RIP, SAP e IPX. Pueden definirse un *filtro de la entrada* y un *filtro de la salida* por circuito. Los criterios de filtro, referidos como *elementos*, se ensamblan en *listas-filtro* y, a continuación, se conectan con los filtros de la entrada y/o la salida. Una lista-filtro puede conectarse con más de un filtro. Esto evita que el usuario tenga que configurar los mismos criterios de filtro en diversos circuitos.

**Nota:** Los filtros globales y los filtros de circuito se excluyen mutuamente. Si se habilita la filtración de SAP global, no pueden habilitarse los filtros de SAP de circuito (y viceversa). Si se habilita la filtración de IPX global (*controles del acceso*), no pueden habilitarse los filtros de IPX de circuito (y viceversa).

## Configuración de filtros de circuito IPX

Para configurar los filtros de circuito IPX:

1. Cree una lista-filtro y proporcione un nombre para la misma utilizando el mandato **create list**.
2. Modifique la lista-filtro utilizando el mandato **update** y sus submandatos para especificar los criterios de filtro y si esta lista-filtro es inclusiva o exclusiva.
3. Cree un filtro en el circuito que desee utilizando el mandato **create filter** y especifique si es un filtro de la entrada o de la salida.
4. Habilite la filtración de circuito IPX utilizando el mandato **enable all**.
5. Conecte las listas-filtro con el filtro utilizando el mandato **attach**.
6. Establezca la acción por omisión para el filtro utilizando el mandato **default**. Se llevará a cabo la acción por omisión si no se produce ninguna coincidencia en ninguna de las listas-filtro conectadas.

También hay mandatos para suprimir un filtro de un circuito IPX, inhabilitar un filtro de un circuito IPX (o de todos los circuitos IPX), desconectar una lista-filtro de un filtro, trasladar las listas-filtro dentro del filtro (ya que las listas-filtro siguen un orden), listar un filtro y establecer el tamaño de la antememoria de un filtro (sólo para la filtración de IPX).

## Filtración de DIRECCIONADOR

El filtro de DIRECCIONADOR funciona con respecto a la cabecera de IPX de todos los paquetes de respuesta RIP recibidos. No se da soporte a la filtración de DIRECCIONADOR de la salida. La filtración de DIRECCIONADOR puede utilizarse para agrupar redes IPX individuales en varias redes internet IPX distintas controlando a qué direccionadores se permite intercambiar información de direccionamiento.

Los filtros de DIRECCIONADOR RIP se mantienen en listas de elementos con un orden por circuito. Se aplican los elementos ordenadamente a cada paquete de respuesta RIP recibido. Si se encuentra una coincidencia, se efectúa la acción especificada en la lista-filtro coincidente (exclusión = desechar paquete, inclusión = recibir paquete para el proceso). Puesto que se desechan los paquetes excluidos, la información contenida en sus entradas de red no entra en las tablas de direccionamiento de RIP. Si no se encuentra ninguna coincidencia, se efectúa la acción de filtro por omisión especificada.

## Filtración de RIP

El filtro de RIP funciona con respecto a las entradas de red de los paquetes de respuesta RIP. Puede utilizarse para controlar hasta qué punto se difunde información de direccionamiento sobre las redes seleccionadas. Como filtro de la *entrada*, este filtro puede impedir el *almacenamiento* de información de direccionamiento sobre las redes seleccionadas. Esto evita que ***todas*** las otras redes aprendan información sobre las redes seleccionadas (al menos mediante este direccionador).

Los filtros de RIP (entrada) se mantienen en listas de elementos con un orden por circuito. Se aplican los elementos ordenadamente a cada entrada de red de cada paquete de respuesta RIP recibido. Si se encuentra una coincidencia, se efectúa la acción especificada en la lista-filtro coincidente (exclusión = ignorar entrada de red, inclusión = procesar entrada de red). Puesto que se ignoran las entradas de red excluidas, no entran en las tablas de direccionamiento de RIP. Si no se encuentra ninguna coincidencia, se efectúa la acción de filtro por omisión especificada.

Como filtro de la *salida*, este filtro puede impedir el *anuncio* (en contraposición al almacenamiento) de información de direccionamiento sobre las redes seleccionadas. Evita que *algunas* redes (en contraposición a todas) aprendan información sobre las redes seleccionadas (al menos mediante este direccionador).

Los filtros de RIP (salida) se mantienen en listas de elementos con un orden por circuito. Se aplican los elementos ordenadamente a cada entrada de red a transmitir en un paquete de respuesta RIP. Si se encuentra una coincidencia, se efectúa la acción especificada en la lista-filtro coincidente (exclusión = excluir entrada de red del paquete, inclusión = incluir entrada de red en el paquete). Este filtro no tiene efecto sobre el contenido de las tablas de direccionamiento de RIP. Si no se encuentra ninguna coincidencia, se efectúa la acción de filtro por omisión especificada.

## Filtración de SAP

El filtro de SAP funciona con respecto a las entradas de servidor de todos los paquetes de respuesta SAP. Puede utilizarse para controlar hasta qué punto se difunde información sobre servicios y puede reducir la cantidad de tráfico de SAP en las WAN de menor velocidad.

Como filtro de la *entrada*, este filtro puede impedir el *almacenamiento* de información de servicios sobre los servidores seleccionados. Esto evita que ***todas*** las otras redes aprendan información sobre los servidores seleccionados (al menos mediante este direccionador).

Los filtros de SAP (entrada) se mantienen en listas de elementos con un orden por circuito. Se aplican los elementos ordenadamente a cada entrada de servidor de cada paquete de respuesta SAP recibido. Si se encuentra una coincidencia, se efectúa la acción especificada en la lista-filtro coincidente (exclusión = ignorar entrada de servidor, inclusión = procesar entrada de servidor). Puesto que se ignoran las entradas de servidor excluidas, no entran en la tabla de servicios de SAP. Si no se encuentra ninguna coincidencia, se efectúa la acción de filtro por omisión especificada.

Como filtro de la *salida*, este filtro puede impedir el *anuncio* (en contraposición al almacenamiento) de información de servicios sobre los servidores seleccionados.

Evita que *algunas* redes (en contraposición a todas) aprendan información sobre los servidores seleccionados (al menos mediante este direccionador).

Los filtros de SAP (salida) se mantienen en listas de elementos con un orden por circuito. Se aplican los elementos ordenadamente a cada entrada de servidor en cada paquete de respuesta SAP a transmitir. Si se encuentra una coincidencia, se efectúa la acción especificada en la lista-filtro coincidente (exclusión = excluir entrada de servidor, inclusión = incluir entrada de servidor en el paquete). Este filtro no tiene efecto sobre el contenido de la tabla de servicios de SAP. Si no se encuentra ninguna coincidencia, se efectúa la acción de filtro por omisión especificada.

## Filtración de IPX

El filtro de IPX funciona con respecto a la cabecera de IPX de los paquetes IPX. Puede utilizarse para controlar hasta qué punto se permite que las estaciones de trabajo y los servidores seleccionados se comuniquen con otras estaciones de trabajo y servidores seleccionados, tomando como base los campos de red, nodo y socket de origen y de destino, así como el tipo de protocolo y la cuenta de saltos.

Como filtro de la *entrada*, una coincidencia que indique que debe desecharse el paquete impide que éste se transmita sobre ***todos*** los circuitos.

Los filtros de IPX (entrada) se mantienen en listas de elementos con un orden por circuito. Se aplican los elementos ordenadamente a cada paquete IPX recibido. Si se encuentra una coincidencia, se efectúa la acción especificada en la lista-filtro coincidente (exclusión = desechar paquete, inclusión = recibir paquete para el proceso o reenvío). Si no se encuentra ninguna coincidencia, se efectúa la acción de filtro por omisión especificada.

Como filtro de la *salida*, la decisión sobre si reenviar el paquete se toma basándose en el circuito de la salida y, por lo tanto, puede permitir que un paquete recibido se reenvíe sobre un circuito pero no sobre otro.

Los filtros de IPX (salida) se mantienen en listas de elementos con un orden por circuito. Se aplican los elementos ordenadamente a cada paquete IPX a transmitir. Si se encuentra una coincidencia, se efectúa la acción especificada en la lista-filtro coincidente (exclusión = desechar paquete, inclusión = transmitir paquete). Si no se encuentra ninguna coincidencia, se efectúa la acción de filtro por omisión especificada.

Puesto que los filtros de IPX se invocan para cada paquete recibido, es recomendable que sólo se utilicen cuando sea necesario un grado elevado de especificación (es decir, cuando no puedan utilizarse los filtros de DIRECCIONADOR, RIP y SAP). Generalmente, los filtros de RIP se encargan de la función de interredes entre ***todas*** las estaciones de un conjunto determinado de redes; los filtros de SAP controlan qué servidores son asequibles para las estaciones de trabajo en toda la internet; los filtros de IPX se encargan de la función de interredes entre estaciones de trabajo ***individuales*** (o aplicaciones individuales de estaciones de trabajo individuales).

La sección “Mandatos de configuración de filtros de circuito para circuitos IPX” en la página 744 describe más detalladamente los mandatos utilizados para configurar los filtros de circuito IPX.

# Ajuste de rendimiento en IPX

El direccionador IPX implementa una vía de acceso dual para el reenvío de paquetes, una vía de acceso rápida y una vía de acceso lenta, con el fin de direccionar el tráfico de una manera más eficiente.

La vía de acceso rápida sólo reenvía paquetes de datos, mientras que la vía de acceso más lenta maneja paquetes de administración, como, por ejemplo, paquetes RIP y SAP. La vía de acceso rápida utiliza una antememoria de direcciones que permite que el direccionador reenvíe un paquete rápidamente.

Las búsquedas en la tabla de direccionamiento más lenta sólo se efectúan durante la creación de una entrada de antememoria. La antememoria tiene un mecanismo para establecer duración que permite tratar los desbordamientos con inteligencia. Puede configurar el tamaño de antememoria mediante el menú de la configuración de IPX.

La antememoria de vía de acceso rápida de IPX incluye dos entradas: local y remota. Cada entrada puede manejar los requisitos de este tipo de direccionamiento.

Los mandatos de antememoria se utilizan para establecer un límite relativo al número máximo de los tipos de entradas que se permiten en la antememoria.

## Antememoria local

El tamaño de la antememoria local debe ser equivalente al número total de clientes de las redes de cliente o locales del direccionador más un almacenamiento intermedio de un 10% para prevenirse contra excesivas peticiones de eliminación. Utilizando el ejemplo de la Figura 54 en la página 711, el direccionador 5 (DIRECCIONADOR D5) tiene 9 clientes (C) más el servidor (S), lo que da un total de 10. Basándose en este total:

1. Multiplique por 10% (10 en el ejemplo).
2. Añada este total (1) al total de clientes (para un margen de seguridad).
3. Utilice el nuevo total (11) para el número de entradas de antememoria local.

Por ejemplo:

```
IPX config>set local-cache size
New IPX local node cache size [32]? 11
```

Cuando están en uso todas las entradas de antememoria, se eliminan las entradas que se utilizan con menos frecuencia.

## Antememoria remota

El tamaño de la antememoria remota debe ser equivalente al número total de redes remotas utilizadas por el direccionador más un almacenamiento intermedio de un 10% para prevenirse contra excesivas peticiones de eliminación. En la Figura 54 en la página 711, hay 10 redes IPX que el DIRECCIONADOR D5 puede leer mediante la red IPX 5. Por lo tanto, el DIRECCIONADOR/D5 tiene un total de 10 clientes. Basándose en este total:

1. Multiplique por 10% (10 en el ejemplo).
2. Añada este total (1) al total de redes remotas (10) para un margen de seguridad.
3. Utilice el nuevo total (11) para el número de entradas de antememoria remota.

Por ejemplo:

```
IPX config>set remote-cache size
New IPX remote network cache size [32]? 11
```

Puede visualizar las entradas de antememoria utilizando el mandato de supervisión de IPX **sizes**.

```
IPX>sizes
Current IPX cache size:
Remote network cache size (max entries): 45
0 entries now in use
Local node cache size (max entries): 86
0 entries now in use
```

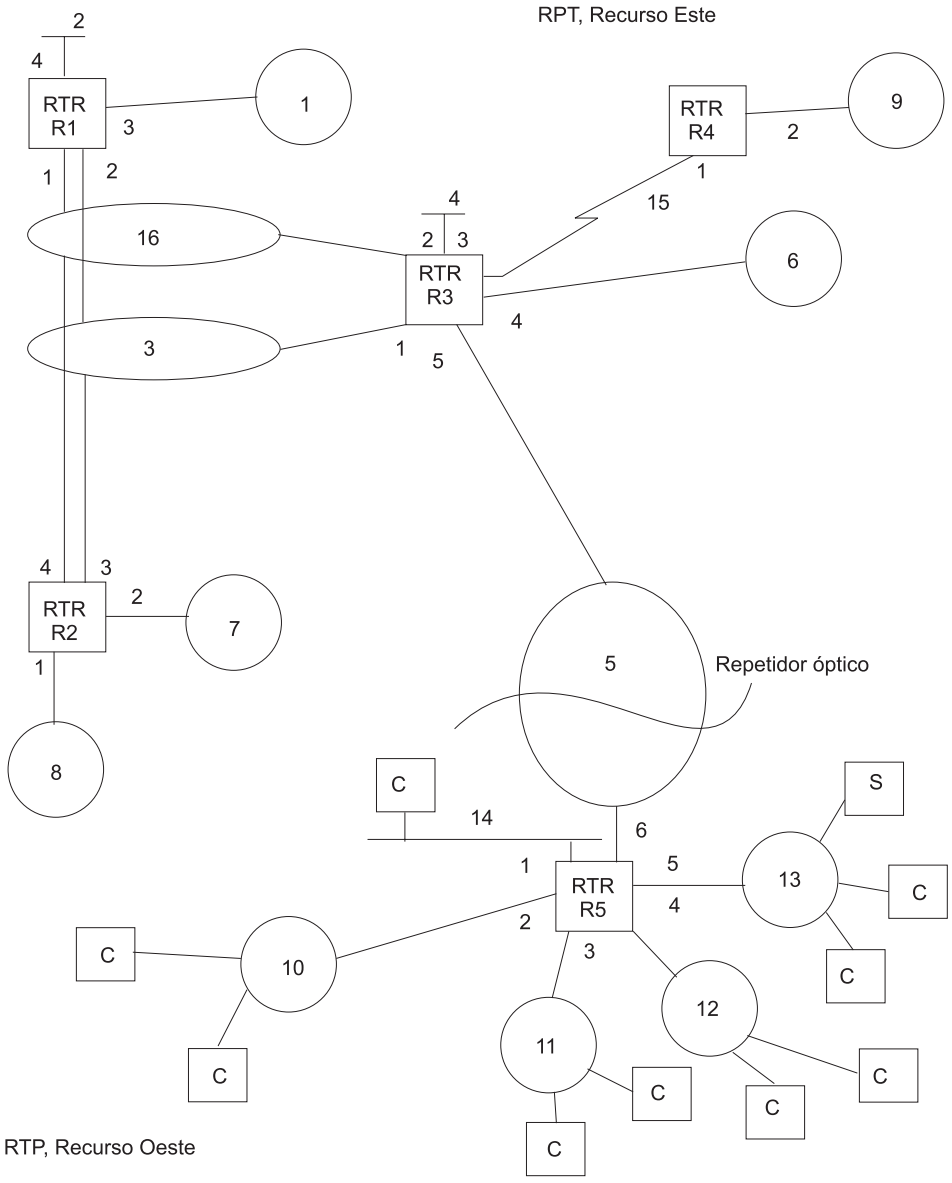



*Figura 54. Red IPX de muestra*

## Direccionamiento de horizonte de división

El horizonte de división es un método de direccionamiento que evita difundir las actualizaciones de RIP y SAP al direccionador del que se han aprendido.

Generalmente, debe habilitarse el horizonte de división en cada circuito para impedir la cuenta de paquetes hasta el infinito y para evitar anuncios de RIP y SAP innecesarios. Sin embargo, hay algunos casos, como, por ejemplo, configuraciones de frame-relay, ATM y X.25 de malla parcial, en que puede ser necesario inhabilitar el horizonte de división.

Una configuración de direccionamiento IPX con soporte de RFC 1483 y de malla parcial es otro caso en que puede ser necesario inhabilitar el horizonte de división.

En una red frame-relay de malla parcial, tal como se muestra en la Figura 55, los direccionadores de las ramas no pueden comunicarse entre sí a menos que el direccionador de la sede central difunda toda la información de direccionamiento a los otros direccionadores. En este caso, el horizonte de división debe inhabilitarse en la sede central del circuito frame-relay y habilitarse en cada una de las ramas para evitar que generen tráfico innecesario.

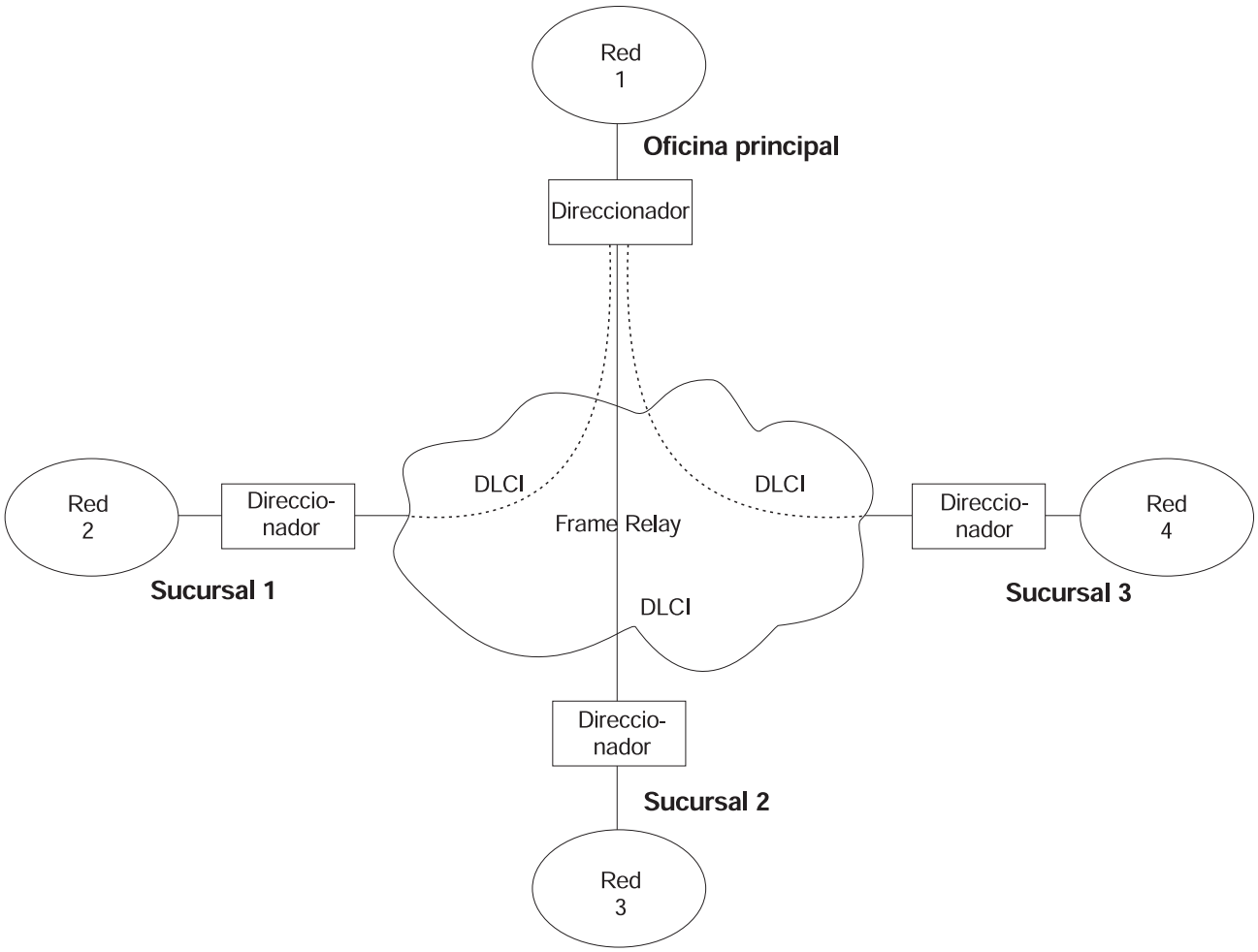



*Figura 55. Red Frame-Relay de malla parcial*

Si tiene que cambiar el valor de horizonte de división, utilice el mandato **set split-horizon** de la manera siguiente:

```
IPX Config>set split-horizon enabled
Which circuit [1]? 2

IPX Config>set split-horizon disabled
Which circuit [1]? 2

IPX Config>set split-horizon heuristic
Which circuit [1]? 2
```

# Configuración y supervisión de IPX

Este capítulo describe cómo configurar el protocolo IPX y utilizar los mandatos de supervisión de IPX. Incluye las siguientes secciones:



## Acceso al entorno de configuración de IPX

Para acceder al entorno de configuración de IPX, entre el mandato siguiente en el indicador `Config>`:

```
Config> protocol IPX
IPX Protocol user configuration
IPX Config>
```

## Mandatos de configuración de IPX

Esta sección trata los mandatos de configuración de IPX. La Tabla 43 en la página 716 lista los mandatos de configuración de IPX. Estos mandatos especifican los parámetros de red para los direccionadores encargados de transmitir paquetes IPX. Se entran en el indicador `IPX config>`. Para activar los cambios de la configuración, reinicie el direccionador.

*Tabla 43. Resumen de los mandatos de configuración de IPX*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Add | Añade un circuito de difusión IPX o punto a punto IPXWAN, filtros de IPX globales (controles del acceso), filtros de SAP globales, rutas o servicios estáticos. |
| Delete | Suprime un circuito de difusión IPX o punto a punto IPXWAN, filtros de IPX globales (controles del acceso), filtros de SAP globales, rutas o servicios estáticos. |
| Disable / Enable | Inhabilita o habilita IPX globalmente o bien en circuitos IPX específicos; inhabilita o habilita globalmente el uso de las rutas o servicios estáticos de IPX. Inhabilita o habilita la filtración de Keepalive,el ritmo de difusión de RIP-SAP, la respuesta a petición SAP para obtener el servidor más próximo, las difusiones de NetBIOS, así como RIP o SAP en circuitos específicos. |
| Filter-lists | Accede a la configuración de filtros de circuito IPX. En este entorno se configuran los filtros basados en circuito IPX: DIRECCIONADOR, RIP, SAP e IPX. |
| Frame | Especifica el formato de enlace de datos para los circuitos Ethernet y Red en Anillo. También se aplica a los clientes LAN Emulation Client Red en Anillo y Ethernet. |
| List | Visualiza la configuración actual de IPX. |
| Move | Reordena los elementos de filtro de IPX global (control del acceso) o traslada un circuito IPX de una interfaz a otra. |
| Set | Establece el número de sistema principal, el ID de nodo y nombre de direccionador IPXWAN, el tipo de direccionamiento de IPXWAN, el tiempo de espera excedido de conexión y el temporizador de reintentos, los números de red IPX, los tamaños máximos de tabla de RIP y SAP, los tamaños de antememoria local y remota, los estados de filtro de IPX global (controles del acceso) y filtro de SAP global, tamaños de antememoria, los intervalos de actualización de RIP y SAP, el coste de circuito de RIP (ciclos de RIP), el tamaño de tabla de filtración de Keepalive y el uso del horizonte de división. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Add

Utilice el mandato **add** para añadir un filtro de IPX global (controles del acceso), un circuito de difusión IPX, un filtro de SAP global, un circuito punto a punto IPX o bien una ruta o servicio estáticos a la configuración de IPX.

**Sintaxis:**

**add** access-control . . .
broadcast-circuit . . .
filter . . .
ipxwan-circuit . . .
route-static . . .
sap-static . . .

**access-control** *tipo red-dest sistemaprincipal-dest rango-sockets-dest red-origen sistemaprincipal-origen rango-sockets-origen*

Determina si se debe pasar un paquete en el nivel de IPX. Los controles del acceso de IPX proporcionan una función de control del acceso global en el nivel de paquete IPX para el protocolo IPX. La lista de controles del acceso es un conjunto de entradas con un orden que el direccionador utiliza para la filtración de paquetes. Cada entrada puede ser inclusiva o exclusiva. Cada entrada tiene números de red, direcciones de sistema principal y rangos de sockets de origen y destino.

Cuando se recibe un paquete de una red para el protocolo IPX y está habilitado el control del acceso, se comprueba con la lista de controles del acceso. Se compara con los pares de redes/direcciones/sockets de la lista hasta que se encuentra una coincidencia. Si se encuentra una coincidencia y la entrada es de tipo inclusivo, procede la recepción del paquete (y el reenvío en potencia). Si la entrada coincidente es de tipo exclusivo, se elimina el paquete. Si no se encuentra ninguna coincidencia, también se elimina el paquete.

Después de crear una lista de controles del acceso con el mandato **add access-control**, habilite las entradas con el mandato **set access-control on**. Utilice el mandato **move** para cambiar el orden de la lista de controles del acceso.

**Nota:** Los controles del acceso se aplican a todos los paquetes recibidos. Si no habilita la recepción de paquetes RIP (socket 453 hexadecimal) o SAP (socket 452 hexadecimal), el reenviador IPX no funcionará.

```
add access I 0 0 453 453 0 0 0 FFFF
add access I 0 0 452 452 0 0 0 FFFF

Enter type [E] i
Destination network number (in hex) [0]? 0
Destination host (in hex) [ ]? 0
Starting destination socket number in hex [0]? 452
Ending destination socket number in hex [0]? 453
Source network number (in hex) [0]? 0
Source host number (in hex) [ ]? 0
Starting source socket number in hex [0]? 0
Ending source socket number in hex [452]? FFFF
```

**Tipo**

Identifica si se envían o se eliminan los paquetes para una dirección específica o un conjunto de direcciones. Entre I para la inclusión. Hace que el direccionador reciba el paquete y lo reenvíe si coincide con los criterios de los argumentos restantes. Entre E para la exclusión. Hace que el direccionador deseche los paquetes.

**Red-dest**

Número de red del destino. Entre el número de red en hexadecimal.

**Valores válidos**: Del X'00000000' al X'FFFFFFFF'

El cero (0) especifica todas las redes.

**Valor por omisión**: 0

**Sistemaprincipal-dest**

Número de sistema principal de la red de destino. Entre el número de sistema principal en hexadecimal.

**Valores válidos**: Del X'000000000000' al X'FFFFFFFFFFFF'

El cero (0) especifica todos los sistemas principales de la red.

**Valor por omisión**: Ninguno

**Rango-sockets-dest**
Dos números que especifican un rango inclusivo de sockets de destino. El valor de socket de destino se utiliza para la filtración de paquetes IPX.

**Valores válidos**: Del X'0000' al X'FFFF'

**Valor por omisión**: 0

**Red-origen**
Número de red del origen. Entre el número de red en hexadecimal.

Este parámetro define el número de red de la red IPX de origen cuyos paquetes se filtran por medio de este direccionador.

Si elige una filtración basada *solamente* en el valor de red de origen, el filtro se aplica a todos los sockets de origen, redes de origen y tipos de paquetes, así como al número de saltos.

**Valores válidos**: Del X'00000000' al X'FFFFFFFF'

El cero (0) especifica todas las redes.

**Valor por omisión**: 0

**Sistemaprincipal-origen**
Número de sistema principal de la red de origen. Entre el número de sistema principal en hexadecimal.

**Valores válidos**: Del X'000000000000' al X'FFFFFFFFFFFF'

El cero (0) especifica todos los sistemas principales de la red.

**Valor por omisión**: Ninguno

**Rango-sockets-origen**
Dos números que especifican un rango inclusivo de sockets de origen.

**Valores válidos**: Del X'0000' al X'FFFF'

**Valor por omisión**: 0

**Nota:** No es necesario utilizar controles del acceso y filtros de SAP para que IPX funcione en un entorno de NetWare. Utilícelos solamente si es necesario.

**Ejemplo:** `add access-control E 201 1 451 451 329 0 0 FFFF`

Este control del acceso impide que todos los nodos de la red 329 accedan al servidor de archivos con el número de red interna 201.

**broadcast-circuit** *núm. interfaz núm. circuito-ipx núm. red*
Añade un circuito de difusión IPX.

**núm. interfaz**
Especifica la interfaz de red en la que se configura el número de circuito IPX.

**Valores válidos:** Un número de interfaz de red válido

**Valor por omisión:** 0

**núm. circuito-ipx**
Especifica el número de circuito IPX. Este número debe ser exclusivo entre todos los circuitos IPX configurados en el direccionador y se utiliza para hacer referencia a circuitos IPX en muchos mandatos de configuración.

**Valores válidos:** 1 - 65535

**Valor por omisión:** El siguiente número de circuito IPX disponible

**núm. red**
Especifica el número de red IPX a utilizar en el circuito IPX. El número de red IPX 0 sólo es válido en RIP o circuitos de direccionamiento estático sin número IPXWAN. El número de red IPX FFFFFFFF no es un número de red IPX válido. El número de red IPX FFFFFFFE está reservado para la Ruta por omisión de IPX y no puede utilizarse como número de red IPX.

**Valores válidos:** 1 - FFFFFFFD

**Valor por omisión:** 1

**Ejemplo:**

```
add broadcast-circuit
Which interface [0]?
IPX circuit number [1]?
IPX network number in hex
(0 is allowed only on IPXWAN unnumbered circuits) [1]? 400
```

**filter** *saltos tipo-servicio nombre-servicio*
Impide desbordamientos de enlace lógico de NetWare para los usuarios de redes grandes permitiendo que el usuario determine el número razonable de saltos para un servicio determinado. Los filtros de SAP en IPX permiten configurar el protocolo de manera que ignore ciertas entradas de anuncios de SAP. Esto se hace para limitar el tamaño de la base de datos de SAP. Puede ser necesario debido a las limitaciones de tamaño de versiones antiguas de los servidores de archivos NetWare. También puede ser necesario para limitar la cantidad de datos SAP enviados a través de los enlaces WAN.

Los filtros de SAP consisten en una lista global de entradas de filtro con un orden. Cada entrada de filtro tiene una cuenta máxima de saltos, un tipo de servicio y un nombre de servicio opcional. Cuando se recibe un paquete de respuesta SAP, se compara cada entrada de SAP con la lista de filtros. Si la entrada de SAP coincide con una entrada de la lista de filtros y tiene más saltos de los especificados, se ignora y no entra en la base de datos de SAP local. Si la entrada de SAP coincide con una entrada de la lista de filtros y tiene un número de saltos inferior o igual al especificado, se acepta y entra en la base de datos de SAP local. Si no se encuentra ninguna coincidencia, se acepta la entrada de SAP. Los argumentos para este mandato son los siguientes:

**Saltos**
Número máximo de saltos permitido para el servicio.

**Valores válidos**: Un entero dentro del rango del 0 al 16.

**Valor por omisión**: 1

**Tipo-servicio**
Clase de servicio numérica.

**Valores válidos**: Un valor hexadecimal dentro del rango del X'0000' al X'FFFF'.

Utilice el valor de X'0000' para que se filtren todos los tipos de servicios.

**Valor por omisión**: 4

Podrá ver una lista de tipos de servicios si entra el mandato **slist** en el indicador IPX>.

**Nombre-servicio**
Identifica el nombre del servidor. En general, este campo no se entra.

**Valores válidos**: Una serie de 1 a 47 caracteres ASCII (del X'20' al X'7E').

**Valor por omisión**: Ninguno

**Ejemplo:** `add filter 2 039B NOTES-CHICAGO`

Este ejemplo ignora todos los anuncios de SAP correspondientes al servidor Lotus Notes “NOTES-CHICAGO” situado a más de 2 saltos.

**ipxwan-circuit** *núm. interfaz núm. circuito-ipx núm. red [uso-PVC] [núm. circ-FR]*
Añade un circuito punto a punto IPXWAN.

**núm. interfaz**
Especifica una interfaz PPP o Frame Relay existente en la que debe configurarse el circuito IPX.

**Valores válidos:** Un número de interfaz de red válido

**Valor por omisión:** 0

**núm. circuito-ipx**
Especifica el número de circuito IPX. Este número debe ser exclusivo entre todos los circuitos IPX configurados en el direccionador y se utiliza para hacer referencia a circuitos IPX en muchos mandatos de configuración.

**Valores válidos:** 1 - 65535

**Valor por omisión:** El siguiente número de circuito IPX disponible

**núm. red**
Especifica el número de red IPX a utilizar en el circuito IPX. El número de red IPX 0 sólo es válido en RIP o circuitos de direccionamiento estático sin número IPXWAN. El número de red IPX FFFFFFFF no es un número de red IPX válido. El número de red IPX FFFFFFFE está reservado para la Ruta por omisión de IPX y no puede utilizarse como número de red IPX.

**Valores válidos:** 0 - FFFFFFFD

**Valor por omisión:** 1

**uso-PVC**
Este parámetro sólo es necesario si el circuito IPXWAN se configura en una interfaz Frame Relay. Especifica si el circuito IPXWAN debe configurarse en un PVC o un SVC Frame Relay. 'Yes' significa que el circuito IPXWAN debe configurarse en un PVC. 'No' significa que el circuito IPX debe configurarse en un SVC.

**Valores válidos:** Yes o No

**Valor por omisión:** Yes

**núm. circ-FR**
Este parámetro sólo es necesario si el circuito se configura en Frame Relay. Si el circuito IPXWAN que se configura es un PVC Frame Relay, el parámetro especifica el número de circuito PVC Frame Relay. Si el circuito IPXWAN que se configura es un SVC Frame Relay, el parámetro especifica el nombre de circuito SVC Frame Relay.

**Valores válidos:** Un número de circuito PVC Frame Relay o un nombre de circuito SVC Frame Relay válido

**Valor por omisión:** 16 (PVC) o Ninguno (SVC)

**Ejemplo:**

```
add ipxwan-circuit
Which interface [0]? 2
IPX circuit number [1]? 3
IPX network number in hex
(0 is allowed only on IPXWAN unnumbered circuits) [0]? 412
Use Frame Relay PVC ? yes
Frame Relay PVC circuit number [16]?

add ipxwan circuit
Which interface [0]? 3
IPX circuit number [2]? 4
IPX network number in hex
(0 is allowed only on IPXWAN unnumbered circuits) [0]? 413
Use Frame Relay PVC ? No
Frame Relay SVC circuit name ? Indianapolis
```

**route-static** *red-dest núm. circuito-ipx siguienteSalto ciclos saltos*
Añade una ruta estática.

**red-dest**
Especifica el número de red IPX de destino.

**Valores válidos**: Del X'1' al X'FFFFFFFE'

**Valor por omisión**: 1

**núm. circuito-ipx**
Especifica un circuito IPX existente en el que debe configurarse la ruta estática.

**Valores válidos**: Un número de circuito IPX existente

**Valor por omisión**: 1

**siguienteSalto**
Especifica el número de sistema principal IPX del direccionador de siguiente salto mediante el cual se puede llegar a la red de destino.

**Valores válidos**: Del X'1' al X'FFFFFFFFFFFE'

**Valor por omisión:**Ninguno

**ciclos**
Indica el número de ciclos entre la red de destino y este direccionador. El número de ciclos representa el período de tiempo que tarda la transmisión de un paquete IPX de 576 bytes desde este direccionador a la red de destino. Cada ciclo son 55 milisegundos.

**Valores válidos**: Del 0 al 30000

**Valor por omisión**: 0

**saltos**
Indica el número de saltos entre la red de destino y este direccionador.

**Valores válidos**: Del 0 al 14

**Valor por omisión**: 0

**Ejemplo:**

```
add route-static
IPX net address: (1-fffffffe) [1]? 30
IPX circuit number [1]? 2
IPX node address (in hex) []? 020000002030
Ticks: (0-3000) [0]? 4
Hops: (0-14) [0]? 4
```

**sap-static** *tipoServicio nombServicio núm. circuito-ipx redServidor nodoServidor socketServidor saltos*
Añade un servicio de SAP estático.

**tipoServicio**
Especifica la clase de servicio hexadecimal del servicio.

**Valores válidos**: Del X'0' al X'FFFF'

**Valor por omisión**: 4

**nombServicio**
Especifica el nombre ASCII del servicio.

**Valores válidos**: Hasta 47 caracteres ASCII de los siguientes: 'A'–'Z', 'a'–'z', '0'–'9', '_', '-', '@'.

**Valor por omisión**: Ninguno

**núm. circuito-ipx**
Especifica un circuito IPX existente en el que debe configurarse el servicio estático de SAP.

**Valores válidos**: Un número de circuito IPX existente

**Valor por omisión**: 1

**redServidor**
Especifica el número de red IPX interna o número de red IPX inicial del servidor.

**Valores válidos**: Del X'1' al X'FFFFFFFE'

**Valor por omisión**: 1

**nodoServidor**
Especifica el nodo IPX del servidor.

**Valores válidos**: Del X'1' al X'FFFFFFFFFFFE'

**Valor por omisión**: Ninguno

**socketServidor**
Especifica el número de socket del servidor.

**Valores válidos**: Del X'0' al X'FFFF'

**Valor por omisión**: 451

**saltos**
Indica el número de saltos entre el servidor y este direccionador.

**Valores válidos**: Del 0 al 14

**Valor por omisión**: 0

**Ejemplo:**

```
add sap-static
Sap type: (0-ffff) [4]? 4
IPX circuit number [1]? 2
IPX net address: (1-fffffffe) [1]? 40
IPX node address, in hex:  []? 000000000001
IPX socket:  (0-ffff) [451]?
Hops: (0-14) [0] 4
```

## Delete

Utilice el mandato **delete** para suprimir un circuito de difusión IPX o punto a punto IPXWAN, un filtro de IPX global (control del acceso), un filtro de SAP global, una ruta estática o un servicio estático.

**Sintaxis:**

**delete** access-control . . .
circuit . . .
filter . . .
route-static . . .
sap-static . . .

**access-control** *núm. línea*
Suprime el control del acceso que coincida con el número de línea que se entre. Entre el mandato **list** para visualizar los números de línea actuales.

**Ejemplo:** `delete access-control 2`

**circuit** *núm. circuito-ipx*
Suprime el circuito de difusión IPX o punto a punto IPXWAN. También suprimirá todas las rutas estáticas, servicios estáticos y filtros de circuito que se hayan asociado con el *núm. circuito-ipx* especificado.

**Ejemplo:** `delete circuit`

```
IPX circuit number [1]? 2
You are about to delete IPX broadcast circuit 2 on interface 4.
All associated static routes, static services and circuit filters
will be deleted as well.  Are you sure? [Yes]: yes
```

**filter** *saltos tipo-servicio nombre-servicio*

Suprime el filtro de SAP especificado. Debe escribir el filtro de SAP exactamente como aparece cuando se ejecuta el mandato list. Los argumentos son los siguientes:

**Saltos**

Número máximo de saltos permitido para el servicio.

**Valores válidos**: Del 0 al 16

**Valor por omisión**: 16

**Tipo-servicio**

Clase de servicio numérica. Entre un número hexadecimal de 2 bytes.

**Valores válidos**: Del X'0000' al X'FFFF'

**Valor por omisión**: Ninguno

**Nombre-servicio**

Si la entrada que va a suprimir tiene un nombre, especifíquelo.

**Valores válidos**: Una serie de 1 a 47 caracteres ASCII (del X'20' al X'7E').

**Valor por omisión**: Ninguno

**Ejemplo:** `delete filter 2 039B NOTES-CHICAGO`

**route-static** *red-dest núm. circuito-ipx siguienteSalto*

Suprime una ruta estática.

**red-dest**

Especifica el número de red IPX de destino.

**Valores válidos**: Del X'1' al X'FFFFFFFE'

**Valor por omisión**: 1

**núm. circuito-ipx**

Especifica el circuito IPX en el que está configurada la ruta estática.

**Valores válidos**: Un número de circuito IPX existente

**Valor por omisión**: 1

**siguienteSalto**

Especifica el número de sistema principal IPX del direccionador de siguiente salto mediante el cual se puede llegar a la red de destino.

**Valores válidos**: Del X'1' al X'FFFFFFFFFFFE'

**Valor por omisión**: Ninguno

**Ejemplo:**

```
delete route-static
IPX net address: (1-fffffffe) [1]? 30
IPX circuit number [1]? 2
IPX node address (in hex) []? 020000002030
```

**sap-static** *tipoServicio nombServicio núm. circuito-ipx*

Suprime un servicio de SAP estático.

**tipoServicio**
Especifica la clase de servicio hexadecimal del servicio.

**Valores válidos**: Del X'0' al X'FFFF'

**Valor por omisión**: 4

**nombServicio**
Especifica el nombre ASCII del servicio.

**Valores válidos**: Hasta 47 caracteres ASCII de los siguientes: 'A'–'Z', 'a'–'z', '0'–'9', '_', '-', '@'.

**Valor por omisión**: Ninguno

**núm. circuito-ipx**
Especifica el circuito IPX en el que está configurado el servicio estático de SAP.

**Valores válidos**: Un número de circuito IPX existente

**Valor por omisión**: 1

**Ejemplo:**

```
delete sap-static
Sap type: (0-ffff) [4]?
Sap name: (0-ffff) []? filesrv1
IPX circuit number [1]? 2
```

## Disable

Utilice el mandato **disable** para inhabilitar globalmente o bien en circuitos IPX específicos; inhabilita globalmente el uso de las rutas y servicios estáticos de IPX. Además, utilice el mandato **disable** si desea inhabilitar las respuestas a las peticiones SAP para obtener el servidor más próximo, el ritmo de difusión de RIP-SAP, así como RIP o SAP en circuitos específicos.

**Sintaxis:**

**disable** circuit . . .
ipx
keepalive-filtering . . .
nebios-broadcast . . .
reply-to-get-nearest-server . . .
rip . . .
rip-sap-pacing . . .
route-static . . .
sap . . .
sap-static . . .

**circuit** *núm. circuito-ipx*
Inhabilita el circuito de difusión IPX o punto a punto IPXWAN especificado mediante *circuito-ipx.*

**Ejemplo: `disable circuit`**

```
IPX circuit number [1]? 2
```

**ipx** Inhabilita el protocolo IPX globalmente.

**Ejemplo: `disable ipx`**

**keepalive-filtering** *núm. circuito-ipx*

Inhabilita la filtración de Keepalive en el circuito de difusión IPX o en los circuitos punto a punto IPXWAN especificados mediante *núm. circuito-ipx*.

**Ejemplo: `disable keepalive-filtering`**

```
IPX circuit number [1]? 2
```

**netbios-broadcast** *núm. circuito-ipx*

Inhabilita la recepción y el envío de difusiones de Novell NetBIOS (tipo de paquete 20) en el circuito IPX especificado mediante *núm. circuito-ipx*. El valor por omisión es la habilitación. La recepción y el envío de difusiones de Novell NetBIOS se inhabilitan automáticamente en los circuitos con direccionamiento estático de IPXWAN aunque se hayan habilitado en la configuración.

**Ejemplo: `disable netbios-broadcast`**

```
IPX circuit number [1]? 2
```

**reply-to-get-nearest-server** *núm. circuito-ipx*

Impide que el direccionador responda a las peticiones SAP para obtener el servidor más próximo en el circuito de difusión IPX o en el circuito punto a punto IPXWAN especificados mediante *núm. circuito-ipx.*

**Nota:** Hay que ir con mucho cuidado al inhabilitar esta función. Este mandato sólo debe utilizarse cuando existen diversos direccionadores (o servidores) en una red IPX y es sabido que el “mejor” servidor no se encuentra detrás de este direccionador.

**Ejemplo: `disable reply-to-get-nearest`**

```
IPX circuit number [1]? 2
```

**rip** *núm. circuito-ipx*

Inhabilita RIP en el circuito de difusión IPX o en el circuito punto a punto IPXWAN especificados mediante *núm. circuito-ipx*. El valor por omisión es que RIP esté habilitado en todos los circuitos. RIP se inhabilitará automáticamente en los circuitos que utilicen el direccionamiento estático de IPXWAN aunque se haya habilitado en la configuración.

**Ejemplo: `disable rip 1`**

**rip-sap-pacing** *núm. circuito-ipx*

Evita el ritmo de difusión de RIP/SAP en el circuito de difusión IPX o punto a punto IPXWAN especificado mediante *núm. circuito-ipx*. Cuando se inhabilita el ritmo, las difusiones periódicas de RIP y SAP se transmiten en el circuito con un intervalo interpaquetes de 55 milisegundos (el valor por omisión). Habilite el ritmo únicamente en los circuitos en que las difusiones de RIP y SAP puedan causar congestión (por ejemplo, puede habilitar el ritmo en los circuitos frame-relay o X.25 con muchos circuitos virtuales).

**Ejemplo: `disable rip-sap-pacing`**

```
IPX circuit number [1]? 2
```

**route-static**

Inhabilita globalmente el uso de las rutas estáticas.

**Ejemplo: `disable route-static`**

**sap** *núm. circuito-ipx*

Inhabilita SAP en el circuito de difusión IPX o punto a punto IPXWAN especificado mediante *circuito-ipx*. El valor por omisión es que SAP esté habilitado en todos los circuitos. SAP se inhabilitará automáticamente en los circuitos RLAN y en el caso del direccionamiento estático de IPXWAN aunque se haya habilitado SAP en la configuración.

**Ejemplo: `disable sap`**

```
IPX circuit number [1]? 2
```

**sap-static**

Inhabilita globalmente el uso de los servicios estáticos.

**Ejemplo:** `disable sap-static`

## Enable

Utilice el mandato **enable** para habilitar IPX globalmente o en circuitos específicos. El mandato enable también puede utilizarse para habilitar globalmente el uso de las rutas o servicios estáticos de IPX; habilita la filtración de keepalive, el ritmo de difusión de RIPS-SAP, la respuesta a petición SAP para obtener el servidor más próximo, así como RIP o SAP en circuitos específicos.

**Sintaxis:**

**enable** circuit . . .
ipx
keepalive-filtering . . .
nebios-broadcast . . .
reply-to-get-nearest-server . . .
rip . . .
rip-sap-pacing . . .
route-static . . .
sap . . .
sap-static . . .

**circuit** *núm. circuito-ipx núm. red*

Habilita el circuito de difusión IPX o punto a punto IPXWAN especificado mediante *núm. circuito-ipx* y especifica el número de red IPX para el circuito IPX. El circuito IPX se habilitará si se configura un número de red IPX válido.

**Ejemplo: enable circuit**

```
IPX circuit number [1]?
IPX network number in hex
(0 is allowed only on IPXWAN unnumbered circuits) [1]?
```

**núm. circuito-ipx**

Especifica el circuito de difusión IPX o punto a punto IPXWANa habilitar.

**Valores válidos**: Cualquier número de circuito IPX válido

**Valor por omisión**: 0

**núm. red**

Especifica la red IPX a utilizar en el circuito. El número de red IPX 0 sólo es válido en RIP o circuitos de direccionamiento estático sin número IPXWAN. El número de red IPX FFFFFFFF no es un número de red IPX válido. El número de red IPX FFFFFFFE está

reservado para la Ruta por omisión de IPX y no puede utilizarse como número de red IPX.

**Valores válidos**: Del X'0' al X'FFFFFFFD'

**Valor por omisión**: 1

**Ejemplo:**

**ipx** Habilita el protocolo IPX globalmente.

**Ejemplo:** **`enable ipx`**

**keepalive-filtering** *núm. circuito-ipx*
Habilita la filtración de Keepalive en el circuito de difusión IPX o punto a punto IPXWAN especificado mediante *núm. circuito-ipx*.

**Ejemplo:** **`enable keepalive-filtering`**

```
IPX circuit number [1]? 2
```

**netbios-broadcast** *núm. circuito-ipx*
Habilita la recepción y el envío de difusiones de Novell NetBIOS (tipo de paquete 20) en el circuito IPX especificado mediante *núm. circuito-ipx*. El valor por omisión es la habilitación. La recepción y el envío de difusiones de Novell NetBIOS se inhabilitan automáticamente en los circuitos con direccionamiento estático de IPXWAN aunque se hayan habilitado en la configuración.

**Ejemplo:** **`enable netbios-broadcast`**

```
IPX circuit number [1]? 2
```

**reply-to-get-nearest-server** *núm. circuito-ipx*
Permite que el direccionador responda a las peticiones SAP para obtener el servidor más próximo en el circuito de difusión IPX o punto a punto IPXWAN especificado mediante *circuito-ipx#.*

**Ejemplo:** **`enable reply-to-get-nearest`**

```
IPX circuit number [1]? 2
```

**rip** *núm. circuito-ipx*
Habilita RIP en el circuito de difusión IPX o punto a punto IPXWAN especificado mediante *núm. circuito-ipx*. El valor por omisión es que RIP esté habilitado en todos los circuitos IPX. RIP se inhabilita automáticamente en los circuitos RLAN y en los circuitos con el direccionamiento estático de IPXWAN aunque se haya habilitado RIP en la configuración.

**Ejemplo:** **`enable rip`**

```
IPX circuit number [1]? 2
```

**rip-sap-pacing** *núm. circuito-ipx*
Habilita el ritmo de difusión de RIP/SAP en el circuito de difusión IPX o punto a punto IPXWAN especificado mediante *núm. circuito-ipx*.

**Nota:** El direccionador calcula un intervalo interpaquetes que garantiza la realización de esta difusión dentro de los intervalos de actualización de RIP y SAP configurados. Puede ser necesaria la configuración de estos intervalos en un valor mayor para que el direccionador calcule un intervalo interpaquetes lo suficientemente amplio.

El ritmo sólo debe habilitarse en los circuitos en que las difusiones de RIP y SAP puedan causar congestión (por ejemplo, en los circuitos frame-relay o X.25 con muchos circuitos virtuales).

**Ejemplo: `enable rip-sap-pacing`**

```
IPX circuit number [1]? 2
```

**route-static**
Habilita globalmente el uso de las rutas estáticas.

**Ejemplo: `enable route-static`**

**sap** *núm. circuito-ipx*
Habilita SAP en el circuito de difusión IPX o punto a punto IPXWAN especificado mediante *núm. circuito-ipx*.

**Ejemplo: `enable sap`**

**sap-static**
Habilita globalmente el uso de los servicios estáticos.

**Ejemplo: `enable sap-static`**

## Filter-lists

Utilice el mandato **filter-lists** para acceder al indicador `IPX` *`tipo-filtro`*`-List Config>`. Los tipos válidos de listas-filtro son direccionador, rip, sap e ipx.

Para obtener información sobre los mandatos disponibles en el indicador `IPX` *`tipo-filtro`*`-List Config>`, consulte la sección “Mandatos de configuración de filtros de circuito para circuitos IPX” en la página 744.

**Sintaxis:**

| | |
|---|---|
| f**ilter-lists** | router-lists<br>rip-lists<br>sap-lists<br>ipx-lists |

**Ejemplo: `filter-lists router-lists`**

## Frame

Utilice el mandato **frame** con el fin de especificar el formato de paquete para circuitos IPX. (La encapsulación también puede establecerse mediante el mandato de CONFIG **network**.)

**Nota:** Cuando hay registros de configuración incorrectos o no válidos, se utilizan los valores de trama por omisión.

**Sintaxis:**

| | |
|---|---|
| fr**ame** | ethernet_II . . .<br>ethernet_8022 . . .<br>ethernet_8023 . . .<br>ethernet_SNAP . . .<br>token-ring MSB . . .<br>token-ring LSB . . .<br>token-ring_SNAP MSB . . .<br>token-ring_SNAP LSB . . . |

**ethernet_II** *núm. circuito-ipx*

Establece el tipo de trama como ethernet_II en el circuito de difusión IPX especificado mediante *núm. circuito-ipx*. La encapsulación ethernet_II utiliza la versión 2.0 de ethernet con el tipo de protocolo 8137. Éste es el valor por omisión de NetWare 4.0 y es el superior.

**Ejemplo: `frame ethernet_II`**

```
IPX circuit number [1]?
```

**ethernet_8022** *núm. circuito-ipx*

Establece el tipo de trama como ethernet_8022 en el circuito de difusión IPX especificado mediante *núm. circuito-ipx*. La encapsulación ethernet_8022 utiliza una encapsulación de LLC con SAP E0.

**Ejemplo: `frame ethernet_8022`**

```
IPX circuit number [1]?
```

**ethernet_8023** *núm. circuito-ipx*

Establece el tipo de trama como ethernet_8023 en el circuito de difusión IPX especificado mediante *núm. circuito-ipx*. La encapsulación ethernet_8023 utiliza la encapsulación ethernet 802.3 sin cabecera de LLC. Éste es el valor por omisión de antes de NetWare 4.0. También es un valor por omisión del direccionador.

**Ejemplo: `frame ethernet_8023`**

```
IPX circuit number [1]?
```

**ethernet_SNAP** *núm. circuito-ipx*

Establece el tipo de trama como ethernet_SNAP en el circuito de difusión IPX especificado mediante *núm. circuito-ipx*. La encapsulación ethernet_SNAP utiliza una encapsulación de SNAP con el PID de 0000008137.

**Ejemplo: `frame ethernet_SNAP`**

```
IPX circuit number [1]?
```

**token-ring MSB** *núm. circuito-ipx*

Establece el tipo de trama como el MSB de Red en Anillo en el circuito de difusión IPX especificado mediante *núm. circuito-ipx*. La encapsulación de tipo MSB de Red en Anillo utiliza una encapsulación de LLC con SAP E0 y las direcciones del MAC no canónicas. Éste es el valor por omisión de NetWare. También es un valor por omisión del direccionador.

**Ejemplo: `frame token-ring MSB`**

```
IPX circuit number [1]?
```

**token-ring LSB** *núm. circuito-ipx*

Establece el tipo de trama como el LSB de Red en Anillo en el circuito de difusión IPX especificado mediante *núm. circuito-ipx*. La encapsulación de tipo LSB de Red en Anillo utiliza una encapsulación de LLC con SAP E0 y las direcciones del MAC no canónicas.

**Ejemplo: `frame token-ring LSB`**

```
IPX circuit number [1]?
```

**token-ring_SNAP MSB** *núm. circuito-ipx*

Establece el tipo de trama como el MSB de Red en Anillo SNAP en el circuito de difusión IPX especificado mediante *núm. circuito-ipx*. La encapsulación de tipo MSB de Red en Anillo SNAP utiliza una

encapsulación de SNAP con el PID 0000008137 y las direcciones del MAC canónicas.

**Ejemplo:** `frame token-ring_SNAP MSB`

```
IPX circuit number [1]?
```

**token-ring_SNAP LSB** *núm. circuito-ipx*
Establece el tipo de trama como el LSB de Red en Anillo en el circuito de difusión IPX especificado mediante *núm. circuito-ipx*. Esta encapsulación de tipo LSB de Red en Anillo utiliza una encapsulación de SNAP con el PID 0000008137 y las direcciones del MAC no canónicas.

## List

Utilice el mandato **list** para visualizar la configuración actual de IPX.

**Sintaxis:**

**list**
access-controls
all
circuit
filters
route-static
sap-static
summary

**access-controls**
Lista los filtros de IPX globales (controles del acceso). Este mandato visualiza la información que se visualiza en la sección “Access Control Configuration” del mandato **list all**.

**all** Lista toda la configuración de IPX.

### Ejemplo:

```
 list all

IPX Globals
------------
IPX Globally                Enabled
Host Number (serial line)   020000003024
Maximum Services                 32
Maximum Networks                 32
Maximum Routes                   32
Maximum Routes per Destination   1
Maximum Local Cache entries      64
Maximum Remote Cache entries     64
Keepalive-Filtering Table Size   32


IPX Configuration:

------------------
                                 NetBIOS    Keepalive
Circ   Ifc    NetNum    IPX      Broadcast  Filtering  Encapsulation
 1      0      400       Enabled   Enabled    Disabled   ETHERNET_II
 2      1      411       Enabled   Enabled    Disabled   N/A
 3      2      412       Enabled   Enabled    Disabled   N/A
        Frame Relay PVC circuit number: 16
 4      3      413       Enabled   Enabled    Disabled   N/A
        Frame Relay SVC circuit name: Indianapolis


RIP Configuration:
------------------
                                 Update    Split      Broadcast  RIP
Circ   Ifc    NetNum    RIP      Interval  Horizon    Pacing     Ticks
1      0      400       Enabled   1         Enabled    Disabled   0
2      1      411       Enabled   1         Enabled    Disabled   3
3      2      412       Enabled   1         Enabled    Disabled   0
4      3      413       Enabled   1         Enabled    Disabled   0



SAP Configuration:
------------------
                                 Update    Split      Broadcast  Get Nearest
Circ   Ifc    NetNum    SAP      Interval  Horizon    Pacing     Reply
1      0      400       Enabled   1         Enabled    Disabled   Enabled
2      1      411       Enabled   1         Enabled    Disabled   Enabled
3      2      412       Enabled   1         Enabled    Disabled   Enabled
4      3      413       Enabled   1         Enabled    Disabled   Enabled



IPXWAN Configuration:
---------------------
Router Name    ipxwan-413
NodeID         413
                           Routing  Connect     Retry
Circ   Ifc    NetNum      Type     Time (sec)  Time (sec)
2      1      411         RIP      60          60
3      2      412         RIP      60          60
4      3      413         RIP      60          60

Static Route Configuration:
---------------------------
Static Routes:  Enabled
Dest Net  Hops   Ticks  Next Hop      Circ   Ifc
ABC       3      4      020000003044  3      2
```

```
Static Services Configuration:
------------------------------
Static Services:  Enabled
Type Service Name                   Srv Net  Host         Sock Hops Circ   Ifc
4    FILESRV01                      ABC      000000000001 451  3    3      2

SAP Filter Configuration:
-------------------------
IPX SAP Filters:  Enabled
Index Max Hops  Type  Service Name
1     5         4     FILESRV02

Access Control Configuration:
-----------------------------
IPX Access Controls:  Enabled
#   T Dest Net Host         Sock Sock Src Net  Host         Sock Sock
1   E 2        000000000000 0    FFFF 3        000000000000 0    FFFF
2   I 0        000000000000 452  453  0        000000000000 0    FFFF
```

**circuit** *núm. circuito-ipx*
Lista el circuito de difusión IPX o punto a punto IPXWANespecificado mediante *núm. circuito-ipx*. Este mandato visualiza la información mostrada en las secciones “IPX Configuration”, “RIP Configuration”, “SAP Configuration” e “IPXWAN Configuration” del ejemplo del mandato **list all**.

**filters** Lista los filtros de SAP globales. Este mandato visualiza la información mostrada en la sección “SAP Filter Configuration” del ejemplo del mandato **list all**.

**route-static**
Lista las rutas estáticas. Este mandato visualiza la información mostrada en la sección “Static Route Configuration” del ejemplo del mandato **list all**.

**sap-static**
Lista los servicios estáticos. Este mandato visualiza la información mostrada en la sección “Static Services Configuration” del ejemplo del mandato **list all**.

**summary** Lista un resumen de la configuración de IPX, de RIP, de SAP, de IPXWAN y de la filtración de Keepalive para todos los circuitos en los que se ha habilitado IPX. Este mandato visualiza la información mostrada en las secciones “IPX Globals”, “IPX Configuration”, “RIP Configuration”, “SAP Configuration” e “IPXWAN Configuration” del ejemplo del mandato **list all**.

**IPX Globals**
Se visualiza la información global siguiente:

- Si se ha habilitado o inhabilitado IPX globalmente
- Número de sistema principal IPX
- Número máximo de servicios
- Número máximo de redes
- Número máximo de rutas
- Número máximo de rutas por destino
- Número máximo de entradas de antememoria local
- Número máximo de entradas de antememoria remota
- Tamaño de tabla de filtración de Keepalive

**IPX Configuration**

Se visualiza lo siguiente para cada circuito en que se ha habilitado IPX:

- Número de circuito IPX
- Número de interfaz de red
- Número de red IPX (Netnum)
- Si se ha habilitado/inhabilitado IPX en el circuito
- Difusión de NetBIOS
- Filtración de Keepalive
- Encapsulación

**PVC circuit number**

Visualiza el número del circuito PVC Frame Relay.

**SVC circuit name**

Visualiza el nombre del circuito SVC Frame Relay.

**RIP Configuration**

Se visualiza la información siguiente para cada circuito en que se ha habilitado IPX:

- Número de circuito IPX
- Número de interfaz de red
- Número de red IPX (Netnum)
- Si se ha habilitado o inhabilitado RIP
- Temporizador de intervalos de actualización de RIP
- Si se ha habilitado o inhabilitado el horizonte de división
- Si se ha habilitado o inhabilitado el ritmo de difusión de RIP
- Coste de ruta de IPX (en ciclos)

**SAP Configuration**

Se visualiza la información siguiente para cada circuito en que se ha habilitado IPX:

- Número de circuito IPX
- Número de interfaz de red
- Número de red IPX (Netnum)
- Si se ha habilitado o inhabilitado SAP
- Temporizador de intervalos de actualización de SAP
- Si se ha habilitado o inhabilitado el horizonte de división
- Si se ha habilitado o inhabilitado el ritmo de difusión de SAP
- Si se ha habilitado la respuesta a petición SAP para obtener el servidor más próximo.

**IPXWAN Configuration**

Se visualiza la información global siguiente:

- Nombre de direccionador
- ID de nodo

Se visualiza la información siguiente para cada circuito IPXWAN:

- Número de circuito IPX
- Número de interfaz de red
- Número de red IPX (Netnum)
- Tipo de direccionamiento
- Temporizador de conexiones
- Temporizador de reintentos

**Static Routes Configuration**
Visualiza si se han habilitado o inhabilitado globalmente las rutas estáticas. Además, se visualiza lo siguiente para cada ruta estática configurada.

- Número de red de destino IPX
- Saltos
- Ciclos
- Dirección de nodo de siguiente salto
- Número de circuito IPX
- Número de interfaz de red

**Static Services Configuration**
Visualiza si se han habilitado o inhabilitado globalmente los servicios estáticos. Además, se visualiza lo siguiente para cada servicio estático configurado:

- Tipo de servicio
- Nombre de servicio
- Número de red IPX del servicio
- Dirección de nodo IPX del servicio (Host)
- Socket
- Saltos
- Número de circuito IPX
- Número de interfaz de red

**SAP Filter Configuration**
Visualiza si se han habilitado o inhabilitado los filtros de SAP globales. Además, se visualiza la información siguiente para cada filtro de SAP global configurado:

- Índice
- Número máximo de saltos
- Tipo de servicio
- Nombre de servicio

**Access Control Configuration**
Visualiza si se han habilitado o inhabilitado los filtros de IPX globales (controles del acceso). Además, se visualiza la información siguiente para cada filtro de IPX global (control del acceso) configurado:

- Índice de control del acceso (núm.)
- Tipo de filtro (de inclusión o exclusión)
- Número de red IPX de destino
- Número de nodo IPX de destino (Host)
- Rango de sockets IPX de destino
- Número de red IPX de origen
- Número de nodo IPX de origen (Host)
- Rango de sockets IPX de origen

## Move

Utilice el mandato **move** para reordenar los elementos de filtro de IPX global (control del acceso) o trasladar un circuito IPX de una interfaz a otra.

**Sintaxis:**

| | |
|---|---|
| m**ove** | access-control *núm. líneaOrigen núm. líneaDest*<br>circuit *núm. circuito-ipx  núm. interfaz [uso-PVC] [núm. circ-FR]* |

**access-control** *núm. líneaOrigen núm. líneaDest*

**núm. líneaOrigen**
Especifica el número de línea del control del acceso que desea trasladar.

**núm. líneaDest**
Especifica hasta después de qué número de línea de control del acceso debe trasladar líneaOrigen.

Después de trasladarse el control del acceso de una línea, las líneas se vuelven a numerar.

**Ejemplo:**

```
move access-control
Enter index of control to move [1]? 1
Move record AFTER record number [0]? 2
About to move:
#   T Dest Net Host         Sock Sock Src Net  Host         Sock Sock
1   E 2        000000000000 0    FFFF 3        000000000000 0    FFFF
to be after:
2   I 0        000000000000 452  453  0        000000000000 0    FFFF
Are you sure this is what you want to do? [Yes]: yes
```

**circuit** *núm. circuito-ipx  núm. interfaz  [uso-PVCnúm.  circ-FR]*
Traslada un circuito IPX de una interfaz de red a otra. Este mandato también traslada todas las rutas estáticas, servicios estáticos y filtros de circuito IPX que se hayan asociado con el *núm. circuito-ipx* determinado a la misma *núm. interfaz*. Si se va a trasladar un circuito IPXWAN a una interfaz Frame Relay, se le solicita que especifique si el nuevo circuito es un PVC o un SVC Frame Relay y que proporcione el número o el nombre de circuito Frame Relay, según lo que corresponda.

**núm. circuito-ipx**
Especifica el circuito IPX que se va a trasladar.

**Valores válidos:** Un número de circuito IPX existente

**Valor por omisión:** 1

**núm. interfaz**
Especifica la interfaz de red a la que se va a trasladar el circuito IPX.

**Valores válidos:** Un número de interfaz de red existente.

**Valor por omisión:** 0

**uso-PVC**
Especifica si el circuito IPXWAN se va a trasladar a un PVC o a un SVC Frame Relay. 'Yes' significa que el circuito IPXWAN se va a trasladar a un PVC. 'No' significa que el circuito IPXWAN se va a trasladar a un SVC. Este parámetro sólo es necesario si el circuito IPXWAN se va a trasladar a una interfaz Frame Relay.

**Valores válidos:** Yes o No

**Valor por omisión:** Yes

**núm. circ-FR**
Especifica el número de circuito PVC Frame Relay o el nombre de circuito SVC Frame Relay. Este parámetro sólo es necesario si el

circuito IPX es un circuito IPXWAN que se va a trasladar a una interfaz Frame Relay.

**Valores válidos:** Un número de circuito PVC Frame Relay o un nombre de circuito SVC Frame Relay existente

**Valor por omisión:** 16 (PVC) o Ninguno (SVC)

**Ejemplo:** move circuit

```
IPX circuit number [1]?
Which interface do you want to move the IPX circuit to []? 5
Use Frame Relay PVC? [Yes]:
Frame Relay PVC circuit number [16]? 18
You are about to move IPXWAN circuit 1,
from Frame Relay interface 2 (FR circuit 16) to
Frame Relay interface 5 (FR circuit 18).
All associated static routes, static services and circuit filters
will be moved as well. Are you sure? [Yes]: Y
```

## Set

Utilice el mandato **set** para configurar el número de sistema principal, el ID de nodo y nombre de direccionador IPXWAN, el tipo de direccionamiento de IPXWAN,el tiempo de espera excedido de conexión y el temporizador de reintentos, los números de red IPX, los tamaños máximos de tabla de RIP y SAP, los tamaños de antememoria local y remota, los estados de filtro de IPX global (control del acceso) y filtro de SAP global, los intervalos de actualización de RIP y SAP, el coste de ruta de IPX (en ciclos),el tamaño de tabla de filtración de Keepalive y el uso del horizonte de división.

**Sintaxis:**

**set**
- access-control . . .
- filter . . .
- host-number . . .
- ipxwan . . .
- keepalive-table-size . . .
- local-cache size . . .
- maximum routes-per-destination . . .
- maximum networks . . .
- maximum services . . .
- maximum total-route-entries . . .
- name . . .
- net-number . . .
- node-id . . .
- remote-cache size . . .
- rip-ticks . . .
- rip-update-interval . . .
- sap-update-interval . . .
- split-horizon . . .

**access-control** *on* **u** *off*

Activa o desactiva los filtros de IPX globales (controles del acceso). Entre **on** u **off**.

**Ejemplo:** `set access-control on`

**filter** *on* **u** *off*

Activa o desactiva los filtros de SAP globales. Entre **on** u **off**.

**Ejemplo:** `set filter on`

**host-number** *sistemaprincipal#*

Especifica el número de sistema principal utilizado para los circuitos serie que ejecuten IPX. Cada direccionador IPX que funcione sobre circuitos serie debe tener un número de sistema principal exclusivo. Es necesario porque los circuitos serie no tienen direcciones de nodo de hardware a partir de las cuales se pueda crear un número de sistema principal. No puede ser una dirección de vertimiento múltiple.

**Nota:** Si configura una mezcla de circuitos de difusión IPX e IPXWAN en la misma interfaz, es muy recomendable que configure el número de sistema principal de manera que sea el identificador de nodo IPXWAN seguido de X'0000'.

**Valores válidos**: Un número hexadecimal de 12 dígitos dentro del rango del X'000000000001' al X'FEFFFFFFFFFF'.

**Valor por omisión**: Ninguno

Este número debe ser exclusivo en cada direccionador.

**Ejemplo:** `set host-number 0000000000F4`

**Nota:** IPXWAN requiere que se configuren un ID de nodo y un nombre de direccionador. Utilice los mandatos **set node-ID** y **set name** para configurar estos parámetros.

**ipxwan** *núm. circuito-ipx tipo-direccionamiento tiempoEsperaExcedido temporizadorReintentos*

Establece el tipo de direccionamiento, el tiempo de espera excedido de conexión y el temporizador de reintentos de IPXWAN. Para poder invocar el mandato **set ipxwan**, debe añadir un circuito IPXWAN.

**núm. circuito-ipx**

Especifica un circuito punto a punto IPXWAN existente en el que se establecerán los parámetros.

**Valores válidos**: Cualquier número de circuito punto a punto IPXWAN existente

**Valor por omisión**: 1

**tipoDireccionamiento**

Especifica el tipo de direccionamiento de IPXWAN a negociar.

- **u** para RIP sin número
- **r** para RIP con número
- **b** para RIP con número y RIP sin número
- **s** Direccionamiento estático

**Valores válidos**: 'u', 'U', 'r', 'R', 'b', 'B', 's', 'S'

**Valor por omisión**: 'u'

**tiempoEsperaExcedido**

Este valor especifica el límite de tiempo, en segundos, dentro del cual debe completarse satisfactoriamente la negociación de IPXWAN. Si no puede completarse satisfactoriamente antes de que caduque el temporizador de conexiones, IPXWAN inicia un temporizador de reintentos. El dispositivo no reintentará la negociación hasta que caduque el temporizador de reintentos.

**Valores válidos**: Un número entero de segundos dentro del rango del 5 al 300.

**Valor por omisión**: 60 segundos

**temporizadorReintentos**
Este parámetro especifica el período de tiempo a esperar, después de que una conexión haya sobrepasado el tiempo de espera excedido, antes de intentar restablecer la conexión.

**Valores válidos**: Un número entero de segundos dentro del rango del 5 al 600.

**Valor por omisión**: 60 segundos

**Ejemplo:** **`set ipxwan`**

```
IPX circuit number [1]? 3
Routing type ('u'=Unnumbered, 'r'=RIP, 'b'=Both, 's'=Static) [u]
Connection Timeout (in sec) [60]?
Retry timer (in sec) [60]?
```

**keepalive-table-size** *valor*
Establece el número de entradas que contiene la tabla de Keepalive. Estas entradas incluyen todos los pares actuales cliente/servidor y servidor/servidor conectados sobre el enlace WAN.

**Valores válidos:** Del 1 al 250

**Valor por omisión:** 32

**Ejemplo:** **`set keepalive-table-size`**

```
Number of entries [32]?
```

**local-cache size** *tamaño*
Especifica el tamaño de la tabla de direccionamiento de antememoria local.

El tamaño de la antememoria local debe ser equivalente al número total de clientes de las redes de cliente o locales del direccionador más un almacenamiento intermedio de un 10% para prevenirse contra excesivas peticiones de eliminación.

**Valores válidos**: El rango es del 1 al 10000.

**Valor por omisión**: 64. Para obtener más información, consulte “Antememoria local” en la página 710 y “Antememoria remota” en la página 710.

**Ejemplo:** **`set local-cache size`**

```
New IPX local node cache size [64]? 80
```

**maximum routes-per-destination** *rutas*
Especifica el número máximo de rutas por red de destino que se van a almacenar en la tabla de rutas de RIP para IPX.

**Valores válidos**: Un entero dentro del rango del 1 al 64.

**Valor por omisión**: 1. Para obtener información adicional sobre la existencia de diversas rutas, consulte “Configuración de diversas rutas” en la página 700.

**Ejemplo:** **`set maximum routes-per-destination 8`**

**maximum networks** *tamaño*

Especifica el tamaño de la tabla de redes IPX de RIP. Refleja el número de redes de la internet en que funciona IPX.

**Valores válidos**: Del 1 al 2048

Restricciones de memoria del direccionador pueden impedir que se utilice el tamaño de tabla máximo.

**Valor por omisión**: 32. Este valor no puede ser superior al valor de maximum total-route-entries *tamaño*.

**Ejemplo:** `set maximum networks 30`

**maximum services** *tamaño*

Especifica el tamaño de la tabla de servicios de SAP de IPX. Refleja el número de servicios de SAP de la internet en que funciona IPX.

**Valores válidos**: Del 1 al 2048

Restricciones de memoria del direccionador pueden impedir que se utilice el tamaño de tabla máximo.

**Valor por omisión**: 32

**Ejemplo:** `set maximum services 30`

**maximum total-route-entries** *tamaño*

Especifica el tamaño de la tabla de rutas de RIP para IPX. Refleja el número total de rutas, incluidas las rutas alternativas, de la internet en que funciona IPX.

**Valores válidos**: Del 1 al 4096

**Valor por omisión**: 32

Este valor debe ser, como mínimo, igual al de *maximum networks tamaño*. Para obtener información adicional sobre la existencia de diversas rutas, consulte “Configuración de diversas rutas” en la página 700.

**Ejemplo:** `set maximum total-route-entries 40`

**name** *nombre_direccionador*

Le permite asignar un nombre simbólico al direccionador. IPXWAN requiere que un direccionador tenga un id de nodo y un nombre.

**Valores válidos**: Una serie de longitud variable de 1 a 47 caracteres.

El nombre_direccionador puede contener los caracteres de la A a la Z, del 0 al 9, signo de subrayado (_), guión (-) y signo de la arroba (@).

**Valor por omisión**: Ninguno.

**Ejemplo:** `set name newyork_accounting`

**net-number** *núm. circuito-ipx núm. red*

Especifica el número de red IPX para el circuito de difusión IPX o punto a punto IPXWAN.

**núm. circuito-ipx**

Especifica un circuito de difusión IPX o punto a punto IPXWAN existente.

**Valores válidos**: Un número de circuito existente

**Valor por omisión**: 1

**núm. red**
Especifica el número de red IPX a utilizar en el circuito IPX. El número de red IPX 0 sólo es válido en RIP o circuitos de direccionamiento estático sin número IPXWAN. El número de red IPX FFFFFFFF no es un número de red IPX válido. El número de red IPX FFFFFFFE está reservado para la Ruta por omisión de IPX y no puede utilizarse como número de red IPX. El mandato set se ignorará si no se configura un número de red IPX válido.

**Valores válidos**: Del X'0' al X'FFFFFFFD'

**Valor por omisión**: 1

**Ejemplo:** **`set net-number`**

```
IPX circuit number [1]? 2
IPX network number in hex
(0 is allowed only on IPXWAN unnumbered circuits) [1]?
```

**node-id** *núm. red*
Especifica el número de red interna para IPXWAN. No son válidos los valores de 0, FFFFFFFF o FFFFFFFE para el número de red interna. IPXWAN no se habilitará a menos que se configure un ID de nodo válido.

**Valor por omisión**: 1

**Ejemplo:** **`set node-id 2`**

**remote-cache size** *tamaño*
Especifica el tamaño de la tabla de direccionamiento de antememoria remota.

El tamaño de la antememoria remota debe ser equivalente al número total de redes remotas utilizadas por el direccionador más un almacenamiento intermedio de un 10% para prevenirse contra excesivas peticiones de eliminación.

**Valores válidos**: El rango es del 1 al 10000.

**Valor por omisión**: 64.

**Ejemplo:** **`set remote-cache size`**

```
New IPX remote network cache size [64]? 80
```

**rip-ticks** *núm. circuito-ipx valor*
Indica el coste de circuito, en ciclos, asociado con este circuito. El número de ciclos representa el período de tiempo que tarda la transmisión de un paquete IPX de 576 bytes por este circuito IPX. Cada ciclo son 55 milisegundos. Un valor de 0 indica que el direccionador calculará el valor en ciclos. Un valor configurado distinto de cero alterará temporalmente cualquier valor calculado, incluido IPXWAN.

**núm. circuito-ipx**
Especifica un circuito de difusión IPX o punto a punto IPXWAN existente.

**Valores válidos**: Cualquier número de circuito IPX válido

**Valor por omisión**: 1

**valor**
Especifica el valor en ciclos

**Valores válidos**: El rango es del 1 al 30000.

**Valor por omisión**: 0

**Ejemplo: `set rip-ticks`**

```
IPX circuit number [1]? 2
RIP ticks value (in 55mec ticks) [0]? 3
```

**rip-update-interval** *núm. circuito-ipx intervalo*
Especifica a qué intervalos en minutos deben producirse las difusiones periódicas de RIP en un circuito IPX específico.

Si se aumenta el intervalo de RIP, se reduce el tráfico en las líneas WAN y circuitos dial. También evita que los circuitos dial-on-demand efectúen la marcación a menudo.

**Nota:** Mientras que los anuncios de RIP completos están controlados por el intervalo, el direccionador propaga los cambios de la topología de red tan pronto como los aprende.

**núm. circuito-ipx**
Especifica un circuito de difusión IPX o punto a punto IPXWAN existente.

**Valores válidos**: Cualquier número de circuito IPX válido

**Valor por omisión**: 1

**intervalo**
Especifica el intervalo en minutos

**Valores válidos**: El rango es de 1 a 1440 minutos.

**Valor por omisión**: 1 minuto. Para obtener información adicional sobre el intervalo de RIP, consulte “Especificación del intervalo de actualización de RIP” en la página 698.

**Ejemplo: `set rip-update-interval`**

```
IPX circuit number [1]? 2
RIP Timer Value (minutes) [1]? 2
```

**sap-update-interval** *núm. circuito-ipx intervalo*
Especifica el retardo de tiempo en minutos con que deben producirse las difusiones periódicas de SAP en un circuito IPX específico.

Si se aumenta el intervalo de SAP, se reduce el tráfico en las líneas WAN y circuitos dial. También evita que los circuitos dial-on-demand efectúen la marcación a menudo.

**Nota:** Mientras que los anuncios de SAP completos están controlados por el intervalo, el direccionador propaga los cambios de los servicios tan pronto como los aprende.

**núm. circuito-ipx**
Especifica un circuito de difusión IPX o punto a punto IPXWAN existente.

**Valores válidos:** Cualquier número de circuito IPX válido

**Valor por omisión:** 1

**intervalo**
Especifica el intervalo en minutos.

**Valores válidos**: El rango es de 1 a 1440 minutos.

**Valor por omisión**: 1 minuto.

**Ejemplo: `set sap-update-interval`**

```
IPX circuit number [1]? 2
SAP Timer Value (minutes) [1]? 2
```

**split-horizon** *heuristic enabled disabled*
Especifica el tipo de horizonte de división utilizado en el circuito IPX.

Si sólo hay un VC Frame Relay en el circuito, el horizonte de división está habilitado; de lo contrario, el horizonte de división está inhabilitado.

Generalmente, el horizonte de división debe establecerse en *enabled*. A veces, es necesario inhabilitar el horizonte de división para configuraciones de circuitos de difusión de malla parcial en Frame-Relay, ATMy X.25. Para obtener información adicional sobre el horizonte de división, consulte “Direccionamiento de horizonte de división” en la página 712.

**heuristic**
Habilita el horizonte de división en el circuito IPX, a excepción de los circuitos de difusión IPX Frame Relay.

**Valores válidos:** Cualquier número de circuito IPX válido

**Valor por omisión:** 1

**enabled**
Habilita el horizonte de división en el circuito IPX.

**Valores válidos:** 1–1440

**Valor por omisión:** 1

**disabled**
Inhabilita el horizonte de división en el circuito IPX.

**Valores válidos:** 1–1440

**Valor por omisión:** 1

**Ejemplo: `set split-horizon enabled 0`**

```
IPX circuit number [1]? 2
```

## Acceso al entorno de configuración de filtros de circuito IPX

Para acceder al entorno de configuración de filtros de circuito IPX, entre el mandato siguiente en el indicador `IPX config>`:

```
IPX Config> filter-lists tipo
IPX tipo-List Config>
```

Donde *tipo* es el tipo del filtro de IPX que se va a configurar. Los tipos válidos son *router-lists, rip-lists, sap-lists* e *ipx-lists*.

Cuando se crea un filtro, es necesario un número de circuito IPX.

# Mandatos de configuración de filtros de circuito para circuitos IPX

Esta sección describe los mandatos utilizados para configurar los filtros basados en circuito IPX; DIRECCIONADOR, RIP, SAP e IPX. Para configurar estos filtros, entre el mandato `filter-lists` *`tipo`* en el indicador `IPX Config>` y, a continuación, entre los mandatos de configuración en el indicador `IPX` *`tipo`*`-List Config>`.

*Tabla 44. Resumen de los mandatos de configuración de filtros de IPX*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Attach | Conecta una lista-filtro especificada con un filtro especificado. |
| Create | Crea un filtro o una lista-filtro. |
| Default | Establece la acción por omisión de un filtro en *include* o *exclude* |
| Delete | Suprime un filtro o una lista-filtro. |
| Detach | Desconecta una lista-filtro de un filtro. |
| Disable | Inhabilita la filtración. |
| Enable | Habilita la filtración. |
| List | Visualiza la configuración actual de la filtración. |
| Move | Reordena las listas-filtro conectadas con un filtro. |
| Set-cache | Establece el tamaño de la antememoria para un filtro especificado. |
| Update | Accede al indicador `IPX` *`tipo`*`-List` *`lista-filtro`* `Config>`. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

# Attach

Utilice el mandato **attach** para conectar una lista-filtro con un filtro.

**Sintaxis:**

a**ttach** *nombre-lista núm. filtro*

**nombre-lista**

Especifica el nombre de la lista-filtro. Puede utilizarse el mandato **list** para visualizar una lista de los nombres de lista-filtro configurados.

**Valores válidos**: Cualquier serie alfanumérica de un máximo de 16 caracteres

**Valor por omisión**: Ninguno

**núm. filtro**

Especifica el número del filtro. Puede obtenerse una lista numerada de los filtros configurados si se utiliza el mandato list.

**Ejemplo:** `attach test_list 1`

## Create

Utilice el mandato **create** para crear una lista-filtro o un filtro.

**Sintaxis:**

**create** list ...
filter ...

**list** *nombre-lista*

Crea una lista con el nombre especificado.

**Valores válidos**: Cualquier serie alfanumérica de un máximo de 16 caracteres

**Valor por omisión**: Ninguno

También puede entrar el mandato **create list** sin ningún nombre de lista. A continuación, se le solicitará el nombre de lista.

**Ejemplo:** `create list example_list`

**filter** *orientación núm. circuito-ipx*

Crea un filtro para la orientación especificada en el circuito especificado. Especifique *input* para que se filtren paquetes recibidos en el circuito especificado. Especifique *output* para que se filtren paquetes a enviar mediante el circuito especificado.

Se asigna automáticamente un número a un filtro cuando se crea y, a partir de entonces, se utiliza para identificar el filtro, en vez de tener que teclear el circuito y la orientación (entrada o salida) en todos los mandatos subsiguientes.

**Ejemplo:** `create filter input 1`

## Default

Utilice el mandato **default** con el fin de establecer la acción por omisión para un filtro. Se lleva a cabo la acción por omisión cuando no se encuentra coincidencia para ninguno de los elementos de filtro.

**Sintaxis:**

**default** *acción núm. filtro*
**Ejemplo:** `default exclude 1`

**acción**

Especifica la acción por omisión. **Include** especifica que, cuando no se encuentre coincidencia con ninguno de los elementos de filtro, el paquete se procesará. **Exclude** indica que, cuando no se encuentre coincidencia, se eliminará el paquete.

**núm. filtro**

Especifica el número del filtro. Utilice el mandato **list** para visualizar una lista numerada de los filtros configurados.

## Delete

Utilice el mandato **delete** para suprimir una lista-filtro o un filtro.

**Sintaxis:**

del**ete** list ...
filter ...

**list** *nombre-lista*
Suprime la lista especificada. Puede utilizarse el mandato list para visualizar los nombres de lista-filtro configurados.

**Ejemplo:** `delete list example_list`

**filter** *núm. filtro*
Suprime el filtro especificado. Puede utilizarse el mandato list para visualizar una lista numerada de los filtros configurados.

**Ejemplo:** `delete filter 1`

## Detach

Utilice el mandato **detach** para desconectar una lista-filtro de un filtro.

**Sintaxis:**

det**ach** *nombre-lista núm. filtro*

**nombre-lista**
Especifica el nombre de la lista-filtro. Puede utilizarse el mandato list para visualizar una lista de los nombres de filtro configurados.

**Valores válidos**: Cualquier serie alfanumérica de un máximo de 16 caracteres

**Valor por omisión**: Ninguno

**núm. filtro**
Especifica el número del filtro. Puede utilizarse el mandato list para visualizar una lista numerada de los filtros configurados.

**Ejemplo:** `detach test_list 1`

## Disable

Utilice el mandato **disable** con el fin de inhabilitar la filtración globalmente o en un filtro especificado.

**Sintaxis:**

di**sable** all
filter ...

**all** Inhabilita todos los filtros del tipo actual (DIRECCIONADOR, RIP, SAP o IPX).

**Ejemplo: disable all**

**filter** *núm. filtro*
Inhabilita el filtro especificado. Utilice el mandato list para visualizar una lista numerada de los filtros configurados.

**Ejemplo: disable filter 1**

## Enable

Utilice el mandato **enable** con el fin de habilitar la filtración globalmente o en un filtro especificado.

**Sintaxis:**

**enable** all
filter ...

**all** Habilita todos los filtros del tipo actual (DIRECCIONADOR, RIP, SAP o IPX).

**Ejemplo: enable all**

**filter** *núm. filtro*
Habilita el filtro especificado. Utilice el mandato list para visualizar una lista numerada de los filtros configurados.

**Ejemplo: enable filter 1**

## List

Utilice el mandato **list** para visualizar globalmente el estado del tipo de filtración actual o para visualizar información sobre un filtro específico.

**Sintaxis:**

**list** all
filter ...

**all** Lista información sobre el estado de todos los filtros del tipo actual.

**Ejemplo: list all**

```
Filtering: ENABLED

Filter Lists:
Name                           Action
------------------------------ ----------
ipx01                          EXCLUDE
ipx02                          INCLUDE
ipx03                          EXCLUDE

Filters:
Id    Circ  Ifc   Direction  State      Default    Cache
----- ----- ----- ---------- ---------- ---------- -----
1     3     2     INPUT      ENABLED    INCLUDE       10
2     2     1     INPUT      ENABLED    INCLUDE       10
```

**filter** *núm. filtro*
Lista información sobre el filtro especificado. Utilice el mandato list para visualizar una lista numerada de los filtros configurados.

**Ejemplo: list filter 2**

```
Filters:
Id    Circ  Ifc   Direction  State      Default    Cache
----- ----- ----- ---------- ---------- ---------- -----
2     2     1     INPUT      ENABLED    INCLUDE       10

Filter Lists:
Name                           Action
------------------------------ ----------
ipx01                          EXCLUDE
```

## Move

Utilice el mandato **move** para cambiar el orden de las listas-filtro dentro de un filtro. Los paquetes se evalúan en relación con las listas-filtro de acuerdo con el orden en que éstas aparecen. La primera coincidencia detiene el proceso de filtración.

**Sintaxis:**

m**ove** *nombre-lista-origen nombre-lista-dest núm. filtro*

**nombre-lista-origen**
Especifica la lista a trasladar dentro del filtro.

**nombre-lista-dest**
Especifica hasta antes de qué lista se trasladará nombre-lista-origen.

**núm. filtro**
Especifica el filtro al que pertenecen las listas. Puede utilizarse el mandato list para visualizar una lista de los filtros configurados y de las listas-filtro conectadas con los mismos.

**Ejemplo:** `move test-list-1 test-list-2 2`

## Set-cache

Utilice el mandato **set-cache** para establecer el tamaño de la antememoria de un filtro. Sólo se da soporte a una antememoria de filtro para el filtro de circuito que es de IPX; los filtros de circuito de DIRECCIONADOR, RIP y SAP no dan soporte a una antememoria.

**Sintaxis:**

s**et-cache** *t*amaño núm. filtro

**tamaño**
Especifica el tamaño de la antememoria de filtro (en número de entradas).

**Valores válidos**: De 4 a 64 entradas de antememoria.

**Valor por omisión**: 10 entradas.

**núm. filtro**
Especifica el número del filtro. Puede utilizarse el mandato list para visualizar una lista numerada de los filtros configurados.

**Ejemplo:** `set-cache 10 1`

## Update

Con el mandato **update**, accederá al indicador `IPX` *`tipo`*`-List` *`nombre-lista`* `Config>`. Desde este indicador, puede emitir mandatos para añadir elementos a la lista que se actualiza, suprimir elementos o trasladarlos dentro de la misma. Desde este indicador, también puede establecer la acción para la lista-filtro que se actualiza.

**Sintaxis:**

u**pdate** *nombre-lista*

**nombre-lista**
Especifica el nombre de la lista-filtro. Puede utilizarse el mandato list para visualizar los nombres de lista-filtro configurados.

**Ejemplo:** `update test-list`

## Add (submandato de Update)

Utilice el submandato **add** para añadir elementos a una lista-filtro. Los parámetros de elemento de lista varían según el tipo de filtro de circuito (DIRECCIONADOR, RIP, SAP o IPX) que se configura. Para todos los tipos de filtro de circuito, el mandato **add** puede entrarse sin parámetros. A continuación, se le solicitarán los parámetros necesarios.

### Add (DIRECCIONADOR)

**Sintaxis:**

a**dd** *número-nodo máscara*

**número-nodo**
Especifica el valor a comparar con el número de nodo de origen del direccionador que ha enviado el paquete de respuesta RIP (después de la relación con la máscara). Si desea que la coincidencia se base en un solo nodo, establezca el parámetro de número de nodo en la dirección y establezca la máscara en FFFFFFFFFFFF. Si desea que la coincidencia se base en todos los nodos, establezca el parámetro de número de nodo y el parámetro de máscara en 000000000000.

**Valores válidos**: Del X'000000000000' al X'FFFFFFFFFFFF'

**Valor por omisión**: Ninguno

**máscara**
Especifica el valor a relacionar con la dirección de nodo de origen del direccionador que ha enviado el paquete de respuesta RIP (antes de la comparación con el parámetro de dirección).

Si desea que la coincidencia se base en una sola dirección, establezca el parámetro de dirección en la dirección y establezca la máscara en FFFFFFFFFFFF. Si desea que la coincidencia se base en todas las direcciones, establezca el parámetro de dirección y el parámetro de máscara en 000000000000.

**Valores válidos**: Del X'000000000000' al X'FFFFFFFFFFFF'

**Valor por omisión**: X'FFFFFFFFFFFF'

**Ejemplo:** `add 400000001000 ffffffff0000`

### Add (RIP)

**Sintaxis:**

a**dd** *inicio-rango-redes final-rango-redes*

**inicio-rango-redes**
Especifica el inicio de un rango (inclusivo) de números de red IPX para la filtración. Si desea que la coincidencia se base en un solo número de red, establezca los parámetros de inicio de rango de redes y final de rango de redes en este número de red. Si desea que la coincidencia se base en todos los

números de red, establezca el inicio de rango de redes en X'00000001' y el final de rango de redes en X'FFFFFFFE'.

**Valores válidos**: Del X'1' al X'FFFFFFFE'

**Valor por omisión**: X'1'

**final-rango-redes**
Especifica el final de un rango (inclusivo) de números de red IPX para la filtración.

**Valores válidos**: Del X'1' al X'FFFFFFFE'

**Valor por omisión**: X'1'

**Ejemplo:** `add 00000001 FFFFFFFE`

## Add (SAP)

**Sintaxis:**

**add** *comparador saltos tipo-sap nombre*

**comparador**
Especifica el tipo de comparador de cuenta de saltos para este elemento de lista.

**Valores válidos**:

<

<=

=

>=

>

**Valor por omisión**: <=. Los parámetros de comparador y saltos se ignoran en los filtros de la salida.

**saltos**
Especifica la cuenta de saltos para este elemento de lista. Si no desea que la filtración se base en la cuenta de saltos, entre <= 16 para el comparador y la cuenta de saltos. Los parámetros de comparador y saltos se ignoran en los filtros de la salida.

**Valores válidos**: Del 0 al 16

**Valor por omisión**: 16

**tipo-sap**
Especifica el tipo de servicio para la filtración. Entre el tipo de servicio, o X'0000' para todos los tipos de servicios.

**Valores válidos**: Del X'0' al X'FFFF'

**Valor por omisión**: 4

**nombre**
Especifica el nombre de servicio para la filtración.

**Valores válidos**:

Una serie de 1 a 47 caracteres ASCII (del X'20' al X'7E').

Los caracteres de signo de interrogación (?) y asterisco (*) sirven de comodines. El signo de interrogación puede utilizarse diversas veces para representar cualquier carácter individual dentro del nombre de servidor. El asterisco puede utilizarse diversas veces para representar cualquier parte del nombre de servidor. El signo de interrogación y el asterisco también pueden utilizarse juntos.

**Valor por omisión**: Ninguno

**Ejemplo:** `add < 6 0004 *`

## Add (IPX)

**Sintaxis:**

a**dd** *comparador saltos tipo-ipx inicio-rango-redes-dest final-rango-redes-dest nodo-dest máscara-dest inicio-rango-sockets-dest final-rango-sockets-dest inicio-rango-redes-origen final-rango-redes-origen nodo-origen máscara-origen inicio-rango-sockets-origen final-rango-sockets-origen*

**comparador**

Especifica el tipo de comparador de cuenta de saltos para este elemento de lista. Los parámetros de comparador y saltos se ignoran en los filtros de la salida.

**Valores válidos**:

- <
- <=
- =
- >=
- >

**Valor por omisión**: <=

**saltos**

Especifica la cuenta de saltos para este elemento de lista. Si no desea que la filtración se base en la cuenta de saltos, entre <= 16 para el comparador y la cuenta de saltos. Los parámetros de comparador y saltos se ignoran en los filtros de la salida.

**tipo-ipx**

Especifica el tipo de paquete IPX para la filtración. Entre el tipo de paquete, o bien 00 para todos los tipos de paquetes.

**Valores válidos**: Del X'0' al X'FF'

**Valor por omisión**: X'0'

**inicio-rango-redes-dest**

Especifica el inicio de un rango (inclusivo) de números de red IPX de destino para la filtración. Si desea que la coincidencia se base en un solo número de red, establezca los parámetros de inicio de rango de redes de destino y final de rango de redes de destino en este número de red. Si desea que la coincidencia se base en todos los números de red, establezca el inicio de rango de redes de destino en X'00000001' y el final de rango de redes de destino en X'FFFFFFFE'.

**Valores válidos**: Del X'00000000' al X'FFFFFFFF'

**Valor por omisión**: X'00000000'

**final-rango-redes-dest**
Especifica el final de un rango (inclusivo) de números de red IPX de destino para la filtración. Si desea que la coincidencia se base en un solo número de red, establezca los parámetros de inicio de rango de redes de destino y final de rango de redes de destino en este número de red. Si desea que la coincidencia se base en todos los números de red, establezca el inicio de rango de redes de destino en X'00000001' y el final de rango de redes de destino en X'FFFFFFFE'.

**Valores válidos**: Del X'00000000' al X'FFFFFFFF'

**Valor por omisión**: X'00000000'

**nodo-dest**
Especifica el valor a comparar con el número de nodo de destino (después de la relación con la máscara de destino). Si desea que la coincidencia se base en un solo nodo, establezca el parámetro de nodo de destino en el número de nodo y establezca la máscara de destino en X'FFFFFFFFFFFF'. Si desea que la coincidencia se base en todos los nodos, establezca el parámetro de nodo de destino y el parámetro de máscara de destino en X'000000000000'.

**Valores válidos**: Del X'000000000000' al X'FFFFFFFFFFFF'

**Valor por omisión**: X'000000000000'

**máscara-dest**
Especifica el valor a relacionar con la dirección de nodo de destino (antes de la comparación con el parámetro de dirección de destino). Si desea que la coincidencia se base en una sola dirección, establezca el parámetro de dirección de destino en la dirección y establezca la máscara de destino en X'FFFFFFFFFFFF'. Si desea que la coincidencia se base en todas las direcciones, establezca el parámetro de dirección de destino y el parámetro de máscara de destino en X'000000000000'.

**Valores válidos**: Del X'000000000000' al X'FFFFFFFFFFFF'

**Valor por omisión**: X'000000000000'

**inicio-rango-sockets-dest**
Especifica el inicio de un rango (inclusivo) de sockets IPX de destino para la filtración. Si desea que la coincidencia se base en un solo socket, establezca los parámetros de inicio de rango de sockets de destino y final de rango de sockets de destino en este socket. Si desea que la coincidencia se base en todos los sockets, establezca el inicio de rango de sockets de destino en X'0000' y el final de rango de sockets de destino en X'FFFF'.

**Valores válidos**: Del X'0000' al X'FFFF'

**Valor por omisión**: 0

**final-rango-sockets-dest**
Especifica el final de un rango (inclusivo) de sockets IPX de destino para la filtración. Si desea que la coincidencia se base en un solo socket, establezca los parámetros de inicio de rango de sockets de destino y final de rango de sockets de destino en este socket. Si desea que la coincidencia se base en todos los sockets, establezca el inicio de rango de sockets de destino en X'0000' y el final de rango de sockets de destino en X'FFFF'.

**Valores válidos**: Del X'0000' al X'FFFF'

**Valor por omisión**: 0

**inicio-rango-redes-origen**
Especifica el inicio de un rango (inclusivo) de números de red IPX de origen para la filtración. Si desea que la coincidencia se base en un solo número de red, establezca los parámetros de inicio de rango de redes de origen y final de rango de redes de origen en este número de red. Si desea que la coincidencia se base en todos los números de red, establezca el inicio de rango de redes de origen en X'00000001' y el final de rango de redes de origen en X'FFFFFFFE'.

**Valores válidos**: Del X'00000000' al X'FFFFFFFE'

**Valor por omisión**: X'00000000'

**final-rango-redes-origen**
Especifica el final de un rango (inclusivo) de números de red IPX de origen para la filtración. Si desea que la coincidencia se base en un solo número de red, establezca los parámetros de inicio de rango de redes de origen y final de rango de redes de origen en este número de red. Si desea que la coincidencia se base en todos los números de red, establezca el inicio de rango de redes de origen en X'00000001' y el final de rango de redes de origen en X'FFFFFFFE'.

**Valores válidos**: Del X'00000000' al X'FFFFFFFE'

**Valor por omisión**: X'00000000'

**nodo-origen**
Especifica el valor a comparar con el número de nodo de origen (después de la relación con la máscara de origen). Si desea que la coincidencia se base en un solo nodo, establezca el parámetro de nodo de origen en el número de nodo y establezca la máscara de origen en X'FFFFFFFFFFFF'. Si desea que la coincidencia se base en todos los nodos, establezca el parámetro de nodo de origen y el parámetro de máscara de origen en X'000000000000'.

**Valores válidos**: Del X'00000000' al X'FFFFFFFF'

**Valor por omisión**: X'00000000'

**máscara-origen**
Especifica el valor a relacionar con la dirección de nodo de origen (antes de la comparación con el parámetro de dirección de origen). Si desea que la coincidencia se base en una sola dirección, establezca el parámetro de dirección de origen en la dirección y establezca la máscara de origen en X'FFFFFFFFFFFF'. Si desea que la coincidencia se base en todas las direcciones, establezca el parámetro de dirección de origen y el parámetro de máscara de origen en X'000000000000'.

**Valores válidos**: Del X'000000000000' al X'FFFFFFFFFFFF'

**Valor por omisión**: X'000000000000'

**inicio-rango-sockets-origen**
Especifica el inicio de un rango (inclusivo) de sockets IPX de origen para la filtración. Si desea que la coincidencia se base en un solo socket, establezca los parámetros de inicio de rango de sockets de origen y final de rango de sockets de origen en este socket. Si desea que la coincidencia se base en todos los sockets, establezca el inicio de rango de sockets de origen en X'0000' y el final de rango de sockets de origen en X'FFFF'.

**Valores válidos**: Del X'0000' al X'FFFF'

**Valor por omisión**: X'0000'

**final-rango-sockets-origen**
Especifica el final de un rango (inclusivo) de sockets IPX de origen para la filtración. Si desea que la coincidencia se base en un solo socket, establezca los parámetros de inicio de rango de sockets de origen y final de rango de sockets de origen en este socket. Si desea que la coincidencia se base en todos los sockets, establezca el inicio de rango de sockets de origen en 0000 y el final de rango de sockets de origen en FFFFF.

**Valores válidos**: Del X'0000' al X'FFFF'

**Valor por omisión**: X'0000'

**Ejemplo:**

```
add  <= 16  0  00000004 00000004 000000000000 000000000000
0000 FFFF 0000005A 0000006A 000000000000 000000000000 0000 FFFF
```

En este ejemplo se filtran todos los paquetes de la red IPX 5A a la red IPX 6A hacia la red IPX 4.

## Delete (submandato de Update)

Utilice el submandato **delete** para suprimir un elemento de la lista-filtro actual.

**Sintaxis:**

**delete** *elemento#*

**elemento#**
Especifica el número del elemento de la lista. El número puede obtenerse si se utiliza el mandato list para listar los elementos de la lista-filtro.

**Ejemplo: `delete 4`**

## List (submandato de Update)

Utilice el submandato **list** para visualizar la acción de la lista-filtro y listar los elementos de filtro.

**Sintaxis:**

**list**

**Ejemplo: `list`**

```
IPX IPX-List 'ipx01' Config>list
Action: EXCLUDE
Id   Hops Type Net Range           Address      Mask         Sock Range
---- ---- ---- ------------------ ------------ ------------ -----------
1    <=16    0     4320 -     4324 4000003A0002 FFFFFFFFFFFF    0 - FFFF (Dest)
                   3A33 -    13A33 400000010000 FFFFFFFF0000    0 - FFFF (Source)
```

## Move (submandato de Update)

Utilice el submandato **move** para cambiar el orden de los elementos de filtro. Una vez cambiado el orden de los elementos de filtro, éstos se vuelven a numerar para reflejar el nuevo orden. Puede utilizarse el mandato list para visualizar una lista numerada de los elementos de filtro configurados.

El parámetro *línea-origen#* indica la línea a trasladar. Esta línea se trasladará para preceder al elemento especificado mediante el parámetro *línea-dest#*.

**Sintaxis:**

m**ove** *línea-origen# línea-dest#*

**Ejemplo:** `move 5 2`

## Set-action (submandato de Update)

Utilice el submandato **set-action** para indicar la acción a llevar a cabo cuando tenga lugar una coincidencia en una lista-filtro.

**Sintaxis:**

s**et-action** include
exclude

**include** Especifica que, si se encuentra una coincidencia para el filtro actual, se procesará (incluirá) el paquete en el caso de los filtros de DIRECCIONADOR e IPX. En el caso de los filtros de RIP y SAP, **include** especifica que se procesará la entrada de RIP o SAP.

**Ejemplo:** `set-action include`

**exclude** Especifica que, si se encuentra una coincidencia para el filtro actual, se eliminará (excluirá) el paquete en el caso de los filtros de DIRECCIONADOR e IPX. En el caso de los filtros de RIP y SAP, **exclude** especifica que, si se encuentra una coincidencia, se ignorará la entrada de RIP o SAP.

**Ejemplo:** `set-action exclude`

# Acceso al entorno de supervisión de IPX

Para obtener información sobre cómo acceder al entorno de supervisión de IPX, consulte “Getting Started (Introduction to the User circuit)” en la publicación *Guía del usuario de software*.

# Mandatos de supervisión de IPX

La Tabla 45 en la página 756 lista los mandatos de supervisión de IPX. Los mandatos de supervisión de IPX le permiten visualizar los parámetros y las estadísticas de los circuitos y las redes que transmiten paquetes IPX. Los mandatos de supervisión visualizan los valores de la configuración para los niveles de tipo físico, trama y paquete. También tiene la opción de visualizar los valores de los tres niveles de protocolo a la vez.

Entre los mandatos de supervisión de IPX en el indicador `IPX>`. La Tabla 45 en la página 756 resume los mandatos de supervisión de IPX.

*Tabla 45 (Página 1 de 2). Resumen de los mandatos de supervisión de IPX*

| Mandato | Función |
|---|---|
| ? (Help) | Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxi. |
| Access-controls | Visualiza si se ha habilitado el filtro de IPX global (control del acceso), las sentencias de control del acceso de IPX y el número de paquetes que han coincidido con cada sentencia de control del acceso. |
| Cache | Lista el contenido actual de la antememoria de direccionamiento. |
| Counters | Visualiza el número de errores de direccionamiento y desbordamientos de paquetes. |
| Delete keepalive connection | Suprime una entrada de tabla de filtración de Keepalive. |
| Disable | Inhabilita IPX globalmente o en circuitos IPX específicos. |
| Dump routing tables | Visualiza el contenido de la tabla de direccionamiento. |
| Enable | Habilita IPX globalmente o en circuitos IPX específicos. |
| Filters | Visualiza si se ha habilitado la filtración de SAP global, las sentencias de filtro de SAP y una cuenta de los anuncios de SAP que se han filtrado. |
| Filter-Lists | Accede a la consola de filtros de circuito IPX. Aquí es donde pueden supervisarse los filtros basados en circuito de direccionador RIP, RIP, SAP e IPX. |
| IPXWAN | Lista información sobre IPXWAN en relación con los circuitos punto a punto IPXWAN. |
| Keepalive | Visualiza el estado de cada conexión cliente/servidor activa de la tabla de filtración de keepalive. |
| List | Lista la configuración o la dirección IPX actual de cada circuito habilitado. |
| Ping | Envía paquetes IPXPING a otro sistema principal y observa si hay una respuesta. Puede utilizarse este mandato para identificar problemas en un entorno de interredes. |
| Recordroute | Envía paquetes de registro de ruta IPXPING a otro sistema principal y observa si hay una respuesta. Utilice este mandato para registrar y visualizar la ruta de ida y vuelta entre este dispositivo y otro sistema principal. Utilice esta información para identificar problemas en un entorno de interredes. |
| Reset | Restablece circuitos IPX específicos, los filtros de SAP globales, los filtros de IPX globales (controles del acceso), las rutas estáticas, los servicios estáticos o bien los filtros basados en circuito de direccionador, RIP, SAP o IPX (listas-filtro). |
| Sizes | Visualiza los tamaños configurados de la antememoria de nodos locales y la de redes remotas, así como el número de entradas de antememoria que actualmente están en uso. |
| Slist | Visualiza el contenido de la tabla de servidores SAP de IPX. |

*Tabla 45 (Página 2 de 2). Resumen de los mandatos de supervisión de IPX*

| Mandato | Función |
|---|---|
| Traceroute | Envía paquetes de rastreo de ruta IPXPING a otro sistema principal y observa si hay una respuesta. Utilice este mandato para rastrear y visualizar cada salto que tome un paquete en su ruta desde este dispositivo a un sistema principal de destino. Utilice esta información para identificar problemas en un entorno de interredes. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxii. |

## Access Controls

Utilice el mandato **access-controls** para listar el estado de los filtros de IPX globales (controles del acceso), las sentencias de control del acceso de IPX y una cuenta de cuántas veces se ha seguido cada sentencia de control.

**Sintaxis:**

a**ccess-controls**

**Ejemplo: `access-controls`**

```
IPX Access Controls:  Enabled
#   T Dest Net Host         Sock Sock Src Net  Host         Sock  Sock Count
1   E 2        000000000000 0    FFFF 3        000000000000 0     FFFF 0
2   I 0        000000000000 452  453  0        000000000000 0     FFFF 0
```

**#** Número de índice de control del acceso

**Type**
Identifica si se envían o se eliminan los paquetes para una dirección específica o un conjunto de direcciones. I significa inclusión. Ésta permite que se envíen los paquetes. E significa exclusión. Hace que el direccionador deseche los paquetes.

**Dest-net**
Número de red del destino. El cero (0) significa todas las redes.

**Dest-host**
Número de sistema principal de la red de destino. (0) significa todos los sistemas principales de la red.

**Dest-sck**
Dos números que especifican un rango inclusivo de sockets de destino.

**Src-net**
Número de red del origen. El cero (0) significa todas las redes.

**Src-host**
Número de sistema principal de la red de origen. El cero significa todos los sistemas principales de la red.

**Src-sck**
Dos números que especifican un rango inclusivo de sockets de origen.

**Count**
Especifica el número de paquetes IPX de entrada que han coincidido con cada sentencia de control del acceso, lo que habrá causado que se llevase a cabo el tipo asociado (inclusión o exclusión).

## Cache

Utilice el mandato **cache** para visualizar el contenido de la antememoria de direccionamiento IPX.

**Sintaxis:**

ca**che**

**Ejemplo: `cache`**

```
Dest Net/Node          Use Count      via Net/Node          Circ  Ifc
     420               1                  412/000004200000  3     2
     412               1                  412/000000000000  3     2
     412/000004200000  1                  412/000004200000  3     2
```

La primera entrada muestra que se puede llegar a la red remota 420 sobre el circuito serie con el número de red IPX 412. La segunda entrada es la red IPX 412. Es una red Ethernet conectada directamente con el direccionador. Esta entrada es una entrada de red local general. Habrá una entrada de red local general para cada una de las redes conectadas directamente una vez que hayan empezado a reenviar paquetes IPX. La última entrada es una entrada local sobre una red Ethernet. Esta entrada de antememoria de IPX se ha utilizado para enviar 1 paquete al número de nodo IPX 0000 0420 0000 en el número de red 412.

## Counters

Utilice el mandato **counters** para visualizar el número de errores de direccionamiento y desbordamientos de paquetes que se han producido. En el ejemplo, los contadores muestran que no se han registrado errores.

**Sintaxis:**

cou**nters**

**Ejemplo: `counters`**

```
Routing errors
Count  Type
0      Unknown
0      Checksum error
0      Destination unreachable
0      Hop count expired
0      circuit size exceeded

Destination errors
Count  Type
0      Unknown
0      Checksum error
0      Non-existent socket
0      Congestion

IPX input packet overflows
Circ   Ifc    Name        Count
1      0       Eth/0      0
2      1       PPP/0      0
3      2       PPP/1      0
```

### Routing Errors

#### Unknown

Se ha producido un error no especificado antes de la llegada al destino.

**Checksum**
La suma de comprobación es incorrecta o bien el paquete ha presentado alguna otra incoherencia grave antes de llegar al destino.

**Destination unreachable**
No se puede llegar al sistema principal de destino desde aquí.

**Hop count expired**
El paquete ha pasado por 15 direccionadores internet sin llegar a su destino.

**circuit size exceeded**
El paquete es demasiado grande para su reenvío a través de una red intermedia.

**Destination errors**

**Unknown**
Se ha detectado un error no especificado en el destino.

**Checksum**
La suma de comprobación es incorrecta o bien se ha detectado alguna otra incoherencia grave del paquete en el destino.

**Nonexistent socket**
El socket especificado no existe en el sistema principal de destino especificado.

**Congestion**
El destino no puede aceptar el paquete debido a limitaciones de los recursos.

**IPX Input Packet Overflows**

**Net** Especifica el nombre del circuito.

**Count**
Especifica el número de paquetes que no se han podido recibir debido a limitaciones de los recursos.

## Delete

Utilice el mandato **delete** para eliminar una entrada de tabla de filtración de Keepalive.

**Sintaxis:**

de**lete** *núm. entrada*

**núm. entrada**
Especifica la entrada de tabla a suprimir. Puede utilizarse el mandato **Keepalive** para listar el contenido de la tabla de filtración de Keepalive.

**Ejemplo:** `delete 1`

## Disable

Utilice el mandato **disable** para inhabilitar IPX globalmente o en circuitos específicos.

**Sintaxis:**

di**sable** circuit ...

ipx

**circuit** *núm. circuito-ipx*
Inhabilita el circuito IPX especificado mediante *núm. circuito-ipx*. IPX puede volver a habilitarse si se utiliza el mandato **enable**.

**Ejemplo: `disable circuit 2`**

**ipx** Inhabilita IPX globalmente en todos los circuitos IPX. IPX puede volver a habilitarse globalmente si se utiliza el mandato **enable**.

**Ejemplo: `disable ipx`**

## Dump

Utilice el mandato **dump** para visualizar el contenido de las tablas de direccionamiento.

**Sintaxis:**

du**mp**

**Ejemplo: `dump`**

```
Type Dest Net Hops Delay Age(M: S)   via Router        Circ  Ifc
Dir  412      0    6        0: 0      412/000004000000 3     2
Dir  400      0    1        0: 0      400/020000000400 1     0
Dir  411      0    3        0: 0      411/400000000400 2     1
Stat 1        3    2        0: 0      400/010101010101 1     0
RIP  420      1    7        0:30      412/000004200000 3     2
Stat 444      2    2        0: 0      400/400000000444 1     0
Stat FFFFFFFD 14   3000     0: 0      400/111111111111 1     0
```

**Type**

- Dir - especifica que esta red está conectada directamente con el direccionador.
- RIP - especifica que esta ruta se ha proporcionado mediante el protocolo de direccionamiento IPX, RIP.
- Old - especifica que esta ruta ha sobrepasado el tiempo de espera excedido y ya no se utiliza. La ruta permanece en la tabla durante un tiempo breve para que se notifique a los otros direccionadores que ésta ya no es válida; después de este breve intervalo, ya no se visualiza.
- Stat - especifica que es una ruta estática.

**Dest net** Especifica el número de red de destino.

**Hops** Especifica el número de saltos hacia este destino.

**Delay** Especifica la estimación de cuánto tarda el direccionador en transmitir el paquete y hacer que éste llegue a su destino. La unidad del retardo representa el número de ciclos de reloj de IBM PC para enviar un paquete de 576 bytes y son 18,21 ciclos de reloj por segundo. El retardo mínimo es de 1 unidad.

**Age** Especifica la duración de la información de direccionamiento en minutos y segundos. Si una entrada de la tabla de direccionamiento no se actualiza, el direccionador realizará las siguientes acciones:

- Después de que hayan pasado tres intervalos de actualización de RIP, la ruta se especificará como Old y el direccionador anunciará

que ésta ya no es válida. El intervalo de actualización de RIP puede visualizarse si se utiliza el mandato de IPX **config**. Para obtener información adicional sobre los intervalos de RIP, consulte la sección “Especificación del intervalo de actualización de RIP” en la página 698.

- Después de 60 segundos adicionales, se suprimirá la ruta y no aparecerá en la visualización de dump.

**Via router** Especifica el siguiente salto para los paquetes dirigidos a redes que no están conectadas directamente. Para las redes conectadas directamente, es la dirección del circuito del direccionador que transmite el paquete.

**Circ** Número de circuito IPX

**Ifc** Número de interfaz de red

En la parte superior de la visualización están el número de entradas de ruta y de red utilizadas y el total de las disponibles. Si están en uso todas las entradas de red, es probable que la tabla de direccionamiento no sea lo suficientemente grande. Utilice el mandato de configuración de IPX **set maximum networks** para aumentar el tamaño.

Si están en uso todas las entradas de ruta, es posible que haya rutas hacia redes IPX que no puedan mantenerse, lo que incluye nuevas redes de entrada. Si no desea aumentar el número de rutas disponibles, reduzca el número relativo a la cantidad máxima de rutas por red.

## Enable

Utilice el mandato **enable** para habilitar IPX globalmente o en circuitos específicos.

**Sintaxis:**

en**able** circuit ...
ipx

**circuit** *núm. circuito-ipx*
Habilita IPX en el circuito especificado mediante *núm. circuito-ipx*. Debe haberse configurado un número de red IPX para el circuito antes de que pueda habilitarse IPX.

**Ejemplo:** `enable circuit 2`

**ipx** Habilita IPX globalmente en todos los circuitos IPX habilitados.

**Ejemplo:** `enable ipx`

## Filters

Utilice el mandato **filters** para visualizar si se ha habilitado la filtración de SAP global, las sentencias de filtro de SAP y una cuenta de los anuncios de SAP que se han filtrado.

**Sintaxis:**

filters

**Ejemplo:** `filters`

```
IPX SAP Filters:  Enabled
Count  Max Hops  Type  Service Name
0      5         4     FILESRV01
```

**Count** Indica el número de anuncios de SAP que se han filtrado (desechado).

**Max Hops**
Indica el número máximo de saltos permitido para el servicio.

**Type** Es la clase de servicio numérica.

**Service name**
Es el nombre del servicio si tiene un nombre.

## Filter-lists

Utilice el mandato **filter-lists** para acceder al indicador `IPX tipo-Lists>`. Los tipos válidos son: router-lists, rip-lists, sap-lists e ipx-lists.

Para obtener información sobre los mandatos disponibles en este indicador, consulte la sección “Mandatos de supervisión de filtros de circuito IPX” en la página 774.

**Sintaxis:**

**filter-lists** router-lists
rip-lists
sap-lists
ipx-lists

**Ejemplo:** `filter-lists router-lists`

## IPXWAN

Utilice el mandato **ipxwan** para listar la información sobre IPXWAN en relación con los circuitos punto a punto IPXWAN.

**Sintaxis:**

**ipxwan** detailed . . .
summary

**detailed** *núm. circuito-ipx*
Lista la información sobre IPXWAN relativa al circuito IPX especificado.

**Ejemplo:** `ipxwan detailed 3`

```
Detailed information for IPXWAN link over circuit 3 interface 2, PPP/1
This side is the IPXWAN slave
Neighbor Name: ipxwan-420
Neighbor Node ID: 420
Negotiated Routing Type: RIP/SAP
Link Delay: 6 1/18th sec ticks
Common Net#: 412
Connection Timeouts: 0
Connection Retries: 0
Timer Requests Sent: 1
Timer Requests Received: 1
Timer Responses Sent: 1
Timer Responses Received: 0
Info Requests Sent: 0
Info Requests Received: 1
Info Responses Sent: 1
Info Responses Received: 0
```

**Neighbor Name**
El nombre de direccionador del contiguo recibido del paquete de petición de información RIP/SAP.

**Neighbor Node ID**
El ID de nodo (conocido también como número de red primaria) del contiguo. Es un número de red IPX exclusivo en toda la internet. Es una cantidad de 32 bits.

**Negotiated Routing Type**
El tipo de direccionamiento negociado. Actualmente, se da soporte a RIP/SAP, a RIP sin número y al direccionamiento estático. Cuando el tipo de direccionamiento negociado es RIP sin número o el direccionamiento estático, no es necesario ningún número de red común en el enlace.

**Link Delay**
El retardo del enlace en ciclos por 1/18 de segundo que ha calculado el maestro. Es una cantidad de 16 bits. Siempre se calcula, por lo que no existe un valor por omisión.

**Common Net#**
El número de red acordado por ambos extremos del enlace. Este número debe ser exclusivo en toda la internet. Es una cantidad de 32 bits. Cuando el tipo de direccionamiento negociado sea RIP sin número o el direccionamiento estático, se visualizará el valor 0 en Common Net# tanto para el mandato **IPXWAN detailed** como para el mandato **IPXWAN summary**. No existe un valor por omisión, debe negociarse.

**Connection Timeouts**
El número de veces que la conexión ha sobrepasado el tiempo de espera excedido. Una conexión sobrepasará el tiempo de espera excedido periódicamente si no procede el intercambio de paquetes IPXWAN. Puede configurar el período de tiempo de espera excedido utilizando el mandato **set ipxwan**. El valor por omisión para el período de tiempo de espera excedido son 60 segundos.

**Connection Retries**
El número de veces que se ha reintentado la conexión después de que se haya sobrepasado el tiempo de espera excedido. El período de tiempo a esperar (antes de un reintento) puede configurarse por medio del mandato **set ipxwan**. Toma por omisión el valor de 60 segundos.

**Timer Requests Sent**
El número de paquetes de petición de temporizador IPXWAN enviados.

**Timer Requests Received**
El número de paquetes de petición de temporizador IPXWAN recibidos.

**Timer Responses Sent**
El número de paquetes de respuesta de temporizador IPXWAN enviados.

**Timer Responses Received**
El número de paquetes de respuesta de temporizador IPXWAN recibidos.

**Info Requests Sent**
El número de paquetes de petición de información IPXWAN enviados.

**Info Requests Received**
El número de paquetes de petición de información IPXWAN recibidos.

**Info Responses Sent**
El número de paquetes de respuesta de información IPXWAN enviados.

**Info Responses Received**
El número de paquetes de respuesta de información IPXWAN recibidos.

**summary** Lista información de resumen sobre IPXWAN en relación con todos los circuitos punto a punto IPXWAN.

**Ejemplo:** **`ipxwan summary`**

```
Circ   Ifc    Name        Common Net#  NodeID   Neighbor Name
3      2       PPP/1      412          420      ipxwan-420
```

**Circ** Número de circuito IPX

**Ifc** Número de interfaz de red

**Common Net#**
Número de red acordado por ambos extremos del enlace. Este número debe ser exclusivo en toda la internet. Common Net# será 0 si el tipo de direccionamiento negociado es RIP sin número o el direccionamiento estático.

**NodeID**
ID de nodo (conocido también como número de red interna) del contiguo.

**Neighbor Name**
Nombre de direccionador del contiguo recibido del paquete de petición de información RIP/SAP.

## Keepalive

Muestra el estado de cada conexión cliente/servidor activa de la tabla de filtración de keepalive.

**Sintaxis:**

k**eepalive**

**Ejemplo:**

```
Keepalive
Conn #     Net  /   Node     /Sock        Net  /   Node     /Sock
          ------------------------------------------------------------------
0         272727/000000000001/4001 &lt;->      302/0000C911EF1C/4004
                (server conn # 1, conn type: passive, last heard  1:00 ago)
1         272727/000000000001/4001 &lt;->      302/0000C911B0D9/4004
                (server conn # 2, conn type: passive, last heard  1:00 ago)
```

## List

Utilice el mandato **list** para listar la configuración o la dirección IPX actual de cada circuito IPX habilitado.

**Sintaxis:**

**list** *direcciones*
*configuración*

**addresses**
Lista la dirección IPX de cada circuito IPX habilitado.

**Ejemplo**:

```
Circ   Ifc    Name        Type                          Network/Address
1      0       Eth/0      Ethernet                      400/020000000400
2      1       PPP/0      SCC Serial Line               411/400000000400
3      2       FR/0       FR PVC                        412/000004000000
        Frame Relay PVC circuit number: 16
4      3       FR/0       FR SVC                        413/000004000000
        Frame Relay SVC circuit name: Indianapolis
```

**Configuration**
Lista la configuración actual de IPX. Este mandato visualiza la misma información que el mandato de configuración **list summary**. Consulte la sección “List” en la página 731 para obtener un ejemplo de la visualización y una explicación de la salida.

## Ping

Utilice el mandato **ping** para hacer que el direccionador envíe paquetes IPXPING a un destino determinado (“acción de ping”) y observe si hay una respuesta. Puede utilizarse este mandato para identificar problemas en un entorno de interredes.

Este proceso se realiza de forma continua. Las respuestas recibidas que coinciden se visualizan con el número de red y número de nodo IPX del emisor, el número de saltos y el tiempo de ida y vuelta en milisegundos.

Para detener el proceso de ping, escriba cualquier carácter durante la supervisión. En ese momento se visualizará un resumen en relación con los paquetes perdidos, el tiempo de ida y vuelta, así como el número de destinos inasequibles.

Cuando se especifica una dirección de vertimiento múltiple como destino, pueden aparecer varias respuestas por cada paquete enviado, una por cada miembro del grupo. Cada respuesta devuelta se visualiza junto con la dirección de origen del emisor de la respuesta.

**Notas:**

1. Hay que ir con cuidado cuando se especifica la dirección de difusión (FFFFFFFFFFFF), ya que ello puede generar un gran número de paquetes de respuesta IPXPING que haría disminuir el rendimiento del software del direccionamiento y de la red.
2. Si entra el mandato **ping** sin ningún parámetro, se le solicitarán todos los parámetros. Si sólo entra la ***red de destino*** y el ***nodo de destino***, se utilizarán los valores por omisión para los parámetros restantes.

**Sintaxis:**

**ping** *red-dest nodo-dest red-origen nodo-origen tamaño velocidad*

**red-dest**
Especifica el número de red IPX de destino. Este parámetro es necesario.

**Valores válidos**: Del X'1' al X'FFFFFFFD'

**Valor por omisión**: 1

**nodo-dest**
Especifica la dirección de nodo IPX de destino. Este parámetro es necesario.

**Valor válido**: Del X'1' al X'FFFFFFFFFFFF'

**Valor por omisión**: Ninguno

**red-origen**
Especifica el número de red IPX de origen. Éste es un parámetro opcional. El valor debe ser un número de red conocido que esté asociado con un circuito IPX conectado directo. Si no se especifica una red de origen, se utilizará como nodo IPX de origen el número de red del circuito IPX en que se envíen los paquetes de petición IPXPING. Si el circuito IPX es un circuito IPXWAN con direccionamiento estático o RIP sin número, se utilizará como nodo de origen la dirección de nodo del circuito IPX utilizado para el número de red de origen.

**Valor válido**: X'1' - X'FFFFFFFD'

**Valor por omisión**: 1

**nodo-origen**
Especifica la dirección de nodo IPX de origen. Éste es un parámetro opcional. El valor debe ser una dirección de nodo conocida que esté asociada con un circuito IPX conectado directo. Si no se especifica un nodo de origen, se utilizará como nodo IPX de origen la dirección de nodo del circuito IPX en que se envíen los paquetes de petición IPXPING. Si el circuito IPX es un circuito IPXWAN con direccionamiento estático o RIP sin número, se utilizará como nodo de origen la dirección de nodo del circuito IPX utilizado para el número de red de origen.

**Valor válido**: X'1' - X'FFFFFFFFFFFE'

**Valor por omisión**: Ninguno

**tamaño**
Especifica el número de bytes de datos a añadir a la petición ping. Éste es un parámetro opcional. Los datos incluyen la hora en que se envía la petición por primera vez, por lo que la cantidad especificada no puede ser inferior a 4 bytes. Tampoco puede ser superior al tamaño máximo de paquete soportado por el direccionador o el circuito de la salida. Este valor puede variar según la configuración.

**Valor válido**: Desde 4 hasta el máximo del direccionador

**Valor por omisión**: 56 bytes

**velocidad**
Especifica el número de segundos entre las peticiones ping. Éste es un parámetro opcional.

**Valor válido**: Del 1 al 60

**Valor por omisión**: 1

**Ejemplo: ping**

```
Destination network number [1]? 20
Destination node number []? 00000001c200
Source network number [1]? 10
Source node number []? 000000019a00
Data size: [56]?
Rate in seconds [1]?

IPXPING 20/00000001C200: 56 data bytes
56 data bytes from 20/00000001C200: hops=3 time=0 ms
56 data bytes from 20/00000001C200: hops=3 time=40 ms
56 data bytes from 20/00000001C200: hops=3 time=0 ms

----20/00000001C200 IPXPING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms) min/ave/max = 0/13/40
```

## RecordRoute

Utilice el mandato **recordroute** para informar de cada circuito reenviador de la vía de acceso hacia el destino y de vuelta. Si invoca recordroute sin ningún parámetro, se le solicitarán todos los parámetros. Sólo son necesarios el número de red IPX de destino y la dirección de nodo IPX de destino.

Hay dos sucesos que terminarán un recordroute. El primero es cuando pulse una tecla. El segundo es al haberse enviado el número máximo de paquetes de petición recordroute.

**Sintaxis:**

r**ecordroute** *red-dest nodo-dest red-origen nodo-origen velocidad número*

**red-dest**

Especifica el número de red IPX de destino. Este parámetro es necesario.

**Valores válidos**: Del X'1' al X'FFFFFFFD'

**Valor por omisión**: 1

**nodo-dest**

Especifica la dirección de nodo IPX de destino. Este parámetro es necesario.

**Valores válidos**: Del X'1' al X'FFFFFFFFFFFE'

**Valor por omisión**: Ninguno

**red-origen**

Especifica el número de red IPX de origen. Éste es un parámetro opcional. El valor debe ser un número de red conocido que esté asociado con un circuito IPX conectado directo. Si no se especifica una red de origen, se utilizará como dirección IPX de origen el número de red del circuito IPX en que se envíen los paquetes recordroute. Si el circuito IPX es un circuito IPXWAN con direccionamiento estático o RIP sin número, se utilizará como dirección de origen el número de red de algún otro circuito IPX que esté numerado, ya que los circuitos IPXWAN con direccionamiento estático y RIP sin número no tienen asignado un número de red IPX.

**Valores válidos**: Del X'1' al X'FFFFFFFD'

**Valor por omisión**: 1

**nodo-origen**
Especifica la dirección de nodo IPX de origen. Éste es un parámetro opcional. El valor debe ser una dirección de nodo conocida que esté asociada con un circuito IPX conectado directo. Si no se especifica un nodo de origen, se utilizará como nodo IPX de origen la dirección de nodo del circuito IPX en que se envíen los paquetes recordroute. Si el circuito IPX es un circuito IPXWAN con direccionamiento estático o RIP sin número, se utilizará como nodo de origen la dirección de nodo del circuito IPX utilizado para el número de red de origen.

**Valores válidos**: Del X'1' al X'FFFFFFFFFFFE'

**Valor por omisión**: Ninguno

**velocidad**
Especifica el número de segundos entre las peticiones recordroute. Éste es un parámetro opcional.

**Valores válidos**: Del 1 al 60

**Valor por omisión**: 1

**número**
Especifica el número máximo de peticiones recordroute a enviar. Éste es un parámetro opcional. Un valor de cero hará que recordroute continúe hasta que se pulse una tecla.

**Valores válidos**: Del 0 al 60

**Valor por omisión**: 0

### Ejemplo: recordroute

```
Destination network number [1]? 20
Destination node number []? 00000001c200
Source network number [1]? 10
Source node number []? 000000019a00
Rate in seconds [1]?
Number of packets to send [0]?

RECORDROUTE 20/00000001C200: 784 data bytes
784 data bytes from 20/00000001C200: seq_no=0 time=0 ms
Recorded Routes (in hex):
                10/000000019A00
                500/0000100A0000
                500/0000100C0000
                10/000000019000
                10/000000019A00 (Final Destination)

784 data bytes from 20/00000001C200: seq_no=1 time=30 ms  (same route)
784 data bytes from 20/00000001C200: seq_no=2 time=10 ms  (same route)
...
784 data bytes from 20/00000001C200: seq_no=18 time=0 ms
Recorded Routes (in hex):
                10/000000019A00
                0/0000100A0000
                20/00000001AE00
                20/00000001C200
                0/0000100B0000
                10/000000019000
                10/000000019A00 (Final Destination)

784 data bytes from 20/00000001C200: seq_no=19 time=0 ms  (same route)
784 data bytes from 20/00000001C200: seq_no=20 time=70 ms  (same route)
784 data bytes from 20/00000001C200: seq_no=21 time=0 ms  (same route)
...
784 data bytes from 20/00000001C200: seq_no=48 time=0 ms
Recorded Routes (in hex):
                10/000000019A00
                500/0000100A0000
                500/0000100C0000
                10/000000019000
                10/000000019A00 (Final Destination)

784 data bytes from 20/00000001C200: seq_no=49 time=0 ms  (same route)
784 data bytes from 20/00000001C200: seq_no=50 time=0 ms  (same route)

----20/00000001C200 RECORDROUTE Statistics----
53 packets transmitted, 38 packets received, 28% packet loss
5 unreachables, 0 no usable source addresses, 0 buffer unavailable
round-trip (ms) min/ave/max = 0/23/100
```

Sólo se informa de toda la vía de acceso una vez en la primera respuesta o bien cuando ha cambiado la vía de acceso. En el ejemplo anterior, la vía de acceso ha cambiado dos veces.

## Reset

Utilice el mandato **reset** para restablecer circuitos IPX específicos, los filtros de SAP globales, los filtros de IPX globales (controles del acceso), las rutas estáticas, los servicios estáticos o bien los filtros basados en circuito de Direccionador, RIP, SAP o IPX (listas-filtro).

**Sintaxis:**

| | |
|---|---|
| re**set** | access-controls |
| | circuit . . . |
| | filters |
| | filter-lists |

route-static
sap-static

**access-controls**
Restablece los filtros de IPX globales (controles del acceso) sobre la base del parámetro de configuración almacenado en la memoria de la configuración. Se activarán los cambios efectuados en la configuración de los filtros de IPX globales.

**Ejemplo**: reset access-controls

**circuit** *núm. circuito-ipx*
Restablece IPX en el circuito IPX especificado utilizando los valores de parámetros de configuración almacenados en la memoria de la configuración. Se activarán los cambios efectuados en la configuración de IPX del circuito IPX.

**Ejemplo**: reset circuit 2

**filters**
Restablece los filtros de SAP globales sobre la base de los valores de parámetros de configuración almacenados en la memoria de la configuración. Se activarán los cambios efectuados en la configuración de los filtros de SAP globales.

**Ejemplo**: reset filters

**filter-lists** *tipo-filtro*
Restablece el filtro basado en circuito partiendo de los valores de parámetros de configuración almacenados en la memoria de la configuración. Se activarán los cambios efectuados en la configuración del filtro basado en circuito. Los ***tipos de filtro*** válidos son direccionador, rip, sap e ipx.

**Ejemplo**: reset filter-lists rip

**route-static**
Restablece las rutas estáticas sobre la base de los valores de parámetros de configuración almacenados en la memoria de la configuración. Se activarán los cambios efectuados en la configuración de las rutas estáticas.

**Ejemplo**: reset route-static

**sap-static**
Restablece los servicios estáticos sobre la base de los valores de parámetros de configuración almacenados en la memoria de la configuración. Se activarán los cambios efectuados en la configuración de los servicios estáticos.

**Ejemplo**: reset sap static

## Sizes

Utilice el mandato **sizes** para visualizar los tamaños configurados de la antememoria de nodos locales y la de redes remotas, así como el número de entradas de antememoria que actualmente están en uso. (Este mandato no visualiza el contenido de las antememorias.)

**Sintaxis:**

si**zes**

**Ejemplo:** `sizes`

```
Current IPX cache size:
Remote network cache size (max entries): 64
       2 entries now in use

Local node cache size (max entries): 128
       1 entries now in use
```

## Slist

Utilice el mandato **slist** para visualizar el contenido de la tabla de servidores SAP de IPX.

**Sintaxis:**

sl**ist**

**Ejemplo: `slist`**

```
9 entries used out of 32

State Typ Service Name                 Hops   Age     Net  /   Host     /Sock
SAP  4    PCS12                         3     0:50        1/000000000048/0451
SAP  4    ACMPCS                        3     0:50        1/00000000004A/0451
SAP  4    DEVEL2                        1     0:50       11/0000000000B4/0451
SAP  4    PLANNING                      2     0:50       BB/0000000000B7/0451
SAP  4    DEVEL                         2     0:50       BB/0000000000EE/0451
SAP  4    SOFT2                         1     0:30      704/000000000094/0451
SAP  4    SKYSURF1                      2     0: 5 2C39ABE9/000000000001/0451
SAP  278  DIRTREE                       2     0: 5 2C29ABE9/000000000001/4005
Stat 26B  DIRTREE                       2     0: 0      444/000000000001/0045
```

**State**
Especifica uno de los parámetros siguientes:

SAP - indica que este servicio se ha obtenido mediante el protocolo de direccionamiento SAP.
Del - indica que este servicio ha sobrepasado el tiempo de espera excedido y ya no se utiliza. El servicio se mantiene durante un tiempo breve en la tabla para que se notifique a los otros direccionadores que el servicio ya no es válido. Después de esto, se suprime y ya no se visualiza.
Stat - indica que este servicio es un servicio estático.

**Typ** Especifica el tipo de servidor en hexadecimal. Los servidores de archivos son del tipo 0004. Los otros números de tipo están asignados por Novell.

**Service name**
Especifica el nombre exclusivo del servidor para este tipo de servidor. Sólo se visualizan los 30 primeros caracteres del nombre de 47 caracteres para conservar espacio.

**Hops**
Especifica el número de saltos de direccionador desde este direccionador al servidor.

**Age** Especifica la duración de la información de servicios. Si una entrada de la tabla de SAP no se actualiza, el direccionador realizará las siguientes acciones:

- Después de que hayan pasado 3 intervalos de actualización de SAP, el servicio se especificará como Del y el direccionador anunciará que el servicio ya no es válido. El intervalo de actualización de SAP puede visualizarse si se utiliza el mandato de IPX **config**.
- Después de 60 segundos adicionales, se suprimirá el servicio y no aparecerá en la visualización de **slist**.

**Net/Host/Sock**
Especifica la dirección del servicio. La dirección incluye los parámetros siguientes:

- Número de red
- Número de sistema principal de la red (la dirección del primer circuito de la red)
- Número de socket mediante el cual se puede llegar al servicio

En la parte inferior de la visualización están el número de entradas utilizadas y el total de las disponibles. Si están en uso todas las entradas, es probable que la tabla de servicios no sea lo suficientemente grande. Utilice el mandato de configuración de IPX **set maximum services** para aumentar el tamaño.

## Traceroute

Utilice el mandato **traceroute** para informar de cada salto que tome una petición ping en su ruta hacia un destino final. Si invoca traceroute sin ningún parámetro, se le solicitarán todos los parámetros. Sólo son necesarios el número de red IPX de destino y la dirección de nodo IPX de destino.

Hay tres sucesos que terminarán un traceroute. El primero es cuando pulse una tecla. El segundo es cuando se reciba una respuesta de la dirección de destino. El tercero es al haberse alcanzado el número máximo de saltos.

**Sintaxis:**

**traceroute** *red-dest nodo-dest red-origen nodo-origen tamaño puntas de prueba velocidad saltos*

**red-dest**
Especifica el número de red IPX de destino. Este parámetro es necesario.

**Valores válidos**: Del X'1' al X'FFFFFFFD'

**Valor por omisión**: 1

**nodo-dest**
Especifica la dirección de nodo IPX de destino. Este parámetro es necesario.

**Valores válidos**: Del X'1' al X'FFFFFFFFFFFE'

**Valor por omisión**: Ninguno

**red-origen**
Especifica el número de red IPX de origen. Éste es un parámetro opcional. El valor debe ser un número de red conocido que esté asociado con un circuito IPX conectado directo. Si no se especifica una red de origen, se utilizará como dirección IPX de origen el número de red del circuito IPX en que se envíen los paquetes traceroute. Si el circuito IPX es un circuito IPXWAN con direccionamiento estático o RIP sin número, se utilizará como dirección de origen el número de red de algún otro circuito IPX que esté numerado, ya que los circuitos IPXWAN con direccionamiento estático y RIP sin número no tienen asignado un número de red IPX.

**Valor válido**: Del X'1' al X'FFFFFFFD'

**Valor por omisión**: 1

**nodo-origen**
Especifica la dirección de nodo IPX de origen. Éste es un parámetro opcional. El valor debe ser una dirección de nodo conocida que esté asociada con un circuito IPX conectado directo. Si no se especifica un nodo de origen, se utilizará como nodo IPX de origen la dirección de nodo del circuito IPX en que se envíen los paquetes traceroute. Si el circuito IPX es un circuito IPXWAN con direccionamiento estático o RIP sin número, se utilizará como nodo de origen la dirección de nodo del circuito IPX utilizado para el número de red de origen.

**Valores válidos**: Del `X'1'` al `X'FFFFFFFFFFFE'`

**Valor por omisión**: Ninguno

**tamaño**
Especifica el número de bytes de datos a añadir a la petición traceroute. Éste es un parámetro opcional. Los datos incluyen la hora en que se envía la petición por primera vez, por lo que el número especificado no puede ser inferior a 4 bytes. Tampoco puede ser superior al tamaño máximo de paquete del direccionador o del circuito de la salida. Este valor puede variar según la configuración.

**Valores válidos**: Desde 4 hasta el máximo del direccionador

**Valor por omisión**: 56

**puntas de prueba**
Especifica cuántas peticiones traceroute se van a enviar por salto. Éste es un parámetro opcional.

**Valores válidos**: Del 1 al 10

**Valor por omisión**: 3

**velocidad**
Especifica el número de segundos a esperar entre las puntas de prueba cuando no hay respuesta a la petición traceroute. Éste es un parámetro opcional.

**Valores válidos**: Del 1 al 60

**Valor por omisión**: 1

**saltos**
Especifica el número máximo de saltos para enviar peticiones traceroute. Éste es un parámetro opcional. Sin NLSP, un paquete puede pasar por un máximo de 16 nodos (por ello, el valor por omisión de 16). Con NLSP o la solución del medio direccionador IBM 6611, el límite ya no es 16.

**Valores válidos**: Del 1 al 255

**Valor por omisión**: 16

**Ejemplo:** `traceroute`

```
Destination network number [1]? 20
Destination node number []? 00000001c200
Source network number [1]? 10
Source node number []? 000000019a00
Data size:  [56]?
Number of probes per hop [3]?
Wait time between retries in seconds [1]?
Maximum Hops [16]?

TRACEROUTE 20/00000001C200: 56 data bytes
1 10/000000019000: 0 ms * 500/0000100B0000 20 ms
2 * * *
3 20/00000001C200: 10 ms 60 ms 20 ms
```

La dirección IPX de origen de una respuesta traceroute sólo aparece notificada una vez siempre y cuando no cambie. En el ejemplo anterior, han respondido a la petición traceroute de un salto dos direccionadores diferentes. Esto sucederá si la ruta hacia el destino cambia entre las puntas de prueba.

Existe otra información notificada por traceroute además del tiempo de ida y vuelta de una punta de prueba:

- '*' - No se ha recibido ningún paquete de respuesta en el tiempo especificado.
- 'H!' - La red de destino es inasequible. Se notificará esto si se pierde la ruta hacia el destino después de iniciarse traceroute.
- 'BF' - No hay almacenamientos intermedios disponibles.

## Mandatos de supervisión de filtros de circuito IPX

La Tabla 46 lista los mandatos disponibles en el indicador IPX *tipo*-Lists>. En esta sección se explica detalladamente cada uno de estos mandatos.

Para acceder al indicador IPX tipo-Lists>, entre **filter-lists** tipo en el indicador IPX>. Los tipos válidos son router-lists, rip-lists, sap-lists e ipx-lists.

*Tabla 46. Resumen de los mandatos de filtros de circuito IPX*

| Mandato | Función |
|---|---|
| Cache | Visualiza el contenido de la antememoria de filtro para el circuito especificado. Sólo el filtro de IPX da soporte a una antememoria de filtro. |
| Clear | Borra los contadores del filtro especificado o borra los contadores de todos los filtros del tipo actual (DIRECCIONADOR, RIP, SAP o IPX). |
| Disable | Inhabilita un filtro especificado o todos los filtros del tipo actual. |
| Enable | Habilita un filtro especificado o todos los filtros del tipo actual. |
| List | Lista un filtro especificado o todos los filtros del tipo actual. |
| Exit | Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxii. |

## Cache

Utilice el mandato **cache** para visualizar el contenido de la antememoria de filtro. Sólo el filtro de IPX da soporte a una antememoria. Los filtros de DIRECCIONADOR, RIP y SAP no dan soporte a una antememoria de filtro.

**Sintaxis:**

ca**che filter** *núm. filtro*

**núm. filtro**
Especifica el número del filtro. Puede utilizarse el mandato list para visualizar una lista numerada de los filtros configurados.

**Ejemplo: `cache filter 1`**

```
IPX IPX-Lists>cache filter 1
Hops Type Dst Net  Address      Sock Src Net  Address      Sock Action
---- ---- -------- ------------ ---- -------- ------------ ---- -------
   4   00 04000000 400003900000  802 03000040 400003004400  966 EXCLUDE
   2   00 0004A300 400000233D00  952 0763A020 4000000DD100  920 INCLUDE
```

## Clear

Utilice el mandato **clear** para borrar los contadores del filtro especificado o para borrar los contadores de todos los filtros del tipo actual (DIRECCIONADOR, RIP, SAP o IPX).

**Sintaxis:**

**clear** all
filter ...

**all** Borra los contadores de todos los filtros del tipo actual (DIRECCIONADOR, RIP, SAP o IPX).

**Ejemplo: `clear all`**

**filter** *núm. filtro*
Borra los contadores del número de filtro especificado. Puede utilizarse el mandato list para visualizar una lista numerada de los filtros configurados.

**Ejemplo: `clear filter 1`**

## Disable

Utilice el mandato **disable** para inhabilitar filtros específicos o para inhabilitar todos los filtros del tipo actual (DIRECCIONADOR, RIP, SAP o IPX).

**Sintaxis:**

**disable** all
filter *núm. filtro*

**all** Inhabilita todos los filtros del tipo actual (DIRECCIONADOR, RIP, SAP o IPX).

**Ejemplo: `disable all`**

**filter** *núm. filtro*
Inhabilita el número de filtro especificado. Puede utilizarse el mandato list para visualizar una lista numerada de los filtros configurados.

**Ejemplo: `disable filter 1`**

## Enable

Utilice el mandato **enable** para habilitar filtros específicos o para habilitar todos los filtros del tipo actual (DIRECCIONADOR, RIP, SAP o IPX).

**Sintaxis:**

en**able** all
filter *núm. filtro*

**all** Habilita todos los filtros del tipo actual (DIRECCIONADOR, RIP, SAP o IPX).

**Ejemplo:** `enable all`

**filter** *núm. filtro*
Habilita el número de filtro especificado. Puede utilizarse el mandato list para visualizar una lista numerada de los filtros configurados.

**Ejemplo:** `enable filter 1`

## List

Utilice el mandato **list** para visualizar información sobre filtros específicos o sobre todos los filtros del tipo actual (DIRECCIONADOR, RIP, SAP o IPX).

**Sintaxis:**

**list** all
filter *núm. filtro*

**all** Lista la configuración de todos los filtros del tipo actual (DIRECCIONADOR, RIP, SAP o IPX).

**Ejemplo:** `list all`

```
IPX IPX-Lists>list all
Filtering: ENABLED

Filter Lists:
Name                           Action
------------------------------ ----------
ipx01                          EXCLUDE
ipx02                          INCLUDE
ipx03                          EXCLUDE

Filters:
Id    Circ  Ifc   Direction  State      Default    Cache
----- ----- ----- ---------- ---------- ---------- -----
1     1     0     INPUT      ENABLED    INCLUDE    10
2     1     0     OUTPUT     ENABLED    INCLUDE    10
3     2     1     INPUT      DISABLED   INCLUDE    10
4     2     1     OUTPUT     DISABLED   INCLUDE    10
```

**filter** *núm. filtro*
Lista la configuración del número de filtro especificado. Puede utilizarse el mandato list para visualizar una lista numerada de los filtros configurados.

### Ejemplo: `list filter 1`

```
IPX IPX-Lists>list filter 1

Filters:
Id    Circ  Ifc   Direction  State      Default    Cache
----- ----- ----- ---------- ---------- ---------- -----
1     1     0     INPUT      ENABLED    INCLUDE    10

Filter Lists:
Name                           Action     Count
------------------------------ ---------- ----------
ipx01                          EXCLUDE    43
ipx02                          INCLUDE    23453
```

# Apéndices

# Apéndice A. Interoperatividad con el direccionador IBM 6611

Hay varias consideraciones sobre configuración a tener en cuenta para que la implantación DLSw de IBM Nways Multiprotocol Routing Services pueda interoperar con la del direccionador IBM 6611.

Las siguientes secciones ofrecen una visión general de estas consideraciones e indican qué características de la implantación DLSw de IBM Nways Multiprotocol Routing Services no pueden interoperar con las del IBM 6611.

**Nota:** Las consideraciones que aquí se citan se han obtenido de una prueba realizada con el software MPNP V1.2 del IBM 6611. Puede que estas consideraciones no se apliquen a otras versiones del software MPNP.

Las consideraciones se han dividido en las siguientes secciones:



## Consideraciones sobre la configuración del puente

A continuación se describen las consideraciones sobre la configuración del puente a tener en cuenta:

- La identificación de la LAN (Número de segmento) de DLSw debe coinciden en los direccionadores IBM 2210 e IBM 6611. Si se produce una falta de coincidencia persistente, entre en el configurador del IBM Nways Multiprotocol Routing Services (Talk 6) y seleccione el protocolo DLSw. Puede utilizar el mandato **set srb** para definir un valor de número de segmento que coincida con el equivalente del IBM 6611.
- El valor de número máximo de MTU que se puede utilizar para la trama de puente es de 2100 bytes. Este es el valor más alto al que actualmente da soporte el IBM 6611. Si se especifican valores de MTU inferiores a 2100, es importante que los valores configurados coincidan en los direccionadores IBM 2210 e IBM 6611.

## Consideraciones relacionadas con DLSw

Las consideraciones de interoperatividad relacionadas con DLSw son las siguientes:

- La implantación DLSw de IBM Nways Multiprotocol Routing Services no da soporte a la generación de un mensaje SSP_IAMOKAY (tipo de mensaje SSP X'x1D') mientras que la implantación DLSw de IBM 6611 sí le da soporte. Este mensaje SSP no aparece documentado en RFC 1434 y la implantación DLSw de IBM Nways Multiprotocol Routing Services lo elimina silenciosamente en cuanto lo recibe.
- La implantación DLSw de IBM 6611 procesa mensajes SSP_ENTER_BUSY/EXIT_BUSY recibidos de la implantación DLSw de IBM

Nways Multiprotocol Routing Services, pero no genera mensajes SSP similares relacionados con el control del flujo.

- La implantación DLSw de IBM Nways Multiprotocol Routing Services no da soporte al mensaje SSP_TEST_CIRCUIT_REQ definido por el usuario (tipo de mensaje SSP X'x7A') que genera el direccionador DLSw IBM 6611 cuando funciona como un nodo de red APPN. Cuando recibe este mensaje, la implantación DLSw de IBM Nways Multiprotocol Routing Services devuelve el mensaje SSP_TEST_CIRCUIT_RSP definido por el usuario (tipo de mensaje SSP X'x7B'). La implantación del nodo de red APPN del direccionador DLSw IBM 6611 espera esta respuesta.

## Consideraciones sobre configuración relacionadas con IP

A continuación se describen las consideraciones sobre la configuración de IP:

- La característica de grupos DLSw cliente/servidor y similar/similar que permite a los direccionadores dinámicos DLSw de IBM Nways Multiprotocol Routing Services encontrarse entre sí de forma dinámica no puede interoperar con la implantación DLSw del IBM 6611. Como resultado, se debe utilizar el mandato de configuración **add tcp neighbor** de DLSw para definir direcciones IP estáticas de similares adyacentes DLSw del IBM 6611.
- La restricción anterior sobre la interoperatividad de la característica de grupos DLSw de IBM Nways Multiprotocol Routing Services tiene implicaciones para la selección de RIP/OSPF:
  - Para poder utilizar grupos DLSw en un 2210, de configurar también OSPF/MOSPF. Pero puesto que estos grupos DLSw no pueden interoperar con el 6611, no se puede configurar el 2210 con sólo RIP activado y sin configuración OSPF.
  - Aunque tanto OSPF como RIP se pueden activar en el lado del IBM 2210, MOSPF (si se selecciona mediante la configuración de OSPF) no recibe soporte del IBM 6611.
- Dentro de la configuración de IP de IBM Nways Multiprotocol Routing Services, asegúrese de que los patrones de relleno configurados para direcciones de difusión general de una determinada interfaz coinciden con sus definiciones equivalentes en el IBM 6611.
- El Sistema de reserva de ancho de banda (BRS) de IBM Nways Multiprotocol Routing Services, que se puede utilizar para garantizar el ancho de banda para el transporte de tráfico SNA sobre DLSw, no puede interoperar con la implantación DLSw del IBM 6611.

  Aunque la prioridad que asigna el hardware del IBM 2210 para BRS se puede implantar en una dirección de salida, el orden de prioridades no se garantiza si los direccionadores IP intermedios no dan soporte a BRS. Además, puesto que el 6611 no da soporte a BRS en su extremo de la línea, BRS sólo se puede aplicar en una dirección.

## Consideraciones relacionadas con TCP

A continuación se describen las consideraciones sobre la interoperatividad de TCP:

**Diferencias en la detección de interrupciones en la conexión TCP**
La implantación DLSw de IBM Nways Multiprotocol Routing Services detecta que una conexión TCP se ha interrumpido cuando no se recibe una respuesta Keepalive (suponiendo que se ha activado la opción Keepalive para la conexión) o cuando no se pueden distribuir datos.

**Diferencias al volver a establecer la conexión TCP**
Cuando se ha interrumpido una conexión TCP, la implantación DLSw de IBM Nways Multiprotocol Routing Services vuelve a establecer la conexión TCP cuando se genera un nuevo SSP_CANUREACH de DLSw tras la recepción de un mensaje DLC TEST procedente de una estación final. El IBM 6611 puede no tener el mismo comportamiento.

**Diferencias relacionadas con la activación/desactivación de la opción Keepalive**
Tal como se ha indicado anteriormente, la implantación DLSw de IBM Nways Multiprotocol Routing Services permite activar y desactivar una opción Keepalive cuando se añade (se configura) una dirección IP de un direccionador contiguo TCP. Aunque TCP en la implantación DLSw de IBM 6611 responde ante los mensajes Keepalive recibidos en una sesión TCP, no hay ningún mecanismo para configurar el TCP del 6611 residente para que active la generación de mensajes Keepalive de TCP.

**Número máximo de conexiones TCP soportadas**
En la implantación DLSw de IBM Nways Multiprotocol Routing Services, no hay ninguna restricción, codificada en el hardware, sobre el número máximo de conexiones TCP soportadas. Como resultado, el número máximo de conexiones TCP soportadas está directamente relacionado con la memoria disponible de un IBM 2210. En el caso del IBM 6611, hay una restricción interna codificada en el hardware de 100 conexiones TCP que pueden recibir soporte en la implantación DLSw.

## Consideraciones varias sobre la interoperatividad

Tenga en cuenta las siguientes consideraciones varias sobre la interoperatividad:

- Si se encuentra un problema al intentar establecer una conexión DLSw iniciada por el IBM 6611, compruebe la configuración del IBM 6611 para asegurarse que la función de filtro de direcciones MAC no se haya activado sin querer para una dirección MAC de origen o destino asociada.
- Aunque RFC 1434 no trata específicamente el tema de las sesiones DLSw huérfanas (por ejemplo, sesiones DLSw que permanecen en un estado de circuito DLSw establecido sin más actividad), las implantaciones DLSw tanto de IBM Nways Multiprotocol Routing Services como de IBM 6611 resuelven este tema especificando tiempos de espera de sesiones DLSw huérfanas. Las sesiones DLSw que permanecen inactivas mientras se está en estado de circuito DLSw establecido durante más de 30 segundos se eliminan en ambas implantaciones.

# Apéndice B. Interoperatividad con el puente IBM 6611

Hay varios temas sobre la configuración a tener en cuenta antes de implantar una conexión por puente en el IBM 2210 para que interopere con la conexión por puente en el IBM 6611.

Este apéndice ofrece una visión general sobre estos temas e indica qué características de la implantación de puente del IBM 2210 **no** pueden interoperar con la implantación de puente del IBM 6611.

Para no crear una red incompatible, debe tener en cuenta los siguientes temas sobre la configuración de puente al utilizar el IBM 6611 y el IBM 2210 como los dos puentes finales sobre enlaces serie PPP y Frame Relay,

Para PPP, el puente IBM 2210 da soporte a distintos tipos de MAC (Ethernet y red en anillo), tal como se describe en RFC 1638, *PPP Bridging Control Protocol* Para Frame Relay, el IBM 2210 da soporte a la *Interconexión multiprotocolo sobre Frame Relay* descrita en RFC 1490/2427.

Actualmente, el puente IBM 6611 da soporte a los tipos de MAC Ethernet y red en anillo sobre PPP y Frame Relay. Sin embargo, el puente IBM 6611 solo da soporte a tramas MAC de red en anillo cuando el puerto de puente asociado a PPP o Frame Relay se ha configurado como un puerto de **direccionamiento de origen**. Esto da lugar a ciertas restricciones en topologías de red cuando el IBM 6611 y el IBM 2210 son los dos puentes finales sobre PPP o Frame Relay.

RFC 1638, sección 5.3, describe el modo en que un proveedor puede anunciar al puente similar el tipo de MAC que recibe soporte sobre PPP para que el similar no envíe tráfico de tipo de MAC no soportado sobre PPP. Actualmente, el puente IBM 2210 no elimina las tramas que no son Ethernet destinadas a la red PPP. Tampoco intenta convertir todas las tramas a tramas Ethernet antes de enviarlas sobre PPP. Esto hace que el puente IBM 6611 reciba tramas que no son Ethernet sobre PPP y las elimina cuando hay una falta de coincidencia en la configuración.

## Otras consideraciones sobre PPP

Debe tener en cuenta las siguientes consideraciones al configurar un 2210 y un 6611 en una red conectada por puente:

- Para conectar por puente tráfico sobre un enlace PPP, la unidad máxima de recepción (MRU) negociada debe ser lo suficientemente grande para contener una trama conectada por puente. La trama conectada por puente contiene los datos y la cabecera de capa MAC procedentes de la LAN original.

  Por ejemplo, una trama Ethernet puede contener 1500 bytes de datos. Cuando se conecta por puente sobre en enlace WAN, se incluyen 14 bytes adicionales de cabecera MAC Ethernet en el tráfico conectado por puente, con lo que el tamaño del paquete alcanza los 1514 bytes. Esto significa que la MRU PPP negociada debe ser de al menos 1514 para conectar por puente la trama.

  Debe definir un tamaño de MRU que sea más que suficiente para albergar cualquier trama conectada por puente. Intente utilizar 2000 ó 2048 como valor inicial de MRU.

- Asegúrese de que ambos extremos del enlace PPP se han configurado para el mismo tamaño de MRU. Si utiliza la MRU por omisión para el 2210, asegúrese de que la MRU del 6611 coincide con el valor de MRU del 2210.

## Ejemplos de configuración

Los siguientes ejemplos de topologías de red ***no*** funcionarán. Las configuraciones posibles alternativas se han marcado con **Alt**. Cuando se tiene en cuenta WAN, los tipos de LAN se pueden ampliar a tipos MAC.

**Ejemplo 1:** Red en anillo (SR) - IBM 2210 (SR-TB) - PPP (TB) - IBM 6611 (TB) - Ethernet

**Alt:** Red en anillo (SR) - IBM 2210 (SRB) - PPP (SR) - IBM 6611 (SR-TB) - Ethernet

**Ejemplo 2:** Red en anillo (TB) - IBM 2210 (TB) - PPP (TB) - IBM 6611 (TB) - ETH/TKR

**Alt:** Red en anillo (SR) - IBM 2210 (SRB) - PPP (SR) - IBM 6611 (SR-TB) - ETH

**Alt:** Red en anillo (SR) - IBM 2210 (SRB) - PPP (SR) - IBM 6611 (SRB) - TKR

**Alt:** Red en anillo (TB) - IBM 2210 (SR-TB) - PPP (SR) - IBM 6611 (SRB) - TKR

**Alt:** Red en anillo (TB) - IBM 2210 (SR-TB) - PPP (SR) - 6611 (SR-TB) - ETH

Las tramas LAN generadas por el Nodo límite de acceso (BAN) y DLSw son tramas de red en anillo direccionadas de origen. En función del tipo de soporte y del comportamiento de la configuración del puente del puerto de puente de salida asociado, el puente IBM 2210 convierte la trama de red en anillo direccionada de origen del siguiente modo.

1. ETH (TB) en Ethernet
2. PPP / FR / Túnel en formato TB de red en anillo
3. PPP / FR / Túnel en formato SR de red en anillo
4. TKR (TB) en formato TB de red en anillo
5. TKR (SR) en formato SR de red en anillo

# 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** Multidifusión

**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 multidifusión

**MSB** Bit más significativo

**MSDU** Unidad de datos de servicio MAC

**MRU** Unidad máxima de recepción

**MTU** Unidad máxima de transmisión

**nak** Sin acuse de recibo

**NBMA** Acceso múltiple sin difusión

**NBP** Name Binding Protocol

**NBR** Direccionador contiguo

**NCP** Network Control Protocol

**NCP** Network Core Protocol

**NetBIOS** Network Basic Input/Output System

**NHRP** Next Hop Resolution Protocol

**NIST** National Institute of Standards and Technology

**NPDU** Unidad de datos de protocolo de red

**NRZ** Sin vuelta a cero

**NRZI** Sin vuelta a cero invertido

**NSAP** Punto de acceso a servicios de red

**NSF** National Science Foundation

**NSFNET** National Science Foundation NETwork

**NVCNFG** Configuración permanente

**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 *Norma ANSI/EIA 440-A de la Fiber Optic Terminology*. Los ejemplares pueden adquirirse en la Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006. Las definiciones se identifican mediante el símbolo (E) que aparece después de la definición.
- El *Information Technology Vocabulary* desarrollado por la Subcomisión 1, Comisión Técnica Mixta 1, de la Organización Internacional para la Normalización y la Comisión Electrotécnica Internacional (JTC1/SC1 de la ISO/IEC). Las definiciones de las secciones publicadas de este vocabulario se identifican mediante el símbolo (I) que aparece después de la definición; las definiciones de los borradores de normas internacionales, borradores de comisiones y documentos de trabajo que está desarrollando la JTC1/SC1 de la ISO/IEC se identifican mediante el símbolo (T) que aparece después de la definición, símbolo que indica que las Corporaciones Nacionales de la SC1 participantes todavía no han llegado a un acuerdo definitivo.
- El *IBM Dictionary of Computing*, New York: McGraw-Hill, 1994.
- Internet Request for Comments: 1208, *Glossary of Networking Terms*
- Internet Request for Comments: 1392, *Internet Users' Glossary*
- El *Object-Oriented Interface Design: IBM Common User Access Guidelines*, Carmel, Indiana: Que, 1992.

En este glosario, se utilizan las siguientes referencias cruzadas:

**Compárese con:** Se refiere a un término que tiene un significado opuesto o esencialmente distinto.

**Sinónimo de:** Indica que el término tiene el mismo significado que un término preferente, el cual está definido en el lugar que le corresponde dentro del glosario.

**Sinónimo con:** Es una referencia hacia atrás de un término definido a los otros términos que tienen el mismo significado.

**Véase:** Remite al lector a términos de diversas palabras que tienen la misma palabra al principio.

**Véase también:** Remite al lector a términos que tienen un significado relacionado, pero no sinónimo.

## A

**AAL**. 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 de Internet Protocol (IP) utilizado entre dominios y sistemas autónomos.

**bucle de direccionamiento**. Situación que ocurre cuando los direccionadores hacen circular información entre ellos hasta que se produce la convergencia o hasta que se consideran inasequibles las redes implicadas.

# C

**cabecera**. (1) Información de control definida por el sistema que precede a los datos de usuario. (2) Parte de un mensaje que contiene información de control para el mismo, como, por ejemplo, uno o más campos de destino, el nombre de la estación de origen, el número de secuencia de entrada, una serie de caracteres que indica el tipo de mensaje y el nivel de prioridad del mensaje.

**cabecera de transmisión (TH)**. Información de control, seguida opcionalmente de una unidad básica de información (BIU) o de un segmento de BIU, que crea y utiliza el control de la vía de acceso para direccionar unidades de mensajes y controlar su flujo dentro de la red. Véase también *unidad de información de vía de acceso*.

**canal**. (1) Vía de acceso por la que pueden enviarse señales, como, por ejemplo, canal de datos, canal de salida. (A) (2) Unidad funcional, controlada por el procesador, que maneja la transferencia de datos entre el almacenamiento del procesador y el equipo de periféricos local.

**canal de entrada/salida**. En un sistema de proceso de datos, unidad funcional que maneja la transferencia de datos entre el equipo interno y el equipo de periféricos. (I) (A)

**canal lógico**. En el funcionamiento en modalidad de paquete, canal de emisión y canal de recepción que se utilizan conjuntamente para enviar y recibir datos sobre un enlace de datos al mismo tiempo. Pueden establecerse varios canales lógicos en el mismo enlace de datos si se interpone la transmisión de paquetes.

**capa**. (1) En una arquitectura de red, grupo de servicios que está completo desde un punto de vista conceptual, que es uno de los grupos de un conjunto de grupos ordenados jerárquicamente y que se extiende por todos los sistemas que se ajustan a la arquitectura de red. (T) (2) En el modelo de referencia interconexión de sistemas abiertos, uno de los siete grupos de servicios, funciones y protocolos ordenados jerárquicamente y completos conceptualmente que se extienden por todos los sistemas abiertos. (T) (3) En SNA, agrupación de funciones relacionadas que están separadas lógicamente de las funciones de otros grupos. La implementación de las funciones de una

capa puede cambiar sin que ello afecte a las funciones de otras capas.

**capa de control de enlace de datos (DLC)**. En SNA, capa que está compuesta por las estaciones de enlace que planifican la transferencia de datos sobre un enlace entre dos nodos y realizan un control de errores para el enlace. Ejemplos de control de enlace de datos son: el SDLC para la conexión de enlaces serie por bit y el control de enlace de datos para el canal de System/370.

**Nota:** Normalmente, la capa de DLC es independiente del mecanismo de transporte físico y asegura la integridad de los datos que alcanzan las capas superiores.

**capa de enlace de datos**. En el modelo de referencia de OSI (interconexión de sistemas abiertos), capa que proporciona servicios para la transferencia de datos entre las entidades de la capa de red sobre un enlace de comunicaciones. La capa de enlace de datos detecta los errores que puedan producirse en la capa física y posiblemente los corrige. (T)

**capa de red**. En la arquitectura interconexión de sistemas abiertos (OSI), capa que es responsable del direccionamiento, de la conmutación y del acceso a la capa de enlace a lo largo del entorno de OSI.

**capa de transporte**. En el modelo de referencia interconexión de sistemas abiertos, capa que proporciona un servicio fiable de transferencia de datos de extremo a extremo. Puede haber sistemas abiertos del tipo Relay en la vía de acceso. (T) Véase también *modelo de referencia interconexión de sistemas abiertos*.

**capa física**. En el modelo de referencia interconexión de sistemas abiertos, capa que proporciona los medios mecánicos, eléctricos, funcionales y de procedimiento para establecer, mantener y liberar conexiones físicas sobre el medio de transmisión. (T)

**carácter comodín**. Sinónimo de *carácter de coincidencia con el patrón*.

**carácter de coincidencia con el patrón**. Carácter especial, como, por ejemplo, un asterisco (*) o un signo de interrogación (?), que puede utilizarse para representar uno o más caracteres. Cualquier carácter o conjunto de caracteres puede sustituir a un carácter de coincidencia con el patrón. Sinónimo con *carácter global* y *carácter comodín*.

**CCITT**. Comisión consultiva de la telefonía y telegrafía Internacionales. Era una organización de la Unión de Telecomunicaciones Internacionales (ITU). El 1 de marzo de 1993 se reorganizó la ITU y las responsabilidades de la normalización recayeron en una organización subordinada que se denomina Sector de normalización de telecomunicaciones de la unión de telecomunicaciones (ITU-TS). La “CCITT” sigue funcionando para las recomendaciones que se aprobaron antes de la reorganización.

**central privada (PBX)**. Central telefónica privada para la transmisión de llamadas desde y hacia la red telefónica pública.

**centro de información de la red (NIC)**. En comunicaciones de Internet, grupos locales, regionales y nacionales de todo el mundo que proporcionan ayuda, documentación, formación y otros servicios a los usuarios.

**circuito de datos**. (1) Par de canales de transmisión y recepción asociados que proporcionan un medio de comunicación de datos de dos direcciones. (I) (2) En SNA, sinónimo de *conexión de enlace*. (3) Véase también *circuito físico* y *circuito virtual*.

**Notas:**

1. Entre los intercambios de conmutaciones de datos, el circuito de datos puede incluir un equipo de terminación de circuito de datos (DCE) de acuerdo con el tipo de interfaz que se utilice en el intercambio de conmutaciones de datos.
2. Entre una estación de datos y un intercambio de 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 del acceso a L2TP (LAC)**. Dispositivo conectado a una o más líneas RDSI o de red telefónica de servicios públicos (PSTN) con posibilidades de manejar el funcionamiento de PPP y el del protocolo L2TP. El LAC implementa el medio sobre el que funciona L2TP. L2TP pasa el tráfico a uno o más Servidores de red L2TP (LNS). L2TP puede proporcionar la función de túnel para cualquier protocolo que conlleve la red PPP.

**concentrador (inteligente)**. Concentrador de cableado, como, por ejemplo, el IBM 8260, que proporciona funciones de puente y direccionamiento a las LAN con diferentes cables y protocolos.

**conectado mediante enlace**. (1) Perteneciente a dispositivos que están conectados a una unidad de control por medio de un enlace de datos. (2) Compárese con *conectado mediante canal*. (3) Sinónimo con *remoto*.

**conexión**. En la comunicación de datos, asociación establecida entre unidades funcionales para comunicar información. (I) (A)

**conexión de enlace**. (1) Equipo físico que proporciona comunicación en dos direcciones entre una estación de enlace y otra u otras estaciones de enlace; por ejemplo, un equipo de terminación de circuito de datos (DCE) y una línea de telecomunicaciones. (2) En SNA, sinonimia con *circuito de datos*.

**conexión Rapid Transport Protocol (RTP)**. En el direccionamiento de alto rendimiento (HPR), conexión establecida entre los puntos finales de la ruta para transportar tráfico de sesión.

**conexión virtual**. En Frame Relay, vía de acceso de vuelta de una conexión potencial.

**configuración**. (1) Manera en que están organizados e interconectados el hardware y el software de un sistema de proceso de información. (T) (2) Dispositivos y programas que componen un sistema, un subsistema o una red.

**configuración del sistema**. Proceso que especifica los dispositivos y programas que componen un sistema de proceso de datos determinado.

**congestión**. Véase *congestión de la red*.

**congestión de la red**. Condición no deseada de carga excesiva causada por la presencia de más tráfico del que puede manejar una red.

**conmutación de la línea**. Sinónimo de *conmutación del circuito*.

**conmutación del circuito**. (1) Proceso que, a petición, conecta dos o más equipos terminales de datos (DTE) y permite el uso exclusivo de un circuito de datos entre ellos hasta que se libera la conexión. (I) (A) (2) Sinónimo con *conmutación de la línea*.

**conmutación del enlace de datos (DLSw)**. Método para transportar protocolos de red que utilizan el tipo 2 de control de enlace lógico (LLC) de IEEE 802.2. SNA y NetBIOS son ejemplos de protocolos que utilizan el tipo 2 de LLC. Véase también *encapsulación* y *simulación*.

**conmutación de paquetes**. (1) Proceso consistente en direccionar y transferir datos por medio de paquetes dirigidos de manera que un canal esté ocupado durante la transmisión de un paquete solamente. Cuando se completa la transmisión, el canal queda disponible para la transferencia de otros paquetes. (I) (2) Sinónimo

con *funcionamiento en modalidad de paquete*. Véase también *conmutación del circuito*.

**contigua activa de donde proceden los datos (NAUN)**. En la Red en Anillo de IBM, estación que envía datos directamente a una estación determinada del anillo.

**control de enlace de datos de alto nivel (HDLC)**. En la comunicación de datos, utilización de una serie de bits especificada para controlar enlaces de datos de acuerdo con las normas internacionales respecto al HDLC: la estructura de trama de ISO 3309 y los elementos de procedimientos de ISO 4335.

**control de enlace de datos (DLC)**. Conjunto de normas utilizado por los nodos de un enlace de datos (como, por ejemplo, un enlace de SDLC o una Red en Anillo) para efectuar un intercambio de información ordenado.

**control de enlace lógico (LLC)**. Subcapa de LAN de control de enlace de datos (DLC) que proporciona dos tipos de operaciones de DLC para el intercambio ordenado de información. El primer tipo es el servicio sin conexiones, que permite enviar y recibir información sin establecer un enlace. La subcapa de LLC no efectúa recuperación de errores ni control del flujo para el servicio sin conexiones. El segundo tipo es el servicio orientado a las conexiones, que requiere el establecimiento de un enlace antes del intercambio de información. El servicio orientado a las conexiones proporciona transferencia de información en secuencia, control del flujo y recuperación de errores.

**control del acceso al medio (MAC)**. En las LAN, subcapa de la capa de control de enlace de datos que da soporte a funciones dependientes del medio y utiliza los servicios de la capa física para proporcionar servicios a la subcapa de control de enlace lógico (LLC). La subcapa del MAC incluye el método para determinar cuándo un dispositivo tiene acceso al medio de transmisión.

**control de la vía de acceso (PC)**. Función que direcciona unidades de mensajes entre las unidades de red accesibles de la red y proporciona las vías de acceso entre éstas. Convierte las unidades básicas de información (BIU) del control de transmisión (posiblemente segmentándolas) en unidades de información de vía de acceso (PIU) e intercambia unidades básicas de transmisión que contienen una o más PIU con el control de enlace de datos. El control de la vía de acceso difiere según el tipo de nodo: algunos nodos (los nodos APPN, por ejemplo) utilizan identificadores de sesión generados localmente para el direccionamiento y otros (los nodos de subárea) utilizan direcciones de red para el direccionamiento.

**control del flujo**. (1) En SNA, proceso consistente en gestionar la velocidad a la que pasa el tráfico de datos entre los componentes de la red. La finalidad del control del flujo es optimizar la velocidad del flujo de unidades de mensajes con la congestión mínima de la red; es decir, ni desbordar los almacenamientos intermedios del receptor o de nodos de direccionamiento intermedio ni dejar al receptor esperando más unidades de mensajes. (2) Véase también *ritmo*.

**Control síncrono de enlace de datos (SDLC)**. (1) Disciplina que se ajusta a los subconjuntos de los Advanced Data Communication Control Procedures (ADCCP) del American National Standards Institute (ANSI) y del High-level Data Link Control (HDLC) de la organización internacional para la normalización, y está destinada a la gestión de la transferencia síncrona de información serie por bit de código transparente sobre una conexión de enlace. Los intercambios de transmisiones pueden ser dúplex o semi-dúplex sobre enlaces conmutados o no conmutados. La configuración de la conexión de enlace puede ser de punto a punto, de multipunto o de bucle. (I) (2) Compárese con *comunicación síncrona en binario (BSC)*.

**correlación**. Proceso consistente en convertir datos que el emisor transmite con un formato determinado en el formato de datos que puede aceptar el receptor.

**corriente de datos general (GDS)**. Corriente de datos utilizada para las conversaciones en sesiones de LU 6.2.

**coste de la vía de acceso**. En los protocolos de direccionamiento de estado de los enlaces, suma de los costes de enlace a lo largo de la vía de acceso entre dos nodos o redes.

**cronometraje**. (1) En la comunicación síncrona en binario, utilización de pulsaciones de reloj para controlar la sincronización de los datos y caracteres de control. (2) Método para controlar el número de bits de datos enviados en una línea de telecomunicaciones en un momento determinado.

**cuenta de saltos**. (1) Métrica o medida de distancia entre dos puntos. (2) En comunicaciones de Internet, número de direccionadores por los que pasa un datagrama cuando se dirige a su destino. (3) En SNA, medida consistente en el número de enlaces por los que se debe pasar en la vía de acceso a un destino.

# D

**daemon**. Programa que se ejecuta desatendido para realizar un servicio estándar. Algunos daemon se desencadenan de manera automática para realizar su tarea; otros realizan las operaciones periódicamente.

**datagrama**. (1) En la conmutación de paquetes,

paquete individual e independiente de otros paquetes que contiene información suficiente para el direccionamiento desde el equipo terminal de datos (DTE) de origen al DTE de destino sin apoyarse en intercambios anteriores entre los DTE y la red. (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.

**Datagram Delivery Protocol (DDP)**. En redes AppleTalk, protocolo que proporciona conectividad de red por medio de un servicio de entrega de socket a socket sin conexiones de la capa de internet.

**DCE preparado**. En la norma EIA 232, señal que indica al equipo terminal de datos (DTE) que el equipo de terminación de circuito de datos (DCE) local está conectado al canal de comunicaciones y se encuentra preparado para enviar datos. Sinónimo con *aparato de datos preparado (DSR)*.

**DECnet**. Arquitectura de red que define el funcionamiento de una familia de módulos de software, bases de datos y componentes de hardware que se utilizan normalmente con el fin de conectar entre sí sistemas Digital Equipment Corporation para el compartimiento de recursos, cálculo distribuido o configuración de sistemas remotos. Las implementaciones de la red DECnet siguen el modelo Digital Network Architecture (DNA).

**detección de colisión**. En el acceso múltiple con detección de portadora y detección de colisión (CSMA/CD), señal que indica que dos o más estaciones están transmitiendo simultáneamente.

**detección (de condición de excepción)**. En Simple Network Management Protocol (SNMP), mensaje enviado por un nodo gestionado (la función de agente) a una estación de gestión para informarle de una condición de excepción.

**detección de portadora**. En una red de área local, actividad continua de una estación de datos para detectar si otra estación está transmitiendo. (T)

**detector de portadora**. Sinónimo de *detector de señal de línea recibida (RLSD)*.

**detector de portadora de datos (DCD)**. Sinónimo de *detector de señal de línea recibida (RLSD)*.

**detector de señal de línea recibida (RLSD)**. En la norma EIA 232, señal que indica al equipo terminal de datos (DTE) que está recibiendo una señal del equipo de terminación de circuito de datos (DCE) remoto. Sinónimo con *detector de portadora* y *detector de portadora de datos (DCD)*.

**determinación de problemas**. Proceso consistente en determinar el origen de un problema; por ejemplo, un componente de un programa, una anomalía en una máquina, recursos de telecomunicaciones, programas o equipos instalados por el contratista o por el usuario, una anomalía del entorno, como, por ejemplo, pérdida de alimentación, o un error del usuario.

**difusión**. (1) Transmisión de los mismos datos a todos los destinos. (T) (2) Transmisión simultánea de datos a más de un destino. (3) Compárese con *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*.

**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 del MAC arbitrario (AMA)**. En la arquitectura DECnet, esquema de direccionamiento utilizado por DECnet Phase IV-Prime que da soporte a direcciones administradas universalmente y direcciones administradas localmente.

**direccionamiento de origen**. En las LAN, método mediante el cual la estación emisora determina la ruta que la trama seguirá e incluye la información de direccionamiento en la trama. A continuación, los puentes leen la información de direccionamiento para determinar si deben reenviar la trama.

**direccionamiento de sesiones intermedias (ISR)**. Tipo de función de direccionamiento de un nodo de red APPN que proporciona información de indisponibilidad y control del flujo de nivel de sesión para todas las sesiones que pasan por el nodo pero cuyos puntos finales están en otra parte.

**direccionamiento dinámico**. Direccionar utilizando rutas aprendidas en lugar de las rutas configuradas estáticamente durante la inicialización.

**direccionamiento intraárea**. En comunicaciones de Internet, direccionamiento de datos dentro de un área.

**dirección canónica**. En las LAN, formato de IEEE 802.1 de la transmisión de direcciones del control del acceso al medio (MAC) para adaptadores de Red en Anillo y Ethernet. En el formato canónico, el bit menos significativo (situado más a la derecha) de cada byte de dirección se transmite en primer lugar. Compárese con *dirección no canónica*.

**dirección de difusión**. En comunicaciones, dirección de estación (ocho números 1) reservada como dirección común a todas las estaciones de un enlace. Sinónimo con *dirección de todas las estaciones*.

**dirección de red**. Según ISO 7498-3, nombre que no es ambiguo en el entorno de OSI y que identifica a un conjunto de puntos de acceso a servicios de red.

**dirección de subred**. En comunicaciones de Internet, extensión del esquema básico de direccionamiento de IP donde una parte de la dirección de sistema principal se interpreta como dirección de red local.

**dirección de todas las estaciones**. En comunicaciones, sinónimo de *dirección de difusión*.

**dirección de usuario de red (NUA)**. En comunicaciones de X.25, dirección X.121 que contiene hasta 15 dígitos en código binario.

**dirección Internet**. Véase *dirección IP*.

**dirección IP**. Dirección de 32 bits definida por Internet Protocol, norma 5, Request for Comments (RFC) 791. Normalmente, se representa mediante formato decimal con puntos.

**dirección no canónica**. En las LAN, formato de la transmisión de direcciones del control del acceso al medio (MAC) para adaptadores de Red en Anillo. En el formato no canónico, el bit más significativo (situado más a la izquierda) de cada byte de dirección se transmite en primer lugar. Compárese con *dirección canónica*.

**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.

**formato decimal con puntos**. Representación sintáctica de un entero de 32 bits que consta de cuatro números de 8 bits escritos en base 10 con puntos que los separan. Se utiliza para representar direcciones IP.

**fragmentación**. (1) Proceso consistente en dividir un datagrama en partes más pequeñas, o fragmentos, para que se ajuste a las posibilidades del medio físico por el que se va a transmitir. (2) Véase también *segmentación*.

**fragmento**. Véase *fragmentación*.

**Frame Relay**. (1) Norma de interfaz que describe el límite entre el equipo de un usuario y una red de paquetes rápidos. En los sistemas Frame-Relay, se eliminan las tramas defectuosas; la recuperación se

produce de extremo a extremo en lugar de efectuarse salto a salto. (2) Técnica derivada de la norma de canal D de red digital de servicios integrados (RDSI). Supone que las conexiones son fiables y prescinde de la actividad general de control y detección de errores en la red.

**funcionamiento en modalidad de paquete**. Sinónimo de *conmutación de paquetes*.

**función de puente**. En las LAN, el reenvío de una trama de un segmento de LAN a otro. El destino está especificado mediante la dirección de subcapa del control del acceso al medio (MAC) codificada en el campo de dirección de destino de la cabecera de la trama.

**función de puente de ruta de origen**. En las LAN, método de función de puente que utiliza el campo de información de direccionamiento de la cabecera del control del acceso al medio (MAC) de IEEE 802.5 de una trama para determinar los anillos o segmentos de Red en Anillo que debe recorrer la trama. El nodo de origen inserta el campo de información de direccionamiento en la cabecera del MAC. La información del campo de información de direccionamiento deriva de los paquetes exploradores generados por el sistema principal de origen.

**función de puente local**. Función de un programa de puente que permite que un solo puente conecte diversos segmentos de LAN sin la utilización de un enlace de telecomunicaciones. Compárese con *función de puente remota*.

**función de puente remota**. Función de un puente que permite que dos puentes conecten diversas LAN utilizando un enlace de telecomunicaciones. Compárese con *función de puente local*.

**función de puente transparente**. En las LAN, método para relacionar redes de área local individuales entre sí en el nivel del control del acceso al medio (MAC). Un puente transparente almacena las tablas que contienen direcciones del MAC para que las tramas que ve el puente puedan reenviarse a otra LAN si las tablas lo indican así.

**función de túnel**. Trata a una red de transporte como si fuera una sola LAN o un solo enlace de comunicaciones. Véase también *encapsulación*.

# G

**gestión de red**. Proceso consistente en planificar, organizar y controlar un proceso de datos o sistema de información orientado a las comunicaciones.

**gestor de red**. Programa o grupo de programas que se utiliza para supervisar y gestionar una red así como para diagnosticar los problemas de la misma.

**grupo de transmisión (TG)**. (1) Conexión entre nodos adyacentes que se identifica mediante un número de grupo de transmisión. (2) En una red de subárea, enlace o grupo de enlaces entre nodos adyacentes. Cuando un grupo de transmisión está compuesto por un grupo de enlaces, los enlaces se ven como un solo enlace lógico y el grupo de transmisión se denomina *grupo de transmisión multienlace (MLTG)*. Un *grupo de transmisión multienlace de mezcla de medios (MMMLTG)* contiene enlaces de diferentes tipos de medios (por ejemplo, Red en Anillo, SDLC conmutado, SDLC no conmutado y enlaces Frame-Relay). (3) En una red APPN, enlace entre nodos adyacentes. (4) Véase también *grupos de transmisión paralelo*.

**grupos de transmisión paralelo**. Diversos grupos de transmisión entre nodos adyacentes, teniendo cada grupo un número de grupo de transmisión distinto.

# H

**Hello**. Protocolo utilizado por un grupo de direccionadores que cooperan y se apoyan entre sí para poder descubrir rutas de retardo mínimo.

**heurístico**. Perteneciente a métodos exploratorios para la resolución de problemas en los que se descubren soluciones mediante una evaluación del progreso realizada respecto al resultado final.

**histéresis**. Cantidad que indica cuánto debe cambiar la temperatura una vez pasado el umbral del establecimiento de alerta y antes de que se elimine la condición de alerta.

**horizonte dividido**. Técnica destinada a minimizar el tiempo para conseguir la convergencia en la red. Un direccionador registra la interfaz sobre la que ha recibido una ruta en particular y no propaga su información sobre la ruta otra vez sobre la misma interfaz.

# I

**identificación de intercambio (XID)**. Tipo específico de unidad básica de enlace que se utiliza para la comunicación de características de nodo y enlace entre nodos adyacentes. Los XID se intercambian entre estaciones de enlace antes de la activación del enlace

y durante la misma para establecer y negociar las características de enlace y nodo, y después de la activación del enlace para comunicar los cambios de estas características.

**identificador de conexión de enlace de datos (DLCI)**. Identificador numérico de un subpuerto Frame-Relay o segmento de PVC en una red Frame-Relay. Cada subpuerto de un puerto Frame-Relay individual tiene un DLCI exclusivo. La tabla siguiente, extraída de la norma T1.618 del American National Standards Institute (ANSI) y la norma Q.922 de la Comisión Consultiva de la telefonía y telegrafía internacionales (ITU-T/CCITT), indica las funciones asociadas con determinados valores de DLCI:

| Valores de DLCI | Función |
|---|---|
| 0 | Señalización de canal de entrada |
| 1–15 | Se reserva |
| 16–991 | Se asigna utilizando procedimientos de conexión de Frame-Relay |
| 992–1007 | Gestión de capa 2 de servicio portador de Frame-Relay |
| 1008–1022 | Se reserva |
| 1023 | Gestión de capa de canal de entrada |

**identificador de puente**. Campo de 8 bytes que se utiliza en un protocolo de árbol de expansión y está compuesto por la dirección MAC del puerto con el identificador de puerto más bajo y un valor definido por el usuario.

**identificador de red**. (1) En TCP/IP, parte de la dirección IP que define a una red. La longitud del identificador de red depende del tipo de la clase de red (A, B o C). (2) Nombre de 1 a 8 bytes seleccionado por el cliente o nombre de 8 bytes registrado por IBM que identifica de manera exclusiva a una subred específica.

**inhabilitado**. (1) Perteneciente a un estado de una unidad de proceso que evita la aparición de determinados tipos de interrupciones. (2) Perteneciente al estado en el cual una unidad de control de transmisión o unidad de respuestas audibles no puede aceptar llamadas de entrada de una línea.

**inhabilitar**. Convertir en no funcional.

**Integrated Digital Network Exchange (IDNX)**. Procesador que integra aplicaciones a base de voz, datos e imágenes. También gestiona los recursos de transmisión y se conecta a multiplexores y sistemas de soporte de gestión de redes. Permite la integración de equipos de diferentes proveedores.

**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 a partir del nombre (serie de caracteres) de una entidad (recurso) AppleTalk en una dirección IP AppleTalk (número de 16 bits) en la capa de transporte.

**NetBIOS**. Network Basic Input/Output System. Interfaz estándar para redes, IBM PC (Personal Computer) y PC compatibles que se utiliza en las LAN para proporcionar funciones de mensajes, de servidor de impresión y de servidor de archivos. Los programas de aplicación que utilizan NetBIOS no necesitan manejar los detalles de protocolos de control de enlace de datos (DLC) de la LAN.

**nivel de enlace**. (1) Parte de la recomendación X.25 que define el protocolo de enlace utilizado para entrar datos en la red y sacarlos de la misma a través del enlace dúplex que conecta la máquina del abonado con el nodo de red. LAP y LAPB son los protocolos de acceso de enlace recomendados por la CCITT. (2) Véase *nivel de enlace de datos*.

**nivel de enlace de datos**. (1) En la estructura jerárquica de una estación de datos, nivel conceptual de control o lógica de proceso entre la lógica de alto nivel y el enlace de datos que mantiene el control del enlace de datos. El nivel de enlace de datos realiza funciones tales como la inserción de bits de transmisión y supresión de bits de recepción; interpretación de campos de dirección y control; generación, transmisión e interpretación de mandatos y respuestas; y cálculo e interpretación de secuencias de comprobación de trama. Véase también *nivel de paquete* y *nivel físico*. (2) En comunicaciones de X.25, sinónimo de *nivel de trama*.

**nivel de trama**. Sinónimo con *nivel de enlace de datos*. Véase *nivel de enlace*.

**nodo**. (1) En una red, punto donde una o más unidades funcionales conectan canales o circuitos de datos. (I) (2) Cualquier dispositivo conectado a una red que transmite y recibe datos.

**nodo Advanced Peer-to-Peer Networking (APPN)**. Nodo de red APPN o nodo final APPN.

**nodo de destino**. Nodo al que se envían datos o una petición.

**nodo de esfera de control (SOC)**. Nodo que está incluido directamente en la esfera de control de un punto focal. Un nodo de SOC ha intercambiado elementos de habilitación de los servicios de gestión con

su punto focal. Un nodo final APPN puede ser un nodo de SOC si da soporte a la función de intercambio de elementos de habilitación de los servicios de gestión.

**nodo de red Advanced Peer-to-Peer Networking (APPN)**. Nodo que ofrece un amplio rango de servicios de usuario final y que puede proporcionar lo siguiente:

- servicios de directorios distribuidos, incluido el registro de los recursos del dominio con un servidor de directorios central
- Intercambios de bases de datos de topología con otros nodos de red APPN, lo que permite que los nodos de red de la red seleccionen las rutas óptimas para sesiones de LU-LU basándose en las clases de servicio solicitadas
- Servicios de sesiones para los nodos finales clientes y las LU locales
- Servicios de direccionamiento intermedio de una red APPN

**nodo de red APPN**. Véase *nodo de red Advanced Peer-to-Peer Networking (APPN)*.

**nodo de red de entrada baja (LEN)**. Nodo que proporciona un rango de servicios de usuario final, se conecta directamente con otros nodos utilizando protocolos de igual a igual y hace derivar servicios de red de un nodo de red APPN adyacente implícitamente, es decir, sin el uso directo de sesiones de CP-CP.

**nodo de red (NN)**. Véase *nodo de red Advanced Peer-to-Peer Networking (APPN)*.

**nodo final Advanced Peer-to-Peer Networking (APPN)**. Nodo que proporciona un amplio rango de servicios de usuario final y da soporte a las sesiones entre su punto de control (CP) local y el CP de un nodo de red adyacente. Utiliza estas sesiones con el fin de registrar dinámicamente sus recursos con el CP adyacente (su servidor de nodos de red) para enviar y recibir peticiones de búsqueda en directorios y obtener servicios de gestión. Un nodo final APPN también puede conectarse a una red de subárea como nodo periférico o a otros nodos finales.

**nodo final de red de entrada baja (LEN)**. Nodo LEN que recibe servicios de red de un nodo de red APPN adyacente.

**nodo final (EN)**. (1) Véase *nodo final Advanced Peer-to-Peer Networking (APPN)* y *nodo final de red de entrada baja (LEN)*. (2) En comunicaciones, nodo que se conecta frecuentemente a un solo enlace de datos y no puede realizar funciones de direccionamiento intermedio.

**nodo intermedio**. Nodo que está al final de más de una rama. (T)

**nodos adyacentes**. Dos nodos conectados conjuntamente por una vía de acceso, como mínimo, que no conecta ningún otro nodo. (T)

**nombre de comunidad**. En el protocolo Simple Network Management Protocol (SNMP), serie de octetos que identifica a una comunidad.

**nombre de dominio**. En el conjunto de protocolos de Internet, nombre de un sistema principal. Un nombre de dominio está compuesto por una secuencia de subnombres separados por un carácter delimitador. Por ejemplo, si el nombre de dominio calificado al completo (FQDN) de un sistema principal es `ralvm7.vnet.ibm.com`, cada uno de los siguientes es un nombre de dominio:

- `ralvm7.vnet.ibm.com`
- `vnet.ibm.com`
- `ibm.com`

**notación de sintaxis de abstracción 1 (ASN.1)**. Método de Interconexión de Sistemas Abiertos (OSI) para la sintaxis de abstracción que se especifica en las normas siguientes:

- ITU-T recomendación X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T recomendación X.680 (1994) | ISO/IEC 8824-1: 1994

Véase también *normas básicas de codificación (BER)*.

**número de puerto**. En comunicaciones de Internet, identificación de una entidad de aplicación para el servicio de transporte.

**número de secuencia**. En comunicaciones, número asignado a una trama o paquete en particular para controlar el flujo de la transmisión y la recepción de datos.

**número de sistema autónomo**. En TCP/IP, número asignado a un sistema autónomo por la misma autorización central que también asigna direcciones IP. El número de sistema autónomo hace posible que los algoritmos de direccionamiento automatizado distingan los sistemas autónomos.

# O

**objeto de la MIB**. Sinónimo de *variable de la MIB*.

**Open Shortest Path First (OSPF)**. En el conjunto de protocolos de Internet, función que proporciona transferencia de información intradominio. Como alternativa al protocolo Routing Information Protocol (RIP), OSPF permite el direccionamiento de menor coste y lo maneja en grandes redes regionales o corporativas.

**organización internacional para la normalización (ISO)**. Organización de corporaciones nacionales de normas de varios países establecida para promocionar el desarrollo de normas con el fin de facilitar el intercambio internacional de artículos y servicios además de desarrollar la cooperación en la actividad intelectual, científica, tecnológica y económica.

**origen**. Unidad lógica (LU) externa o programa de aplicación de donde parten un mensaje u otros datos. Véase también *destino*.

# P

**paquete**. En la comunicación de datos, secuencia de dígitos binarios, con inclusión de señales de control y datos, que se transmite y se conmuta como un todo compuesto. Los datos, las señales de control y, posiblemente, la información de control de errores se ordenan siguiendo un formato específico. (I)

**paquete de datos**. En comunicaciones de X.25, paquete utilizado para la transmisión de datos de usuario dentro de un circuito virtual en la interfaz DTE/DCE.

**paquete de petición de llamada**. (1) Paquete de supervisión de llamada que un equipo terminal de datos (DTE) transmite con el fin de solicitar que se establezca una conexión para una llamada en la red. (2) En comunicaciones de X.25, paquete de supervisión de llamada transmitido por un DTE para solicitar el establecimiento de una llamada en la red.

**paquete de petición de restablecimiento**. En comunicaciones X.25, paquete transmitido por el equipo terminal de datos (DTE) al equipo de terminación de circuito de datos (DCE) para solicitar que se restablezca una llamada virtual o un circuito virtual permanente. En el paquete también puede especificarse la razón de la petición.

**paquete de recepción no preparada (RNR)**. Véase *paquete de RNR*.

**paquete de RNR**. Paquete utilizado por un equipo terminal de datos (DTE) o por un equipo de terminación de circuito de datos (DCE) con el fin de indicar una incapacidad temporal para aceptar paquetes adicionales de petición de llamada virtual o circuito virtual permanente.

**paquete explorador**. En las LAN, paquete que está generado por el sistema principal de origen y que atraviesa toda la parte de direccionamiento de origen de una LAN con el fin de recoger información sobre las posibles vías de acceso que se encuentran disponibles para el sistema principal.

**parámetro de configuración**. Variable de una definición de configuración cuyos valores pueden caracterizar la relación de un producto con otros productos de la misma red o pueden definir características del producto en sí.

**par de valores de atributo (AVP)**. Método uniforme de codificación de tipos y cuerpos de mensajes. Este método maximiza la extensibilidad mientras permite la interoperatividad de L2TP.

**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 que pueden utilizar diferentes protocolos de control del acceso al medio. Un puente reenvía una trama a otro puente basándose en la dirección del control del acceso al medio (MAC).

**puente de ruta**. Función de un programa de puente de IBM que permite que dos sistemas de puente utilicen un enlace de telecomunicaciones para conectar dos LAN. Cada sistema de puente se conecta directamente a una de las LAN y el enlace de telecomunicaciones conecta los dos sistemas de puente.

**puente raíz**. Puente que es la raíz de un árbol de expansión formado entre otros puentes activos de la red de funciones de puente. El puente raíz origina y transmite unidades de datos de protocolo de puente (BPDU) a otros puentes activos para mantener la topología de árbol de expansión. Es el puente con la prioridad superior de la red.

**puentes paralelo**. Par de puentes conectados al mismo segmento de LAN que crean vías de acceso redundantes para el segmento.

**puerto**. (1) Punto de acceso para la entrada o salida de datos. (2) Conector de un dispositivo al que se conectan cables para otros dispositivos, como, por ejemplo, estaciones de pantalla o impresoras. (3) Representación de una conexión física con el hardware de enlace. A veces, un puerto viene referido como adaptador; no obstante, en un adaptador puede haber más de un puerto. Un solo proceso de DLC puede controlar uno o más puertos. (4) En el conjunto de protocolos de Internet, número de 16 bits utilizado para la comunicación entre TCP o el protocolo User Datagram Protocol (UDP) y una aplicación o protocolo de nivel superior. Algunos protocolos, como, por ejemplo, File Transfer Protocol (FTP) y Simple Mail Transfer Protocol (SMTP), utilizan el mismo número de puerto conocido en todas las implementaciones de TCP/IP. (5) Abstracción utilizada por protocolos de transporte para establecer diferencias entre los diversos destinos en una máquina de sistema principal. (6) Sinónimo con *socket*.

**puerto de destino**. Adaptador asíncrono de 8 puertos que sirve de punto de conexión con un servicio serie.

**punto de acceso a servicios de destino (DSAP)**. En SNA y TCP/IP, dirección lógica que permite que un sistema 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 acceso a servicios (SAP)**. (1) En la arquitectura interconexión de sistemas abiertos (OSI), punto en el que una entidad de una capa proporciona los servicios de esta capa a una entidad de la capa superior más próxima. (T) (2) Punto lógico que queda disponible mediante un adaptador y donde puede recibirse y transmitirse información. Muchos enlaces pueden terminar en un solo punto de acceso a servicios.

**punto de control (CP)**. (1) Componente de un nodo APPN o LEN que gestiona los recursos de dicho nodo. En un nodo APPN, el CP puede dedicarse a establecer sesiones de CP-CP con otros nodos APPN. En un nodo de red APPN, el CP también proporciona servicios a nodos finales adyacentes de la red APPN. (2) Componente de un nodo que gestiona los recursos de dicho nodo y, opcionalmente, proporciona servicios a otros nodos de la red. Pueden citarse como ejemplos el punto de control de servicios del sistema (SSCP) de un nodo de subárea de tipo 5, el punto de control de nodo de red (NNCP) de un nodo de red APPN y el punto de control de nodo final (ENCP) de un nodo final APPN o LEN. Un SSCP y un NNCP pueden proporcionar servicios a otros nodos.

**punto de control de servicios del sistema (SSCP)**. Componente de una red de subárea destinado a gestionar la configuración, coordinar las peticiones del operador de red y las de determinación de problemas y proporcionar servicios de directorios además de otros servicios de sesiones para los usuarios de la red. Diversos SSCP, cooperando como iguales entre sí, pueden dividir la red en dominios de control y tener, cada uno de los SSCP, una relación de control jerárquica con las unidades físicas y las unidades lógicas de su propio dominio.

**punto de entrada (EP)**. En SNA, nodo de tipo 2.0, tipo 2.1, tipo 4 ó tipo 5 que proporciona soporte de gestión de redes distribuidas. Envía datos de gestión de redes sobre sí mismo y los recursos que controla a un punto focal para el proceso centralizado, y recibe y ejecuta los mandatos iniciados por el punto focal para gestionar y controlar sus recursos.

# R

**rastreo**. (1) Registro de la ejecución de un programa de sistema. Muestra las secuencias en que se han ejecutado las instrucciones. (A) (2) Para los enlaces de datos, registro de las tramas y bytes transmitidos o recibidos.

**recepción no preparada (RNR)**. En comunicaciones, mandato o respuesta de enlace de datos que indica una condición temporal de incapacidad para aceptar tramas de entrada.

**reconfiguración dinámica (DR)**. Proceso consistente en cambiar la configuración de una red (las PU y LU periféricas) sin regenerar las tablas de configuración al completo ni desactivar el nodo principal afectado.

**red**. (1) Configuración de software y dispositivos de proceso de datos conectados para el intercambio de información. (2) Grupo de nodos y los enlaces que los interconectan.

**red Advanced Peer-to-Peer Networking (APPN)**. Conjunto de nodos de red interconectados y sus nodos finales clientes.

**red APPN**. Véase *red Advanced Peer-to-Peer Networking (APPN)*.

**red de área amplia (WAN)**. (1) Red que proporciona servicios de comunicación a un área geográfica mayor que la servida por una red de área local o una red de área metropolitana, y que puede utilizar o proporcionar recursos públicos de comunicación. (T) (2) Red de comunicación de datos diseñada para servir a un área de cientos o miles de kilómetros; por ejemplo, las redes públicas y privadas de conmutación de paquetes y las redes telefónicas nacionales. (3) Compárese con *red de área local (LAN)* y *red de área metropolitana (MAN)*.

**red de área local (LAN)**. (1) Red de sistema ubicada en el lugar de un usuario dentro de un área geográfica limitada. La comunicación dentro de una red de área local no está sujeta a reglamentos externos; no obstante, la comunicación más allá del límite de una LAN puede estar sujeta a alguna forma de reglamento. (T) (2) Red en la que un conjunto de dispositivos están conectados entre sí para la comunicación y que puede conectarse a una red mayor. (3) Véase también *Ethernet* y *Red en Anillo*. (4) Compárese con *red de área metropolitana (MAN)* y *red de área amplia (WAN)*.

**red de área metropolitana (MAN)**. Red formada por la interconexión de dos o más redes que puede 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 identificador de sistema principal ocupa los tres octetos situados más a la derecha.

**red de clase B**. En comunicaciones de Internet, red en la que los dos bits situados más a la izquierda (más significativo y próximo al más significativo) de la dirección IP están establecidos en 1 y 0, respectivamente, y el identificador de sistema principal ocupa los dos octetos situados más a la derecha.

**red de entrada baja (LEN)**. Posibilidad de los nodos de conectarse directamente entre sí utilizando protocolos básicos de igual a igual para dar soporte a sesiones múltiples y en paralelo entre unidades lógicas.

**red de tipo anillo**. (1) Red en la que cada nodo tiene exactamente dos ramas conectadas y en la que hay exactamente dos vías de acceso entre dos nodos cualesquiera. (T) (2) Configuración de red en la que los dispositivos están conectados mediante enlaces de transmisión unidireccional para formar una vía de acceso cerrada.

**red digital de servicios integrados (RDSI)**. Red digital de telecomunicaciones de extremo a extremo que da soporte a diversos servicios, los cuales incluyen voz y datos pero no se limitan a ello.

**Nota:** Las RDSI se utilizan en arquitecturas de red públicas y privadas.

**Red en Anillo**. (1) Según la norma IEEE 802.5, tecnología de red que controla el acceso al medio pasando una señal (paquete o trama especial) entre las estaciones conectadas al medio. (2) IEEE 802.5 con una topología de anillo que pasa señales de una estación de anillo de conexión (nodo) a otra. (3) Véase también *red de área local (LAN)*.

**red según Red en Anillo**. (1) Red de tipo anillo que permite la transmisión de datos unidireccional entre estaciones de datos, mediante un procedimiento consistente en pasar señales, de tal manera que los datos transmitidos vuelven a la estación transmisora. (T) (2) Red que utiliza una topología de anillo, según la cual pasan señales en un circuito de nodo a nodo. Un nodo que está preparado para emitir puede capturar la señal e insertar datos para la transmisión.

**red troncal**. Red central a la que se conectan redes más pequeñas, casi siempre de menor velocidad. 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 (NAU) que puede activarse, adaptarse, para proporcionar varios protocolos y desactivarse de la manera solicitada. Cada sesión está identificada de manera exclusiva en la cabecera de transmisión (TH) que acompaña a cualquier transmisión intercambiada durante la sesión. (3) En L2TP, L2TP crea una sesión cuando se intenta una conexión PPP de extremo a extremo entre un usuario de marcación y los LNS; sin tener en cuenta si el usuario inicia la sesión o si el LNS inicia una llamada hacia fuera. Los datagramas para la sesión se envían por el túnel entre el LAC y el LNS. Los LNS y LAC mantienen la información de estado para cada usuario conectado a un LAC.

**Simple Network Management Protocol (SNMP)**. En el conjunto de protocolos de Internet, protocolo de gestión de red que se utiliza para supervisar direccionadores y redes conectadas. SNMP es un protocolo de capa de aplicación. La información sobre los dispositivos gestionados está definida y almacenada en la base de la información de gestión (MIB) de la aplicación.

**simulación**. Para los enlaces de datos, técnica mediante la cual un protocolo iniciado en una estación final se reconoce con acuse de recibo y se procesa en un nodo intermedio en nombre del destino final. En la conmutación del enlace de datos del IBM 6611, por ejemplo, las tramas de SNA se encapsulan en paquetes de TCP/IP para el transporte a través de una red de área amplia diferente de SNA, se desempaquetan en otro IBM 6611 y pasan al destino final. Una ventaja de la simulación es que se evitan tiempos de espera excedidos de sesión de final a final.

**síncrono**. (1) Perteneciente a dos o más procesos que dependen de la aparición de sucesos específicos, como, por ejemplo, señales comunes de temporización. (T) (2) Que se produce con una relación temporal regular o previsible.

**sintaxis de abstracción**. Especificación de datos que incluye todas las distinciones necesarias en las transmisiones de datos, pero que omite (excluye) otros detalles, como, por ejemplo, los que dependen de las arquitecturas específicas de los sistemas. Véase también *notación de sintaxis de abstracción 1 (ASN.1)* y *normas básicas de codificación (BER)*.

**sistema**. En el proceso de datos, conjunto de personas, máquinas y métodos organizados para llevar a cabo un conjunto de funciones específicas. (I) (A)

**sistema autónomo**. En TCP/IP, grupo de redes y direccionadores bajo una sola autorización administrativa. Estas redes y estos direccionadores cooperan estrechamente para propagar la información de asequibilidad (y direccionamiento) de la red entre ellos utilizando un protocolo de pasarela interior de su elección.

**sistema de juego reducido de instrucciones (RISC)**. Sistema que utiliza un juego pequeño y simplificado de instrucciones de uso frecuente para la ejecución rápida.

**sistema de nombres de dominio (DNS)**. En el conjunto de protocolos de Internet, sistema de bases de datos distribuidas utilizado para correlacionar nombres de dominio con direcciones IP.

**sistema principal**. En el conjunto de protocolos de Internet, sistema final. El sistema final puede ser cualquier estación de trabajo; no es necesario que sea un sistema principal.

**socket**. (1) Punto final para la comunicación entre procesos o programas de aplicación. (2) Abstracción proporcionada por la Distribución de software de Berkeley de la Universidad de California (software que suele recibir el nombre de UNIX de Berkeley o UNIX de BSD) que funciona como punto final para la comunicación entre procesos o aplicaciones.

**sonda de paquetes Internet (PING)**. (1) En comunicaciones de Internet, programa utilizado en redes TCP/IP para probar la capacidad de alcanzar destinos enviando a los mismos una petición con eco de Internet Control Message Protocol (ICMP) y esperando una respuesta. (2) En comunicaciones, prueba de asequibilidad.

**sondeo**. (1) En una conexión multipunto o conexión punto a punto, proceso consistente en invitar a las estaciones de datos a transmitir, una por una. (I) (2) Interrogar a dispositivos con el fin de evitar contenciones, determinar el estado operativo o determinar la disposición para enviar o recibir datos. (A)

**soporte de diversos dominios (MDS)**. Técnica para transportar datos de servicios de gestión entre conjuntos de funciones de servicios de gestión sobre

sesiones de LU-LU y CP-CP. Véase también *unidad de mensaje de soporte de diversos dominios (MDS-MU)*.

**StreetTalk**. En VIrtual NEtworking System (VINES), sistema exclusivo de denominación y direccionamiento de red amplia que permite que los usuarios ubiquen cualquier recurso de la red y accedan al mismo sin conocer la topología de la red. Véase también *Internet Control Protocol (ICP)* y *RouTing update Protocol (RTP)*.

**subárea**. Parte de la red SNA compuesta por un nodo de subárea, nodos periféricos conectados y recursos asociados. En un nodo de subárea, todas las unidades de red accesibles (NAU), enlaces y estaciones de enlace adyacentes (de nodos de subárea o nodos periféricos conectados) que son dirigibles dentro de la subárea comparten una dirección de subárea común y tienen direcciones de elementos distintas.

**subcapa del control del acceso al medio (MAC)**. En una red de área local, parte de la capa de enlace de datos que aplica un método de acceso al medio. La subcapa del MAC da soporte a funciones dependientes de la topología y utiliza los servicios de la capa física para proporcionar servicios a la subcapa de control de enlace lógico. (T)

**Subnetwork Access Protocol (SNAP)**. En las LAN, protocolo encargado de establecer diferencias entre protocolos de 5 bytes que identifica la familia de protocolos estándares distintos de IEEE a la que pertenece un paquete. El valor de SNAP se utiliza para diferenciar los protocolos que utilizan `$AA` como valor de punto de acceso a servicios (SAP).

**subred**. (1) En TCP/IP, parte de una red que se identifica mediante una parte de la dirección IP. (2) Sinónimo de *subred (grupo de nodos)*.

**subred (grupo de nodos)**. (1) Cualquier grupo de nodos que tienen un conjunto de características comunes, como, por ejemplo, el mismo identificador de red. (2) Sinónimo con *subred*.

**subsistema**. Sistema secundario o subordinado que a menudo puede funcionar de manera independiente o asíncrona respecto a un sistema de control. (T)

**suma de comprobación**. (1) Suma de un grupo de datos que se asocia con el grupo y se utiliza con fines de comprobación. (T) (2) En la detección de errores, función de todos los bits de un bloque. Si las sumas grabadas y las calculadas no coinciden, se indica que hay un error. (3) En un disquete, datos grabados en un sector con fines de detección de errores; una suma de comprobación calculada que no coincide con la suma de comprobación de los datos grabados en el sector indica que hay un sector anómalo. Los datos son numéricos u otras series de caracteres consideradas numéricas con el fin de calcular la suma de comprobación.

**supervisor**. (1) Dispositivo que observa y registra actividades seleccionadas en un sistema de proceso de datos para el análisis. Sus usos posibles son para indicar cualquier desviación significativa de la norma o para determinar los niveles de utilización de unidades funcionales en particular. (T) (2) Software o hardware que observa, supervisa, controla o verifica operaciones de un sistema. (A) (3) Función necesaria para iniciar la transmisión de una señal del anillo y para proporcionar recuperación de errores de software en el caso de que se pierdan señales, tramas en circulación u otras dificultades. La posibilidad está presente en todas las estaciones de anillo.

**supervisor activo**. En una Red en Anillo, función realizada en cualquier momento por una estación de anillo que inicia la transmisión de señales y proporciona recursos de recuperación de errores de señales. Cualquier adaptador activo del anillo tiene la posibilidad de proporcionar la función de supervisor activo si falla el supervisor activo actual.

**SYNTAX**. En el protocolo Simple Network Management Protocol (SNMP), cláusula del módulo de la MIB que define la estructura de datos abstracta correspondiente a un objeto gestionado.

**Systems Network Architecture (SNA)**. Descripción de la estructura lógica, formatos, protocolos y secuencias operativas para la transmisión de unidades de información a través de las redes y para el control de la configuración y del funcionamiento de las mismas. La estructura de capas de SNA permite que los orígenes y destinos finales de la información, es decir, los usuarios, sean independientes de los servicios y recursos de red SNA específicos utilizados para el intercambio de información y que no se vean afectados por dichos servicios y recursos.

**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.

# T

**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/Internet Protocol (TCP/IP)**. Conjunto de protocolos de comunicaciones que dan soporte a funciones de conectividad de igual a igual para redes de área local y amplia.

**Transmission Control Protocol (TCP)**. Protocolo de comunicaciones utilizado en Internet y en cualquier red que siga las normas del Departamento de Defensa de los EE.UU. para el protocolo interredes. TCP proporciona un protocolo fiable de sistema principal a sistema principal entre sistemas principales en redes de comunicaciones de paquetes conmutados y en los sistemas interconectados de dichas redes. Utiliza Internet Protocol (IP) como protocolo subyacente.

**transporte de vector de gestión de red (NMVT)**. Unidad de petición/respuesta (RU) de servicios de gestión que fluye sobre una sesión activa entre servicios de gestión de unidad física y servicios de gestión de punto de control (sesión de SSCP-PU).

**troncal**. (1) En una configuración de anillo de diversos puentes de una red de área local, enlace de gran velocidad al que se conectan los anillos por medio de puentes o direccionadores. Un troncal puede configurarse como bus o como anillo. (2) En una red de área amplia, enlace de gran velocidad al que se conectan nodos o intercambios de conmutaciones de datos (DSE).

**túnel**. Un túnel está definido mediante un par LNS-LAC. El túnel lleva datagramas de PPP entre el LAC y el LNS. Un solo túnel puede multiplexar muchas sesiones. Una conexión de control que funciona sobre el mismo túnel controla el establecimiento, liberación y mantenimiento de todas las sesiones y del túnel en sí.

# U

**umbral**. (1) En programas de puente de IBM, valor asignado al número máximo de tramas que no se reenvían por un puente debido a errores antes de que se cuente una aparición de “umbral sobrepasado” y se indique en los programas de gestión de red. (2) Valor inicial a partir del cual un contador disminuye hasta 0 o valor hasta el que aumenta o disminuye un contador a partir de un valor inicial.

**unidad básica de transmisión (BTU)**. En SNA, unidad de datos e información de control que pasa entre los componentes del control de la vía de acceso. Una BTU puede constar de una o más unidades de información de vía de acceso (PIU).

**unidad de datos de protocolo de control de enlace lógico (LLC)**. Unidad de información intercambiada entre estaciones de enlace de diferentes nodos. La unidad de datos de protocolo de LLC contiene un punto de acceso a servicios de destino (DSAP), un punto de acceso a servicios de origen (SSAP), un campo de control y datos de usuario.

**unidad de datos de protocolo (PDU)**. Unidad de datos especificada en un protocolo de una capa determinada y compuesta por información de control de protocolo de esta capa además de, posiblemente, datos de usuario de esta capa. (T)

**unidad de información de vía de acceso (PIU)**. Unidad de mensaje compuesta por una sola cabecera de transmisión (TH) o por una TH seguida de una unidad básica de información (BIU) o un segmento de BIU.

**unidad de mensaje de soporte de diversos dominios (MDS-MU)**. Unidad de mensaje utilizada en el soporte de diversos dominios que contiene datos de servicios de gestión y fluye entre conjuntos de funciones de servicios de gestión sobre las sesiones de LU-LU y CP-CP. Esta unidad de mensaje, así como los datos reales de servicios de gestión que contiene, tiene el formato de corriente de datos general (GDS). Véase también *unidad de servicios de gestión de punto de control (CP-MSU)*, *unidad de servicios de gestión (MSU)* y *transporte de vector de gestión de red (NMVT)*.

**unidad de red accesible (NAU)**. Unidad lógica (LU), unidad física (PU), punto de control (CP) o punto de control de servicios del sistema (SSCP). Es el origen o el destino de la información transmitida por la red de control de la vía de acceso. Sinónimo con *unidad de red direccionable*.

**unidad de red direccionable (NAU)**. Sinónimo de *unidad de red accesible*.

**unidad de servicio de canal (CSU)**. Unidad que proporciona la interfaz a una red digital. La CSU proporciona funciones de acondicionamiento (o igualación) de línea, que mantienen la uniformidad del rendimiento de la señal a lo largo del ancho de banda de canal; remodelación de señal, que constituye la corriente de pulsaciones binarias; y prueba de bucle de retorno, que incluye la transmisión de señales de prueba entre la CSU y la unidad de canal de oficina de la portadora de red. Véase también *unidad de servicio de datos (DSU)*.

**unidad de servicio de datos (DSU)**. Dispositivo que proporciona una interfaz de servicio de datos digital al equipo terminal de datos de manera directa. La DSU proporciona igualación de bucle y posibilidades de pruebas locales y remotas, así como una interfaz EIA/CCITT estándar.

**unidad de servicios de gestión de punto de control (CP-MSU)**. Unidad de mensaje que contiene datos de servicios de gestión y fluye entre los conjuntos de funciones de servicios de gestión. Esta unidad de mensaje tiene el formato de corriente de datos general (GDS). Véase también *unidad de servicios de gestión (MSU)* y *transporte de vector de gestión de red (NMVT)*.

**unidad EIA**. Unidad de medida que ha establecido la Electronic Industries Association y es igual a 44,45 milímetros (1,75 pulgadas).

**unidad física (PU)**. (1) Componente que gestiona y supervisa los recursos (como, por ejemplo, enlaces conectados y estaciones de enlace adyacentes) asociados con un nodo tal como lo solicita un SSCP mediante una sesión de SSCP-PU. Un SSCP activa una sesión con la unidad física con el fin de gestionar indirectamente, a través de la PU, recursos del nodo, como, por ejemplo, enlaces conectados. Este término sólo se aplica a los nodos de tipo 2.0, tipo 4 y tipo 5. (2) Véase también *PU periférica* y *PU de subárea*.

**unidad lógica (LU)**. Tipo de unidad de red accesible que permite que los usuarios obtengan acceso a recursos de red y se comuniquen entre sí.

**unidad máxima de transmisión (MTU)**. En las LAN, la mayor unidad de datos posible que puede enviarse por un medio físico determinado en una sola trama. Por ejemplo, la MTU para Ethernet tiene 1500 bytes.

**unión de telecomunicaciones internacionales (ITU)**. Agencia de telecomunicaciones especializada de las Naciones Unidas que se ha establecido con el fin de proporcionar procedimientos y prácticas para la normalización de las comunicaciones, lo cual incluye asignación de frecuencia y regulaciones de la radio universales.

**User Datagram Protocol (UDP)**. En el conjunto de protocolos de Internet, protocolo que proporciona un servicio no fiable de datagramas sin conexiones. Permite que un programa de aplicación de una máquina o proceso envíe un datagrama a un programa de aplicación de otra máquina o proceso. UDP utiliza Internet Protocol (IP) para entregar datagramas.

**V.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.36**. En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito de datos (DCE) con las velocidades de 48, 56, 64 ó 72 kilobits por segundo.

**V.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.24**. En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito de datos (DCE).

# V

**valor por omisión**. Perteneciente a un atributo, condición, valor u opción que se supone cuando no se especifica nada de forma explícita. (I)

**variable de corriente de datos general (GDS)**. Tipo de subestructura de RU que va precedida de un identificador y un campo de longitud e incluye datos de aplicación, datos de control de usuario o datos de control definidos según SNA.

**variable de la MIB**. En el protocolo Simple Network Management Protocol (SNMP), instancia específica de datos definida en un módulo de la MIB. Sinónimo con *objeto de la MIB*.

**vector de control de selección de ruta (RSCV)**. Vector de control que describe una ruta de una red APPN. El RSCV consta de una secuencia ordenada de vectores de control que identifican los TG y nodos que componen la vía de acceso de un nodo de origen a un nodo de destino.

**velocidad de información comprometida**. Cantidad máxima de datos en bits que la red acepta entregar.

**velocidad de transferencia de datos**. Promedio de los bits, caracteres o bloques por unidad de tiempo que pasan entre los miembros del equipo correspondiente en un sistema de transmisión de datos. (I)

**Notas:**

1. La velocidad se expresa en bits, caracteres o bloques por segundo, minuto u hora.
2. Debe indicarse el equipo correspondiente; por ejemplo, módems, equipo intermedio u origen y destino.

**versión**. Programa bajo licencia independiente que a menudo tiene un nuevo código o una nueva función significativos.

**vertimiento múltiple**. (1) Transmisión de los mismos datos a un grupo seleccionado de destinos. (T) (2) Forma especial de difusión en que se entregan copias de un paquete a un subconjunto de todos los destinos posibles solamente.

**vía de acceso**. (1) En una red, cualquier ruta entre dos nodos cualesquiera. Una vía de acceso puede incluir más de una rama. (T) (2) Serie de componentes de red de transporte (control de la vía de acceso y control de enlace de datos) por los que pasa la información intercambiada entre dos unidades de red accesibles. Véase también *ruta explícita (ER)*, *extensión de ruta* y *ruta virtual (VR)*.

**VINES**. VIrtual NEtworking System.

**VIrtual NEtworking System (VINES)**. Sistema operativo de red y software de red de Banyan Systems, Inc. En una red VINES, la función de enlace virtual permite que todos los dispositivos y servicios aparenten estar conectados directamente entre sí cuando en realidad pueden encontrarse a miles de kilómetros de distancia. Véase también *StreetTalk*.

**vista de la MIB**. En el protocolo Simple Network Management Protocol (SNMP), conjunto de objetos gestionados, conocidos por el agente, que es visible en una comunidad en particular.

**vuelco**. (1) Datos que se han volcado. (T) (2) Copiar el contenido de la totalidad o de parte del almacenamiento virtual con el fin de reunir información de errores.

# W

**X.25**. (1) recomendación de la comisión consultiva de la telefonía y telegrafía internacionales (CCITT) relativa a la interfaz entre un equipo terminal de datos y las redes de datos de paquetes conmutados. (2) Véase también *conmutación de paquetes*.

# X

**X.21**. recomendación de la comisión consultiva de la telefonía y telegrafía internacionales (CCITT) relativa a una interfaz de fines generales entre un equipo terminal de datos y un equipo de terminación de circuito de datos para las operaciones síncronas en una red pública de datos.

**Xerox Network Systems (XNS)**. Conjunto de protocolos de internet desarrollados por Xerox Corporation. Aunque es similar a los protocolos TCP/IP, XNS utiliza unos formatos de paquete y una terminología diferentes. Véase también *Internetwork Packet Exchange (IPX)*.

# Z

**zona**. En redes AppleTalk, subconjunto de nodos dentro de una internet.

**Zone Information Protocol (ZIP)**. En redes AppleTalk, protocolo que proporciona un servicio de gestión de zonas manteniendo una correlación de los nombres de zonas y los números de red de la internet en la capa de sesión.

# Índice

## A

# B



# C

# CH



# D

# E

# F



# H



# I

# J



# L

# M

# N



# O



# P

# Q



# R



# S

# T

# U



# V



# W

# Hoja de Comentarios

**Nways Multiprotocol Routing Services**
**Consulta de configuración y supervisión**
**de protocolos, Volumen 1**
**Versión 3.3**

**Número de Publicación SC10-3426-00**

### 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**
SC10-3426-00

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

SC10-3426-00

Corte o Doble
Por la Línea

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

SC10-3426-00