Access Integration Services

Configuración y supervisión de protocolos
Manual de consulta, volumen 1
Versión 3.4

SC10-3438-01

Access Integration Services

Configuración y supervisión de protocolos
Manual de consulta, volumen 1
Versión 3.4

SC10-3438-01

Nota

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

Segunda edición (octubre de 1999)

Este manual es la traducción del original en inglés *Protocol Configuration and Monitoring Reference Volume 1 Version 3.4*, SC30-3990-02.

Esta edición es aplicable a la Versión 3 Release 4 de IBM Access Integration Services y a todos los releases y modificaciones subsiguientes hasta que se indique lo contrario en nuevas ediciones o boletines técnicos.

Efectúe el pedido de publicaciones a su representante de ventas IBM o a la sucursal de IBM de su localidad. En la dirección que figura más abajo no hay existencias de publicaciones.

IBM agradece sus comentarios. Al final de la publicación hay una hoja de comentarios del lector. Si ya se ha utilizado, puede enviar sus comentarios a la dirección siguiente:

IBM S. A.
National Language Solutions Center
Avda. Diagonal, 571
08029 Barcelona
España

Si lo prefiere, puede utilizar el sitio Web de soporte de IBM para remitirnos sus comentarios. Para ello, pulse en el enlace *Overall Site Feedback* del URL siguiente:

| **http://www.networking.ibm.com**

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

Contenido

Figuras

Avisos

Es posible que en otros países IBM no ofrezca los productos, los servicios o las características que se describen en este documento. Consulte con el representante local de IBM para obtener información acerca de los productos y servicios que actualmente están disponibles en su localidad. Las referencias a productos, programas o servicios IBM no pretenden afirmar ni dar a entender que únicamente puedan utilizarse dichos productos, programas o servicios IBM. Puede utilizarse en su lugar cualquier otro producto, programa o servicio funcionalmente equivalente que no vulnere ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio no IBM.

IBM puede tener patentes o solicitudes de patente en tramitación que cubran alguno de los temas tratados en este documento. La posesión de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar las consultas sobre licencias, por escrito, a la siguiente dirección:

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

Para realizar consultas relacionadas con los caracteres de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM de su país o bien envíelas por escrito a la siguiente dirección:

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

El párrafo siguiente no puede aplicarse en el Reino Unido ni en cualquier otro país en el que tales disposiciones sean incompatibles con la legislación local: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN “TAL CUAL” SIN GARANTÍA DE NINGUNA CLASE, EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERABILIDAD, COMERCIALIZACIÓN O IDONEIDAD PARA UN PROPÓSITO DETERMINADO. Algunas legislaciones no contemplan la declaración de limitación de responsabilidad, ni implícita ni explícita, en determinadas transacciones, por lo que cabe la posibilidad de que esta declaración no se aplique en su caso.

Marcas registradas

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

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

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

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

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

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

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

Prefacio

Este manual pertenece a la biblioteca de productos descrita en “Visión general de la biblioteca” en la página xxvii y describe un grupo de protocolos soportados por 2212. Puede ser que un 2212 específico no de soporte a todas las características y funciones descritas en estos manuales. Si una característica o una función es específica de un dispositivo, dicha restricción se indica en el manual pertinente.

Este manual hace referencia a 2212 como “el direccionador” o bien como “el dispositivo”. Los ejemplos de la biblioteca representan la configuración de un 2212, pero la salida real visualizada puede variar. Utilice los ejemplos como guía acerca de lo que vería al configurar su dispositivo.

A quién va dirigido este manual

Este manual está dirigido a aquellas personas que instalan y trabajan con redes informáticas. Aunque tener experiencia en hardware y software de redes informáticas puede resultar útil, no se necesita experiencia en programación para utilizar el software de protocolos.

Obtener información adicional

Pueden efectuarse cambios en la documentación después de que se impriman los manuales. Si hay disponible información adicional o si es necesario realizar cambios una vez impresos los manuales, encontrará los cambios en un archivo (denominado README) del CD-ROM. Podrá visualizar el archivo con un editor de texto de código ASCII.

Acerca del software

IBM Access Integration Services es el software que da soporte al IBM 2212 (número de programa bajo licencia 5639-F73). 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 Access Integration 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 2212.
- El programa de configuración de IBM Access Integration 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.

El programa de configuración de IBM Access Integration Services se puede obtener también en la página de presentación IBM Networking Technical Support. En la publicación *Guía del usuario del programa de configuración para Nways Multiprotocol y Access Services,*, GC10-3430 (GC30-3830), hallará los directorios y la dirección de servidor.

Convenios utilizados en este manual

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

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

   ```
   reload
   ```

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

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

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

   Elija una de las palabras clave como valor del parámetro.

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

   ```
   time host ...
   ```

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

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

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

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

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

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

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

6. Los nombres de las teclas que deben pulsarse se indican así: **Intro**

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

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

Visión general de la biblioteca

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 2212 en:

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

La lista siguiente muestra los manuales de la biblioteca de IBM 2212 agrupados según las tareas.

Planificación

GA10-5240 (GA27-4215) *IBM 2212 Guía de introducción y planificación*

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

Instalación

GA10-5241 (GA27-4216)
IBM 2212 Access Utility Guía de instalación y configuración inicial

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

GX10-8543 (GX27-4048)
2212 Consulta rápida de la configuración del hardware

Esta tarjeta de consulta sirve para entrar y guardar la información de configuración de hardware utilizada para determinar cuál es el estado correcto de un IBM 2212.

Diagnóstico y mantenimiento

GY10-8068 (GY27-0362) *IBM 2212 Access Utility Manual de mantenimiento y servicio*

Esta publicación se entrega junto con el IBM 2212. En ella se dan instrucciones para el diagnóstico de problemas que puedan surgir en el IBM 2212 y para repararlos.

Operaciones y gestión de red

En la lista siguiente figuran los manuales del programa Access Integration Services.

SC10-3436 (SC30-3988) *Guía del usuario de software*

En este manual se explica cómo:

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

SC10-3437 (SC30-3989) *Utilización y configuración de las funciones*

SC10-3438 (SC30-3990) *Configuración y supervisión de protocolos - Manual de consulta, volumen 1*

SC10-3439 (SC30-3991) *Configuración y supervisión de protocolos - Manual de consulta, volumen 2*

En estos manuales se describe el modo de acceder a la interfaz de usuario de línea de mandatos de Access Integration Services y la manera de utilizarla para configurar y supervisar el software de protocolos de direccionamiento que se entrega con el producto.

En ellos se incluye información sobre cada uno de los protocolos a los que dan soporte los dispositivos.

SC10-3431 (SC30-3682) *Guía de mensajes del sistema para el registro cronológico de sucesos*

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

Configuración

GC10-3430 (GC30-3830)
Guía del usuario del programa de configuración para Nways Multiprotocol y Access Services

En esta publicación se explica cómo utilizar el programa de configuración.

Seguridad

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

En esta publicación, que se entrega con el IBM 2212, se proporciona la traducción de los avisos de precaución y peligro aplicables a la instalación y al mantenimiento de un IBM 2212.

Información comercial

En la página Web de IBM siguiente hallará información sobre productos:

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

Resumen de los cambios correspondientes a la biblioteca software IBM 2212

En la siguiente lista figuran los cambios realizados en el software de la Versión 3 Release 4:

- Mejoras en Frame Relay:
  - Soporte del nuevo manejador de tramas (FH)
  - Aceleración PU para manejar ráfagas de tráfico para soportar controladores 3745
  - Nuevo tipo de interfaz (subinterfaz Frame Relay) para permitir interfaces virtuales en la misma interfaz física
  - Soporte de IP no numerado

- Mejoras en VPN:
  - Mejoras en CPE:
    - Información de políticas de servidores LDAP almacenada localmente.
    - Configuración rápida de políticas.
    - Comprobación de coherencia de políticas.
    - Ahora la información de políticas puede recuperarse desde servidores LDAP en un dominio administrativo.
    - Ping de túnel IPSec.
  - Mejoras en IP:
    - Mejoras en direccionamiento de voz:
      - Compresión de cabecera IP en PPP (RFC 2507, 2508 y 2509)
      - Intercalado de tráfico de voz entre paquetes de datos fragmentados en PPP multienlace
      - Intercalado de tráfico de voz entre paquetes de datos fragmentados en Frame Relay
      - Elusión de PPP o compresión y cifrado de paquetes de Frame Relay para tráfico de voz
    - Dirección de bucle de retorno IP

      Este soporte permite que los usuarios definan direcciones IP en una interfaz especial que da soporte a los requisitos de TN3270 Gateway, Network Dispatcher e IPSec.
    - IPv6
      - Se proporciona una función de direccionamiento entre dominios (BGP4+) para IPv6 que da soporte al direccionamiento IPv6 y a la información de direcciones y utiliza TCP6 como transporte.
    - Múltiples vías de reenvío

      El direccionamiento IP puede utilizar hasta cuatro rutas IP estáticas de igual coste para dar soporte a múltiples enlaces paralelo a una dirección y máscara determinadas.
    - Adición de rutas IP
    - Mejoras en multidifusión:
      - PIM-DM (Protocol Independent Multicast-Dense Mode) para IPv4.
      - Los administradores de redes ahora pueden controlar el flujo de datos de multidifusión IP que entra y sale de sus redes mediante la utilización de filtros de entrada y salida de tráfico.
    - Área NSSA (not-so-stubby area)

      OSPF da soporte al área NSSA tal como se define en RFC 1587 y ahora se da soporte al ultimo borrador de Internet.
    - RED (Random Early Detection)
    - Mejoras en políticas de servicios diferenciales
    - Mejoras en VRRP:
      - Puede utilizar la dirección MAC de hardware en lugar de una dirección MAC virtual para identificar una pasarela redundante; de este modo puede obtener una mejora en el rendimiento.

- Cuando hay disponible más de un candidato de reserva, se pueden configurar las opciones de preferencia.
- Para seleccionar el direccionador IP maestro, se pueden utilizar criterios adicionales, como la ruta disponible o la interfaz de red para dar soporte a las funciones no IP.

- Interfaz altenativa de marcación a petición para redireccionamiento de WAN
- Mejoras en TN3270
  - Terminación de LU
  - Equilibrio de carga de la agrupación de LU
  - Desconexión de Talk 5 de sesiones TN3270
  - Información adicional de generación de informes
  - Soporte de direcciones 1 y 255
- Mejoras en Network Dispatcher
  - Anuncios de direcciones de cluster de Network Dispatcher mediante protocolos de direccionamiento
  - Un nuevo asesor SSL
- Soporte de PU1 SDLC DLSw
- Soporte de encapsulación Ethernet para Ethernet tipo II (valor por omisión) y 802.3 simultáneamente en la misma interfaz
- Mejoras en DHCP:
  - Copia de seguridad en disco duro para información de alquiler
  - Soporte de múltiples direcciones IP para interfaces DHCP
  - Soporte de alquiler breve
- Mejoras RADIUS
  - Escalabilidad Radius
  - Inicio de sesión de último recurso
- Escalabilidad L2TP
- Mejora de servidor ligero

  Conexión a un servidor alternativo o maestro de reserva de seguridad
- Mejoras en recuperación de archivos de servicio

Aclaraciones y correcciones

En copia impresa y en archivo PDF, los cambios técnicos y las adiciones se indican mediante una línea vertical (|) situada a la izquierda del cambio.

Cómo obtener ayuda

En los indicadores de mandatos, puede obtener ayuda en forma de listado de los mandatos disponibles en el 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, se puede entrar el signo **?** después de un nombre de mandato concreto para listar las opciones del mismo.

Cómo salir de un entorno de nivel inferior

La naturaleza multinivel del software le llevará a entornos de nivel secundario, terciario e incluso inferiores a medida configure o trabaje con el 2212. Para volver al nivel superior más próximo, entre el mandato **exit**. Para llegar al nivel secundario, vaya entrando **exit** hasta que reciba el indicador de nivel secundario (`Config>` o `+`).

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

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

Si es necesario llegar hasta el nivel primario (OPCON), entre el carácter de interceptación (**Control-P** por omisión).

Configuración y supervisión de las funciones de puente

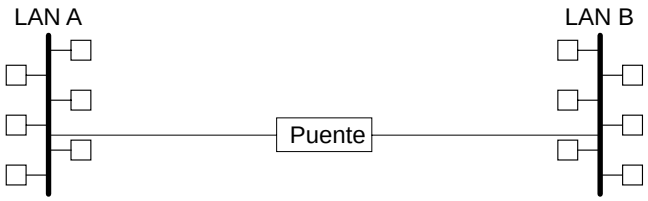
Fundamentos de puenteo

En este capítulo se tratan cuestiones básicas sobre los puentes y su funcionamiento. Consta de los siguientes apartados:

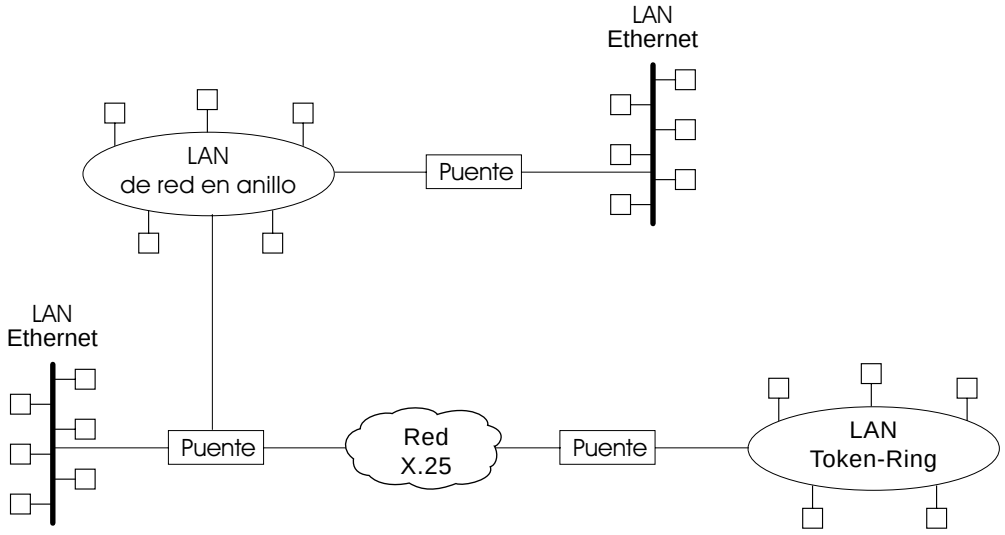
Visión general del funcionamiento de los puentes

Un puente es un dispositivo que enlaza dos o más redes de área local. Un puente acepta tramas de datos de todas las redes conectadas y determina las que reenviará basándose en la cabecera de control de acceso al medio (MAC) que contienen cada una de las tramas.Originalmente, los puentes enlazaban dos o más redes homogéneas. El término *homogénea* significa que las redes conectadas utilizan el mismo método de puenteo y los mismos tipos de soporte. Algunos ejemplos de redes homogéneas son las redes con soporte ***sólo*** para el método de puente de direccionamiento en origen o ***sólo*** para el algoritmo de puente transparente (estos métodos se explicarán más adelante).

Actualmente, los puentes también permiten la comunicación entre redes no homogéneas. El término *no homogénea* hace referencia a las redes con capacidad para combinar diferentes métodos de puenteo y que ofrecen mayor número de opciones de configuración. La Figura 1 en la página 4 ilustra ejemplos de configuraciones de puente complejo y simple.



Puente simple que conecta dos LAN (Ethernet) homogéneas



Configuración de puentes compleja que conecta diferentes tecnologías LAN

Figura 1. Configuración de puente simple y complejo

Puentes y direccionamiento

El 2212 admite tanto puentes como direccionamiento. El proceso de filtrado de protocolo consiste en determinar si los datos de entrada se direccionan o se envían por puente.

Filtrado de protocolo

Al procesar un paquete de datos de entrada, se producen las siguientes acciones:

- Los paquetes se direccionan si se ha habilitado globalmente un reenviador de protocolo específico.
- Los paquetes se filtran si se configuran filtros de protocolos específicos.
- Los paquetes que no se han direccionado ni se han filtrado pueden enviarse por puente, en función de la dirección MAC (control de acceso al medio).

La Tabla 1 en la página 5 muestra cómo se resuelve la cuestión “¿enviar por puente o direccionar?” según el contenido de las direcciones de destino.

Tabla 1. Tabla de criterios de direccionamiento o envío por puente	
Si la dirección MAC de destino de la trama recibida contiene:	**El puente actuará de la siguiente forma:**
Dirección del puente	El puente pasa la trama al protocolo configurado que a su vez la direccionará.
Dirección de difusión general o de multidifusión	Si la trama dispone de un protocolo configurado, la trama se direcciona. De lo contrario, la trama se puentea.
Unidifusión	La trama se puentea.

Direccionamiento y puentes según la interfaz

Para IP, IPX, y AppleTalk, se utilizan los siguientes criterios para las funciones de puenteo o direccionamiento a través de una determinada interfaz:

- Los paquetes se direccionan si se ha configurado un protocolo específico para la interfaz de recepción.
- Los paquetes se filtran si se configuran filtros de protocolos específicos en la interfaz de recepción.
- Los paquetes que no se han direccionado ni se han filtrado pueden enviarse por puente, en función de la dirección MAC (control de acceso al medio).

Conexiones de direccionador

La conexión a la capa 3 mediante un direccionador permite la conexión y la selección de rutas entre estaciones finales de áreas geográficas distantes. Los protocolos de direccionamiento permiten seleccionar la mejor ruta para conectar LAN remotas y diversas. Debido a la gran variedad de opciones de configuración de redes y subredes que ofrecen las grandes redes, la conexión de la LAN a través de la capa de red es el método más utilizado. Los protocolos de capa de red han demostrado ser muy eficientes para transferir información en configuraciones de redes grandes y diversas.

Conexiones de puente

Si se conecta a la capa 2 mediante un puente, proporciona conexión a través de un enlace físico. Esta conexión es esencialmente “transparente” al sistema principal conectado a la red.

Nota: Los puentes de direccionamiento en origen no se consideran totalmente “transparentes”. Véase el “Métodos de puenteo” en la página 13 si desea obtener más información acerca del direccionamiento en origen y los puentes transparentes.

La capa de enlace mantiene métodos de direccionamiento físico (en lugar de direccionamiento lógico de la capa 3), disciplina de línea, información sobre la topología, notificación de errores, control de flujo y entrega ordenada de tramas de datos. El aislamiento de los protocolos de capas superiores constituye una de las ventajas de los puentes. Dado que los puentes trabajan al nivel de la capa de enlace, no consultan la información acerca de los protocolos que se registra en las capas superiores, de forma que se reduce la actividad general de proceso y se acelera la comunicación del tráfico del protocolo de la capa de red. Asimismo,

dado que los puentes no consultan la información de la capa 3, pueden reenviar diferentes tipos de tráfico de protocolo (por ejemplo, IP o IPX) entre dos o más redes (tal como hacen los direccionadores).

Los puentes también filtran tramas basadas en campos de la capa 2. De esta forma, un puente puede configurarse para aceptar y reenviar sólo tramas de un tipo determinado o las que proceden de una red específica. La capacidad de configurar filtros resulta muy útil para mantener un flujo de trafico efectivo.

Los puentes son preferibles cuando es necesario dividir grandes redes en segmentos manejables. Las ventajas de los puentes en grandes redes puede resumirse de la siguiente forma:

- Los puentes permiten aislar áreas de red específicas para que estén menos expuestas a los principales problemas de red.
- El filtrado le permite regular la cantidad de tráfico que se reenvía a segmentos específicos.
- Los puentes permiten la comunicación entre un mayor número de dispositivos de interconexión de redes que los que estarían soportados en una sola LAN conectada a un puente.
- Los puentes eliminan el límite de nodos (el numero total de nodos de un segmento). El tráfico de la red local no se transfiere a todas las demás redes conectadas.
- Los puentes amplían la “longitud” conectada de una LAN al permitir la conexión de LAN remotas. Los puentes conectan dos segmentos de LAN en la capa 2 para que puedan formarse redes más grandes. De esta forma, se supera el problema de congestión cuando hay muchas estaciones en una red Ethernet y el límite de 256 estaciones de la arquitectura de red en anillo.

Puentes frente a direccionadores

Los dispositivos de interconexión de redes como, por ejemplo, los puentes y los direccionadores son similares, ya que ambos conectan segmentos de red. Sin embargo, cada uno de estos dispositivos utiliza un método diferente para establecer y mantener las conexiones 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 puente

Los siguientes apartados describen diferentes tipos de puente y cómo se clasifican según sus características hardware y software.

Puentes simples

Los puentes simples constan de dos o más interfaces de red que conectan dos redes de área local (Figura 1 en la página 4). Los puentes interconectan distintas redes de área local (LAN) retransmitiendo tramas de datos entre las entidades MAC (control de acceso al medio) de las LAN puenteadas.

Las principales funciones de un puente simple se resumen de la siguiente forma:

- El puente lee todas las tramas de datos transmitidas en la LAN A y recibe las dirigidas a la LAN B. Los puentes simples no modifican el contenido ni el

formato de las tramas de datos que reciben. Tampoco encapsulan las tramas con cabeceras adicionales.

La mayoría de los puentes simples contienen direcciones de rutas e inteligencia de direccionamiento. El puente debe disponer como mínimo de las direcciones que se encuentran en cada una de las redes conectadas para determinar las tramas que debe transferir.

- El puente transfiere a la LAN B las tramas de datos dirigidas a la LAN B mediante el protocolo MAC de esa LAN. Los puentes deben disponer de suficiente espacio de almacenamiento intermedio para satisfacer la demanda del tráfico de datos, ya que es posible que las tramas de datos se reciban más rápidamente de lo que el puente es capaz de transmitirlas.
- El puente actúa de la misma manera con el tráfico de las tramas de datos desde la LAN B a la LAN A.

Puentes complejos

Los puentes complejos realizan funciones más sofisticadas que los puentes simples. Estas funciones incluyen el mantenimiento de información de estado en otros puentes. Esta información incluye el coste de la ruta de comunicación así como el número de saltos necesarios para acceder a las redes conectadas. Los intercambios periódicos de información entre puentes actualizan la información acerca de estos últimos. Este tipo de intercambios permiten el direccionamiento dinámico entre puentes.

Los puentes complejos también pueden modificar tramas y reconocer y transmitir paquetes de diferentes tecnologías LAN (por ejemplo, Red en anillo, y Ethernet). En este caso, el puente también se conoce como puente *translacional*.

El puente transparente de direccionamiento en origen adaptable (ASRT) constituye la implementación de la tecnología de puentes del 2212. El puente ASRT es un conjunto de componentes de software con capacidad para realizar algunas de las funciones de puenteo descritas anteriormente y mucho más. Todas estas funciones se explican en mayor detalle más adelante en este capítulo.

Puentes locales

Los puentes locales proporcionan conexiones entre segmentos de LAN de la misma área local. Un ejemplo de puente local es el tipo de puente que se utiliza para conectar las diversas LAN de la sede principal de su empresa.

Puentes remotos

Los puentes remotos conectan múltiples segmentos de LAN de diferentes áreas geográficas. Un ejemplo de puente remoto es el tipo de puente que se utiliza para conectar las LAN de la sede principal de su empresa a las LAN de las filiales que su empresa posee en todo el país. Debido a las diferencias geográficas, la configuración de red de área local debe convertirse en una configuración de red de área amplia (WAN).

Los puentes remotos se diferencian de los puentes locales en varios aspectos. La principal diferencia es la velocidad de transmisión de los datos. Las conexiones de WAN pueden ser más lentas que las conexiones de LAN. Esta diferencia de velocidad es significativa cuando se ejecutan aplicaciones en las que el tiempo es un factor fundamental. Otra diferencia radica en la forma en que los puentes locales y

remotos se conectan a las LAN físicamente. En los puentes locales, las conexiones se realizan a través de soportes de cableado locales (por ejemplo, Ethernet o Thinet). Las conexiones de puente remoto se realizan a través de las líneas serie.

Funcionamiento básico de los puentes

Según el estándar de LAN IEEE 802, todas las direcciones de estación se especifican a nivel de MAC. En el nivel de control de enlace lógico (LLC), sólo se designan las direcciones de punto de acceso a servicio (SAP). Por lo tanto, el nivel MAC es el nivel en el que funciona el puente. Los siguientes ejemplos ilustran cómo las funciones de puenteo operan en este nivel.

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

La Figura 2 muestra un modelo de puente de dos puertos que conecta dos estaciones finales en dos LAN. En este ejemplo, el puente local conecta dos LAN con idénticas capas LLC y MAC (es decir, dos redes LAN en anillo). Para conceptualizar este ejemplo, imagínese que el puente es un enlace de datos que reenvía tramas entre las subcapas de control de acceso al medio (MAC) y los canales físicos conectados a la LAN, de forma que permite la conectividad para el enlace de datos entre ambas.

Resumen del proceso de puenteo: 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 las tramas transmitidas). A continuación, las reenvía al destino LAN pertinente. A lo largo de este proceso, se establece un diálogo entre las entidades LLC iguales de las dos estaciones finales. Por lo que respecta a la arquitectura, el puente no necesita una capa LLC, ya que la función de ésta simplemente consiste en retransmitir las tramas MAC procedentes de los niveles superiores del modelo OSI.

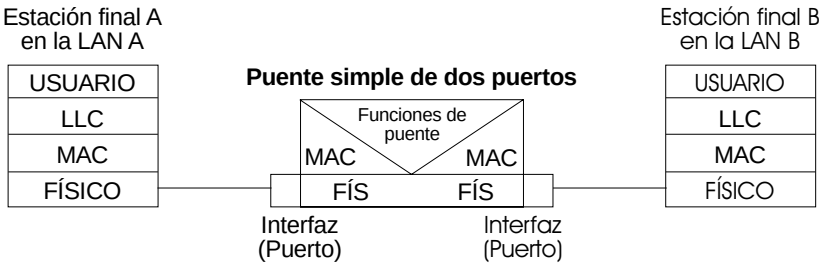


Figura 2. Un puente de dos puertos que conecta dos LAN

Ejemplo de funcionamiento 2: Puente remoto a través de un enlace serie

La Figura 3 en la página 9 muestra dos puentes conectados a través de un enlace serie. Estos puentes locales conectan redes LAN con idénticas capas LLC y MAC (es decir, dos redes LAN en anillo).

En resumen, el puente captura la trama MAC cuya dirección de destino no se encuentra en la LAN local y, a continuación, la envía al destino LAN pertinente a través del puente de esa LAN. A lo largo de este proceso, se establece un diálogo entre las entidades LLC iguales de las dos estaciones finales. Por lo que respecta a la arquitectura, el puente no necesita una capa LLC, ya que la función de ésta

simplemente consiste en retransmitir las tramas MAC procedentes de los niveles superiores del modelo OSI.

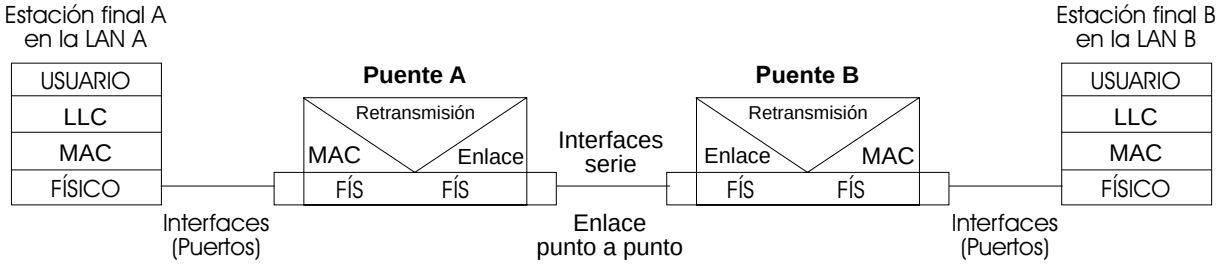


Figura 3. Puente a través de un enlace punto a punto

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

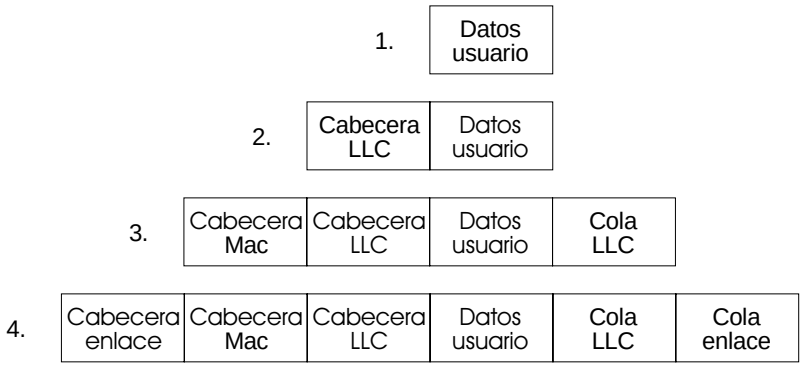


Figura 4. Encapsulación de datos a través de un enlace punto a punto

El proceso de encapsulación consiste en lo siguiente:

1. La estación final A proporciona datos a su LLC.
2. LLC añade una cabecera y transfiere la unidad de datos resultante al nivel MAC.
3. A continuación, 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 volver a transferir la trama MAC intacta al destino LAN. En la configuración punto a punto, sin embargo, el puente añade una cabecera y una cola de capa de enlace (por ejemplo, HDLC) y transmite la trama MAC a través del enlace.

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

Formatos de trama de puente MAC

Como se ha mencionado anteriormente, los puentes interconectan redes LAN retransmitiendo tramas de datos, en particular tramas MAC, entre las diferentes entidades MAC de las LAN puenteadas. Las tramas MAC proporcionan la información de “ubicación” necesaria para reenviar tramas en forma de direcciones de

origen y de destino. Esta información es esencial para la correcta transmisión y recepción de datos.

IEEE 802 proporciona soporte para tres tipos de tramas MAC: CSMA/CD (802.3), bus con paso de testigo (802.4) y de 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 el siguiente apartado.

Nota: Se utiliza un formato de trama distinto en el nivel LLC. Esta trama se incorpora en la trama MAC pertinente.

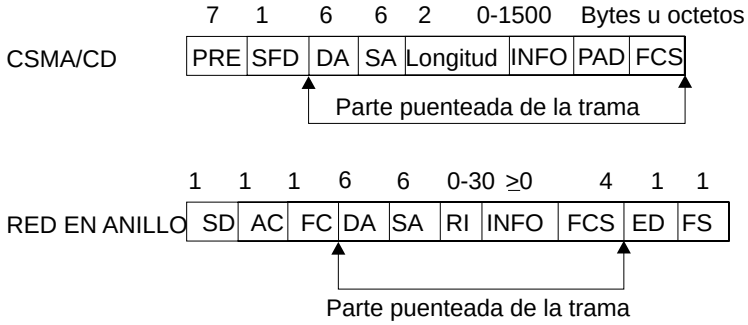


Figura 5. Ejemplos de formatos de trama MAC

Tramas MAC CSMA/CD (Ethernet)

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

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

La parte de la trama que se envía por puente está formada por los siguientes campos:

- *Dirección de destino (DA)*. Especifica la estación final a la que se destina la trama. Esta dirección puede ser una dirección física única (un destino), una dirección 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 el mismo para todas las estaciones de una LAN determinada.
- *Dirección origen (SA)*. Especifica la estación final que transmitió la trama. El formato debe ser el mismo que el de la dirección de destino.
- *Longitud*. Especifica el número de bytes LLC.
- *Información (INFO)*. Campos incorporados que se han creado en el nivel LLC y que contienen información acerca del punto de acceso a servicio, información de control y datos del usuario.
- *Relleno*. Secuencia de bytes que garantiza que la longitud de la trama es suficiente para realizar adecuadamente las operaciones de detección de colisiones (CD).

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

Tramas MAC de red en anillo

La siguiente información describe cada uno de los campos que se encuentran en 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 las variables de prioridad y reserva de 3 bits, M es el bit del monitor y T indica si se trata de una trama de datos o una trama testigo. Si se trata de una trama testigo, el único campo adicional es el delimitador de final (ED).
- *Control de trama (FC)*. Indica si se trata de una trama de datos LLC. Si no se trata de una trama de este tipo, los bits de este campo controlan el funcionamiento del protocolo MAC de red en anillo.

La parte de la trama que se envía por puente está formada por los siguientes campos:

- *Dirección de destino (DA)*. El mismo campo que en las tramas CSMA/CD y bus con paso de testigo.
- *Dirección origen (SA)*. Identifica la estación de donde procede la trama. Este campo puede ser una dirección de 2 ó 6 octetos. Ambas longitudes incorporan un bit indicador de información de direccionamiento (RII) que señala si la trama dispone de un campo de información de direccionamiento (RIF) a continuación de la dirección de destino:

  RII=1 Dispone del campo de información de direccionamiento.
  RII=0 No dispone del campo de información de direccionamiento.

  Este campo se describe con mayor detalle en “Puentes de direccionamiento en origen (SRB)” en la página 23.
- *Campo de información de direccionamiento (RIF)*. El protocolo de direccionamiento en origen requiere el campo RIF. Consiste en un campo de control de direccionamiento de 2 octetos y un conjunto de campos de designador de rutas de 2 octetos. Este campo se describe con mayor detalle en “Puentes de direccionamiento en origen (SRB)” en la página 23.
- *Información (INFO)*. Campos incorporados que se han creado en el nivel LLC y que contienen información acerca del punto de acceso a servicio, información de control y datos del usuario.
- *Secuencia de comprobación de la trama (FCS)*. Un valor de 32 bits de comprobación de redundancia cíclica. Este valor está basado en todos los campos, empezando por la dirección de destino.

Finalmente, el *Delimitador de final (ED)* contiene el bit de detección de errores (E) y el bit de trama intermedia (I). El bit I indica que no se trata de la trama final de una transmisión de múltiples tramas. El campo *Estado de trama (FS)* contiene el bit de dirección reconocida (A) y el de trama copiada (C).

Métodos de puenteo

En este capítulo se describen los métodos de puenteo a los que da soporte el puente transparente de direccionamiento en origen adaptable (ASRT). Cada uno de los apartados del capítulo ofrece una visión general de una tecnología determinada y va seguido de la descripción de las tramas de datos a las que da soporte la tecnología. Consta de los siguientes apartados:

Puentes transparentes

Un puente transparente también se conoce generalmente como un puente de árbol de extensión (STB). El término *transparente* hace referencia al hecho de que el puente reenvía silenciosamente, de forma no visible o *transparente* para el usuario, el tráfico no local a las LAN conectadas. Las aplicaciones de estación final desconocen la existencia del puente. El puente sabe de la existencia de las estaciones finales estando a la escucha del tráfico que pasa a través de él. A partir de este proceso de escucha, construye una base de datos de las direcciones de estaciones finales conectadas a las LAN.

Para cada cada trama que recibe, el puente coteja la dirección de destino de la trama con las direcciones que hay en la 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, se reenvía la trama. Si la dirección de destino no consta en la base de datos, la trama se reenvía a todas las LAN conectadas al puente, excepto a la LAN de la cual procede la trama.

Todos los puentes transparentes utilizan el algoritmo y el protocolo de árbol de extensión. El algoritmo de árbol de extensión crea y mantiene una topología sin bucles en una red puenteada que puede contener bucles en su diseño físico. En una topología en malla en la que existe más de un puente conectado entre dos LAN, se produce la *repetición en bucle*. En estos casos, los paquetes de datos "rebotan" entre las dos LAN en puentes paralelos. Esta situación crea una redundancia en el tráfico de datos y origina el fenómeno llamado repetición en bucle.

Cuando se produce la repetición en bucle, debe configurar las LAN local y remota para eliminar el bucle físico. Con el árbol de extensión, un algoritmo autoconfigurable permite añadir un puente en cualquier parte de la LAN sin crear bucles. Cuando se añade el nuevo puente, el protocolo de árbol de extensión vuelve a configurar automáticamente todos los puentes de la LAN en un solo *árbol de extensión* sin bucles.

En un árbol de extensión jamás existe más de una ruta de datos activa entre dos estaciones finales, de forma que se eliminan los bucles de datos. El algoritmo determina, para cada puente, cuáles son los puertos que pueden reenviar datos y cuáles son los que deben bloquearse a fin de formar una topología sin bucles. Las características del árbol de extensión son:

- *Detección de bucles*. Detecta y elimina los bucles físicos de enlace de datos en las configuraciones de LAN ampliadas.
- *Reserva automática de las rutas de datos*. Los puentes que se conectan a rutas redundantes entran automáticamente en modalidad de reserva. Cuando un puente primario falla, se activa uno de reserva.
- *Configuración por usuario*. Permite que el usuario adapte la topología de red. Algunas veces, los valores por omisión no crean la topología de red deseada. Se puede ajustar la prioridad de puente, la prioridad de puerto y los parámetros de coste de ruta con el fin de que el árbol de extensión adopte la forma de la topología de red.
- *Interoperatividad uniforme*. Permite que la interoperatividad de LAN no sufra las limitaciones de configuración que derivan de la diversidad de entornos de comunicaciones.
- *Puenteo de protocolos sin direccionamiento*. Ofrece un puenteo con una buena relación calidad-precio de los protocolos sin direccionamiento.

Puentes transparentes y direccionadores

Durante el funcionamiento de un direccionador equipado con la opción de árbol de extensión, el software de puente y de direccionador se ejecuta de forma concurrente. En esta modalidad, el direccionador es a la vez puente y direccionador.

Con este tipo de funcionamiento, se llevan a cabo las acciones siguientes:

- Los paquetes se direccionan si se ha habilitado globalmente un reenviador de protocolo específico.
- Los paquetes se filtran si se configuran filtros de protocolo específicos.
- Los paquetes que no se han direccionado ni filtrado son candidatos a enviarse por puente, en función de la dirección MAC (control de acceso al medio).

Requisitos de red

La tecnología de puentes transparentes implementa un puente de árbol de extensión conforme la normativa IEEE 802.1D. Todos los puentes transparentes (como Ethernet y red en anillo) de la red deben ser puentes de árbol de extensión 802.1D. Este protocolo de árbol de extensión no es compatible con los puentes que implementan protocolo de árbol de extensión exclusivo de Digital Equipment Corporation utilizado en algunos puentes antiguos.

Funcionamiento de los puentes transparentes

En una topología en malla en la que existe más de un puente conectado entre dos LAN, puede producirse el fenómeno de la repetición en bucle, que se da cuando dos LAN se lanzan paquetes por puentes paralelos. Un bucle es una situación en la que existen varias rutas de datos entre dos LAN. El protocolo de árbol de extensión en funcionamiento elimina automáticamente los bucles bloqueando las rutas redundantes.

Durante el proceso de inicio, todos los puentes participantes en la red se intercambian unidades de datos de protocolo de puente (BPDU) Hello que facilitan información de configuración sobre cada puente. Las BPDU incluyen información como el ID de puente, el ID de raíz y el coste de la ruta al raíz. Esta información les sirve de ayuda a los direccionadores para determinar unánimemente qué puente es

el raíz y qué puentes son los designados para las LAN a las que están conectados.

De toda la información intercambiada en los mensajes HELLO, los parámetros siguientes son los más importantes para calcular el árbol de extensión:

- *ID de puente raíz*. El ID de puente raíz es el ID del puente. El puente raíz es el puente designado para todas las LAN a la que está conectado.
- *Coste de la ruta al raíz*. Suma total de los costes de ruta hasta llegar a la ruta raíz a través del puerto raíz de este puente. Esta información la transmiten tanto el puente raíz y los puentes designados para actualizar todos los puentes que figuran en la información de ruta si cambia la topología.
- *ID de puente*. ID exclusivo utilizado por el algoritmo de árbol de extensión para determinar cómo será el árbol de extensión. A cada puente de la red se le asigna un identificador de puente exclusivo.
- *ID de puerto*. ID del puerto desde el que se ha transmitido el mensaje de BPDU HELLO actual.

Una vez que se dispone de esta información, el árbol de extensión comienza a determinar la forma y el sentido que tomará y, a continuación, crea una configuración de ruta lógica. Este proceso puede resumirse de la manera siguiente:

1. Se selecciona un puente raíz para la red comparando el ID de cada uno de los puentes de la red. El puente con el ID inferior (es decir, con el valor más alto) gana.
2. A continuación, el algoritmo de árbol de extensión selecciona un puente designado para cada LAN. Si hay más de un puente conectado a la misma LAN, se selecciona como puente designado aquél cuyo coste de ruta al raíz sea inferior. En caso de existir costes de ruta duplicados, se selecciona el puente con el ID de puente más bajo.
3. Los puentes no designados de las LAN ponen los puertos que no han sido seleccionados como puerto raíz en estado BLOCKED (bloqueado). En el estado BLOCKED, el puente sigue estando a la escucha de BPDU Hello, de manera que puede actuar al producirse cambios en la red (por ejemplo, falla el puente designado) y cambiar el estado BLOCKED por FORWARDING (es decir, reenviará datos).

En este proceso, el algoritmo de árbol de extensión reduce una red LAN puenteada de tipología arbitraria a un único árbol de extensión. Con el árbol de extensión, jamás existe más de una ruta de datos activa entre dos estaciones finales, de forma que se eliminan los bucles de datos. Para cada puente de la red, el árbol de extensión determina los puertos que se han de bloquear para evitar que se formen bucles.

Esta nueva configuración está delimitada por el factor tiempo. Si un puente designado falla o se elimina físicamente, los demás puentes de la LAN detectan la situación cuando no reciben las BPDU Hello en el plazo de tiempo establecido por el tiempo de antigüedad máximo de puente. Este evento desencadena 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.

Dar forma al árbol de extensión

Cuando el árbol de extensión utiliza los valores por omisión, el algoritmo suele, por lo general, dar un resultado aceptable. No obstante, en ocasiones, puede generar un árbol de extensión con un bajo rendimiento de la red. En ese caso, se puede ajustar la prioridad de puente, la prioridad de puerto y el coste de ruta a fin de que el árbol de extensión adopte la forma que responda a las expectativas de rendimiento de red. En los ejemplos que siguen se explica la manera de hacerlo.

La Figura 6 en la página 17 muestra tres LAN conectadas en red por medio de tres puentes. Cada puente utiliza los valores por omisión de prioridad de puente para la configuración del árbol de extensión. En este caso, como puente raíz se elige el puente que tiene la dirección física más baja porque la prioridad de puente de cada uno de ellos es la misma. En el ejemplo, se trata del puente 2.

El árbol de extensión acabado de configurar permanece intacto gracias a las repetidas transmisiones de BPDU Hello desde el puente raíz en un intervalo preestablecido (tiempo de mensajes HELLO de puente). En este proceso, los puentes designados se actualizan con la información de configuración. A continuación, generan de nuevo la información a partir de las BPDU Hello y la distribuyen a las LAN de las que son puentes designados.

Tabla 2. Valores por omisión del árbol de extensión

Puente 1	**Puente 2**	**Puente 3**
Prioridad de puente: 32768 Dirección: 00:00:90:00:00:10 **Puerto 1** Prioridad: 128 Coste de ruta: 100 **Puerto 2** Prioridad: 128 Coste de ruta: 17857 **Puerto 3** Prioridad: 128 Coste de ruta: 17857	Prioridad de puente: 32768 Dirección: 00:00:90:00:00:01 **Puerto 1** Prioridad: 128 Coste de ruta: 100 **Puerto 2** Prioridad: 128 Coste de ruta: 17857 **Puerto 3** Prioridad: 128 Coste de ruta: 17857	Prioridad de puente: 32768 Dirección: 00:00:90:00:00:05 **Puerto 1** Prioridad: 128 Coste de ruta: 100 **Puerto 2** Prioridad: 128 Coste de ruta: 17857 **Puerto 3** Prioridad: 128 Coste de ruta: 17857

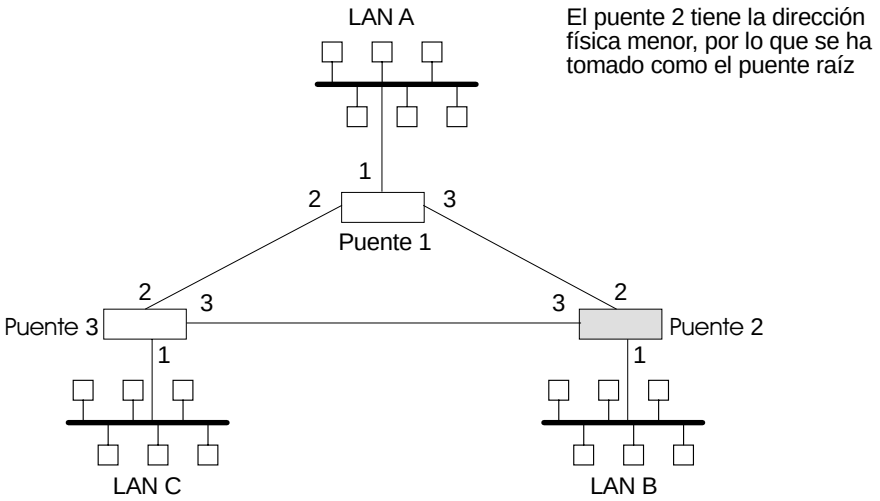


Figura 6. LAN unidas en red antes de crear el árbol de extensión

El algoritmo de árbol de extensión designa el puerto que conecta el puente 1 con el puente 3 (puerto 2) como puerto de reserva y lo bloquea para que no reenvíe tramas, cosa que provocaría una condición de bucle. El árbol de extensión que crea el algoritmo con los valores por omisión de la Tabla 2 en la página 16 aparece en la Figura 7; está formado por las líneas de trazo grueso que conectan el puente 1 con el puente 2 y éste con el puente 3. El puente raíz es el puente 2.

Este árbol de extensión da como resultado un bajo rendimiento de red porque las estaciones de trabajo de la LAN C llegan al servidor de archivos de la LAN A únicamente de forma indirecta a través del puente 2, en lugar de utilizar la conexión directa entre el puente 1 y el puente 3.

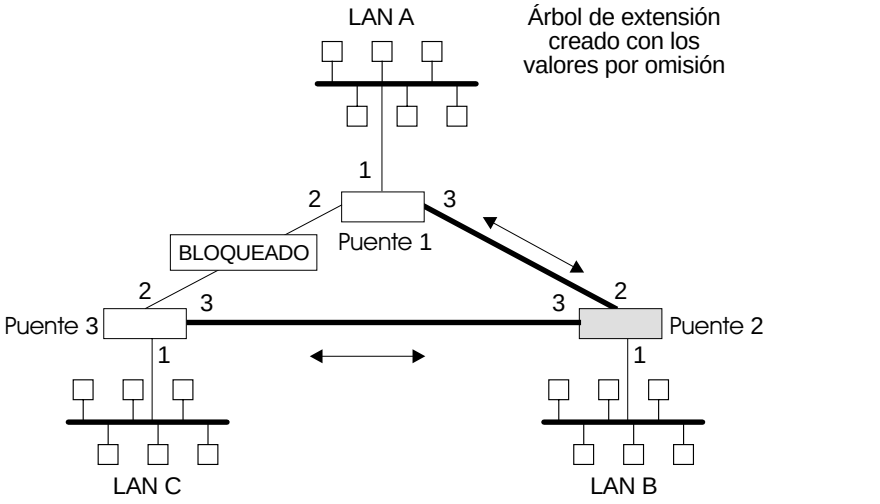


Figura 7. Árbol de extensión creado con los valores por omisión

Normalmente, esta red no utiliza habitualmente el puerto que hay entre el puente 2 y el puente 3. Por lo tanto, se puede mejorar el rendimiento de red haciendo que el puente 1 sea el puente raíz del árbol de extensión. Para ello, hay que configurar el puente 1 con la prioridad más alta, 1000. El árbol de extensión que resulta de esta modificación aparece en la Figura 8 en la página 18; está formado por las líneas de trazo grueso que conectan el puente 1 con el puente 3 y con el puente 2. El

puente raíz es ahora el puente 1. La conexión entre el puente 2 y el puente 3 está bloqueada y sirve de ruta de datos de reserva.

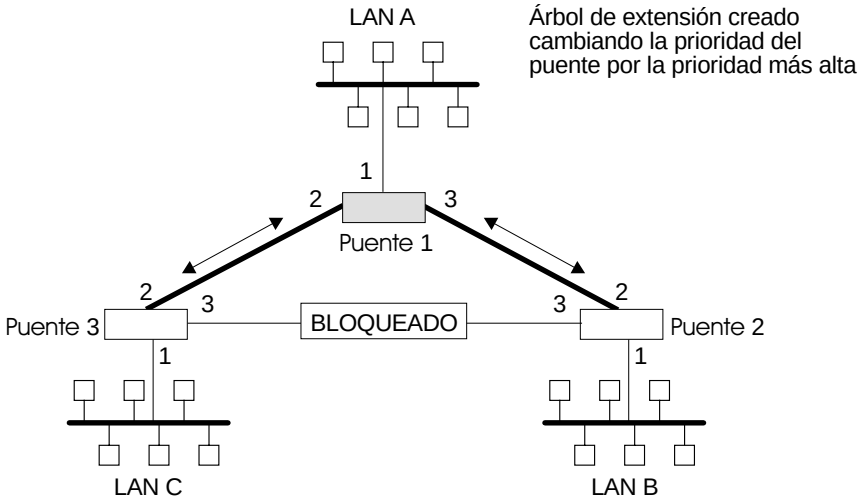


Figura 8. Árbol de extensión ajustado por el usuario

Los puentes de árbol de extensión y la conversión del formato de paquete Ethernet

El protocolo de puente de árbol de extensión 2212 proporciona reenvío de paquetes a los dispositivos de puente de acuerdo con la normativa IEEE 802.1D-1990, puentes MAC (control de acceso al medio). El protocolo también proporciona la oportuna conversión de cabecera para los paquetes Ethernet.

Una red Ethernet/IEEE 802.3 puede dar soporte simultáneamente a la capa de enlace de datos Ethernet y a la capa de enlace de datos IEEE 802.2, en función del valor que tenga el campo de longitud/tipo de la cabecera MAC. El puente debe realizar la conversión a y desde el formato Ethernet con el objeto de ofrecer transparencia entre tipos mixtos de LAN. El algoritmo que se utiliza está basado en nuevas normativas IEEE.

El planteamiento básico consiste en convertir los paquetes Ethernet en paquetes UI (información no numerada) IEEE 802.2 mediante el SAP SNAP IEEE 802. El identificador de protocolo SNAP tiene 00-00-00 como OUI (identificador exclusivo de organización), siendo los 2 últimos bytes el valor de *tipo* Ethernet.

Característica IBM RT para tráfico SNA

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

El proceso de estas tramas puede habilitarse/inhabilitarse a nivel de puerto individual. En la modalidad habilitada, el puerto averigua el comportamiento de la estación de origen. Cuando las tramas están dirigidas a tales estaciones, el puente genera el formato de trama correcto. Si no existe información acerca del comportamiento de la estación (como ocurre en el caso de las estaciones desconocidas o

de multidifusión), el puente genera tramas duplicadas, una con formato IEEE 802.3 e IEEE 802.2 y otra con la cabecera IBM-RT.

Encapsulación UB de tramas XNS

Las tramas Ethernet XNS utilizan Ethertype 0x0600. Cuando se convierten a formato de red en anillo, obtienen SNAP según lo especificado en IEEE 802.1H. Dado que algunas estaciones finales de red en anillo utilizan el OUI de Ungermann-Bass en el SNAP para tales tramas, existe un conmutador de configuración para activar esta encapsulación. Este conmutador se establece con el mandato **frame token_ring_SNAP**.

Puentes transparentes y Frame Relay

La interfaz Frame Relay reenvía las tramas transparentes procedentes de redes Ethernet y en anillo, siempre y cuando tales puentes estén habilitados en el circuito. No hace falta utilizar túneles IP.

Se generan y se transmiten BPDU Hello para cada circuito que esté configurado para puentes transparentes. El protocolo de árbol de extensión hace que los circuitos Frame Relay no designados como parte de la ruta de datos activa estén bloqueados, con lo que se eliminan los bucles.

Puentes transparentes en adaptadores Ethernet 10/100

El hardware del adaptador Ethernet 10/100 proporciona funciones de filtrado de puente transparente de los paquetes de LAN local a fin de aligerar la carga del software de puente. El filtro se inicializa y se habilita cuando se activa el adaptador y funciona de la manera siguiente:

- Los adaptadores averiguan las direcciones MAC de origen y las almacenan en una antememoria de hardware.
- Los adaptadores supervisan la dirección MAC de destino de cada una de las tramas. Filtran las tramas cuyo destino son direcciones locales de la LAN.
- Los adaptadores eliminan las entradas de dirección de la antememoria de hardware mediante un algoritmo de cálculo de la antigüedad.

Conceptos y terminología de los puentes transparentes

En este apartado se hace un repaso de los conceptos y los términos utilizados habitualmente al hablar de puentes transparentes.

Tiempo de antigüedad

Período de tiempo (antigüedad) que debe transcurrir para que se elimine una entrada de la base de datos que sirve de filtro cuando el puerto al que corresponde la entrada se halla en estado de reenvío. Si no se hace referencia a las entradas dinámicas por el tiempo de antigüedad, éstas se suprimen.

Puente

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

Dirección de puente
Parte, formada por 6 octetos, menos significativa del identificador de puente que utiliza el algoritmo de árbol de extensión para identificar un puente de la red. Por omisión, la dirección de puente se establece en la dirección MAC del puerto que tiene la numeración más baja. La dirección por omisión se puede alterar temporalmente con el mandato de configuración **set bridge**.

Tiempo de mensaje HELLO de puente
Especifica la frecuencia con la que un puente envía BPDU Hello (que contienen la información de configuración del puente) cuando se convierte en el puente raíz del árbol de extensión. Este valor es útil sólo para el puente raíz porque controla el tiempo de mensaje HELLO de todos los puentes del árbol de extensión. Para establecerlo, se utiliza el mandato **set protocol bridge**.

Retardo de reenvío de puente
Tiempo que un puerto de puente invierte en el estado de escucha, así como en el estado de averiguación. El retardo de reenvío es el tiempo que el puerto del puente está a la escucha a fin de ajustar la topología del árbol de extensión. También es el tiempo que el puente invierte en saber la dirección de origen de cada paquete que recibe mientras se está configurando el árbol de extensión. Este valor es útil sólo para el puente raíz porque controla el retardo de reenvío de todos los puentes del árbol de extensión.

El puente raíz hace llegar este valor a todos los puentes. Este tiempo se establece con el mandato **set protocol bridge**. El procedimiento para establecer este parámetro se explica en el siguiente capítulo.

Identificador de puente
Identificador exclusivo que utiliza el algoritmo de árbol de extensión para determinar cómo será el árbol de extensión. Cada puente de la red debe tener un identificador de puente exclusivo.

El identificador de puente consta de dos partes: la dirección de puente, que está formada por 6 octetos y es la parte menos significativa, y la prioridad de puente, que está formada por 2 octetos y es la parte más significativa. Por omisión, la dirección de puente se establece en la dirección MAC del puerto que tiene la numeración más baja. La dirección por omisión se puede alterar temporalmente con el mandato de configuración **set bridge**.

Antigüedad máxima de puente
Período de tiempo durante el se considera que la información del protocolo de árbol de extensión es válida antes de que el protocolo la descarte y cambie la topología. Todos los puentes del árbol de extensión utilizan esta antigüedad para controlar la vigencia de la información de configuración recibida que figura en sus bases de datos. Con esto se puede conseguir que la vigencia de la información sea uniforme en todos los puentes del árbol de extensión. Para establecer la antigüedad máxima de puente, se utiliza el mandato **set protocol bridge**.

Prioridad de puente

Parte, formada por 2 octetos, más significativa del identificador de puente establecido por el mandato **set protocol bridge**. Este valor indica las probabilidades que tiene cada uno de los puentes de llegar a ser el puente raíz de la red. Al establecer la prioridad de puente, el algoritmo de árbol de extensión elige como puente raíz del árbol de extensión el puente que tiene el valor de prioridad más alto. El puente que tiene el valor numérico más bajo es el que tiene el valor de prioridad más alto.

Puente designado

Puente que afirma ser el más cercano al puente raíz de una LAN determinada. El grado de cercanía se mide en función del coste de ruta acumulado con respecto al puente raíz.

Puerto designado

ID de puerto del puente designado conectado a la LAN.

Bases de datos de filtrado y permanente

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

La base de datos de filtrado se inicializa con entradas procedentes de la base de datos permanente. Estas entradas son permanentes y sobreviven al encendido/apagado y a las restauraciones del sistema. Estas entradas se añaden o suprimen mediante los mandatos de configuración del árbol de extensión. Las entradas de la base de datos permanente se almacenan en forma de registros SRAM (memoria de acceso aleatorio estática) y su número está limitado por el tamaño de la SRAM.

Nota: También se pueden añadir entradas (estáticas) con los mandatos de supervisión, pero estas entradas ***no*** sobreviven al encendido/apagado ni a las restauraciones del sistema.

La base de datos de filtrado también acumula las entradas que ha averiguado el puente (entradas dinámicas) y que tienen asociado un tiempo de antigüedad. Si no se hace referencia a las entradas durante un determinado período de tiempo (tiempo de antigüedad), se suprimen. Las entradas estáticas no tienen antigüedad, por lo que las entradas dinámicas no pueden grabarse encima de ellas.

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

- *Dirección*. Dirección MAC de 6 bytes de la entrada.
- *Mapa de puertos*. Especifica todos los números de puerto asociados con la entrada
- *Tipo de entrada*. Especifica uno de los tipos siguientes:
  - Entradas reservadas. Reservadas por el comité IEEE 802.1d.
  - Entradas registradas. Constan de direcciones de unidifusión pertenecientes al hardware de comunicaciones conectado al equipo o de direcciones de multidifusión habilitadas por los reenviadores de protocolo.

  - Entradas permanentes. Entradas por el usuario en el proceso de configuración. Sobreviven al encendido/apagado y a las restauraciones del sistema.
  - Entradas estáticas. Entradas por el usuario en el proceso de supervisión. No sobreviven al encendido/apagado ni a las restauraciones del sistema y no tienen antigüedad.
  - Entradas dinámicas. El puente las averigua de forma dinámica. No sobreviven al encendido/apagado ni a las restauraciones del sistema y tienen asociada una antigüedad.
  - Libre. Ubicaciones de la base de datos que están libres y pueden ser ocupadas por entradas de dirección.
- *Antigüedad de dirección (sólo entradas dinámicas)*. Resolución del período de tiempo durante el que las direcciones tienen vigencia antes de ser descartadas. Este valor puede establecerse.

Los cambios en la base de datos permanente se realizan por medio de mandatos de configuración del árbol de extensión y los cambios en la base de datos de filtrado por medio del proceso de supervisión GWCON.

Puertos paralelos
Dos o más puentes que están conectados a las mismas LAN.

Coste de ruta
Cada interfaz de puerto tiene asociado un coste de ruta que es el valor relativo de utilizar el puerto para llegar hasta el puerto raíz de una red puenteada. El algoritmo de árbol de extensión utiliza el coste de ruta para calcular una ruta que minimice el coste de ir desde el puente raíz a todos los demás puentes de la topología de red. La suma total de todos los costes designados y del coste de ruta del puerto raíz recibe el nombre de coste de ruta al raíz.

Puerto
Conexión del puente con cada LAN o WAN conectada. Un puente necesita tener dos puertos como mínimo para servir de puente.

ID de puerto
Identificador de puerto de 2 octetos. El octeto más significativo representa la prioridad de puerto y el octeto menos significativo representa el número de puerto. Tanto el número de puerto como la prioridad de puerto puede asignarlos el usuario. El ID de puerto debe ser exclusivo dentro del puente.

Número de puerto
Parte, de 1 octeto de longitud y asignada por el usuario, del ID de puerto cuyo valor representa la conexión al medio físico. Cero no está permitido como número de puerto.

Prioridad de puerto
Segunda parte, de 1 octeto de longitud, del ID de puerto. Este valor representa la prioridad del puerto que utiliza el algoritmo de árbol de extensión a la hora de realizar comparaciones a fin de tomar decisiones de bloqueo y selección de puerto.

Resolución
Factor de tiempo por el que se mide la vigencia de las entradas dinámicas a medida que aumenta su antigüedad en la base de datos. El valor está comprendido entre 1 y 60 segundos.

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

Puerto raíz
ID del puerto de un puente que ofrece la ruta de menor coste al puente raíz.

Árbol de extensión
Topología de puentes en la que hay una y sólo una ruta de datos entre dos estaciones finales cualesquiera.

Puentes transparentes
Este tipo de puentes conlleva un mecanismo que resulta *transparente* para las aplicaciones de las estaciones finales. Los segmentos de red de área local están interconectados por medio de puentes designados para reenviar las tramas de datos mediante un algoritmo de árbol de extensión.

Puentes de direccionamiento en origen (SRB)

El direccionamiento en origen es un método de reenvío de tramas a través de una red puentada en el que la estación de origen identifica la ruta que seguirá la trama. En un esquema de direccionamiento distribuido, las tablas de direccionamiento que hay en cada puente determinan el camino que siguen los datos por la red. Por el contrario, en un esquema de direccionamiento en origen, es la estación de origen la que define la totalidad de la ruta en la trama transmitida.

El puente de direccionamiento en origen (SRB) proporciona un puenteo local en redes en anillo de 4 y 16 Mbps, como se indica en la Figura 9. También puede conectar redes LAN remotas a través de un enlace de telecomunicaciones que funcione a una velocidad de E1 como máximo.

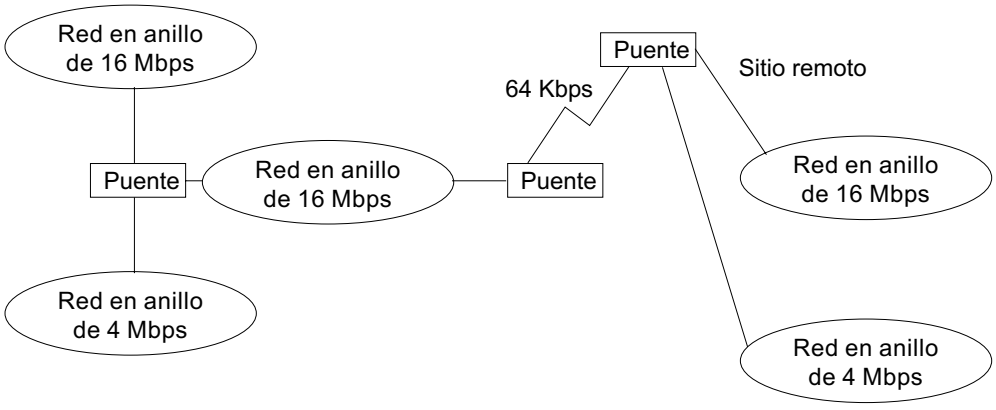


Figura 9. Ejemplo de conectividad por puente de direccionamiento en origen

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

- *Compatibilidad de puentes*. Se puede utilizar el puente para conectar redes de PC en las que se ejecuten sistemas tales como OS/2®, PC LAN Manager y NetBIOS. El puente puede también llevar tráfico SNA entre sistemas principal y LAN de PC.
- *Rendimiento y velocidad*. Dado que el puenteo tiene lugar en la capa de enlace de datos, en lugar de en la capa de red, la conversión de paquetes y el mantenimiento de tablas de direcciones no son necesarios. Con ello disminuye el nivel de actividad general y se posibilita una toma más rápida de decisiones con respecto a las rutas.
- *Túneles de puente*. Al encapsular los paquetes de direccionamiento en origen, el puente/direccionador los direcciona de forma dinámica a través de interredes hasta la estación final de destino deseada sin degradación alguna ni restricciones en el tamaño de red.

  Las estaciones finales de direccionamiento en origen ven esta ruta como un solo salto, independientemente de la complejidad de la red. Esto ayuda a paliar el límite de distancia de 7 saltos habitual que se encuentra en las configuraciones de direccionamiento en origen. Esta característica permite conectar estaciones finales de direccionamiento en origen en medios que no sean de direccionamiento en origen (por ejemplo, redes Ethernet).

Funcionamiento de los puentes de direccionamiento en origen

Como ya se ha dicho, en un esquema de direccionamiento en origen, es la estación de origen la que define la totalidad de la ruta en la trama transmitida. El puente de direccionamiento en origen es dinámico. Tanto las estaciones finales como los puentes participan en el proceso de descubrimiento de la ruta y de reenvío. Este proceso realiza en los pasos siguientes:

1. Una estación de origen envía una trama y se encuentra con que el destino de ésta no se halla en su anillo o segmento (local).
2. La estación de origen construye una trama de difusión para *descubrimiento de ruta* y la transmite al segmento local.
3. Todos los puentes del segmento local capturan la trama de descubrimiento de ruta y la envían a través de sus redes conectadas.

   A medida que la trama de descubrimiento de ruta procede en su búsqueda de la estación final de destino, cada puente que la reenvía añade su propio número de puente y de segmento al campo de información de direccionamiento (RIF) de la trama. Mientras la trama continúa atravesando la red puenteada, el RIF compila una lista de los pares de números de puente y segmento que describen la ruta al destino.

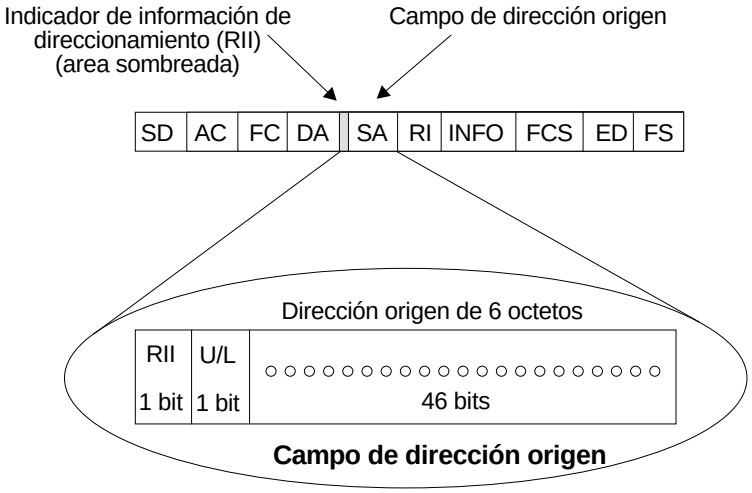
   Cuando la trama de difusión alcanza finalmente su destino, contiene la secuencia exacta de direcciones que van del origen al destino.
4. Cuando la estación final de destino recibe la trama, genera una trama de respuesta que incluye la ruta para las comunicaciones. Las tramas que se extravían por otras partes de la red conectada puenteada (y van acumulando mientras tanto información de direccionamiento que es irrelevante) no llegan nunca a su estación final de destino y no las recibe nunca ninguna estación.
5. La estación final de origen recibe la ruta averiguada. A continuación, ya puede transmitir información por la ruta establecida.

Tramas de direccionamiento en origen

Como ya se ha dicho anteriormente, los puentes interconectan las LAN retransmitiendo tramas de datos, en concreto tramas MAC, entre las diferentes entidades MAC de las LAN puenteadas. Las tramas MAC proporcionan la información de "ubicación" necesaria en forma de direcciones de origen y de destino. Esta información es esencial para la correcta transmisión y recepción de datos.

En el direccionamiento en origen, la decisión de reenviar las tramas de datos se toma en base a la información de direccionamiento que hay dentro de la trama. Antes de que se reenvíe la trama, las estaciones obtienen la ruta que lleva a la estación de destino por medio del proceso de *descubrimiento de ruta*. La estación de la que es originaria la trama designa la ruta por la que viajará la trama; para ello, intercala la descripción de la ruta en el campo de información de direccionamiento (RIF) de la trama transmitida. Si estudiamos con más detenimiento los diversos tipos de tramas de los puentes de direccionamiento en origen, comprenderemos mejor la manera en que el puente obtiene y transmite esta información de direccionamiento.

Dado que las tramas MAC de direccionamiento en origen contienen la información de direccionamiento necesaria para las comunicaciones de datos en entornos multianillo, tiene un formato ligeramente distinto al de las tramas MAC de red en anillo típicas. Si figura un "1" en el RII que hay dentro del campo de dirección de origen, indica que la dirección de origen va seguida de un RIF que contiene la información de direccionamiento. La Figura 10 nos permite estudiar con más detenimiento el formato del campo de dirección de origen de una trama de direccionamiento en origen.



RII = Indicador de información de direccionamiento
U/L = Bit universal o local

RII = 0 - el campo RI no se encuentra en la trama
RII = 1 - el campo RI se encuentra en la trama

Figura 10. Formato de dirección de origen 802.5

Si el RII del campo de dirección de origen está establecido en 1, significa que hay un RIF a continuación de la dirección de origen. El RIF es necesario porque facilita la información de ruta durante el direccionamiento en origen. Consta de un campo de control de direccionamiento (RC), de 2 octetos de longitud, y de una serie de campos de designador de ruta (RD), también de 2 octetos de longitud. La

Figura 11 en la página 26 nos permite estudiar con más detenimiento el formato del campo de información de direccionamiento.

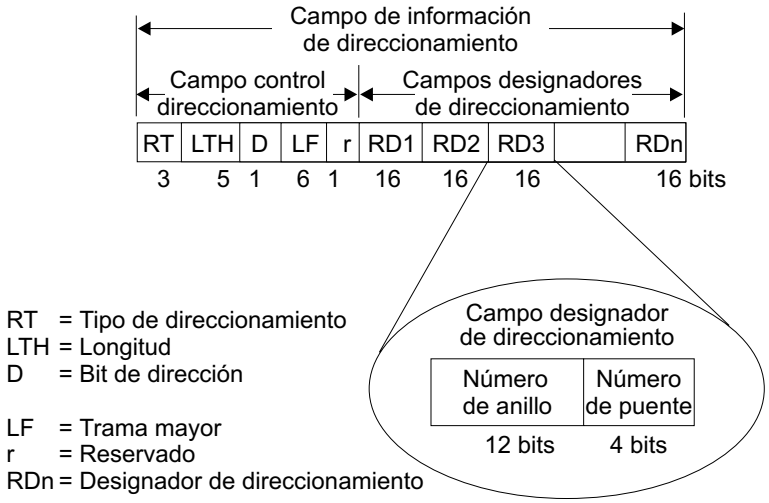


Figura 11. Campo de información de direccionamiento 802.5

A continuación, se describe cada uno de los campos del RIF:

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

  Indica por medio de valores de bit si la trama debe reenviarse a través de la red siguiendo una ruta determinada o bien siguiendo una ruta (o rutas) que llegue a todas las LAN interconectadas. En función de los valores de bit de este campo, la trama de direccionamiento en origen puede ser de los tipos siguientes:

  – Trama exploradora de todas las ruta (trama exploradora)
  – Trama exploradora del árbol de extensión (trama exploradora)
  – Trama direccionada específicamente (trama de direccionamiento)
  – Trama direccionada por árbol de extensión (trama de direccionamiento)

  Las *tramas exploradoras de todas las ruta* existen si los bits de RT están establecidos en 100. Estas tramas se generan y se direccionan siguiendo cada una de las rutas no repetitivas de la red (desde el origen hasta el destino). Este proceso da como resultado el que a la estación final de destino lleguen tantas tramas como rutas distintas haya desde la estación final del origen. Este tipo de direccionamiento se da como respuesta a la recepción de una trama de descubrimiento de ruta enviada, siguiendo el árbol de extensión y utilizando todas las rutas disponibles, a la estación emisora. Los puentes de reenvío añaden designadores de direccionamiento a la trama.

  Una *trama exploradora del árbol de extensión* existe si los bits de RT están establecidos en 110. Sólo los puentes del árbol de extensión retransmiten la trama de una red a otra. Esto significa que la trama aparece una sola vez en cada anillo de la red y, por tanto, una sola vez en la estación final de destino. Las estaciones que dan inicio al proceso de descubrimiento de ruta utilizan este tipo de trama. El puente añade campos de designador de direccionamiento a la trama. También puede servir para las tramas que se envían a las estaciones utilizando una dirección de grupo, aspecto que se trata con más detalle en el siguiente apartado.

Las *tramas direccionadas específicamente* existen si el primer bit de RT está establecido en 0. Si es este el caso, los campos de designador de ruta (RD) que contienen la información de direccionamiento concreta guían la trama en su recorrido por la red hasta la dirección de destino. Una vez que la trama ha llegado a su destino y ha descubierto una ruta, la estación de destino devuelve una trama direccionada específicamente (SRF) a la estación de origen. Entonces, la estación de origen transmite los datos en una trama direccionada específicamente.

- **Bits de longitud (LTH)**. Indica la longitud (en octetos) del campo RI.
- **Bit de sentido (D)**. Indica el sentido en que sale la trama para cruzar las redes conectadas. Si este bit está establecido en 0, la trama viaja por las redes conectadas siguiendo el orden en que están especificadas dentro del campo de información de direccionamiento (por ejemplo, de RD1 a RD2 a... a RDn). Si el bit de sentido está establecido en 1, la trama viaja por la red en sentido inverso.
- **Bits de trama más grande (LF)**. Indica el tamaño mayor de trama del campo INFO que puede transmitirse entre dos estaciones finales comunicadas por una ruta concreta. Los bits LF tienen significado sólo para las tramas STE y ARE. En las tramas direccionadas específicamente (SRF), el puente hace caso omiso de los bits LF y no puede alterarlos. Las estaciones en las que se originan tramas exploradoras establecen los bits LF en el tamaño máximo de trama que pueden manejar. Los puentes de reenvío establecen los bits LF en el valor más alto que no rebasa el mínimo de:
  - El valor indicado de los bits LF recibidos
  - El tamaño de unidad máxima de datos de servicio (MSDU) más grande al que da soporte el puente
  - El tamaño de MSDU más grande al que da soporte el puerto desde el que se ha recibido la trama.
  - El tamaño de MSDU más grande al que da soporte el puerto al que se ha de transmitir trama.

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

  La codificación de bits LF está compuesta por una codificación base de 3 bits y una codificación ampliada de 3 bits (6 bits en total). El puente SRT (explicado en un apartado posterior) contiene un indicador de modalidad LF que permite al puente seleccionar los bits LF base o los ampliados. Si el indicador de modalidad LF está definido como *modalidad base*, el puente establece los bits LF de las tramas exploradoras con los valores base de trama más grande. Si el indicador de modalidad LF está definido como *modalidad ampliada*, el puente establece los bits LF de las tramas exploradoras con los valores ampliados de trama más grande.
- **Campos de designador de ruta (RDn)**. Indican la ruta concreta por la red en función de la secuencia de campos RD. Cada campo RD contiene un número exclusivo, formado por 12 bits, de anillo de red y un número de puente, de 4 bits, que sirve para diferenciar dos o más puentes cuando éstos están conectados a los mismos anillos (puentes paralelos). El último número de puente que figura en el campo de información de direccionamiento tiene un valor nulo (todo ceros).

La opción de exploración del árbol de extensión

La función de exploración del árbol de extensión permite seleccionar una única ruta que lleve al destino, cuando la red tiene dos o más puentes que están conectados a las mismas LAN. Si se habilita esta función, sólo los puentes que seleccione recibirán las tramas exploradoras del árbol de extensión (STE). Esta opción no debe confundirse con el protocolo de árbol de extensión; permite lo siguiente:

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

Simular una red de árbol de extensión

Una red de árbol de extensión contiene una única ruta de datos entre dos estaciones finales cualesquiera. Si la red utiliza dos o más puentes paralelos, como los de la Figura 12, se puede configurar manualmente un árbol de extensión; para ello, hay que impedir la existencia de tramas de descubrimiento duplicadas en la red. Si la exploración del árbol de extensión no está habilitada, cuando la estación Q trasmita una trama de descubrimiento a la estación R, tanto el puente A como el B la retransmitirán. El segmento 2 recibirá dos copias de una misma trama.

Si la exploración del árbol de extensión está habilitada, cada segmento LAN de la red recibirá tan sólo una copia de la trama transmitida. Sólo los puentes que usted seleccione podrán recibir tramas STE, con lo que se reduce la creación de tramas redundantes y disminuye el nivel de actividad general de la red.

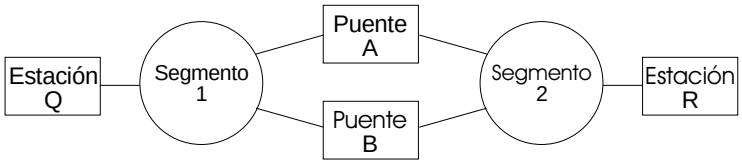


Figura 12. Ejemplo de puentes paralelos

Equilibrar las cargas de tráfico

La opción de exploración del árbol de extensión sirve también para equilibrar la carga. Por ejemplo, en la Figura 13, el puente A está configurado para aceptar tramas STE por la interfaz que le conecta al segmento 2. El puente B está configurado para aceptar tramas STE por la interfaz que le conecta al segmento 1. El tráfico viaja en el sentido de las flechas. Esta configuración permite a los puertos paralelos repartirse la carga del tráfico.

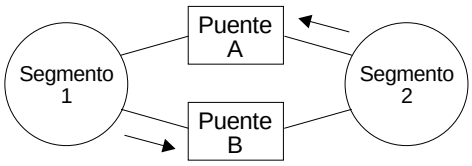


Figura 13. Utilización de la exploración del árbol de extensión para equilibrar la carga

Nota: Para que el direccionamiento en origen funcione, algunas aplicaciones de nodo final, como los programas de LAN PC, requieren que se habilite la exploración del árbol de extensión en las interfaces conectadas. En el caso de la configuración de puentes paralelos, la opción de exploración del árbol de extensión debe habilitarse solamente en una de las interfaces paralelas. Sin embargo, tampoco se producirán daños de consideración (excepto que

habrá un poco más de tráfico) si hay muchas interfaces habilitadas para el árbol de extensión.

Si utiliza la opción de exploración del árbol de extensión y cualquiera de los puentes de ruta única queda inactivo, parte del tráfico de direccionamiento en origen no podrá llegar a su destino. Tendrá que reconfigurar manualmente una ruta alternativa.

Puentes de direccionamiento en origen y Frame Relay

Si los puentes de direccionamiento en origen están habilitados, se reenvían tramas direccionadas en origen entre la interfaz Frame Relay y el reenviador de los puentes. Se puede configurar el puente para que trate el circuito virtual Frame Relay como si fuese un puerto de puente con un número de anillo exclusivo. Asimismo, los circuitos virtuales Frame Relay que no están configurados como puertos de puente pueden agruparse para formar un puerto de puente con un número de anillo exclusivo. Si desea obtener más información, consulte el apartado “En qué consisten los puertos de puente de multiacceso” en la página 55. Algunos circuitos virtuales que no forman parte de la ruta de datos activa se bloquean a fin de mantener una topología sin bucles.

Conceptos y terminología de los puentes de direccionamiento en origen

En este apartado se hace un repaso de los conceptos y los términos utilizados habitualmente al hablar de puentes de direccionamiento en 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 puente serían 1 y 2.

Las instancias de puente dentro de un solo puente son independientes y no están comunicadas entre sí. Por ejemplo, en la Figura 14, la estación A no puede pasar datos a ninguna de las estaciones de la instancia de puente 2. Sólo puede pasar tramas a la estación B. A efectos prácticos la instancia de puente permite crear dos redes separadas. Estas redes no estarán comunicadas entre sí a menos que estén físicamente interconectadas en cualquier otro punto.

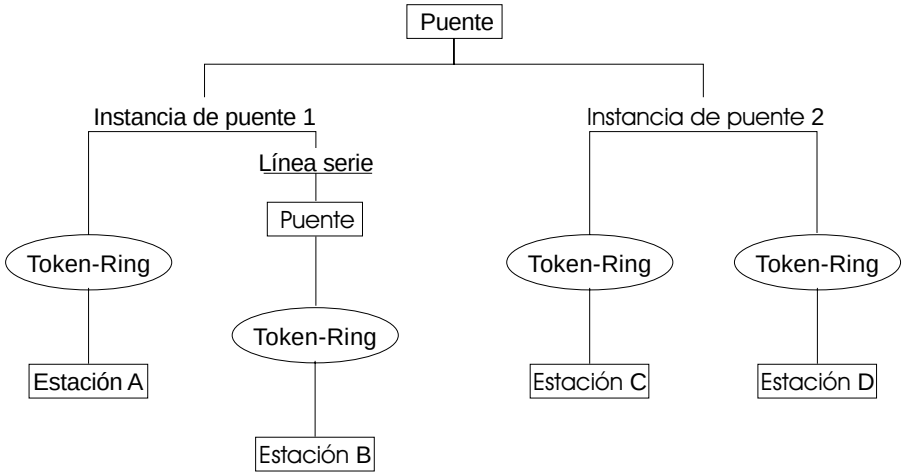


Figura 14. Instancias de puente dentro de un puente

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

Tramas exploradoras
El puente de direccionamiento en origen añade la información de direccionamiento a una trama exploradora al tiempo que reenvía la trama a través de la red hasta que esta llega a su estación final de destino. La trama exploradora sirve para descubrir rutas. Existen dos tipos de trama exploradoras: las de todas las rutas (ARE) y las del árbol de extensión (STE). Las tramas ARE las reenvían todos los puertos mientras que las tramas STE las reenvían únicamente los puertos que han sido asignados para ello por el protocolo de árbol de extensión.

Número de interfaz
El número de interfaz identifica una interfaz “física” dentro del hardware/producto y debe estar ligada a la interfaz “lógica” que un puente reconoce (es decir, un puerto). Cuando se configura el software de dispositivo, el direccionador/puente numera los puertos por orden. Para utilizar el puente de direccionamiento en origen, debe utilizar los números de puerto a fin de identificar la interfaz que conecta cada segmento de red.

Ruta
La ruta es un camino que atraviesa una serie de redes LAN y de puentes, que pueden ser, por ejemplo, puentes SRB.

Descubrimiento de ruta
El descubrimiento de ruta es el proceso por el que se averigua cuál es la ruta que lleva a una estación final de destino.

Número de segmento
El número de segmento identifica cada LAN individual, que puede ser una red en anillo o una línea serie. Los segmentos están conectados al puente, pero también pueden funcionar de manera independiente.

Direccionamiento en origen
El direccionamiento en origen es un mecanismo de puenteo que direcciona las tramas a través de una red multi-LAN especificando en la trama la ruta que debe recorrerse.

Puente transparente de direccionamiento en origen (SRT)

Después de haberse esforzado por adoptar tecnologías normalizadas (Ethernet y las redes en anillo están ambas definidas por el IEEE), es posible que se vea obligado a recurrir a tecnología exclusiva cuando intente conectarlas entre sí. Esto es así porque los puentes funcionan de distinta manera en las redes en anillo y en las Ethernet.

Dejando a un lado diferencias tales como el orden de los bits, el tamaño de los paquetes y los bits de acuse de recibo, otro obstáculo lo constituyen las diferencias de método de puenteo. Los puentes Ethernet utilizan el método de puenteo transparente, en el que los puentes determinan qué ruta seguirá el tráfico por la red.

Las redes en anillo utilizan el puenteo transparente sólo en algunos casos, de manera que, por lo general, se apoyan en el direccionamiento en origen como método principal de puenteo.

El direccionamiento en origen no funciona en un entorno transparente porque los paquetes transparentes no contienen información de direccionamiento. En este caso, el puente no tiene forma alguna de saber si ha de reenviar el paquete o no. Si bien los puentes transparentes funcionan en un entorno de direccionamiento en origen, lo hacen sin que se pase información de direccionamiento alguna a las estaciones finales. Falta la información significativa (por ejemplo, el tamaño de los paquetes), lo que constituye una fuente potencial de problemas.

El IEEE ha ratificado una ampliación de la normativa de puentes transparentes 802.1D denominada transparencia de direccionamiento en origen (SRT). SRT es una tecnología de puenteo que intenta resolver una buena parte de la incompatibilidad inherente al puenteo de redes en anillo y Ethernet. Ahorra el coste de tener que instalar varios puentes y enlaces diferentes para dar soporte a los dos tipos de tráfico y lo hace añadiendo una arquitectura de puentes paralelos (en lugar de buscar una alternativa) a la normativa de puentes transparentes.

Descripción general

Un puente transparente de direccionamiento en origen (SRT) es un puente MAC que realiza el direccionamiento en origen cuando se reciben tramas de direccionamiento en origen sin información de direccionamiento y que realiza el puenteo transparente cuando se reciben 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 a las estaciones finales.

Para distinguir entre los dos tipos de tramas, el puente SRT comprueba el valor que figura en el campo RII de la trama (en el apartado “Tramas de direccionamiento en origen” en la página 25 hallará más información). Si el valor de RII es 1, indica que la trama lleva información de direccionamiento, mientras que si es 0, indica que no. Con este método, el puente SRT reenvía tramas de puente transparente sin efectuar ninguna conversión al medio de salida (incluido red en anillo). Las tramas de direccionamiento en origen están limitadas al dominio de los puentes de direccionamiento en origen.

El protocolo y el algoritmo de árbol de extensión forman un único árbol que abarca todas las redes conectadas por puentes SRT. La red puenteada SRT ofrece un dominio mayor de puentes transparentes con un subdominio de direccionamiento en origen. Así, las tramas transparentes pueden llegar hasta el extremo más lejano de la LAN puenteada TB y SRT, mientras que las tramas direccionadas en origen están limitadas sólo a la LAN puenteada SRB y SRT. En el modelo de puentes SRT, las partes correspondientes a direccionamiento en origen y a puentes transparentes utilizan el mismo árbol de extensión. En el dominio de puentes SRT, las estaciones finales son las encargadas de responder a la cuestión de “direccionamiento en origen o puentes transparentes”.

Arquitectura y funcionamiento de los puentes transparentes de direccionamiento en origen

Con un puente SRT, cada puerto de puente recibe y transmite tramas en las redes de área local mediante los servicios MAC proporcionados por la entidad MAC individual asociada con el puerto. La entidad de retransmisión MAC se encarga de la tarea, que es independiente de MAC, de retransmitir las tramas entre los puertos de puente. Si la trama recibida no está direccionada en origen (RII = 0), la trama de puente se reenvía o se descarta utilizando la lógica de puentes transparentes. Si la trama recibida está direccionada en origen (RII = 1), se maneja en función de la lógica de direccionamiento en origen. Este proceso se ilustra en la Figura 15. Las flechas representan la ruta de los datos.

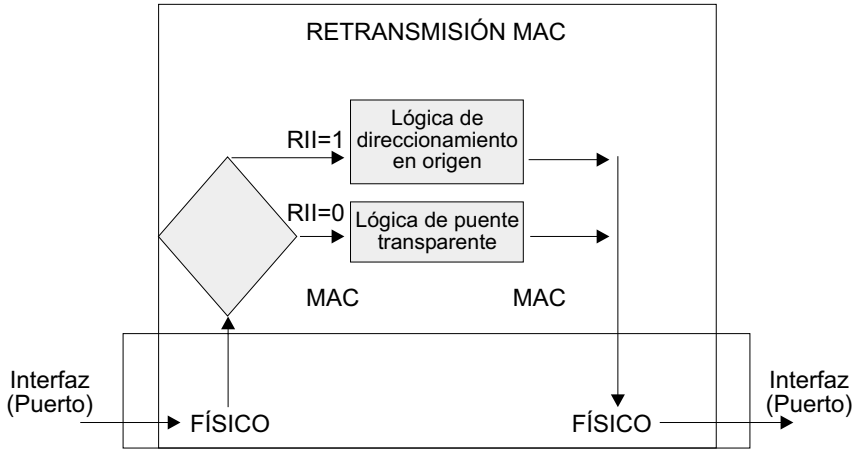


Figura 15. Funcionamiento de los puentes SRT

SRT distingue entre el tráfico direccionado en origen y el que no lo está, para cada trama. Si el paquete está direccionado en origen, el puente lo reenvía como tal. Si se trata de un paquete de puente transparente, el puente determina cuál es la dirección de destino y reenvía el paquete.

Puentes transparentes de direccionamiento en origen y Frame Relay

Si los puentes SRT están habilitados en el circuito, se reenvían tramas direccionadas en origen y tramas transparentes entre la interfaz Frame Relay y el reenviador de los puentes.

Terminología de los puentes transparentes de direccionamiento en origen

En este apartado se hace un repaso de los conceptos y los términos utilizados habitualmente al hablar de puentes SRT.

Tramas exploradoras

El puente de direccionamiento en origen añade la información de direccionamiento a una trama exploradora al tiempo que reenvía la trama a través de la red hasta que esta llega a su estación final de destino. La trama exploradora descubre rutas. Existen dos tipos de tramas exploradoras:

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

Las tramas ARE están pensadas para que las reenvíen todos los puertos mientras que las tramas STE las reenvían únicamente los puertos que han sido asignados para ello por el protocolo de árbol de extensión.

Campo de información de direccionamiento (RIF)

En el direccionamiento en origen, la decisión de reenviar las tramas de datos se toma en base a la información de direccionamiento que hay dentro de la trama. Antes de reenviar la trama, las estaciones obtienen la ruta que lleva a la estación de destino, por medio del proceso de *descubrimiento de ruta*. La estación de la que procede la trama (es decir, la estación *de origen*) designa la ruta por la que viajará la trama; para ello, intercala la descripción de la ruta en el campo de información de direccionamiento (RIF) de la trama transmitida.

Indicador de información de direccionamiento (RII)

Dado que las tramas MAC de direccionamiento en origen contienen la información de direccionamiento necesaria para las comunicaciones de datos en entornos multianillo, su formato es ligeramente distinto al de las tramas MAC de red en anillo típicas. Si figura un 1 en el campo llamado indicador de información de direccionamiento que hay dentro de la dirección de origen, indica que la dirección de origen va seguida de un campo que contiene la información de direccionamiento. El puente SRT distingue entre las tramas direccionadas en origen y las que no lo están comprobando si el valor que figura en el campo RII es 1 o 0.

Direccionamiento en origen

Mecanismo de puenteo que direcciona las tramas a través de una red multi-LAN especificando en la trama la ruta que debe recorrerse.

Árbol de extensión

Topología de puentes en la que hay una única una ruta de datos entre dos estaciones finales cualesquiera.

Puentes transparentes

Tipo de puentes que conllevan un mecanismo que resulta transparente para las aplicaciones de las estaciones finales. Los segmentos de red de área local están interconectados por medio de puentes designados para reenviar las tramas de datos mediante un algoritmo de árbol de extensión.

Visión general del puente ASRT

El puente transparente de direccionamiento en origen adaptable (ASRT) constituye una colección de software que reúne diversas opciones de puenteo. El software de puentes ASRT combina los puentes transparentes y el direccionamiento en origen de manera que ambos conceptos funcionen con independencia entre sí o bien combinados en un único puente ASRT. Esta función ampliada permite la comunicación entre una estación final estrictamente de direccionamiento en origen y una estación final transparente por medio de un puente ASRT. En función del conjunto de mandatos de configuración que se utilice, el puente ASRT ofrece las opciones de puenteo siguientes:

- Puente transparente (STB)
- Puente de direccionamiento en origen (SRB)
- Puente transparente de direccionamiento en origen adaptable (ASRT)

- Puente transparente—direccionamiento en origen (SR-TB)

El puente ASRT toma como modelo el puente transparente de direccionamiento en origen descrito en el documento IEEE 802.5M/Draft 6 (1991), que trata sobre SRT. Se han incorporado modificaciones al puente ASRT con el fin de proporcionar a los usuarios una función ampliada que va más allá del cumplimiento de la normativa SRT. El puente ASRT ofrece compatibilidad con la base instalada de puentes de direccionamiento en origen, al tiempo que les permite enlazar redes Ethernet y en anillo. ASRT también mejora el funcionamiento básico de SRT en ciertos aspectos decisivos que se describen en los siguientes apartados.

Puente transparente de direccionamiento en origen adaptable (ASRT) (conversión SR-TB)

Si bien el direccionamiento en origen está disponible en el modelo SRT, lo está únicamente entre redes en anillo de direccionamiento en origen adyacente. Los puentes de sólo direccionamiento en origen no pueden coexistir con puentes SRT que enlacen LAN Ethernet y en anillo. Dado que un nodo final de red en anillo necesita comunicarse con un nodo Ethernet, debe configurarse de manera que omita los RIF. Pero, si el nodo final está configurado para omitir los RIF, no podrá comunicarse por medio de los puentes de direccionamiento en origen ordinarios que requieren el RIF.

Descripción general

La opción puente transparente - direccionamiento en origen (SR-TB) interconecta las redes utilizando el puenteo de direccionamiento en origen (dominio de direccionamiento en origen) y el puenteo transparente (dominio de puentes transparentes). Une ambos dominios de forma transparente. Mientras está en funcionamiento, las estaciones de ambos dominios no son conscientes de la existencia de las demás ni del puente SR-TB. Desde el punto de vista de la estación, cualquier estación de la red combinada está aparentemente en su propio dominio.

El puente consigue realizar esta función convirtiendo las tramas procedentes del dominio de puenteo transparente en tramas de direccionamiento en origen antes de reenviarlas al dominio de direccionamiento en origen (y a la inversa). Esto es posible gracias a que el puente mantiene una base de datos de direcciones de estación final, cada una de ellas con su correspondiente campo de información de direccionamiento, del dominio de direccionamiento en origen. Asimismo, el puente efectúa el descubrimiento de ruta en nombre de las estaciones finales existentes en el dominio de puenteo transparente. El proceso de descubrimiento de ruta sirve para hallar la ruta que lleva a la estación de destino en el dominio de direccionamiento en origen. Las tramas enviadas a un destino desconocido se envían con el formato de exploración del árbol de extensión (STE).

El puente SR-TB prevé tres tipos de árboles de extensión:

- Un árbol de extensión formado por el dominio de puenteo transparente
- Un árbol de extensión formado por el dominio de direccionamiento en origen
- Un árbol de extensión especial que comprende todos los puentes SR-TB

En el siguiente apartado de explica más detalladamente el funcionamiento del puente SR-TB.

Funcionamiento del puente transparente-direccionamiento en origen

Mientras está en funcionamiento SR-TB, se particiona la red en una serie de dos o más dominios separados. Cada dominio está compuesto por un conjunto de segmentos LAN interconectados por medio de puentes que funcionan con un método de puenteo común. Con ello pueden crearse redes que consten de dos tipos de dominio (en función del método de puenteo):

- Dominios de direccionamiento en origen
- Dominios de puenteo transparente

La Figura 16 muestra un ejemplo de estos dominios. Dado que los dominios están separados, cada dominio de direccionamiento en origen tiene configurada para sus puentes una topología de difusión por una sola ruta. Tan sólo los puentes pertenecientes a ese *árbol de extensión* de direccionamiento en origen son designados para reenviar tramas de difusión por una sola ruta. En este caso, las tramas que llevan el indicador de difusión por una sola ruta se direccionan a todos y cada uno de los segmentos del dominio de direccionamiento en origen. A cada segmento llega una única copia de la trama porque el árbol de extensión de direccionamiento en origen no permite la existencia de varias ruta entre dos estaciones cualesquiera del dominio.

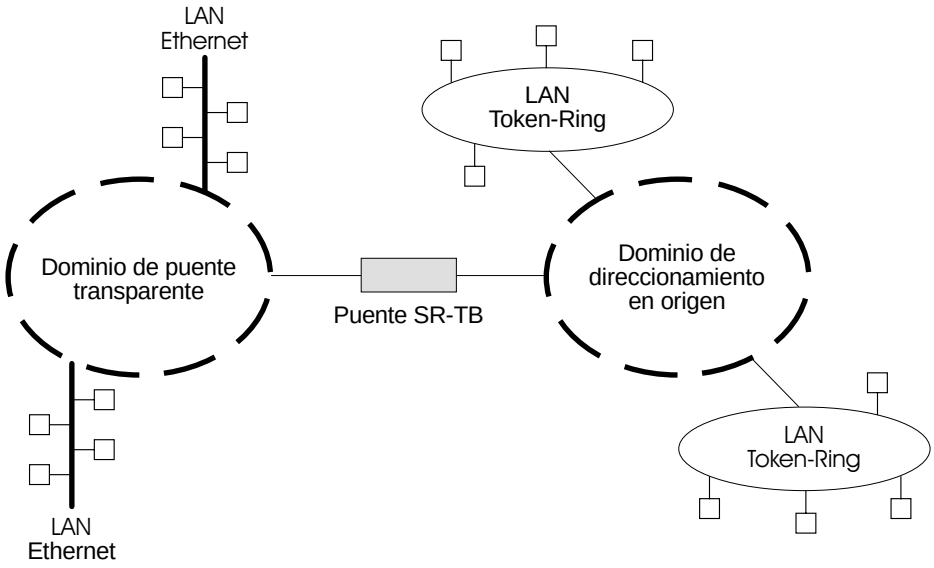


Figura 16. Puente SR-TB que conecta dos dominios

Operaciones concretas de puenteo transparente y de direccionamiento en origen

El puente SR-TB es un *dispositivo de dos puertos* con una interfaz MAC asignada al segmento LAN que se encuentra en el lado de direccionamiento en origen y otra asignada al segmento LAN que se encuentra en el lado de puenteo transparente. Cada una de las estaciones finales lee la capa MAC pertinente para su segmento LAN. Esto significa que las funciones de puenteo pueden dividirse en dos tipos de operaciones:

- Operaciones de puenteo transparente
- Operaciones de puenteo de direccionamiento en origen

En el lado de puenteo transparente, el puente SR-TB funciona como cualquier otro puente transparente. El puente posee una tabla de direcciones correspondientes a las estaciones que sabe que son estaciones de puente transparente. El puente SR-TB se rige por los protocolos *interpuente* necesarios para crear y mantener el árbol de extensión de la red porque varios puentes SR-TB unen los diferentes dominios.

El puente SR-TB reenvía las tramas recibidas desde su estación de puenteo transparente al lado de direccionamiento en origen del puente sólo si la dirección de destino que lleva la trama no figura en la tabla de direcciones del lado de puenteo transparente del puente.

En el lado de puenteo de direccionamiento en origen, el puente SR-TB combina las funciones de un puente de direccionamiento en origen y las de una estación final de direccionamiento en origen de una manera concreta. En su calidad de estación final de direccionamiento en origen, el puente mantiene una asociación de direcciones de destino e información de direccionamiento en el lado de direccionamiento en origen. Se comunica o bien como estación final de las aplicaciones del propio puente (por ejemplo, gestión de red) o bien como intermediario de las estaciones que se hallan en el lado de puenteo transparente.

El puente SR-TB reenvía las tramas recibidas desde su estación de puenteo transparente al lado de direccionamiento en origen del puente sólo si la dirección de destino que lleva la trama no figura en la tabla de direcciones del lado de puenteo transparente del puente. Las tramas transmitidas por la estación de direccionamiento en origen del puente llevan la información de direccionamiento en origen asociada al puente, si el puente conoce y mantiene dicha información.

En su calidad de puente de direccionamiento en origen, el puente SR-TB participa en el proceso de descubrimiento de ruta y en el direccionamiento de las tramas que ya llevan información de direccionamiento. El designador de ruta exclusivo del puente SR-TB consta del número de la LAN individual que se halla en el lado de direccionamiento en origen y del número individual del puente.

El puente también mantiene un número de LAN que representa todas las LAN que se encuentran en el lado de puenteo transparente. El puente SR-TB trata las tramas recibidas y reenviadas de una forma diferente en cada caso, tal como se explica en la Tabla 3.

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

Tipo de trama recibida	**Acción del puente SR-TB**
Tramas no direccionadas recibidas por la estación de direccionamiento en origen.	No copia ni reenvía las tramas que llevan información de direccionamiento.
Trama de difusión por todas las rutas recibida por la estación de direccionamiento en origen.	Copia la trama y establece los bits A y C del indicador de difusión de la trama repetida. Si la dirección de destino figura en la tabla de puenteo transparente, el puente reenvía la trama sin la información de direccionamiento en la red de puenteo transparente. Si no figura, no se reenvía la trama.

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

Tipo de trama recibida	Acción del puente SR-TB
Trama de difusión por una sola ruta recibida por la estación de direccionamiento en origen. El puente no está designado como puente de difusión por una sola ruta.	No copia ni reenvía la trama.
Trama de difusión por una sola ruta recibida por la estación de direccionamiento en origen. El puente está designado como puente de difusión por una sola ruta.	Copia la trama, establece los bits A y C del indicador de difusión, elimina la información de direccionamiento de la trama y reenvía la trama modificada al lado de puenteo transparente. Añade su número de puente a la información de direccionamiento guardada y el número de LAN correspondiente al lado de puenteo transparente. Cambia el indicador de direccionamiento para que pase a ser de no direccionamiento, complementa el bit D y almacena esta información de direccionamiento para la dirección de origen de la trama.
Trama de no difusión recibida por la estación de direccionamiento en origen.	Si la trama lleva en sí una ruta determinada, 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 en origen y el número de LAN correspondiente al lado de puenteo transparente, el puente copia la trama y establece los bits A y C de la trama repetida. Reenvía la trama al lado de puenteo transparente sin la información de direccionamiento. Si el puente no tiene todavía una ruta permanente para la dirección de origen, guarda una copia de la información de direccionamiento, complementa el bit D y almacena la información de direccionamiento guardada para la dirección de origen de la trama.
Trama recibida desde el lado de puenteo transparente.	Para reenviar la trama al lado de direccionamiento en origen, el puente determina en primer lugar si tiene información de direccionamiento asociada con la dirección de destino que lleva la trama. En caso afirmativo, el puente añade la información de direccionamiento a la trama, establece el RII en 1 y pone la trama en cola para su transmisión al lado de direccionamiento en origen. En caso negativo, el puente añade a la trama un campo de control de direccionamiento que contiene un indicador para direccionamiento por una sola ruta y dos designadores de ruta que contienen los dos primeros números de LAN y su propio número de puente individual.

Puentes SR-TB: Cuatro ejemplos

El puente SR-TB interconecta dominios de direccionamiento en origen con dominios de puenteo transparente uniéndolos de forma transparente. Mientras está en funcionamiento, las estaciones de ambos dominios no son conscientes de la existencia de las demás ni del puente SR-TB. Desde el punto de vista de la estación, cualquier estación de la red combinada está aparentemente en su propio dominio.

En los siguientes apartados se dan ejemplos concretos del reenvío de tramas mientras está en funcionamiento un puente SR-TB. En estos ejemplos se supone que el puente SR-TB está designado como puente de difusión por una sola ruta. La Figura 17 ofrece la información siguiente que acompaña a las situaciones descritas en cada apartado:

- Q es el número propio del puente
- X es el número de LAN correspondiente a la LAN que se halla en el lado de direccionamiento en origen
- Y es el número de LAN correspondiente a la LAN que se encuentra en el lado de puenteo transparente
- A, B, C y D representan estaciones finales

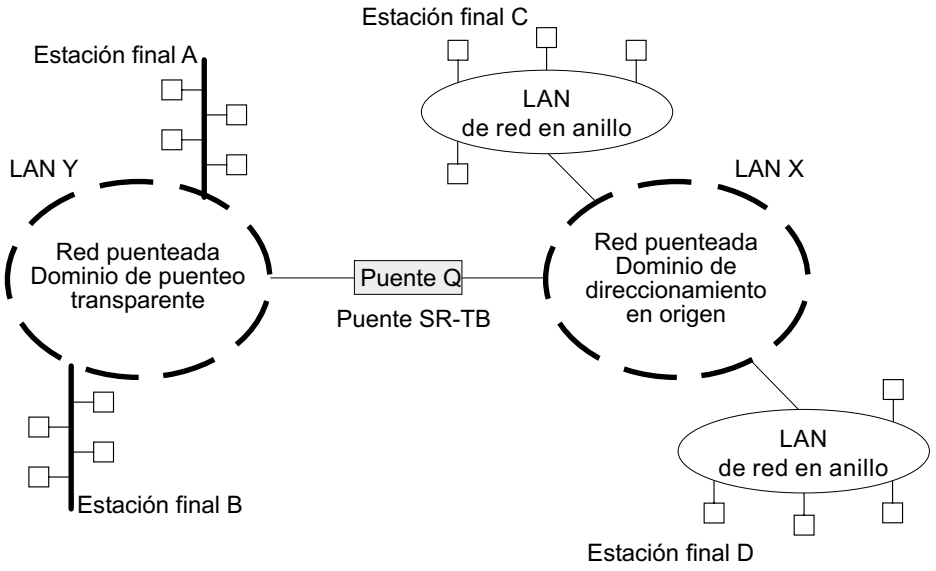


Figura 17. Ejemplos de puente SR-TB

Ejemplo 1: Trama enviada desde la estación final A a la estación final B

Cuando el puente SR-TB recibe una trama cuya dirección de origen es la estación final A y cuya dirección de destino es la estación final B, entra la dirección de la estación final A en la tabla de direcciones del lado de puenteo transparente. Esta tabla contiene las direcciones de las estaciones que se sabe que se hallan en el lado de puenteo transparente del puente, que es el proceso normal de puenteo transparente.

Si la dirección de la estación final B figura en la tabla de direcciones del lado de puenteo transparente, el puente SR-TB no reenvía la trama. Si la dirección de la estación final B no figura en la tabla de direcciones del lado de puenteo transparente ni en la tabla de direcciones del lado de direccionamiento en origen, el puente SR-TB desconoce su ubicación. En este caso, la trama se reenvía en el

lado de direccionamiento en origen como difusión por una sola ruta sin ninguna petición de devolución de exploradora de ruta. Cualquier trama que envíe la estación B (independientemente de cuál sea su destino) hace que se añada su dirección a la tabla de direcciones de puenteo transparente. Con ello se evita que en el futuro se reenvíen al lado de direccionamiento en origen las tramas dirigidas a la estación final B.

Ejemplo 2: Trama enviada desde la estación final A a la estación final C

En este ejemplo, la dirección de la estación final A recibe el mismo tratamiento que en el ejemplo anterior. Dado que la dirección de la estación final C no figurará definitivamente en la tabla de direcciones de puente transparente, el puente SR-TB direccionará la trama en el lado de direccionamiento en origen.

A continuación, el puente busca la dirección de la estación final C en su tabla de direcciones de direccionamiento en origen. Esta tabla contiene todas las direcciones conocidas con información de direccionamiento relacionada para las estaciones que se sabe están en el lado de direccionamiento en origen del puente. Si la dirección de C figura en la tabla de direccionamiento en origen, el puente reenvía la trama utilizando la información de direccionamiento que hay en la tabla. Si la dirección de C no figura en la tabla de direccionamiento en origen (o si aparece pero tiene una información de direccionamiento nula), el puente reenvía la trama en el lado de direccionamiento en origen como difusión por una sola ruta sin ninguna petición de devolución de exploradora de ruta.

Cuando la estación final C recibe esta trama, entra la dirección de la estación final A en su tabla de direccionamiento en origen junto con el sentido inverso de la ruta construida a partir del puente SR-TB y la marca como entrada temporal. Posteriormente, cuando la estación final C intente enviar una trama a la estación final A, utilizará esta ruta específica y, dado que la ruta está marcada como temporal, la trama se enviará como ruta de no difusión *con* una petición de devolución de exploradora de ruta.

Cuando la trama de retorno llega al puente SR-TB, se reenvía en el lado de puenteo transparente sin información de direccionamiento, pero hace que la ruta que lleva a la estación final C se entre en la tabla de direccionamiento en origen como ruta temporal. Esto, a su vez, hace que la entidad de gestión de red envíe una trama exploradora de ruta con una difusión por todas las rutas que llevan de vuelta a la estación final C. Esto permite a la estación final C seleccionar el direccionamiento óptimo para las tramas dirigidas a la estación final A con el fin de entrarlo como ruta permanente en la tabla de direccionamiento en origen del puente SR-TB.

Ejemplo 3: Trama enviada desde la estación final C a la estación final D

Si la trama que se envía es de no difusión y atraviesa el segmento al que está conectado el puente SR-TB, éste examina el campo RII en busca de la secuencia de direccionamiento (de la LAN X al puente Q a la LAN Y). No podrá hallar la secuencia y, en consecuencia, no reenviará la trama.

Si la trama que se envía es de difusión por una sola ruta, el puente descartará la trama si se sabe que la estación D se encuentra en el lado de direccionamiento en origen. Si no se sabe que la estación D se halla en el lado de direccionamiento en origen, el puente reenvía la trama al lado de puenteo transparente (sin la infor-

mación de direccionamiento) y añade “de Q a Y” a la información de direccionamiento. Por último, guarda la información de direccionamiento correspondiente a la estación final C como ruta temporal de la tabla de direccionamiento en origen con un indicador de no difusión y el bit de sentido complementado.

Si la trama enviada es de difusión por todas las rutas, el puente SR-TB la descarta (porque la dirección de la estación final D no figura en la tabla de direcciones de puenteo transparente) y se asegura de que la dirección de la estación final C figura en la tabla de direccionamiento en origen.

Ejemplo 4: Trama enviada desde la estación final C a la estación final A

Si la trama que se envía es de no difusión, el puente examina el campo RII en busca de la secuencia de direccionamiento (de X a Q a Y). Cuando la encuentra, reenvía la trama al lado de puenteo transparente. También almacena la información de direccionamiento correspondiente a la estación final C.

Si la trama que se envía es de difusión por una sola ruta, el puente reenvía la trama (sin la información de direccionamiento) al lado de puenteo transparente y añade “de Q a Y” a la información de direccionamiento. También establece el indicador de no difusión, complementa el bit de sentido y entra la información de direccionamiento correspondiente a la dirección de C en su tabla de direccionamiento en origen.

Si ya existe una entrada temporal para la estación final C en la tabla de direccionamiento en origen, el puente SR-TB actualiza la información de direccionamiento. Si la trama enviada es de difusión por todas las rutas, el puente SR-TB la descarta pero se asegura de que la dirección de la estación final C figura en la tabla de direccionamiento en origen.

SR-TB y Frame Relay

La interfaz Frame Relay da soporte a los puentes SR-TB reenviando todas las tramas enviadas por puente al reenviador de puenteo pertinente siempre y cuando el puenteo esté habilitado en el circuito.

Conceptos y terminología de los puentes transparentes-direccionamiento en origen (SR-TB)

En este apartado se describen los conceptos y términos que se utilizan al hablar de puentes SR-TB.

Difusión por todas las rutas

Proceso por el que se envía una trama a través de cada una de las rutas que no se repiten de la LAN punteada.

Difusión a todas las estaciones

Proceso por el que se dirige una trama (estableciendo en 1 todos los bits de la dirección de destino) de manera que la copian todas y cada una de las estaciones del anillo en el que aparece la trama.

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

Número de puente
Número exclusivo que identifica un puente. Distingue entre sí varios puentes que se conectan a los mismos anillos.

Tramas exploradoras
El puente de direccionamiento en origen añade la información de direccionamiento a una trama exploradora al tiempo que reenvía la trama a través de la red hasta que esta llega a su estación final de destino. La trama exploradora descubre rutas. Existen dos tipos de trama exploradoras: las de todas las rutas (ARE) y las del árbol de extensión (STE). Las tramas ARE las reenvían todos los puertos mientras que las tramas STE las reenvían únicamente los puertos que han sido asignados para ello por el protocolo de árbol de extensión.

Número de anillo
Número exclusivo que identifica un anillo de una red puenteada.

Ruta
Camino que atraviesa una serie de redes LAN y de puentes (que pueden ser, por ejemplo, puentes de direccionamiento en origen).

Designador de ruta
Número de anillo y número de puente que figuran en el campo de información de direccionamiento utilizado para construir una ruta a través de la red.

Descubrimiento de ruta
Proceso por el que se averigua cuál es la ruta que lleva a una estación final de destino.

Número de segmento
Número que identifica cada LAN individual, que puede ser una red en anillo o una línea serie. Los segmentos están conectados al puente, pero también pueden funcionar de manera independiente.

Difusión por una sola ruta
Proceso por el que se envía una trama a través de una red de manera que en cada uno de los anillos de la red aparezca exactamente una sola copia de la trama.

Puentes de direccionamiento en origen
Mecanismo de puenteo que direcciona las tramas a través de una red multi-LAN especificando en la trama la ruta que debe recorrerse.

Árbol de extensión
Topología de puentes en la que hay una única ruta de datos entre dos estaciones finales cualesquiera.

Puentes transparentes
Tipo de puente que conlleva un mecanismo que resulta *transparente* para las aplicaciones de las estaciones finales. Los segmentos de red de área local están interconectados por medio de puentes designados para reenviar las tramas de datos mediante un algoritmo de árbol de extensión.

Compatibilidad entre transparencia y direccionamiento en origen - problemas y soluciones

En primer lugar, el puente ASRT proporciona compatibilidad de puente transparente con los puentes de direccionamiento en origen normales por medio de la conversión de puente de direccionamiento en origen (SR-TB). Originariamente, se propuso SR-TB como parte de la especificación 802.5. Esta implementación es similar y puede interoperar con el puente de conversión 8209 de IBM.

SR-TB convierte las tramas de puenteo transparente en tramas de direccionamiento en origen y a la inversa. Dicho de otra manera, en lugar de únicamente comprobar si existe un RIF en un paquete y reenviarlo a tal destino, el puente ASRT puede convertir el paquete a cualquiera de los dos formatos; funciona o bien como puente transparente o bien como puente de direccionamiento en origen insertando o eliminando un RIF, según convenga. Con esta función, los paquetes pueden desplazarse entre las LAN en anillo SRT y Ethernet y seguir siendo compatibles con la base instalada de las LAN en anillo de direccionamiento en origen.

Eliminación de los problemas de tamaño de paquete
SR-TB también elimina los problemas de tamaño de paquete en las redes en anillo que se puentean juntas atravesando un dominio Ethernet. En esta configuración, las estaciones finales utilizan el protocolo de direccionamiento en origen, que les permite determinar dinámicamente que entre ellas hay una red cuyo tamaño máximo de trama es de 1518 bytes. La estación final respeta automáticamente este límite sin reconfiguración manual. En la situación inversa, puentear redes Ethernet atravesando un dominio de red en anillo, el tamaño de paquete no supone ningún problema porque la tolerancia de tamaño de paquete de las redes en anillo es mucho mayor.

Filtrado de direcciones de hardware
Otra característica clave que proporciona el puente ASRT es el filtrado de direcciones de hardware, que resuelve el conflicto entre métodos de acuse de recibo de paquete existente en las tecnologías LAN en anillo y Ethernet. Tiene lugar en la capa MAC y es la única técnica que establece con precisión los bits de acuse de recibo en base a la dirección MAC de destino. El puente ASRT utiliza memorias direccionables por contenido (CAM) para implementar el filtrado de direcciones de hardware. Esta tecnología da al puente un alto nivel de inteligencia al proporcionar una consulta instantánea de las direcciones MAC sin crear ninguna merma de rendimiento.

Orden de los bits en los puentes STB y SRB

Dado que los puentes se construyen continuamente para conectar las LAN con distintos tipos de direcciones MAC, el orden de los bits en la transmisión de los datos afecta a la interoperabilidad de estas tecnología.

A la hora de administrar las direcciones MAC, IEEE asigna direcciones denominadas direcciones MAC exclusivas asignadas globalmente por IEEE de 48 bits. Estas direcciones están soportadas por las LAN 802.3, 802.4 y 802.5. La falta de normativas que existía en el momento en que se desarrolló este esquema de direcciones ha dado lugar a dos situaciones distintas:

- Las LAN 802.3 (Ethernet) y 802.4 transmiten las direcciones de origen y de destino poniendo el bit de grupo en primer lugar, y los campos de datos LLC poniendo el bit menos significativo (LSB) en primer lugar.
- Las LAN 802.5 (en anillo) transmiten las direcciones de origen y de destino poniendo el bit de grupo en primer lugar, y los campos de datos LLC poniendo el bit más significativo (MSB) en primer lugar.

Nota: Para simplificar, las LAN y los puentes 802.3 y 802.4 recibirán en lo sucesivo el nombre de LAN y puentes LSB. Las LAN y los puentes 802.5 recibirán el nombre de LAN y puentes MSB.

La diferencia que existe en la normativa de transmisión de bits significa que un puente que va de una LAN LSB a una LAN MSB tiene que invertir el orden de los bits de las direcciones de origen y de destino al inicio de la trama MAC. La razón es que los distintos tipos de LAN utilizan el mismo orden de bits para la dirección MAC (es decir, primero el bit de grupo) y, en cambio, un orden de bits diferente para los datos de usuario (primero LSB o bien MSB).

Los errores de interpretación de las direcciones debido a la inversión del orden de los bits se ven aumentados por el hecho de que algunos protocolos de comunicaciones de alto nivel interpretan de una manera totalmente equivocada las direcciones MAC. Los protocolos como IP y Novell IPX interpretan las direcciones de puenteo incorrectamente porque en el momento de su desarrollo inicial no existía ninguna representación estándar de las direcciones MAC.

El diferencial del orden de bits se resuelve mejor combinando la tecnología de puentes (tecnología de capa de enlace de datos) con la tecnología de direccionamiento (tecnología de capa de red). En lugar de pedir al usuario que “realice operaciones de ingeniería inversa” en los protocolos de comunicaciones actuales y que configure cada uno de los puentes para que “dé la vuelta” o invierta las direcciones caso por caso, el problema se resuelve más fácilmente direccionando los protocolos.

El direccionamiento elimina los problemas de direcciones de protocolo y de orden de los bits mediante el acceso a las direcciones detalladas de paquete que circulan por la capa superior. El direccionamiento por sí solo no es una solución completa porque otros protocolos como IBM Frames y NetBIOS no pueden direccionarse y el direccionamiento de SNA es limitado. Por lo tanto, es importante implementar SRT en un dispositivo en el que los puentes y el direccionamiento trabajen conjuntamente.

Consideraciones en torno a la configuración de ASRT

El puente ASRT utiliza el algoritmo y el protocolo de árbol de extensión descritos en la normativa de puentes IEEE 802.1D en todas las interfaces. Es posible que se forme más de un árbol de extensión en un entorno en el que existan distintos tipos de puentes. Por ejemplo, puede existir un árbol de extensión que abarque todos los puentes que practiquen el protocolo 802.1d de IEEE (por ejemplo, STB y SRT) junto con otro árbol de puentes IBM 8209. Los bucles que surgen a partir de esta configuración hacen necesario corregir la situación.

Los servicios de sistema principal TCP/IP dan soporte a la retransmisión SDLC. Cuando se ejecutan como puente puro, y no como direccionador IP, las funciones normalmente asociadas con un direccionador IP no están disponibles. Por ejemplo, no existe ninguna función de reenviador BootP ni ninguna función de direccionamiento de subred ARP.

Matriz de configuración de ASRT

Con un puente ASRT, la colección de parámetros de configuración del puente y todas las interfaces dan lugar a la *personalidad* de dicho puente. La matriz siguiente constituye una guía de los valores de configuración que se necesitan para que cada tipo de interfaz de lugar a la personalidad de puente deseada a fin de manejar la red.

Personalidad de puente	**¿Conversión SR <-> TB habilitada?**	**Tipo de interfaz y valor de método de puenteo**			
		Red en anillo	**Ethernet**	**Túnel o línea serie**	
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 extensión)
SRB = puente de direccionamiento en origen
SR-TB = puente de conversión transparente de direccionamiento en origen
SRT = puente transparente de direccionamiento en origen
ASRT = puente transparente de direccionamiento en origen adaptable

Clave de método de puenteo:

SR = direccionamiento en origen TB = puentes transparentes

Funciones de puenteo

Este capítulo describe las funciones de puenteo que están disponibles con el puente transparente de direccionamiento en origen adaptable (ASRT). Consta de los siguientes apartados:

Túnel de puente

El túnel de puente (encapsulación) es otra función del software de puente ASRT. Al encapsular paquetes en paquetes TCP/IP estándar del sector, el dispositivo de puente puede direccionar de manera estos paquetes de manera dinámica a través de redes de Internet a 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 paliar el límite de distancia de 7 saltos habitual que se encuentra en configuraciones de direccionamiento en origen. Le permite también conectar estaciones finales de direccionamiento en origen en medios de direccionamiento no origen, como pueden ser redes Ethernet.

El túnel de puente también palia las graves limitaciones del direccionamiento en origen normal, que son:

- Las limitaciones de distancia de siete saltos
- El elevado nivel de actividad general que el direccionamiento en origen causa en redes de área amplia (WAN)
- La sensibilidad del direccionamiento en origen ante errores y anomalías de WAN (si falla una vía de acceso, todos los sistemas deben reiniciar sus transmisiones)

Teniendo la función de túnel de puente habilitada, el software encapsula paquetes en paquetes TCP/IP. Por lo que se refiere al dispositivo, el paquete tiene el aspecto de un paquete TCP/IP. Una vez se ha encapsulado una trama en un sobre IP, el reenviador IP es responsable de la selección de la interfaz de red adecuada según la dirección IP de destino. Este paquete se debe direccionar de manera dinámica a través de redes de internet grandes sin degradación o restricciones de tamaños de red. Las estaciones finales ven la vía de acceso o el túnel como un solo salto, independientemente de la complejidad de la red de internet. La Figura 18 en la página 46 muestra un ejemplo de una red de internet IP mediante la función de túnel de su configuración.

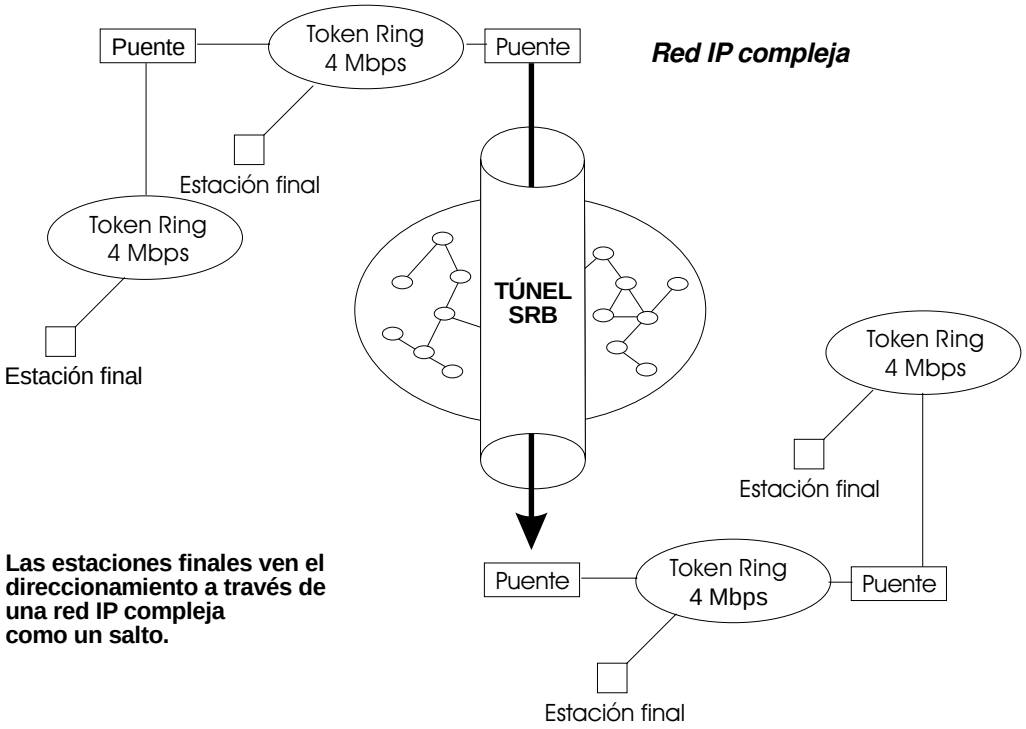


Figura 18. Ejemplo de la Función de túnel de puente

El túnel es transparente para las estaciones finales. Los dispositivos de puente que participan en túneles tratan a la internet IP como uno de los segmentos de puente. Cuando el paquete alcanza la interfaz de destino, las cabeceras TCP/IP se eliminan de manera automática y el paquete interno continúa trabajando como si fuera un paquete de direccionamiento en origen estándar.

Encapsulación y OSPF

Uno de las principales ventajas de la función de encapsulación es la adición del protocolo de direccionamiento dinámico OSPF al proceso de direccionamiento. OSPF ofrece las siguientes ventajas cuando se utiliza con encapsulación:

- *Direccionamiento de menor coste*. OSPF accede a la vía de acceso más rápida (túnel) con los intervalos de retraso más bajos, lo que permite que los administradores de red distribuyan tráfico por la ruta menos cara.
- *Direccionamiento dinámico*. OSPF busca la vía de acceso de menor coste y detecta también anomalías y redirecciona tráfico con gastos generales bajos.
- *Direccionamiento de varias vías de acceso*. El compartimiento de carga hace más eficaz el uso del ancho de banda disponible.

Con OSPF, los túneles gestionan automáticamente vías de acceso dentro de la red de internet. Si una línea o un puente falla a lo largo de la vía de acceso, el puente de túnel redirecciona de manera automática el tráfico a lo largo de una nueva vía de acceso. Si se restaura una vía de acceso, el túnel se actualiza de manera automática a la mejor vía de acceso. Este redireccionamiento es completamente transparente para las estaciones finales. Si desea obtener más información sobre OSPF, consulte los capítulos de configuración y supervisión empezando por “Utilización de OSPF” en la página 363.

TCP/IP Host Services (gestión sólo de puentes)

El IBM 2212 da soporte también a TCP/IP Host Services, lo que permite configurar y supervisar un puente cuando se inhabilitan las funciones de direccionamiento. Esta opción le ofrece las siguientes posibilidades:

- Gestión a través de SNMP
- Función de servidor Telnet
- Bajada y subida de configuraciones a través del protocolo TFTP
- Función de arranque desde vecino TFTP
- Herramientas de diagnóstico IP: ping y rastreo de ruta
- Control del dispositivo a través de conjuntos SNMP y el cliente Telnet

Visto desde la interfaz de supervisión del puente, TCP/IP Host Services se maneja como un nuevo protocolo que dispone de sus propios indicadores de configuración y de supervisión. Se accede a estos indicadores a través del mandato **protocol** de `talk 6` y `talk 5`.

La función de gestión sólo de puentes se activa asignando una dirección IP al puente y habilitando los TCP/IP Host Services (consulte el “Configuración y supervisión de TCP/IP Host Services” en la página 221). Esta dirección IP se asocia con el puente como conjunto, en lugar de asociarse con una sola interfaz. Cuando se arranca en la red, se pueden conocer automáticamente la dirección IP del puente y una pasarela por omisión a través de la interfaz ROMCOMM con los PROM de arranque. El usuario también puede configurar las asignaciones de pasarela por omisión.

TCP/IP Host Services está disponible cuando los puentes son una opción de la carga de software de dispositivo.

Soporte de MIB de puentes

Por lo que se refiere a la gestión de puentes a través de SNMP, el IBM Access Integration Services ofrece soporte a todas las bases de información de gestión (MIB), tal y como especifica en los documentos RFC 1493 y RFC 1525, ***excepto*** las siguientes:

- dot1dStaticTable
- dot1dTpFdbTable
- dot1dPortPairTable

Antememoria de nombres de NetBIOS

La función de antememoria de nombres de NetBIOS permite que el dispositivo de puente reduzca de manera significativa el número de tramas Name-Query que dejan un anillo de origen y que se reenvían a través de un puente. La configuración de la antememoria de nombres de NetBIOS es parte de la configuración de NetBIOS. Encontrará más detalles al respecto en “Antememoria de nombres y antememoria de rutas NetBIOS” en la página 159.

Filtro de tramas duplicadas de NetBIOS

Habitualmente se envían tres tipos de tramas en grupos de seis:

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

El filtro de tramas duplicadas utiliza un temporizador para que se pueda reenviar sólo una instancia de cada tipo de trama a través del puente en el tiempo establecido por el usuario.

Este proceso utiliza una base de datos independiente de la que se utiliza en la antememoria de nombres. Las entradas de bases de datos duplicadas contienen la dirección MAC del cliente y tres impresiones de la hora, una para cada una de los tipos de trama mencionados. El filtro de tramas duplicadas se procesa antes de la antememoria de nombres. Encontrará más detalles al respecto en “Filtro de tramas duplicadas” en la página 151.

Filtros por nombre y por bytes de NetBIOS

El filtro de NetBIOS es una función que le permite mejorar el rendimiento del puente ASRT. Gracias a dicha función puede configurar filtros específicos mediante el proceso de configuración de dispositivos. Los filtros de NetBIOS son conjuntos de reglas aplicadas a paquetes de NetBIOS que determinan si los paquetes se deben enviar a través del puente (reenviar) o se deben filtrar (eliminar).

Tipos de filtro de NetBIOS

Existen dos tipos de filtro de NetBIOS, *por nombre de sistema principal* y *por bytes*:

Por nombre de sistema principal Los filtros por nombre de sistema principal se implementan utilizando aquellos campos de los paquetes de NetBIOS que permiten seleccionar paquetes con nombres de sistema principal de NetBIOS específicos para enviarlos por puente o filtrarlos. Los filtros por nombre de sistema principal sólo sirven a efectos de puenteo. Se pueden utilizar en base a un origen NetBIOS o a nombres de destino, dependiendo del tipo de trama.

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

Por bytes Los filtros por bytes se implementa utilizando los bytes (campos arbitrarios) de los paquetes de NetBIOS que permiten especificar que ciertos paquetes de NetBIOS se deben enviar por el puente o bien filtrar.

Estos filtros no tienen asociado ningún umbral ni temporizador y permanecerán activos hasta que los inhabilite o los elimine. Un filtro de NetBIOS consta de tres partes: el filtro real, las listas de filtro y los elementos de filtro (que se describen con más detalle en el apartado “Creación de un filtro” en la página 50).

La configuración y la supervisión de NetBIOS se describe en el “Configuración y supervisión de NetBIOS” en la página 171. El resto de esta sección describe el filtro por nombre de sistema principal de NetBIOS y el filtro por bytes de NetBIOS.

Filtro por nombre de sistema principal de NetBIOS

El filtro de NetBIOS mediante nombres de sistema principal permite seleccionar paquetes con nombres de sistema principal de NetBIOS específicos para enviarlos por puente o bien filtrarlos. Cuando se especifica que los paquetes con un nombre de sistema principal de NetBIOS concreto (o conjunto de nombres de sistema principal de NetBIOS) se deben filtrar o se deben enviar por puente, se examinan los campos de nombre origen y nombre destino de los tipos de paquetes de NetBIOS siguientes:

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

Las listas de filtro por nombre de sistema principal especifican los nombres de NetBIOS que se deben comparar con los campos de nombres origen o destino en los cuatro tipos de paquetes de NetBIOS. El resultado de aplicar una lista de filtro por nombre de sistema principal a un paquete de NetBIOS que no pertenece a ninguno de esos cuatro tipos es *Inclusivo*.

Cuando se configura el filtro de NetBIOS mediante nombres de sistema principal, se debe especificar los puertos a los que se aplica el filtro y si éste se aplica para entrada o salida de paquetes en dichos puertos. Sólo se tienen en cuenta para el filtro los paquetes de información no numerada (UI) de NetBIOS. El filtro se aplica a paquetes de NetBIOS que llegan al dispositivo para su envío por puente de direccionamiento en origen (todos los tipos RIF) o por puente transparente.

Cuando se especifica un nombre de sistema principal de NetBIOS en un filtro, puede indicar el 16 carácter del nombre (el último) como argumento independiente en su formato hexadecimal. Si lo hace, los 15 primeros bytes del nombre se toman tal y como están especificados y el 16 byte (si se especifica) lo determina el argumento final. Si especifica menos de 16 caracteres (y ningún 16 byte), el nombre se rellena con caracteres en blanco ASCII hasta alcanzar los 15 caracteres y el 16 se trata como si fuese un comodín.

Cuando se evalúa un nombre de sistema principal de NetBIOS específico, ese nombre se compara sólo con ciertos campos de ciertos paquetes de NetBIOS. Los nombres de sistema principal de NetBIOS que figuran en elementos de filtro pueden incluir un carácter comodín (?) en cualquier punto, o un asterisco (*) como carácter final. El carácter ? se compara con todos y cada uno de los caracteres individuales de un nombre de sistema principal. El carácter * se compara con uno o varios de los caracteres finales de un nombre de sistema principal.

Filtro por bytes de NetBIOS

Otro mecanismo de filtro, el filtro por bytes, permite especificar los paquetes de NetBIOS que se deben filtrar o enviar por puente tomando como base los campos de los paquetes de NetBIOS que están relacionados con la dirección MAC. En este caso, todos los paquetes de NetBIOS se examinan para determinar si coinciden con los criterios de filtro configurados.

Para crear un filtro por bytes, especifique los elementos de filtro siguientes:

- Un desplazamiento desde el inicio de la cabecera de NetBIOS
- Un patrón de coincidencia de bytes

- Una máscara opcional a aplicar a los campos seleccionados de la cabecera de NetBIOS

La longitud de la máscara, si está presente, debe ser de la misma longitud que el patrón de bytes. La máscara especifica los bytes que deben unirse por medio del operador AND lógico con los bytes de cabecera de NetBIOS antes de que el dispositivo compare los bytes de cabecera con el patrón hexadecimal para encontrar bytes iguales. Si no se especifica ninguna máscara, se supondrá que son todas. La longitud máxima del patrón hexadecimal (y por lo tanto de la máscara) es de 16 bytes (32 dígitos hexadecimales).

Cuando se configura el filtro de NetBIOS mediante bytes específicos, también se especifican los puertos a los que se aplica el filtro y si se aplica a los paquetes de entrada o salida en esos puertos.

Creación de un filtro

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

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

- Envia por puente el paquete si la lista de filtro está especificada como *inclusiva*
- Elimina el paquete si la lista de filtro está especificada como *exclusiva*

Si ningún elemento de filtro de la lista de filtro genera una coincidencia, el dispositivo:

- Reenvía el paquete si todo el filtro está especificado como *inclusivo*
- Elimina el paquete si todo el filtro está especificado como *exclusivo*

Un elemento de filtro es una regla individual aplicada a un campo concreto de un paquete de NetBIOS. El resultado de la aplicación de la regla es una indicación inclusiva (puente) o exclusiva (filtro). Los siguientes elementos de filtro se pueden configurar con el filtro de NetBIOS (los dos primeros elementos son filtros por nombre de sistema principal, los dos últimos elementos son filtros por bytes):

- Incluir el 16 carácter (hexadecimal) opcional de nombre de sistema principal de NetBIOS
- Excluir el 16 carácter (hexadecimal) opcional de nombre de sistema principal de NetBIOS
- Incluir el desplazamiento de bytes decimales en el patrón hexadecimal de cabecera de NetBIOS empezando por la máscara hexadecimal de desplazamiento
- Excluir el desplazamiento de bytes decimales del patrón hexadecimal de cabecera de NetBIOS empezando por la máscara hexadecimal de desplazamiento

Parte de la especificación de un filtro indica si los paquetes que no coinciden con ninguno de los elementos de filtro de la lista de filtro deben enviarse por puente (incluirlos) o bien filtrarse (excluirlos). Ésta es la acción por omisión de la lista de filtro. La acción por omisión de una lista de filtro es, inicialmente, la de inclusión, pero el usuario puede cambiar este valor.

Filtros simples y complejos

Un filtro simple se construye 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 de NetBIOS que se reciban o se transmitan en el puerto determinado. Si la evaluación de la lista de filtro es incluir, el paquete que se está examinando se envía por el puente. De lo contrario, el paquete se filtra.

Un filtro complejo se puede construir especificando un número de puerto, una designación de entrada/salida y varias listas de filtro separadas por el operador lógico AND o bien OR. Las listas de filtro que componen un filtro complejo se evalúan de izquierda a derecha, y se evalúan todas y cada una de ellas. Si el resultado de una lista de filtro es incluir, se interpreta como verdadero; y si es excluir, se interpreta como falso. El resultado de aplicar todas las listas de filtro y sus operadores a un paquete es verdadero o falso, lo que indica que el paquete se envía por puente o que se filtra. Cada combinación de entrada/puerto o salida/puerto puede tener como máximo de un filtro.

Varias opciones de protocolo de árbol de extensión

El puente ASRT le permite ampliar las opciones de protocolo de árbol de extensión para cubrir tantas opciones de configuración como sea posible. Las siguientes secciones ofrecen información sobre dichas funciones.

Fondo: Problemas con varios protocolos de árbol de extensión

La tecnología de puentes emplea diferentes versiones de algoritmos de árbol de extensión para dar soporte a diferentes métodos de puenteo. El objetivo común de cada algoritmo es producir una topología sin bucles.

En el algoritmo de árbol de extensión que utilizan los puentes transparentes (TB), se envían BPDU Hello y BPDU de notificación de cambio de topología (TCN) en una trama transparente a direcciones de grupos conocidas públicamente de todos los medios participantes (red en anillo, Ethernet, etc). Se crean tablas a partir de esta información intercambiada y se calcula una topología sin bucles.

Los puentes de direccionamiento en origen (SRB) transmiten tramas exploradoras del árbol de extensión (STE) por otros SRB a fin de determinar una topología sin bucles. El algoritmo envía BPDU Hello en una trama transparente a direcciones funcionales conocidas públicamente. Como los SRB no utilizan BDPU TCN, el valor del estado del puerto creado como resultado de este algoritmo de árbol de extensión no afecta a la trama exploradora de todas las rutas (ARE) y al tráfico de trama direccionado específicamente (SRF).

En las configuraciones de puente IBM 8209, se utiliza un método de árbol de extensión diferente para detectar puentes IBM 8209 paralelos. Dicho algoritmo utiliza BPDU Hello enviadas como tramas STE a direcciones de grupos IEEE 802.1d de la red en anillo. En Ethernet, se utilizan BPDU Hello enviadas como tramas a la misma dirección de grupo. Este método permite que los 8209 creen árboles de extensión con puentes transparentes y otros puentes IBM 8209. Sin embargo, no participa en el protocolo de árbol de extensión de SRB y las BPDU Hello enviadas por los SRB se filtran. Por lo tanto, no hay manera de evitar que el 8209 se convierta en el puente raíz. Si el puente 8209 se *selecciona* como raíz,

puede que el tráfico entre dos dominios de puente transparente deba pasar a través de dominios de red en anillo/SRB.

Como puede comprobar, la ejecución de protocolos de varios árboles de extensión puede ocasionar problemas de compatibilidad con la manera con la que el algoritmo crea su propia topología sin bucles.

STP/8209

La función de puentes STP/8209 se encuentra disponible para permitirle ampliar más el protocolo de árbol de extensión. Antes los SRB sólo permitían la configuración manual de un árbol sin bucles en la red en anillo. Era el único mecanismo que evitaba los bucles en el caso de puentes SR-TB paralelos. Con la adición de la función STP/8209 son posibles las siguientes combinaciones de algoritmos de árbol de extensión:

- Puente transparente (TB) puro - se utiliza el protocolo de árbol de extensión IEEE 802.1d.
- Puente de direccionamiento en origen (SRB) puro - se utiliza el protocolo de árbol de extensión SRB.
- Puentes transparentes y de direccionamiento en origen como entidades independientes - se utiliza el protocolo de árbol de extensión IEEE 802.1d para TB y la configuración manual (sin protocolo de Árbol de extensión) para SRB.
- Puente SR-TB - se utiliza el protocolo de árbol de extensión IEEE 802.1d para los puertos TB y las BBDU de IBM 8209 en puertos SRB para formar un sólo árbol de TB y SR-TB. Las BPDU Hello de SRB pueden pasar al dominio SR pero no se procesan. Los puentes IBM 8209 filtran estas tramas pero esto se puede realizar porque se trata de un puente de dos puertos en el que el otro puerto es un puerto TB.
- Puente SRT puro - ***Sólo*** se utiliza el protocolo de árbol de extensión IEEE 802.1d. Las BPDU Hello SRB y las BPDU de IBM 8209 pueden pasar pero no se procesan.
- Puente ASRT - se utiliza el protocolo de árbol de extensión IEEE 802.1d para crear un árbol con puentes TB y SRT. Se generan también BPDU “similares a los 8209” en todas las interfaces SR. Estas BPDU se procesan tan pronto como se reciben. Esto hace que se generen y que se reciban dos BPDU en todas las interfaces SR. Como ambas BPDU transportan la misma información, no se producirá ningún conflicto de información de puerto. Ello permite al puente ASRT crear un árbol de extensión con puentes IBM 8209 y SR-TB junto con otros puentes TB y SRT.

Hebras (descubrimiento de direccionador)

Las hebras son 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 con puente de direccionamiento en origen.

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

Hebras IP con ARP

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

1. Una estación final IP mantiene una tabla ARP y una tabla RIF. La dirección MAC de la tabla ARP se utiliza como referencia cruzada para el RIF de destino en la tabla RIF. Si no existe un RIF para esa dirección MAC específica, la estación final transmite un paquete ARP REQUEST con un ARE (explorador de todas las rutas) o un STE (explorador del árbol de extensión) al segmento local.
2. Todos los puentes del segmento local capturan el paquete ARP REQUEST y lo envían por 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 de segmento al RIF del paquete. Mientras la trama continúa pasando a través de la red puenteada, el RIF compila una lista de pares de número de segmento y puente que describen la vía de acceso al destino.

   Cuando el paquete ARP REQUEST alcanza finalmente su destino, contiene la secuencia exacta de números de puentes y de segmentos del origen al destino.
3. Cuando la estación final de destino recibe la trama, sitúa la dirección MAC y su RIF en sus propias tablas ARP y RIF. Si la estación final de destino recibe algún otro paquete ARP REQUEST del mismo origen, dicho paquete se elimina.
4. La estación final de destino genera entonces un paquete ARP REPLY que incluye el RIF y lo envía de vuelta a la estación final de origen.
5. La estación final de origen recibe la vía de acceso de la ruta averiguada. A continuación, se entran la dirección MAC y su RIF en las tablas ARP y RIF. El RIF se adjunta al paquete de datos y se reenvía al destino.
6. El temporizador de renovación de IP ARP maneja la antigüedad de las entradas RIF.

Hebras IPX

Las estaciones finales IPX comprueban cada paquete que reciben para un RIF. Si el RIF no existe en la tabla, añaden el RIF a la tabla y designan esa 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 necesita enviar un paquete y no existe ninguna entrada en la tabla RIF para la dirección MAC, la estación final transmite los datos como un STE.

Cuando el temporizador RIF finaliza, la entrada de la tabla se borra y no se volverá a entrar hasta que llegue otro paquete que contenga un RIF para esa entrada.

Hebras AppleTalk 2

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

1. Si no existe un RIF para una dirección MAC específica, 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 por 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 de segmento al RIF del paquete. Mientras la trama continúa pasando a través de la red puenteada, el RIF compila una lista de pares de número de segmento y puente que describen la vía de acceso al destino.
3. Cuando la estación final de destino recibe la trama, sitúa 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 recibe algún otro paquete ARP REQUEST del mismo origen, dicho paquete se elimina.
4. La estación final de destino genera entonces un paquete ARP REPLY que incluye el RIF y lo envía de vuelta a la estación final de origen con el bit de dirección del RIF invertido.
5. La estación final de origen recibe la vía de acceso de la ruta averiguada. La dirección MAC y su RIF se entran entonces 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 finaliza, se envía un XIS con un ARE y el estado cambia a *DISCOVERING*. Si no se recibe ninguna respuesta XID, la entrada se descarta.

Función de direcciones MAC duplicadas de SR-TB

La función de direcciones MAC duplicadas (DMAC) le permite conectar un puente SR-TB a una red con puente SR que tiene direcciones MAC duplicadas configuradas. La función de direcciones MAC duplicadas se puede habilitar con dos opciones:

- **Función de MAC duplicadas sin equilibrio de carga**

  Esta opción le permite habilitar direcciones MAC duplicadas sin equilibrio de carga. En tal caso, sólo se averigua un RIF para la dirección MAC duplicada y se aplica la antigüedad a dicho RIF averiguado. Todas las estaciones del dominio TB utilizarán este RIF para comunicarse con esa dirección MAC. Cuando la entrada de este RIF caduque, la siguiente trama se enviará desde el dominio TB como trama exploradora del árbol de extensión (STE).

- **Función de MAC duplicadas con equilibrio de carga**

  Esta opción le permite habilitar direcciones MAC duplicadas con equilibrio de carga y sólo se puede habilitar después de habilitar DMAC sin equilibrio de carga. En tal caso, se averiguan y se mantienen dos RIF para cada dirección

MAC duplicada. Cada uno de los dos RIF dispone de su propio temporizador de antigüedad. Siempre que el puente reciba una trama con un RIF concreto, se renovará el valor de antigüedad correspondiente a ese RIF. La primera vez que una estación de un dominio TB envía una trama a una dirección MAC duplicada, el software de puentes decide el RIF que se utilizará para enviar dicha trama. Todas las tramas posteriores de la estación emisora se enviarán mediante ese mismo RIF. El puente mantendrá RIF primarios y secundarios para un máximo de siete direcciones MAC duplicadas. Si especifica valores de antigüedad independientes para direcciones MAC duplicadas, se utilizará el valor adecuado para caducar las entradas correspondientes a esa dirección MAC duplicada, lo que le permite ajustar el valor de antigüedad de las direcciones MAC duplicadas.

En qué consisten los puertos de puente de multiacceso

Un puerto de puente de multiacceso es un puerto de puente que incorpora todos los circuitos virtuales Frame Relay que no están configurados individualmente como puertos de puente.Al puerto de puente de multiacceso se le asigna un número de segmento de puente exclusivo, que se utiliza a efectos de puente de direccionamiento en origen.

Un puerto de puente de multiacceso tiene las características siguientes:

- Da soporte sólo a puentes de direccionamiento en origen (SR).
- Las configuraciones de malla completa ofrecen soporte a conectividad entre todos los nodos y pueden utilizar el protocolo de árbol de extensión para evitar bucles de puente.
- Las configuraciones que no son de malla completa sólo dan soporte a conectividad entre el centro de datos y ramas ya que los puentes puente entre circuitos virtuales del mismo segmento multiacceso no están soportados. Esta configuración no puede utilizar el protocolo de árbol de extensión, de manera que se debe habilitar el reenvío de tramas STE. Por omisión, el protocolo de árbol de extensión está inhabilitado y el reenvío de tramas STE está habilitado.

  Nota: Se trata de la configuración preferida porque el protocolo del árbol de extensión puede consumir una ancho de banda WAN considerable y la mayoría de configuraciones no son de malla completa.
- Requiere el segmento virtual de puente de 1 a N.
- Proporciona conectividad independiente de protocolo entre estaciones finales similares y conectividad limitada entre estaciones finales en medios no similares.
- Puede proporcionar atrapadores de datos efectivos para varios dispositivos IBM 2218. (Consulte “Funcionamiento conjunto con dispositivos IBM 2218” en la página 56.)

La base de datos multiacceso

Cada puerto de puente de multiacceso mantiene una base de datos de multiacceso que correlaciona el número de segmento de salto siguiente con el circuito virtual Frame Relay en el que se ha recibido la trama. Las entradas de la base de datos se crean o se actualizan mientras el segmento recibe ARE, STE o tramas direccionadas de manera específica desde los circuitos. Las tramas STE y ARE que deben reenviarse al segmento multiacceso se desbordan a todos los circuitos

virtuales del segmento multiacceso. Las tramas direccionadas de manera específica que deben reenviarse al segmento multiacceso sólo se reenvían si existe una entrada de base de datos de multiacceso que correlaciona el número de segmento de salto siguiente con un circuito virtual.

El software “caduca” entradas en la base de datos de multiacceso a una velocidad que se especifica con el mandato **multiaccess-age**.

Configuración de los puertos de puente multiacceso

El siguiente ejemplo muestra la manera de configurar los puertos de puente de multiacceso en las interfaces de Frame Relay 1 y 4. El puerto 5 es el siguiente puerto de puente disponible y esta es la primera vez que el direccionamiento en origen se habilita.

```
* 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: Después de configurar el primer puerto de puente de multiacceso, no se le solicita el número de puente y el número de segmento de virtual.

Funcionamiento conjunto con dispositivos IBM 2218

La utilización de puertos de multiacceso con dispositivos 2210/2212/2216 como atrapadores de datos puede proporcionar una topología de alta densidad y alta disponibilidad para los 2218 de la red.

- La alta densidad se produce porque se pueden conectar muchos dispositivos 2218 a un puente de centro de datos a través de un único puerto de puente de multiacceso.
- La alta disponibilidad se produce al configurar un único 2218 para que se conecte con puentes primarios y de centros de datos de reserva a través de sus puertos de puente de multiacceso. El 2218 se puede conmutar, pues, entre los circuitos primarios y de reserva mientras el 2218 detecta problemas en la red Frame Relay.

Para que el 2218 se conmute entre los puentes primarios y centrales sin que se pierdan las conexiones LLC entre él y el puente central:

- Configure los puentes primarios y de centros de datos de reserva con el mismo número de segmento virtual de 1 a N de puente.
- Configure los puentes primarios y de centros de datos de reserva con el mismo número de puente de ruta origen.
- Configure los puentes primarios y de centros de datos de reserva con el mismo número de segmento multiacceso.

Nota: Esta configuración sólo ofrece soporte a conectividad entre centro de datos y ramas.

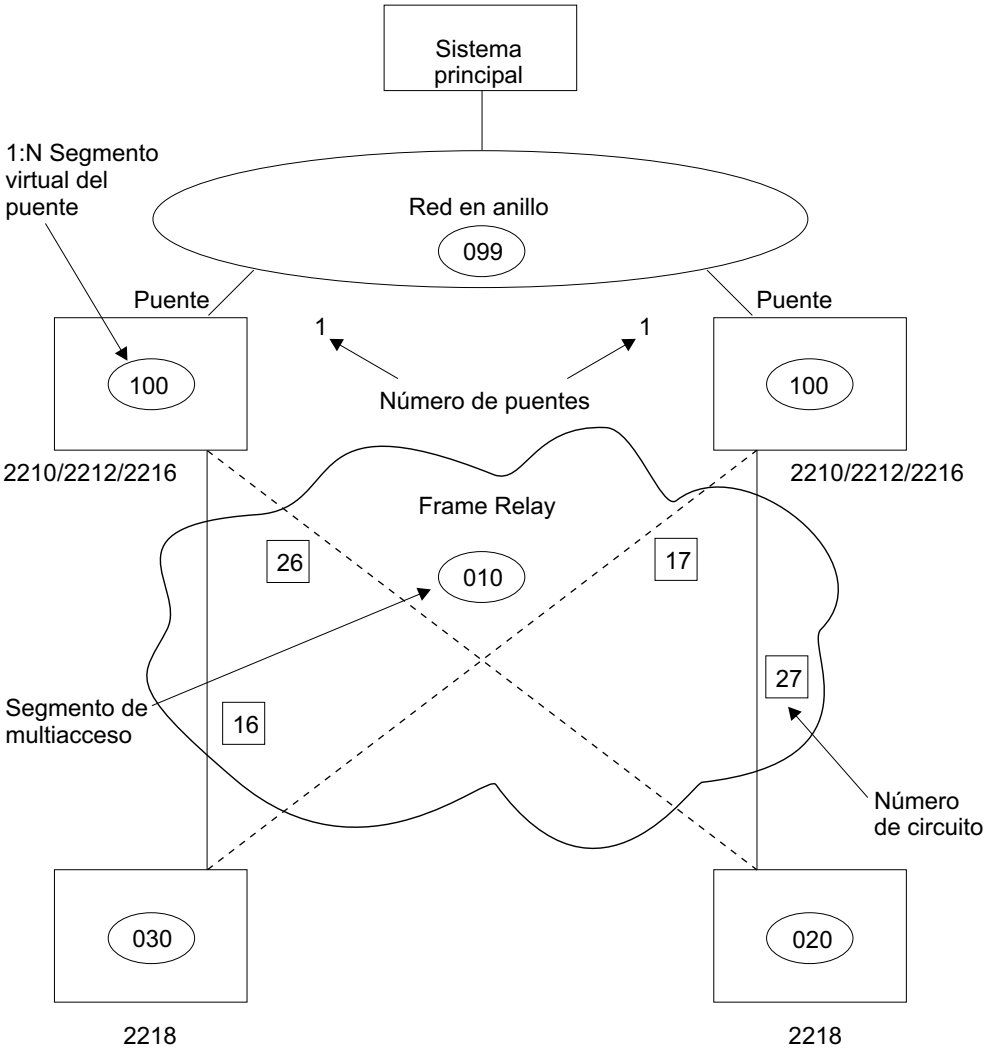


Figura 19. Ejemplo de configuración con 2218 y puertos de puente de multiacceso

La Figura 19 en la página 57 muestra una conexión de red habitual entre 2212 y 2218.

Utilización de la función de nodo de acceso de límites (BAN)

Este capítulo describe la función de nodo de acceso de límites (BAN) del 2212. BAN ofrece un método de confianza y bajo coste para estaciones finales PU de tipo 2.0 y 2.1 para comunicación con el entorno SNA en enlaces de área amplia. Este capítulo consta de las siguientes secciones:

Acerca de la función de nodo de acceso de límites

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

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

IBM Network Control Program (NCP) es un ejemplo de un nodo de subárea y, junto con VTAM, de un nodo de red APPN compuesto.

La función BAN es una mejora de las posibilidades de Frame Relay, DLSw y ASRT del software 2212. Esta función permite que las estaciones finales IBM Tipo 2.0 y 2.1 conectadas a un 2212 efectúen una conexión directa a través de Frame Relay con un nodo SNA que ofrezca soporte al formato de trama Bridged 802.5 (para red en anillo) descrito en el documento RFC 1490/2427. La función BAN proporciona una manera mejor y más económica de comunicar con el entorno SNA de IBM. IBM ha modificado el software de IBM Network Control Program (NCP) para ofrecer soporte a esta mejora.

Cuando se utiliza BAN, las estaciones finales funcionan como si estuvieran conectadas directamente a un nodo SNA a través de una línea de red en anillo, Ethernet, o SDLC, tal y como muestra la Figura 20 en la página 60. A pesar de que sus datos pasan de hecho a través de un 2212 y en una red Frame Relay, es transparente a las estaciones finales.

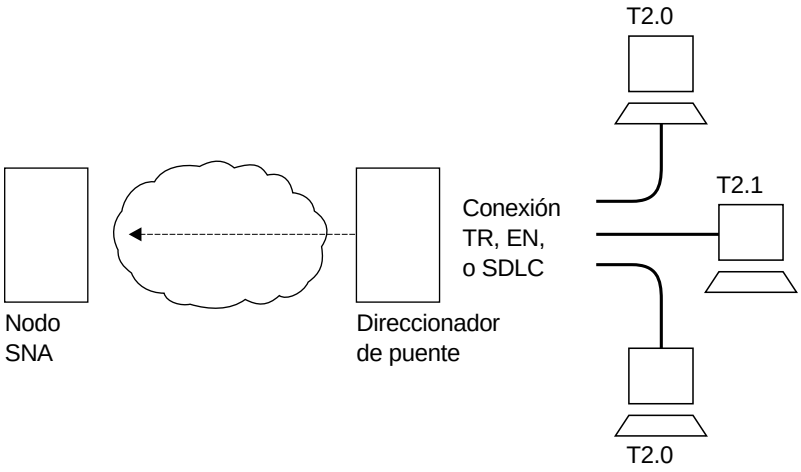


Figura 20. Conexión directa de estaciones finales a un nodo SNA mediante BAN

Ventajas de BAN

Diseñado para satisfacer las necesidades de clientes que no necesitan una implementación total de DLSw, BAN proporciona un método económico de conexión a entornos IBM. Gracias a una vía de acceso a todas las posibilidades de DLSw, BAN proporciona tres ventajas principales a clientes que necesitan trabajar en Internet con el entorno IBM:

1. La capacidad de enviar por puente el tráfico Ethernet o de red en anillo directamente al nodo SNA sin conversión de tramas mediante otro direccionador DLSw. Ello puede representar un importante ahorro en costes de equipos al eliminar la necesidad de otro direccionador y un sistema principal en el sitio central.
2. No existe límite de arquitectura alguno para el número de conexiones LLC de tipo 2 (*LLC2*) multiplexadas en un solo identificador de conexión de datos (DLCI) Frame Relay. En cambio, el soporte de nodo de límite (BN) de Frame Relay NCP limita el número de conexiones LLC2 por DLCI a 127. Esto puede representar un ahorro significativo en costes de proveedores de DLCI de Frame Relay.
3. Elimina la necesidad de configurar direcciones de estaciones finales en el direccionador DLSw que es local para las estaciones finales. Ello facilita la configuración y la gestión de de BAN.

   Nota: Puede utilizar un DLCI BAN para tráfico IP. Esto le permite gestionar el direccionador (a través de SNMP) en el mismo DLCI que está utilizando para SNA (a través de BAN).

Cómo funciona BAN

La función BAN del direccionador funciona filtrando las tramas que las estaciones finales tipo 2.0 o 2.1 envían. El direccionador modifica cada trama BAN para que sea compatible con el formato de trama Bridged 802.5 (para red en anillo). El direccionador examina cada trama y sólo permite que las que disponen de la dirección MAC DLCI BAN pasen en un DLCI al sistema principal. La dirección MAC de destino de la trama con formato Bridged 802.5 es sustituida por el identificador de nodos de límite en las tramas destinadas al nodo SNA.

Con BAN, generalmente sólo se necesita un DLCI. De todos modos, BAN puede utilizar muchas conexiones DLCI entre el direccionador y el entorno IBM. En algunos casos, es probable que desee configurar más de un DLCI para manejar tráfico BAN. Consulte “Instalación de varios DLCI” en la página 67 si desea obtener más información.

Existen dos maneras de utilizar la función BAN:

- Puente directo mediante la posibilidad de puente del 2212
- Interrupción de DLSw, en la que BAN interrumpe la conexión LLC2 en el direccionador que ejecuta DLSw.

Las secciones que siguen explican la manera de configurar cada método.

BAN con puente frente a BAN DLSw

Puede implementar BAN de dos maneras: puente directo e interrupción de DLSw. En el primer caso, se configura BAN para enviar por puente las tramas LLC2 desde estaciones finales del tipo 2.0 o del tipo 2.1 al nodo SNA. En el segundo caso, BAN interrumpe la conexión LLC2 en el direccionador que ejecuta DLSw. En esta explicación denominaremos a lo primero *BAN de tipo 1* y a lo segundo *BAN de tipo 2*.

La Figura 21 muestra una conexión de BAN de tipo 1 (por puente). Observe que en esta figura el direccionador no interrumpe el tráfico LLC2 que se recibe de las estaciones finales. En lugar de ello, convierte las tramas que recibe en tramas de formato Bridged Token-Ring (RFC 1490/2427) y realiza una conexión por puente directamente con el nodo SNA.

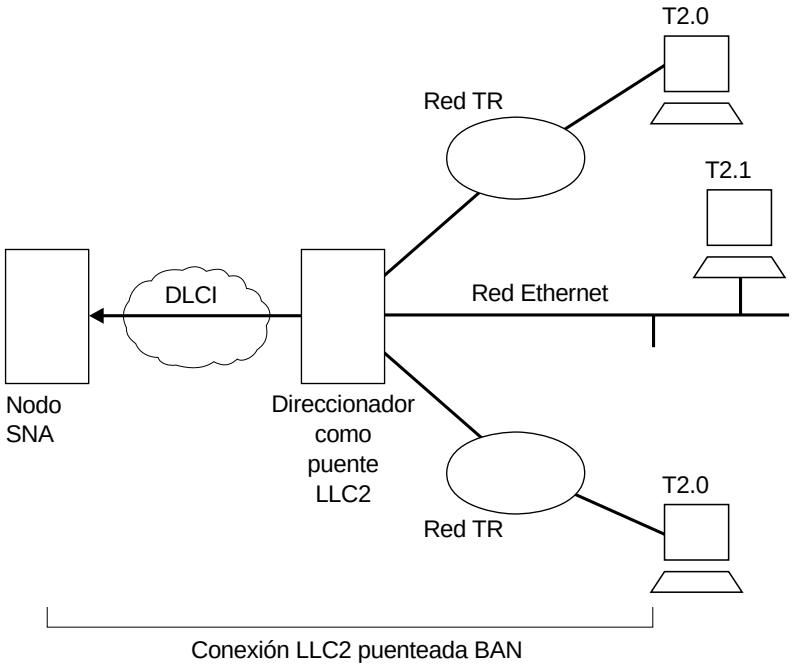


Figura 21. BAN de tipo 1: El direccionador como puente LLC2

En este caso, el direccionador actúa como puente entre el nodo SNA y las estaciones finales. DLSw no interrumpe las sesiones de LLC2 en el direccionador, como lo hace BAN de tipo 2. Las tramas de las estaciones finales pueden tener el

formato de red en anillo o Ethernet, siempre que el puente esté configurado para ofrecer soporte a ese tipo de trama.

La Figura 22 muestra una conexión BAN de tipo 2 (DLSw de BAN virtual). Observe que en esta figura el direccionador DLSw no funciona como puente. El direccionador interrumpe el tráfico LLC2 que se recibe de las estaciones finales conectadas. Al mismo tiempo, el direccionador establece una nueva conexión LLC2 con el nodo SNA en la red Frame Relay. Por lo tanto, existen dos conexiones LLC2 dentro de la transacción y el espacio entre ellas es transparente tanto para el nodo SNA como para las estaciones finales. El resultado es una conexión LLC2 virtual entre el nodo SNA y las estaciones finales.

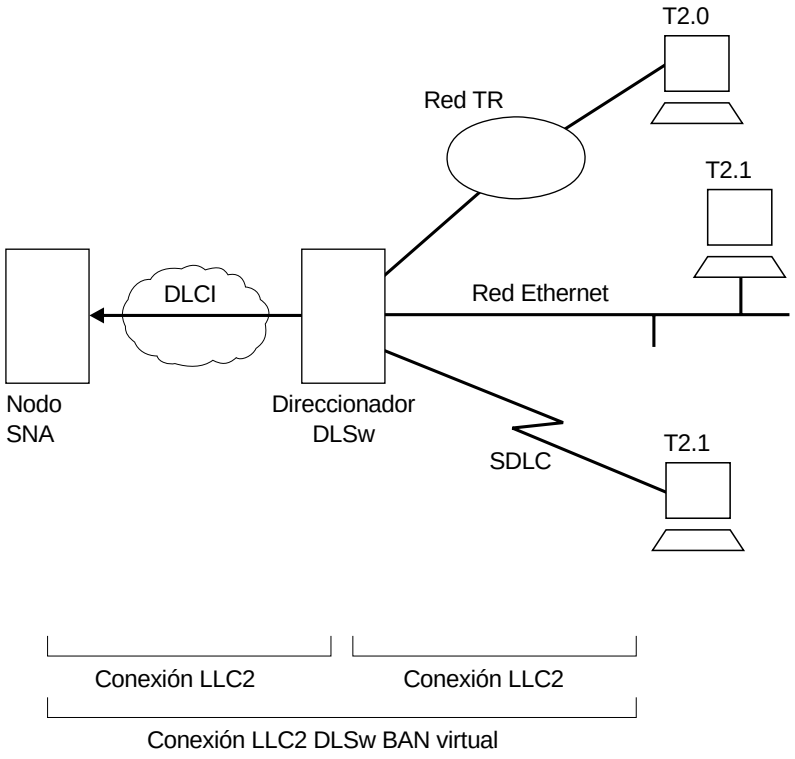


Figura 22. BAN de tipo 2: Conversión de DLSw local

La sesión de SDLC se interrumpe en el direccionador y existe una sesión LLC2 independiente entre el direccionador y el nodo SNA. La estación SDLC aparece en el nodo SNA como una estación conectada Frame Relay.

DLSw remoto recibe soporte para ambos tipos de BAN. Tanto las conexiones de BAN de tipo 1 como las conexiones de BAN de tipo 2 pueden ser utilizadas por direccionadores que funcionan como asociados de DLSw para conectar estaciones finales de tipo 2.0 o 2.1 con un nodo SNA.

¿Qué método debe utilizarse?

Por lo general, es preferible envíar las tramas por puente directo (BAN de tipo 1) porque proporciona una entrega de datos rápida con el mínimo de actividad general en la red. De todos modos, existen excepciones. Si la utilización en un DLCI es demasiado alta, es probable que se excedan los tiempos de espera en una configuración de puente. Y, a la inversa, rara vez se exceden los tiempos de espera en una configuración DLSw (BAN de tipo 2) ya que este tipo de configu-

ración interrumpe y, a continuación, vuelve a crear sesiones de LLC2 en el direccionador local (DLSw).

Utilización de la función BAN

Cuando se configura BAN, el sistema le solicita información. A menudo, el sistema ofrece valores por omisión que se aceptan pulsando **Intro**.

Para utilizar la función BAN, debe:

1. Configurar el direccionador para Frame Relay (FR)
2. Configurar el direccionador para ASRT
3. Configurar el direccionador para BAN
4. Configurar el direccionador para DLSw (sólo BAN de tipo 2)

Estos pasos se documentan en el ejemplo siguiente. El ejemplo presupone que está instalando un solo DLCI para transportar tráfico BAN. En función de las circunstancias y las necesidades, es probable que desee instalar varios DLCI para obtener redundancia o ancho de banda total aumentado para el entorno IBM. En ese caso, la dirección MAC DLCI BAN del 2212 debe ser idéntica a la dirección MAC DLCI BAN del 2212 de reserva RDSI. Así mismo, el valor del segmento de puente interno del 2212 debe ser diferente del valor del segmento de puente interno del 2212 de reserva. Consulte “Instalación de varios DLCI” en la página 67 si desea obtener más información.

Paso 1: Configurar el 2212 para Frame Relay

Para acceder al indicador de configuración de Frame Relay, escriba **network** *núm_interfaz* en el indicador `Config>`, tal y 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>
```

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

- El número del circuito. Es el número del 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 se crea se convierte en el PVC que conecta el 2212 y el nodo SNA cuando se utiliza BAN . El siguiente paso consiste en configurar este PVC como puerto de puente.

Nota: Si desea instalar varios DLCI BAN conectados con el mismo o diferentes nodos SNA, debe configurar frame relay independientemente para cada DLCI. Consulte “Instalación de varios DLCI” en la página 67 si desea obtener más información.

Paso 2: Configurar el direccionador para el puente de direccionamiento en origen adaptable

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

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

Añada un puerto en el indicador ASRT Config>, tal y 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 ser el mismo que el número utilizado al configurar el dispositivo para puente en Frame Relay que se describe en el Paso 1.

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

A continuación, habilite el direccionamiento en origen y defina números de segmentos de direccionamiento en 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, inhabilite los puentes transparentes en el puerto de puente, tal y como se indica:

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

Si se están utilizando conexiones de BAN tipo 2, habilite DLSw para puente.

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

El siguiente paso 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 reinicie el direccionador. Observe que, tal y como sucede en los pasos 1 y 2, en este paso se utiliza el puerto de puente 5.

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

Añada en el indicador BAN config> el número de puerto (5) en el que desea habilitar la función BAN. Se le solicitará que entre una dirección MAC DLCI BAN y la dirección del identificador de nodos de límite, tal y como se muestra:

```
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 datos. (Consulte Figura 21 en la página 61 y Figura 22 en la página 62). La otra dirección, 4FFF00000000, es la dirección del identificador de nodos de límite por omisión. Para aceptarla, pulse **Intro**.

Nota: El identificador de nodos de límite corresponde a la dirección MAC de destino ubicada en las tramas con formato Bridged 802.5 enviadas desde el 2212 al nodo SNA. El valor por omisión 4FFF00000000 coincide con el valor por omisión utilizado por IBM Network Control Program (NCP). La dirección NCP se especifica en la definición NCP mediante la palabra clave LOCADD de la sentencia LINE que define el puerto Frame Relay físico. Para otros nodos SNA que dan soporte a tramas con formato Bridged 802.5 en Frame Relay, el identificador de nodos de límite se debe establecer en la dirección MAC que el nodo SNA ha configurado para este circuito virtual.

Especificación del tipo de conexión BAN: La siguiente solicitud le pide que especifique el tipo de conexión BAN que desea añadir: puente o interrupción de DLSw. Estos dos métodos se describen en las secciones anteriores como BAN de tipo 1 y BAN de tipo 2. El tipo 1, puente directo, es el valor por omisión. Debe aceptar el valor por omisión a menos que desee que el tráfico de entrada se interrumpa en el direccionador.

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

```
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 de tipo 2)

Si se están utilizando conexiones BAN de tipo 2, se debe configurar DLSw. Ello implica habilitar DLSw, establecer el número de segmento DLSw, añadir el asociado TCP DLSw local y abrir los puntos de acceso a servicio (SAP) asociados con la interfaz FR y la interfaz LAN. Si no consigue llevar a cabo esta configuración DLSw, no podrá utilizar conexiones de BAN de tipo 2 (interrupción de DLS).

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

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

Para añadir un asociado TCP DLSw local, realice la siguiente operación 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 y como se muestra en este ejemplo:

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

Al ejecutar el mandato **open** para la interfaz 0, se abre el SAP en la interfaz de la LAN. Ejecute el mismo mandato para abrir el SAP en la interfaz FR. Observe que en cada caso, se entra 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 normalmente un DLCI es suficiente para manejar el tráfico BAN desde y hasta el entorno IBM, instalar dos o más DLCI puede resultar útil en algunas circunstancias.

Situación 1: Configuración de una conexión BAN que tolera errores

Las conexiones redundantes con varios nodos SNA sirven de protección contra la anomalía de un único nodo SNA. Además, al compartir tráfico BAN entre varios DLCI reduce las posibilidades de que un nodo SNA se sobrecargue. En una configuración DLCI redundante, las estaciones finales PU del tipo 2.0 y 2.1 pueden pasar tráfico BAN a diferentes nodos SNA, tal y como se muestra en la Figura 23.

Nota: Cada DLCI se configura en un puerto ASRT FR independiente con la misma dirección MAC DLCI.

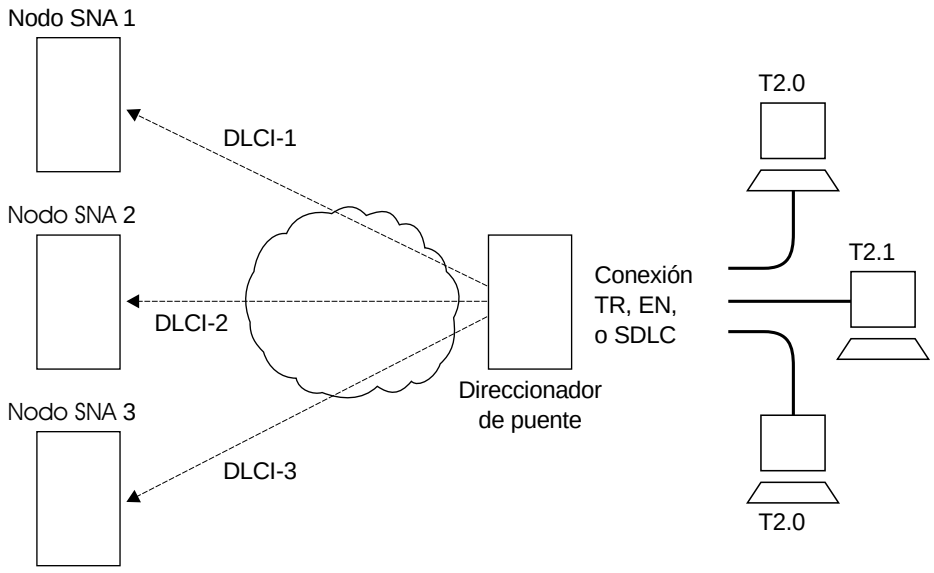


Figura 23. Configuración BAN con varios DLCI a diferentes nodos SNA

Situación 2: Aumento del ancho de banda para el entorno IBM

Varias conexiones con el mismo nodo SNA aumentan el ancho de banda total disponible para comunicar con el entorno IBM. Esto reduce la posibilidad de congestión en un único DLCI.

Es posible que desee instalar dos o más DLCI si dispone de una gran cantidad de tráfico BAN y de otra conexión FR. Un segundo DLCI le puede proporcionar un ancho de banda mayor para el nodo SNA y puede servirle de protección contra anomalías inesperadas.

Instalación de varios DLCI

La instalación de varios DLCI es sencilla, especialmente si lo hace durante la configuración inicial de BAN. Cuando instale varias conexiones, recuerde que cada DLCI Frame Relay corresponde a un nodo SNA específico en el entorno IBM. Para pasar tramas BAN a ese nodo SNA, debe especificar el número de circuito correcto al establecer la conexión Frame Relay. Su proveedor de Frame Relay puede facilitarle el número de circuito de cada una de las conexiones.

Para instalar conexiones DLCI en diferentes nodos SNA (consulte la “Situación 1: Configuración de una conexión BAN que tolera errores” en la página 66), debe:

1. Llevar a cabo una de las siguientes acciones:
   - **En la configuración de ASRT**, añadir un puerto de puente para ese DLCI.
   - **En la configuración de Frame Relay**, definir otro DLCI Frame Relay en un segundo puerto de puente.
2. Configurar el puerto de puente para BAN, tal y como se muestra en el “Paso 3: Configurar el direccionador para BAN” en la página 64.

Para instalar una segunda conexión DLCI con el mismo nodo SNA (consulte la “Situación 2: Aumento del ancho de banda para el entorno IBM”), siga los mismos pasos. En la “Situación 2: Aumento del ancho de banda para el entorno IBM”, el número de circuito que se proporciona para el segundo puerto Frame Relay difiere del primero. De todos modos, cada número de circuito identifica un DLCI diferente y una vía de acceso distinta al entorno IBM.

Comprobación de la configuración de BAN

Cuando reinicie el direccionador, éste validará el hecho de que el puerto de puente BAN sea un puerto de puente Frame Relay con funcionamiento de direccionamiento en origen. Debe comprobar la configuración BAN con el mandato list, tal y 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>
```

Como muestra este ejemplo, el mandato **list** muestra cada aspecto de la configuración BAN, facilitando el puerto de puente (5 en este caso), la dirección MAC del

DLCI y el identificador de nodos de límite para el nodo SNA e indicando si el puerto es de puente o de interrupción por DLSw.

Para verificar que BAN se ha inicializado adecuadamente en el arranque, puede utilizar GWCON del modo siguiente:

```
+ 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 proporciona tres mensajes de estado:

- Un estado de `Init Fail` indica que existe un problema de configuración.
- Un estado de `Down` indica que el DLCI no se está ejecutando.
- Un estado de `Up` indica que el DLCI Frame Relay está activo y en funcionamiento, como se pretendía.

Si recibe un estado que no sea `Up`, debe comprobar los mensajes de ELS del direccionador para diagnosticar el problema. “Habilitación de los mensajes del sistema para el registro cronológico de sucesos (ELS) para BAN” explica cómo habilitar mensajes de ELS.

Habilitación de los mensajes del sistema para el registro cronológico de sucesos (ELS) para BAN

Después de la configuración inicial de BAN y de reiniciar, es conveniente habilitar los mensajes de ELS para comprobar si la configuración funciona como estaba previsto. Puede habilitar mensajes específicos de BAN desde el indicador `Config> prompt`, tal y como se muestra:

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

Al entrar este mandato aparecen todos los mensajes del subsistema BAN. Esto hará que ELS le notifique todo el funcionamiento relacionado con BAN. Después de ejecutar BAN durante algún tiempo, es probable que desee desactivar algunos mensajes. Puede desactivar los mensajes BAN ELS específicos utilizando el mandato **nodisplay** y el número de mensaje específico. Este ejemplo ilustra cómo desactivar el mensaje ban.9:

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

Si desea obtener una lista de todos los mensajes relacionados con BAN, consulte la publicación *Guía de mensajes del sistema para el registro cronológico de sucesos*.

Utilización de puentes

Este capítulo describe cómo crear configuraciones básicas para el puente transparente de direccionamiento en origen adaptable (ASRT) mediante los mandatos de configuración de ASRT. El capítulo incluye “Procedimientos de configuración básica de puentes”.

Si necesita más información sobre los mandatos de configuración del puente ASRT, consulte el “Configuración y supervisión de puentes” en la página 73.

Si desea una introducción a la modificación de los puentes ASRT, consulte “Filtros por nombre y por bytes de NetBIOS” en la página 48.

Si desea obtener ejemplos de configuración de filtros NetBIOS, consulte “Procedimientos de configuración de filtro por nombre de sistema principal y por bytes de NetBIOS” en la página 163.

Si desea información sobre cómo acceder al entorno de configuración de ASRT, consulte “Cómo empezar” en la publicación *Guía del usuario de software*.

Procedimientos de configuración básica de puentes

El puente ASRT le permite llevar a cabo configuraciones de puente básicas mediante el menor número posible de mandatos. Por ejemplo, si se utiliza el mandato **enable bridge**, este proceso se inicia dejando que todos los dispositivos configurados correctamente participen en los puentes transparentes. Así mismo, se habilitan todos los valores por omisión del algoritmo de árbol de extensión.

La función de puenteo, más allá de los puentes transparentes, se habilita de manera “individual para cada puerto”. Cuando el direccionamiento en origen está habilitado, las entradas del usuario como pueden ser el número del segmento, el número del puente, etc., todavía son necesarias y se deben entrar además de los mandatos básicos que se explican.

Interfaces de puente

El puente ASRT ofrece soporte al puenteo en combinaciones de una o más de las siguientes interfaces:

- Ethernet
- Red en anillo
- Línea serie

La interfaz Ethernet da soporte a los puentes transparentes, mientras que las interfaces de red en anillo dan soporte al direccionamiento en origen y a los puentes transparentes.

La interfaz de línea serie proporciona conectividad punto a punto para tráfico de direccionamiento transparente y origen. Es importante observar que una configuración de puerto en una línea seria debe ser coherente en ambos puntos finales. Esto significa que ambos puntos finales se deben configurar del siguiente modo:

- Transparente a transparente
- Direccionamiento en origen a direccionamiento en origen

- Direccionamiento en origen/transparente a direccionamiento en origen/transparente

Es mejor que la línea serie esté configurada para ambos métodos de puenteo si se desea tener puentes mixtos. Otra pauta propuesta es asegurarse de que los direccionadores de puente sean coherentes con su método de puenteo o con su direccionamiento de protocolos concretos.

La información que sigue señala los pasos iniciales necesarios para habilitar las opciones de puenteo que ofrece el puente ASRT. Encontrará más detalles sobre la manera de efectuar más cambios de configuración en las secciones de mandatos de este capítulo. Después de llevar a cabo estas tareas, debe reiniciar el direccionador a fin de que la nueva configuración empiece a tener efecto.

Habilitación del puente transparente

Utilice los mandatos siguientes para habilitar el puente transparente:

- **Enable bridge** para habilitar el puente transparente en todas las interfaces de red de área local (LAN). Las interfaces de red de área amplia (WAN) (como pueden ser líneas serie) se pueden incluir mediante el mandato **add port**.
- **Disable transparent** *núm_puerto* para excluir las interfaces de red en anillo especificadas de la participación en el puente transparente. Repita el mandato para todas las interfaces que desee excluir de la configuración de puente transparente.

Habilitación del puente de direccionamiento en origen

Utilice los mandatos siguientes para habilitar el puente de direccionamiento en origen:

- **Enable bridge** para habilitar el puente en todas las interfaces de red de área local. Las interfaces WAN (por ejemplo, líneas serie) se pueden incluir mediante el mandato **add port**.
- **Disable transparent** *núm_puerto* para inhabilitar el puente transparente en todos los puertos.
- **Enable source-routing** *núm_puerto núm_segmento [núm_puente]* para habilitar el direccionamiento en origen de puertos concretos. Cuando se habilita el direccionamiento en origen en más de dos puertos, es necesario un número de segmento adicional para asignar un segmento virtual interno necesario para las configuraciones 1:N SRB.

Si la única función que necesita es el direccionamiento en origen, inhabilite el puente transparente en las interfaces.

Nota: Debe tener cuidado en ***no*** incluir interfaces que no ofrecen soporte tradicionalmente a direccionamiento en origen. Por ejemplo, el puente transparente está inhabilitada y el direccionamiento en origen está habilitado en un puerto de Ethernet , se inhabilita el recurso de puente para este puerto.

Habilitación del puente SR-TB

Utilice los siguientes mandatos para habilitar el puente SR-TB:

- **Enable bridge** para habilitar el puente en todas las interfaces de red de área local. Las interfaces WAN (por ejemplo, líneas serie) se pueden incluir mediante el mandato **add port**.
- **Disable transparent** *núm_puerto* para inhabilitar el puente transparente en todas las interfaces de direccionamiento en origen subyacentes.
- **Enable source routing bridge** *núm_puerto núm_segmento [núm_puente]* para habilitar el direccionamiento en origen de puertos determinados. Cuando se habilita el direccionamiento en origen en más de dos puertos, es necesario un número de segmento adicional para asignar un segmento virtual interno necesario para las configuraciones 1:N SRB.
- **Enable sr-tb-conversion** *núm_segmento* para habilitar la conversión de tramas direccionadas origen a tramas transparentes y viceversa. Así mismo, es necesario que asigne un número de segmento de dominio y un tamaño de MTU de dominio para representar todo el dominio de puente de transparente.

Después de llevar a cabo los procedimientos que se acaban de describir, se aconseja que utilice el mandato **list bridge** para visualizar la configuración de puente actual. Ello le permite verificar y comprobar la configuración.

Si desea más información sobre todos los mandatos que se acaban de comentar, consulte “Configuración y supervisión de puentes” en la página 73.

Configuración y supervisión de puentes

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

Acceso al entorno de configuración de ASRT

Para acceder al entorno de configuración de 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 de ASRT

Los mandatos de configuración de ASRT le permiten especificar los parámetros de red del puente ASRT y sus interfaces de red. Estos mandatos le permiten también habilitar y configurar el túnel IP de puente, y NetBIOS.

Se debe reiniciar el dispositivo para que la nueva configuración empiece a tener efecto.

Nota: Los mandatos de configuración de ASRT no empiezan a tener efecto de manera inmediata. Quedan pendientes hasta que el dispositivo se reinicia o se vuelve a cargar.

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

- Entre los mandatos de configuración del túnel IP en el indicador `TNL config>`. El indicador `TNL config>` es un subconjunto de los principales mandatos ASRT y se accede a él entrado el mandato `ASRT config>` **tunnel** que se describe más adelante en este capítulo.
- Entre los mandatos de configuración de NetBIOS en el indicador `NetBIOS config>`. El indicador `NetBIOS config>` es un subconjunto de los principales mandatos ASRT y se accede a él entrando el mandato `ASRT config>` **netbios** que se describe más adelante en este capítulo.

- Entre los mandatos de configuración de filtro de NetBIOS en el indicador `NetBIOS Filter config>`. Este indicador es un subconjunto de los mandatos de NetBIOS.

Tabla 4 muestra los mandatos de configuración de ASRT.

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

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Add	Añade entradas de dirección de estación a la base de datos permanente, la correlación de direcciones específicas, los puertos de LAN/WAN, los puertos de multiacceso, los filtros de protocolo, las direcciones MAC duplicadas y un túnel entre estaciones finales en una red de internet IP.
Ban	Permite el acceso al indicador del nodo de acceso de límites (BAN) a fin de que se puedan entrar los mandatos de configuración de BAN.
Change	Permite al usuario cambiar los números de puerto y de segmento.
Delete	Suprime las entradas de dirección de estación, la correlación de direcciones específicas, los puertos de LAN/WAN, los filtros de protocolo, las direcciones MAC duplicadas y un túnel entre estaciones finales en una red de internet IP.
Disable	Inhabilita las siguientes funciones: • Puentes • Tramas duplicadas • Correlación entre direcciones de grupo y funcionales • Propagación de las tramas exploradoras del árbol de extensión • Direccionamiento en origen en un puerto determinado • Recepción de tramas exploradoras del árbol de extensión en un túnel • Conversión SR-TB • Función de puente transparente (árbol de extensión) en un puerto determinado • Túnel entre puentes • Función de direcciones MAC duplicadas • Equilibrio de carga de MAC duplicadas • Conversión IPX

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

Mandato	Función
Enable	Habilita las siguientes funciones: • Puentes • Tramas duplicadas • Correlación entre direcciones de grupo y funcionales • Propagación de las tramas exploradoras del árbol de extensión • Direccionamiento en origen en un puerto determinado • Recepción de tramas exploradoras del árbol de extensión en un túnel • Conversión SR-TB • Función de puente transparente (árbol de extensión) en un puerto determinado • Túnel entre puentes • Función de direcciones MAC duplicadas • Equilibrio de carga de MAC duplicadas • Conversión IPX
List	Visualiza información sobre la configuración de puentes completa o sobre los parámetros de configuración seleccionados.
NetBIOS	Visualiza el indicador de configuración de NetBIOS.
Set	Establece los siguientes parámetros: • Antigüedad de las entradas de dirección dinámicas • Dirección de puente • Tamaño de trama máximo para la creación de túneles • Codificación de bits de trama más grande (LF) • Tamaño máximo de trama • Parámetros de puente y de puerto del protocolo de árbol de extensión • Valores del descriptor de rutas (RD) • Tamaño de la base de datos de filtro • Valor de antigüedad para campos de información de direccionamiento de direcciones MAC • Valor de antigüedad de las entradas de bases de datos de multiacceso • Modalidad de conversión IPX • Preferencia de Ethernet
Tunnel	Permite acceder al indicador de configuración del túnel a fin de que se puedan entrar los mandatos de configuración de túnel.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Respuesta a los mandatos de configuración de ASRT

Los mandatos de configuración de ASRT (Talk 6) no empiezan a tener efecto de manera inmediata. Quedan pendientes hasta que se ejecuta el mandato **reload** o **restart**.

Add

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

- Entradas de dirección de estación a la base de datos permanente
- Correlación de direcciones específicas de un protocolo determinado
- Puertos de multiacceso
- Puertos de LAN/WAN
- Filtros de protocolo que filtran paquetes de manera selectiva según el tipo de protocolo.
- Túnel IP entre estaciones finales y en segmentos de red IP
- Un máximo de 7 direcciones MAC duplicadas

Para la función de túnel IP del puente, el mandato **add** le permite crear un túnel IP entre las estaciones finales en una red internet IP. Este túnel se cuenta sólo como un salto entre las estaciones finales, sin tener en cuenta la complejidad de la vía de acceso a través de la internet IP.

Sintaxis:

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

address *valor-direc*

Añade entradas de dirección de estación exclusivas a la base de datos permanente. Dichas entradas se copian a la base de datos de filtro como entradas permanentes cuando se reinicia el puente. El *valor-direc* es la dirección MAC de la entrada deseada. Puede ser una dirección individual, una dirección de multidifusión o una dirección de difusión. Tiene también la opción de especificar la correlación de puerto de reenvío saliente de cada puerto entrante. El proceso de encendido/apagado no destruye las entradas de las bases de datos permanentes y éstas 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 sobre cómo se utiliza el mandato **add address** para gestionar entradas de dirección:

Adición de 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: En las preguntas “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 establecer el filtro de la dirección de destino de esta entrada. Si se responde *yes* (sí) a la solicitud, se filtran todas las tramas que contienen esta dirección como dirección de destino sin tener en cuenta el puerto de donde procede.

Use same output mapping...

Si responde *yes* a esta solicitud, podrá crear una correlación de puertos salientes para todos los puertos entrantes en lugar de permitir sólo la correlación con puertos específicos. Si contesta *no* a esta solicitud, aparecerá otra solicitud (`Input Port Number [1]?`) para seleccionar cada puerto de entrada. Desde esta solicitud de puerto de entrada específica puede crear una correlación de puertos exclusiva para este puerto de entrada.

Input Port 1, Port 2

Si contesta “No” a la solicitud anterior, aparecerá una solicitud de puerto por entrada (`Input Port Number [1]?`) para seleccionar cada puerto de entrada y sus puertos de puente salientes.

Bridge to all ports?

Si contesta *yes* a esta solicitud, se creará una correlación de puertos saliente que incluye todos los puertos. Por lo tanto, cuando se recibe una trama con esta dirección como dirección de destino, dicha trama se reenvía a todos los puertos de reenvío salientes excepto al puerto entrante. Los siguientes son ejemplos de cómo esto se lleva a cabo según la correlación de puertos:

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

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

Si la correlación de puertos indica que no hay ningún puerto (NONE/DAF), la trama se filtra. Esta operación se conoce como filtro de direcciones de destino (DAF).

Si no se encuentra ninguna entrada de dirección para hacer coincidir la trama recibida, se reenvía a todos los puertos de reenvío excepto el puerto origen.

Bridge to Port 1, Port 2, etc.
Esta solicitud le permite asociar una entrada de direcciones con el puerto de puente específico. Si responde *yes* (sí), se correlaciona la dirección con el puerto especificado a fin de que el puerto se incluya en la correlación de puertos de la entrada de direcciones. Si responde *no*, se saltará la correlación de direcciones de ese puerto.

continue to another bridge port?
Esta solicitud le permite seleccionar el siguiente puerto de entrada a configurar.

Source address filtering
Permite el filtro de direcciones origen específicas de puertos (SAF). Cuando se aplica SAF (se responde *yes* (sí) a la solicitud), las tramas recibidas con direcciones origen que coinciden con las entradas de dirección de la base de datos de filtro que tienen el filtro de direcciones origen habilitado se descartarán. Este mecanismo permite a un gestor de red aislar una estación final al prohibir que se puentee su tráfico.

Habilitación del filtro de direcciones de destino para entradas

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

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

Después de añadir la entrada de direcciones, puede verificar su estado utilizando el mandato **list range**. El ejemplo siguiente muestra que no existe ninguna correlación de puertos para esa entrada (en negrita) y que el 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 direcciones con más de un puerto de entrada

Este ejemplo muestra cómo responder a los indicadores de mandatos para crear correlaciones de puertos de salida independientes para una entrada de direcciones que dispondrá de 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 direcciones, puede verificar su estado utilizando el mandato **list range**. El siguiente ejemplo muestra una entrada (en negrita) que tiene los puertos 1 y 2 como puertos de entrada y que tiene correlaciones de puertos independientes para ambos puertos de entrada. También se ha habilitado el filtro de direcciones origen (SAF).

```
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
```

Correlación exclusiva de puerto de salida creada para todos los puertos de entrada asociados con una entrada de direcciones

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

```
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 direcciones, puede verificar su estado utilizando el mandato **list range**. El ejemplo que aparece a continuación muestra una entrada (en negrita) que tiene una correlación exclusiva de puertos para todos los puertos de entrada. También se ha habilitado el filtro de direcciones origen (SAF).

```
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-direc*

Añade hasta 7 entradas de dirección MAC duplicadas a la base de datos. El *valor-direc* es la dirección MAC de la entrada deseada. Consulte “Función de direcciones MAC duplicadas de SR-TB” en la página 54 si desea obtener más información acerca de la función 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 verificar la información DMAC utilizando 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-dlh campo-tipo dirección-ga dirección-fa*

Añade direcciones funcionales específicas para agrupar correlaciones de direcciones de un identificador de protocolo determinado. La correlación de direcciones se convierte sólo en direcciones de destino que cruzan de red en anillo a Ethernet o a la inversa.

Nota: Para cada valor correlacionado de tipo Ether, se debe añadir el valor de tipo SNAP correspondiente. Esto es necesario para correlaciones bidireccionales.

tipo-dlh (Tipo de cabecera de enlace de datos) es una elección de DSAP, tipo Ether o SNAP.

campo-tipo

Campo de tipo de protocolo.

El tipo de protocolo de punto de acceso al 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 (utilizado sólo para 802.5)
- Novell SAP - E0 (utilizado sólo para 802.5)
- NetBIOS SAP - F0
- ISO Connectionless Internet - FE

Valor por omisión 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 de Ethernet (valor hexadecimal)
- IP - 0800
- ARP - 0806
- CHAOS - 0804
- Maintenance Packet Type - 7030
- DECnet MOP Dump/Load - 6000
- DECnet MOP Remote Console - 6002
- DECnet- 6003
- DEC LAT - 6004
- DEC LAVC - 6007
- XNS - 0600
- Apollo Domain - 8019 (Ethernet)
- Novell NetWare IPX - 8137 (Ethernet)
- AppleTalk Fase 1 - 809B
- Apple ARP Fase 1 - 80F3
- Loopback assistance - 9000

Valores por omisión de Ethernet: 1
El tipo de protocolo 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-ga

Dirección de grupo/multidifusión de 6 bytes (hexadecimal de 12 dígitos).

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

Valor por omisión: ninguno

dirección-fa

Dirección funcional en formato no canónico. Las direcciones funcionales son direcciones de grupo administradas localmente. Son las más utilizadas 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 de multiacceso a la configuración de puente. Este

mandato asocia un número de puerto con una interfaz Frame Relay y habilita el puerto para los puentes de direccionamiento en origen.

núm-interfaz Especifica la interfaz de Frame Relay en la que se está configurando el puerto de multiacceso.

Valores válidos: cualquier número de interfaz de Frame Relay existente

Valor por omisión: 0

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

Valores válidos: 1 a 254

Valor por omisión: el siguiente número de puerto disponible

núm-segmento Especifica un número de segmento de direccionamiento en origen hexadecimal de 12 bits que representa el segmento de multiacceso. Todos los puentes conectados con el segmento de 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 en origen hexadecimal de 4 bits que representa este puente en el segmento de multiacceso. Este parámetro sólo es necesario cuando se habilita el direccionamiento en origen la primera vez. El número de puente debe ser exclusivo entre todos los puentes del segmento de multiacceso.

Valores válidos: X'0' a X'F'

Valor por omisión: X'0'

núm-segmento-virtual Especifica un número de segmento de direccionamiento en origen hexadecimal de 12 bits. Este parámetro sólo es necesario cuando se habilita el direccionamiento en origen por primera vez en más de dos puertos de puente o la primera vez que se configura un puerto de puente de 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 de LAN/WAN a la configuración de puente. Este mandato asocia un número de puerto con el número de interfaz y habilita la participación de dicho puerto en los puentes transparente.

Valores válidos de números de puerto: 1 a 254

Valor por omisión de número de puerto: ninguno

Ejemplo: añadir un puerto

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

prot-filter snap ether dsap

Permite que el puente se configure de manera que pueda filtrar paquetes de modo selectivo en función del tipo de protocolo de éstos. Los filtros se pueden aplicar a todos los puertos o sólo a los puertos seleccionados.

Este parámetro especifica los identificadores de protocolo para los que se descartan exclusivamente las tramas recibidas de ese protocolo específico sin aplicar la lógica de puentes. Se descartarán también los paquetes ARP de ese tipo de protocolo. El filtro de protocolo se aplica sólo en los paquetes recibidos. Los filtros de protocolo disponibles son:

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

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

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

Notas:

1. No se pueden filtrar todos los paquetes de formato SNAP añadiendo un filtro DSAP para el tipo X'AA'. El(los) protocolo(s) SNAP encapsulado(s) se deben filtrar de manera individual. Considere la posibilidad de utilizar un filtro de ventana deslizante. Consulte el capítulo titulado “Utilización del filtro MAC” de *Utilización y configuración de las funciones*.
2. No se pueden configurar filtros de protocolo para un protocolo que esté direccionado en una interfaz específica si la interfaz también está configurada para puentes.

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

Tipos DSAP

Protocolo	SAP (valor hexadecimal)
SAP Banyan	BC (utilizado sólo para 802.5)
SAP IPX Novell	E0 (utilizado sólo para 802.5)
SAP NetBIOS	F0
Internet sin conexión ISO	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 de Ethernet

Protocolo	Tipo de Ethernet (valor hexadecimal)
IP	0800
ARP	0806
CHAOS	0804
Maintenance Packet Type	7030
DECnet MOP Dump/Load	6000
DECnet MOP Remote Console	6002
DECnet	6003
DEC LAT	6004
DEC LAVC	6007
XNS	0600
Apollo Domain	8019 (Ethernet)
Novell NetWare IPX	8137 (Ethernet)
Apple ARP Fase 1	80F3
Loopback assistance	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 para un puerto de puente. El túnel de puente permite que dominios de puente de ruta origen o dominios de puente transparente se comuniquen en una red IP.

A fin de que el tráfico de IBM LAN y de terminal se fusione con tráfico no IBM (es decir, Novell) en una única red troncal, las funciones de túnel de puente de direccionamiento en origen y de retransmisión SDLC (control de enlaces de datos síncrono) del software de dispositivo de puente encapsulan el tráfico IBM en paquetes TCP/IP estándar del sector. El dispositivo de puente direcciona entonces dichos paquetes mediante una vía de acceso IP o *túnel* a través de redes de internet IP grandes. Las ventajas que todo ello proporciona son una mayor funcionalidad y utilización de la red, así como una mayor disponibilidad de la red y facilidad de utilización.

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 superar el límite de distancia habitual de 7 saltos que se encuentra en las configuraciones de direccionamiento en origen. Le permite también conectar estaciones finales de direccionamiento en origen en medios de direccionamiento no origen, como pueden ser redes Ethernet.

El túnel de puente también supera las diversas limitaciones del direccionamiento en origen habitual, entre las que se incluyen:

- La limitación de distancia de siete saltos
- Las grandes cantidades de gastos generales que el direccionamiento en origen causa en redes de área amplia (WAN)
- La sensibilidad del direccionamiento en origen ante errores y anomalías de WAN (si falla una vía de acceso, todos los sistemas deben reiniciar sus transmisiones)

Teniendo la función de túnel de puente habilitada, el software encapsula paquetes en paquetes TCP/IP. Por lo que se refiere al dispositivo, el paquete tiene el aspecto de un paquete TCP/IP. Una vez se ha encapsulado una trama en un sobre IP, el reenviador IP es responsable de la selección de la interfaz de red adecuada según la dirección IP de destino. Este paquete se debe direccionar de manera dinámica a través de redes de internet grandes sin degradación o restricciones de tamaños de red. Las estaciones finales ven la vía de acceso, o el túnel, como un solo salto, independientemente de la complejidad de la red de internet.

El túnel es transparente para las estaciones finales. Los dispositivos de puente que participan en la creación de túneles tratan a la internet IP como uno de los segmentos de puente. Cuando el paquete alcanza la interfaz de destino, las cabeceras TCP/IP se eliminan de manera automática y el paquete interno continúa trabajando como si fuera un paquete de direccionamiento en origen estándar.

Add Tunnel crea el túnel IP definido por el usuario para un puerto de túnel. Este túnel se cuenta sólo como un salto entre los puentes, sin tener en cuenta la complejidad de la vía de acceso a través de la internet IP. Para utilizar la función de túnel, se debe habilitar el reenviador IP.

Sólo se puede añadir un túnel. Debe utilizar un *Número de puerto* que no se utilice para ningún otro puerto de LAN. Una vez se ha asignado un número de puerto al túnel de puente, se deben utilizar los demás mandatos de puente que necesiten un número de puerto como parámetro para configurar las características del túnel. Para la configuración

específica de túnel, como pueden ser las direcciones IP de los puntos finales, utilice el mandato **tunnel** (consulte “Tunnel” en la página 116).

El puente transparente está habilitado por omisión en este puerto. De todos modos, el direccionamiento en origen se puede habilitar utilizando la opción **Enable Source-Routing**.

Ejemplo:
```
add tunnel 3
Port Number   [1] ? 3
```

Port Number Un número de puerto exclusivo que no esté utilizando el puente.

BAN

Utilice el mandato **ban** para acceder al indicador de configuración del nodo de acceso de límite (BAN). Los mandatos BAN se entran en el indicador de configuración de BAN (`BAN config>`). Consulte “Mandatos de configuración de BAN” en la página 116 si desea obtener una explicación de dichos mandatos.

Sintaxis:

ban

Ejemplo:
```
ban
BAN (Boundary Access
Node) configuration
BAN config>
```

Change

Utilice el mandato **change** para cambiar el puente de direccionamiento en origen y los números de segmentos en la configuración de puente.

Sintaxis:

change bridge . . .

segment . . .

bridge *nuevo-núm-puente*

Cambia el número de puente en la configuración de puente.

Ejemplo: `change bridge 3`

segment *antiguo-núm-segmento nuevo-núm-segmento*

Cambia el número de segmento en la configuración de puente.

Ejemplo: `change segment 2 3`

Delete

Utilice el mandato **delete** para suprimir la siguiente información de la configuración de puente.

- Entradas de dirección de estación a la base de datos permanente
- Correlación de direcciones específicas de un protocolo determinado
- Puertos de LAN/WAN y de multiacceso
- Filtros de protocolo que filtran paquetes de manera selectiva según el tipo de protocolo.
- Direcciones MAC duplicadas

Para la función de túnel IP, el mandato **delete port** con el número de puerto correspondiente para el túnel elimina el túnel entre los puentes en una red de internet IP.

Sintaxis:

de**lete** address
dmac-addr
mapping . . .
port . . .
prot-filter . . .

address *valor-direc*
Elimina una entrada de direcciones de la base de datos permanente. La dirección es la dirección MAC de la entrada deseada. Entre el valor-direc (en formato hexadecimal de 12 dígitos) de la entrada que se debe suprimir y pulse **Intro**. Las direcciones de multidifusión no se pueden suprimir. SI intenta suprimir una entrada de direcciones 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-direc*
Suprime entradas de dirección MAC duplicadas de la base de datos. *Valor-direc* es la dirección MAC de la entrada que se 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-dlh campo-tipo dirección-ga*

Suprime una correlación de direcciones específica de un protocolo determinado.

tipo-dlh (Tipo de cabecera de enlace de datos) es una elección de DSAP, tipo Ether o SNAP.

campo-tipo Campo de tipo de protocolo.

El tipo de protocolo de punto de acceso al 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 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-ga Dirección de grupo/multidifusión 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 <group address>`

port *núm-puerto*

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

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

Ejemplo: `delete port 2`

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

Suprime los identificadores de protocolo especificados anteriormente que se han utilizado en el filtro. Puede suprimir filtros de todos los puertos o de los puertos seleccionados. Estos filtros incluyen lo siguiente:

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

Paquetes Ether
El Tipo Type con el tipo de protocolo entrado en un rango de 5DD – FFFF (hexadecimal).

Paquetes DSAP
El protocolo de punto de acceso al servicio de destino con el tipo de protocolo entrado en un rango de 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** (used for DSAP packets)

```
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 inhabilitar las siguientes funciones de puente:

- Puentes
- Tramas duplicadas
- Correlación entre direcciones de grupo y funcionales
- Propagación de las tramas exploradoras del árbol de extensión
- Direccionamiento en origen en un puerto determinado
- Conversión SR-TB
- Función de puente transparente (árbol de extensión) en un puerto determinado
- Función de direcciones MAC duplicadas
- Equilibrio de carga de MAC duplicadas
- DLSw

En la función de túnel, el mandato disable inhabilita un túnel entre estaciones finales en una red de internet 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 Inhabilita por completo la función de puenteo. De todos modos, este mandato no elimina los valores de puente configurados anteriormente.

Ejemplo: `disable bridge`

dls Inhabilita el funcionamiento de DLSw en el puente. (El dispositivo que ejecuta DLSw aparece como un puente para las estaciones finales). Consulte “Utilización de DLSw” en la página 535 si desea obtener más detalles al respecto.

Ejemplo: `disable dls`

duplicate *tipo-trama*
Inhabilita la creación de tramas duplicadas presentes en entornos de puentes mixtos. Cuando se habilita la función de puenteo SR-TB en una interfaz 802.5 (con el direccionamiento en origen y los puentes transparentes habilitados), surgen incoherencias cuando se envían por puente tramas a un destino desconocido (o de multidifusión). El puente no sabe si el destino se encuentra tras un direccionamiento en origen (sólo) o tras un puente transparente.

Para resolver esta situación, el puente envía duplicados de dichas tramas (por omisión). Una trama tiene campos de direccionamiento en origen presentes (un RIF explorador del árbol de extensión) y la otra está formateada para puente transparente (no hay ningún RIF presente). El mandato **disable duplicate** le permite eliminar esta duplicación al permitir que inhabilite la creación de uno de estos tipos de tramas. El mandato **disable duplicate** no le permitirá que inhabilite simultáneamente ambos tipos de tramas.

Si entra **STE** después del mandato, le estará indicando al puente que se abstenga de enviar tramas exploradoras del árbol de extensión generadas para el entorno de direccionamiento en origen. Si entra **TSF** después del mandato, le estará indicando al puente que se abstenga de enviar tramas de árbol de extensión transparente para el entorno de puente transparente. En ambos casos, se trata de un situación en la que normalmente ambos tipos de tramas se pueden enviar. Al el puente transparente en la interfaz también se inhabilita la creación de tramas transparentes.

Ejemplo: `disable duplicate TSF`

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

dmac-addr

Inhabilita la función 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

Inhabilita el equilibrio de carga de MAC duplicadas para la función 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

Inhabilita la conversión de tramas SNA al formato Ethernet de tipo 2, tal y como la utilizan los IBM RT que ejecutan OS/2 EE.

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

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

fa-ga-mapping

Inhabilita la correlación de dirección de grupo con dirección funcional (y a la inversa). En ciertas circunstancias, es probable que desee inhabilitar la correlación entre la dirección de grupo y la dirección funcional de manera global.

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

ibm8209-spanning-tree

Elimina la participación de puentes en protocolos de árbol de extensión con puentes IBM 8209.

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

ipx-conversion

Inhabilita de manera global la conversión de tramas Novell IPX cuando el puente une puertos de puente Ethernet/802.3 y de red en anillo (802.5). Cuando se inhabilita, las tramas Novell IPX pueden enviarse por puente entre estaciones finales del mismo tipo de medio a través de una LAN troncal de un tipo de medio diferente, pero no así entre estaciones finales de diferentes medios.

Ejemplo: **disable ipx-conversion**

spanning-tree-explorer *núm-puerto*

Inhabilita a un puerto para que no permita la propagación de tramas exploradoras del árbol de extensión si el direccionamiento en origen está habilitado. Este mandato sólo se utiliza si el puente transparente no está habilitado en el puerto. En tal caso, se reconoce automáticamente de acuerdo con el árbol de extensión transparente.

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

source-routing *núm-puerto*

Inhabilita el direccionamiento en origen en un puerto determinado. Este mandato se utiliza para disponer de un direccionamiento en origen discontinuo de interfaz de puente de participación ya activa.

Ejemplo: **disable source-routing 2**

sr-tb-conversion

Inhabilita la conversión de tramas direccionadas de origen en tramas transparentes y viceversa.

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

stp Inhabilita el protocolo de árbol de extensión en el puente. Por omisión está habilitado.

Ejemplo: **disable stp**

transparent *núm-puerto*

Inhabilita la función de puente transparente en el puerto determinado. Este mandato es útil para los casos en que es recomendable un método de comunicación alternativo como puede ser el direccionamiento en origen.

Nota: Este mandato puede generar una configuración absurda si no se utiliza correctamente. Por ejemplo, si se utiliza en una interfaz

Ethernet, se inhabilitará la función de puenteo para dicha interfaz. Este mandato se utiliza para generar la función de puente SRB y SR-TB.

Ejemplo: `disable transparent 2`

tree *núm-puerto*
Inhabilita la participación STP del puente según los puertos.

Ejemplo: `disable tree 1`

Nota: La inhabilitación de STP según los puertos puede producir bucles de red a causa de la existencia de puentes paralelos.

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

Ejemplo: `disable ub-encapsulation`

Enable

Utilice el mandato **enable** para habilitar las siguientes funciones de puenteo:

- Puentes
- Tramas duplicadas
- Correlación entre direcciones de grupo y funcionales
- Propagación de las tramas exploradoras del árbol de extensión
- Direccionamiento en origen en un puerto determinado
- Conversión SR-TB
- Función de puente transparente (árbol de extensión) en un puerto determinado
- Función de direcciones MAC duplicadas
- Equilibrio de carga de 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 Habilita la función de puente transparente en todos los dispositivos LAN (interfaces) configurados en el dispositivo de puente. Los números de puerto se asignan a cada interfaz como el número de interfaz anterior más 1. Por ejemplo, si la interfaz 0 es un dispositivo LAN, su número de puerto será 1.

Ejemplo: `enable bridge`

dls Habilita el funcionamiento de DLSw en el puente. El dispositivo que ejecuta DLSw aparece como un puente para las estaciones finales. Consulte “Utilización de DLSw” en la página 535 si desea obtener más información.

Ejemplo: `enable dls`

duplicate *tipo-trama*
Habilita la generación de tramas STE (explorador de árbol de extensión) duplicadas o tramas TSF (tramas de árbol de extensión transparente). Este mandato está disponible para contrarrestar el mandato **disable duplicate**. La generación de tramas duplicadas está habilitada por omisión. El mandato **enable duplicate** puede ir seguido de un tipo de trama **TSF** o **STE**, para habilitar de manera específica uno de estos tipos de trama, o del tipo de trama **BOTH**, que produce el mismo comportamiento que el no especificar un tipo de trama para este parámetro.

Ejemplo: `enable duplicate STE`

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

dmac-addr
Habilita la función de direcciones MAC duplicadas. Consulte “Función de direcciones MAC duplicadas de SR-TB” en la página 54 si desea obtener más información acerca de la función 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

Habilita el equilibrio de carga de MAC duplicadas para la función de direcciones MAC duplicadas. Consulte “Función de direcciones MAC duplicadas de SR-TB” en la página 54 si desea obtener 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

Habilita la conversión de tramas SNA en Ethernet de tipo 2, tal y como la utilizan los RT de PC que ejecutan OS/2 EE. Ello hará que las tramas SNA se dupliquen tanto en formato 802.3/802.2 como en formato IBM-RT para sistemas principales desconocidos de una Ethernet.

Ejemplo: `enable ethertype-ibmrt-pc`

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

fa-ga-mapping

Habilita la correlación de dirección de grupo con dirección funcional (y a la inversa). Esta correlación se lleva a cabo cuando se reenvían tramas entre la red en anillo y otros medios (excepto la línea serie). En el entorno de red en anillo, las direcciones funcionales son más populares aunque se les asignan direcciones de grupo localmente a causa de las restricciones de hardware. En otros medios, se utilizan mucho las direcciones de grupo. En condiciones normales la correlación de dirección de grupo con dirección funcional es inevitable.

La correlación se habilita por omisión si se han añadido direcciones de correlación. La correlación de habilitación/inhabilitación ofrece a los usuarios una opción cuando se deben suprimir registros de correlación añadidos.

Ejemplo: `enable fa-ga-mapping`

ibm8209-spanning-tree

Permite la participación de puentes en protocolos de árbol de extensión con puentes IBM 8209.

Ejemplo: `enable ibm8209-spanning-tree`

ipx-conversion

Habilita de manera global la conversión de tramas Novell IPX cuando el puente une puertos de puente Ethernet/802.3 y de red en anillo (802.5). Cuando se habilita, las tramas Novell IPX pueden enviarse por puente entre estaciones finales de medios diferentes.

Ejemplo: `enable ipx-conversion`

spanning-tree-explorer *núm-puerto*

Habilita al puerto para que permita la propagación de tramas exploradoras del árbol de extensión si el direccionamiento en origen está habilitado. Este mandato sólo es válido en puertos de red en anillo y WAN. Esta función se habilita por omisión cuando el direccionamiento en origen está configurado en el puerto.

Ejemplo: `enable spanning-tree-explorer 2`

source-routing *núm-puerto núm-segmento [núm-puerto]*

Habilita el direccionamiento en origen de un puerto determinado. Este mandato se utiliza habitualmente cuando se requiere el direccionamiento en origen en parte del puente. Si la única función que desea es el direccionamiento en origen, debe inhabilitar el puente transparente en la interfaz. Es necesario entrar el número de puente para la primera instancia del mandato. Dicha entrada ya no es necesaria en posteriores ocasiones.

núm-puerto

El puerto válido que participa en la configuración de puentes.

Valores válidos: X'0' a X'FFF'

Valor por omisión: 1

núm-segmento

Un número de 12 bits que representa la LAN/WAN a la que se conectan los medios. Todos los medios de otros puentes conectados a esta LAN/WAN se deben configurar con el mismo valor. Para obtener un correcto funcionamiento de la función de direccionamiento en origen es muy importante que todos los puentes conectados a esta LAN/WAN dispongan de la misma perspectiva del valor de identificación de LAN/WAN.

núm-puente

Valor de 4 bits exclusivo entre todos los puentes conectados a la misma LAN/WAN. Este valor es necesario cuando se habilita el direccionamiento en origen en la primera interfaz. Esta entrada es opcional para interfaces posteriores. Se recomienda que el núm de puente sea exclusivo en el segmento.

Valores válidos: X'0' a X'F'

Valor por omisión: 1

Nota: Si en la configuración existen dos segmentos ya configurados (es decir una configuración 1:N SRB), se le solicitará un parámetro de *núm-segmento-virtual* adicional.

Ejemplo: `enable source-routing 2 1 1`

sr-tb-conversion

Esta opción habilita la conversión del formato de trama de direccionamiento en origen en formato de trama de puente transparente y viceversa. Permite la compatibilidad entre los dominios de direccionamiento en origen y de puente transparente. Cuando esta función está habilitada, el puente deja que las tramas direccionadas de

origen sean aceptadas en un dominio transparente quitando el campo RIF y convirtiéndolas en tramas transparentes.

El puente también reúne información de direccionamiento referente a las estaciones de direccionamiento en origen de las tramas de direccionamiento en origen pasajeras. Esto se obtiene a partir del RIF. Esta información de RIF se utiliza entonces para convertir una trama transparente en una trama direccionada de origen. Si no hay disponible un RIF para una estación, la trama se envía como trama exploradora del árbol de extensión del dominio de direccionamiento en origen.

A fin de que la función de conversión funcione correctamente, es necesario dar un número de segmento al dominio de puente transparente. Todos los puentes SR-TB que se conectan a este dominio se deben configurar también con el mismo número de segmento.

Valores válidos del número de segmento del dominio TB: X'1' - X'FFF'

Valor por omisión del número de segmento del dominio TB: 1

La unidad máxima de transmisión (MTU) es el número máximo de octetos por trama de datos que se puede transferir por una red física determinada. Cuando un datagrama IP viaja de un sistema principal a otro, puede cruzar diferentes redes físicas. Algunas redes físicas pueden tener establecida esta MTU, lo que no permitirá situar grandes datagramas IP en una trama física. Si intenta transmitir tramas más grandes que las que puede manejar la red física, se producirá una fragmentación.

Valores válidos de MTU del dominio TB: de 576 a 18000 bytes

Valor por omisión de MTU del 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 Habilita el protocolo de árbol de extensión en el puente. Es el valor por omisión.

Ejemplo: `enable stp`

transparent *núm-puerto*
Habilita la función de puente transparente en el puerto indicado. En circunstancias normales, este mandato no es necesario.

Ejemplo: `enable transparent`

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

tree *núm-puerto*
Habilita la participación STP del puente según los puertos.

Ejemplo: `enable tree 1`

ub-encapsulation
Hace que tramas de Ethernet de tipo 2 de XNS se conviertan en tramas de Red en anillo mediante el Ungermann-Bass OUI de la cabecera SNAP. Las tramas de red en anillo que contienen la cabecera UB OUI

se reenviarán a las Ethernets como tramas de Ethernet de tipo 2 0x0600 en lugar de tramas 802.3/802.2.

Ejemplo: `enable ub-encapsulation`

List

Utilice el mandato **list** para visualizar información sobre la configuración completa de puentes o para visualizar información sobre los parámetros de configuración seleccionados.

Sintaxis:

list address
bridge
dmac
filtering . . .
mapping . . .
multiaccess
permanent . . .
port . . .
prot-filter . . .
protocol
range . . .

address *valor direc* Lee una entrada de direcciones de la base de datos permanente. El valor direc es la dirección MAC de la entrada necesaria. Puede ser una dirección individual, una dirección de multidifusión o una dirección de difusión. El proceso de encendido/apagado no destruye las bases de datos permanentes y éstas 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 Una entrada de dirección en formato hexadecimal de 12 dígitos.

Entry Type

Permanent
Indica que la entrada es permanente por naturaleza y que resistirá a los apagados y encendidos o a las reinicializaciones del sistema.

Reserved

Indica que la entrada está reservada por el comité IEEE 802.1d para su futura utilización. Se descartan las tramas destinadas a direcciones reservadas.

Registered

Indica que la entrada está destinada al propio puente.

SAF Aparece después del tipo de entrada si se ha configurado el filtro de direcciones origen.

Input Port

Visualiza los números de puerto o puertos de entrada asociados con dicha entrada de dirección.

Output Port

Visualiza los números de puerto o puertos de salida asociados con dicha entrada de dirección. Visualiza "NONE/DAF", lo cual indica que se aplica el filtro de direcciones de destino porque no se han seleccionado puertos que se deban asociar con esa entrada de dirección.

bridge Lista toda la información general referente 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 (habilitado) o DISABLED (inhabilitado).

Bridge Behavior
Indica el método de puenteo que utiliza dicho puente. Los valores son STB si es transparente, SRB si es de direccionamiento en origen y ADAPTIVE SRT si es de conversión de direccionamiento en origen a puente transparente.

Bridge Number
El número exclusivo que identifica un puente. Se utiliza para distinguir varios puentes que conectan los mismos dos anillos.

Segments
Indica el número de segmentos de puente de direccionamiento en origen configurados para el dominio de direccionamiento en origen.

Max ARE/STE Hop cnt
El número máximo de saltos para las tramas que transmiten desde el puente para una interfaz determinada asociada con el puente de direccionamiento en origen.

1:N SRB Indica el estado actual del direccionamiento en origen 1:N como ACTIVE (activo) o NOT ACTIVE (no activo).

Internal Segment
Visualiza el número de segmentos virtuales configurados para puentes 1:N SRB.

LF-bit interpretation
Indica la modalidad de interpretación de codificación de bits de trama más grande (LF) si el direccionamiento en origen se ha habilitado. Dicha modalidad aparece listada como BASIC (básica) o EXTENDED (ampliada).

SR-TB Conversion
Indica si la conversión de tramas de direccionamiento en origen/puente transparente está habilitada o inhabilitada.

TB-Virtual Segment
Indica el número de segmentos del dominio de puente transparente.

MTU for TB-Domain
Especifica el tamaño máximo de trama (unidades máximas de transmisión) que el puente transparente puede transmitir y recibir.

Bridge address
La dirección de puente especificada por el usuario (si se ha establecido).

Bridge priority
Una dirección de puente de 2 octeto de orden alto que se encuentra en el identificador del puente, la dirección MAC obtenida del puerto con el número más bajo o la dirección establecida por el mandato Set Bridge.

STP Participation
Visualiza los tipos de protocolos de árbol de extensión en los que participa el puente.

FA-GA conversion
Indica si la conversión FA-GA está habilitada o inhabilitada.

UB Encapsulation
Indica si la encapsulación UB está habilitada o inhabilitada.

DLS for the bridge
Indica si el protocolo de conmutador de enlace de datos está habilitado o inhabilitado en el puente.

IPX Conversion
Indica si la conversión IPX está habilitada o inhabilitada.

Conversion Mode
Indica la modalidad de conversión IPX como automática o manual.

Ethernet Preference
Indica el tipo de tramas de Ethernet preferibles utilizados para la conversión IPX Conversion como IEEE-802.3 o Ethernet.

Number of ports added
El número de puertos de puente añadidos a la configuración de puente.

Port Number
Un número definido por el usuario asignado a una interfaz por el mandato Add Port.

Interface Number
Identifica dispositivos conectados a un segmento de red a través del puente. Debe añadir, como mínimo, dos interfaces que participen en el puente. Para el puente, se utiliza el número de interfaz 255.

Port Behavior
Indica el método de puenteo que utiliza ese puerto, STB si es de puente transparente y SRB si es de puente de direccionamiento en origen.

Circuit Number
Especifica la DLCI asociada con el puerto Frame Relay.

dmac Visualiza las opciones configuradas para la función de direcciones MAC.

Ejemplo: `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-grupo_datos* Los siguientes grupos de datos generales se pueden visualizar con el mandato **list filtering**:

All Visualiza todas las entradas de bases de datos de filtro.

Ethertype Visualiza las entradas de bases de datos de filtros de tipo de protocolo Ethernet.

SAP Visualiza las entradas de bases de datos de filtros de protocolos SAP.

SNAP Visualiza las entradas de bases de datos de filtros de identificadores 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 que se utilizan para explicar la manera como se comunican los paquetes son:

Routed Describe los paquetes que han pasado al reenviador de direccionamiento y que se deben reenviar.

Filtered Describe los paquetes que se filtran de manera administrativa estableciendo los filtros de protocolo que el usuario establece.

Bridged and routed
Describe un identificador de protocolo para el que existe una entidad de protocolo dentro del sistema que no es un reenviador. Por ejemplo, un protocolo de eco de nivel de enlace. Los paquetes de unidifusión de este protocolo se puentean o bien se procesan localmente si se envían a una dirección registrada. Los paquetes de multidifusión se reenvían y se procesan localmente para una dirección de multidifusión registrada.

Todos estos descriptores también se aplican a paquetes ARP con este tipo de Ethernet.

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-adición campo-tipo* Lista una correlación de direcciones específica para un protocolo determinado.

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-adición
Elija DSAP, Ether (Ethernet) o SNAP.

campo-tipo

Campo de tipo de protocolo:

- El tipo de protocolo de punto de acceso al 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 SNAP se entra en formato hexadecimal de 10 dígitos.

multiaccess Visualiza la antigüedad de las entradas de la base de datos de multiacceso y visualiza los puertos de puente de multiacceso. Consulte la salida del mandato **list port** si desea obtener una descripción de los parámetros de puertos de puentes.

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 Visualiza 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* Visualiza información sobre puertos relacionada con los puertos que ya están configurados. Al especificar el núm_puerto se selecciona el puerto que se desea listar. Si no se especifica ningún puerto, 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 El ID consta de dos partes: la prioridad del puerto y el número del puerto. En el ejemplo, 128 es la prioridad y 1, 2 y 3 son los números de puerto. El byte de orden bajo, en formato hexadecimal, denota el número de puerto y el byte de orden alto denota la prioridad.

Port state
Visualiza el estado actual del puerto o los puertos especificados. Puede ser ENABLED (habilitado) o DISABLED (inhabilitado).

Port supports
Visualiza el método de puenteo soportado en este puerto (por ejemplo, puentes transparentes).

SRB Sólo se visualiza cuando SRB está habilitado y presenta información de puente de direccionamiento en origen. Dicha información incluye el número de segmento SRB (en formato hex), el tamaño de la unidad máxima de transmisión y si la transmisión de tramas exploradoras del árbol de extensión está habilitada o inhabilitada.

Duplicate Frames Allowed
Visualiza un desglose y un recuento de los tipos de tramas duplicadas que se permiten.

Assoc interface
Visualiza el número de interfaz asociado con el puerto que se visualiza.

Path Cost
El coste asociado con el puerto que se utiliza para el coste posible 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 filtros. Los filtros se pueden listar de manera selectiva por puerto o se pueden visualizar todos los puertos a la vez. Al especificar el núm_puerto se selecciona el puerto que desea listar.

Ejemplo: `list prot-filter 1`

```
PORT 1
Protocol Class   :  DSAP
Protocol Type    :  01
Protocol State:  :  Filtered
Port Map         :  1, 2, 3
```

Port Number
Se visualiza el número de puerto de cada puerto si se ha seleccionado la visualización de todos los puertos.

Protocol Class
Visualiza la clase de protocolo (SNAP, Ether o DSAP).

Protocol Type
Visualiza el ID de protocolo en formato hexadecimal.

Protocol State
Denota que se está filtrando el protocolo del puerto seleccionado.

Port Map Visualiza los números de los puertos en los que está presente este tipo de filtro de protocolo.

protocol Visualiza información de puente relacionada con el protocolo de árbol de extensión.

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 puentes se describen también en el capítulo anterior.

Bridge Identifier
Valor de 8 bytes en formato ASCII. Si no ha establecido la dirección de puente antes de visualizar esta información, los 6 bytes de orden bajo se visualizarán como cero, lo que significa que se está utilizando la dirección MAC por omisión de un puerto. Cuando se ha seleccionado un puente como puente raíz, éste transmite la antigüedad máxima del puente

y el tiempo entre BPDU Hello del puente a todos los puentes de la red a través de las BPDU Hello.

Bridge-Max-Age
La antigüedad máxima (periodo de tiempo) al cabo de la cual la información relacionada con el árbol de extensión excede el tiempo de espera.

Bridge-Hello-Timer
Intervalo de tiempo entre las BPDU Hello.

Bridge-Forward-Delay
Intervalo de tiempo que transcurre antes de cambiar a otro estado (si este puente se convierte en raíz).

range *índice-inicial* *índice-final* Lee una rango de entradas de dirección de la base de datos permanente. Para especificarlo, determine primero el tamaño de la base de datos utilizando el mandato **list permanent**. A partir de este valor puede determinar un valor de "índice inicial" para el rango de entradas. El índice inicial está comprendido en el rango de 1 hasta el tamaño de la base de datos. A continuación puede elegir un "índice final" para visualizar un número limitado de entradas. Esta entrada es opcional. Si no especifica el índice final, el valor por omisión es el tamaño de la base de datos.

Las entradas de dirección 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 La dirección MAC de 6 bytes de la entrada.

Entry Type
Especifica uno de los siguientes tipos:

- Reserved - entradas reservadas por el comité IEEE 802.1d
- Registered - entradas que constan de direcciones de unidifusión que pertenecen a hardware de comunicaciones propietario conectado a la caja o direcciones de multidifusión habilitadas por reenviadores de protocolo.
- Permanent - entradas que el usuario especifica en el proceso de configuración que permanecen después de apagar y encender el sistema o después de reinicializarlo.
- Static - entrada que el usuario especifica en el proceso de supervisión que no permanecen después de encender o apagar el sistema o después de reinicializarlo y que no caducan

- Dynamic - entradas que el puente “averigua” de manera “dinámica” que no permanecen después de encender o apagar el sistema o después de reiniciarlo y que tienen una “antigüedad” asociada con la entrada.
- Free - ubicaciones de la base de datos que se pueden rellenar con entradas de dirección

Port Map Visualiza la correlación de puertos de salida de los puertos de entrada.

NetBIOS

Visualiza el indicador de configuración de NetBIOS. Entre **netbios** en el indicador `ASRT config>` para visualizar el indicador de configuración de NetBIOS. Consulte “Mandatos de NetBIOS” en la página 174 si desea obtener una explicación de los mandatos de configuración de NetBIOS.

Sintaxis:

netbios

Ejemplo: **`netbios`**

```
NetBIOS Support User Configuration
NetBIOS config>
```

Nota: Si no ha adquirido la 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 establecer ciertos valores, funciones y parámetros asociados con la configuración de puentes. Éstos pueden ser:

- La antigüedad de las entradas de dirección dinámicas de la base de datos de filtro
- La dirección del puente
- La modalidad de conversión IPX y la preferencia de Ethernet
- La interpretación de la codificación de bits de las tramas más grandes (LF) para el direccionamiento en origen
- El tamaño de la unidad de datos del servicio MAC (MSDU)
- Los parámetros de puente y de puerto del protocolo de árbol de extensión
- El límite del descriptor de ruta (RD)
- El tamaño de la base de datos de filtro de puentes
- La antigüedad de los RIF asociados con direcciones MAC duplicadas
- La antigüedad de las entradas de la base de datos de 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 *segundos resolución*

Establece el intervalo de tiempo al cabo del cual caducan las entradas dinámicas de la base de datos de filtro cuando el puerto que dispone de la entrada se encuentra en estado de reenvío. Esta antigüedad también se utiliza para entradas RIF de antigüedad en la base de datos adaptable en el caso de una personalidad de puente SR-TB.

Entre el valor necesario después de cada indicador y pulse **Intro**.

Valores válidos de antigüedad: 10 a 1000000

Valor por omisión de antigüedad: 30

El valor de resolución especifica la frecuencia con la que se debe explorar las entradas dinámicas de la base de datos de filtro a fin de determinar si han excedido el límite de antigüedad que el temporizador de antigüedad ha establecido.

Valores válidos de resolución: 1 a 60 segundos

Valor por omisión de resolución: 5 segundos

Ejemplo: **`set age`**

```
seconds [300]  ?  400
resolution [5] ?  6
```

bridge *dirección-puente*

Establece la dirección del puente. Es la dirección de puente de 6 octetos de orden bajo que se encuentra en el identificador del puente. Por omisión, el valor de la dirección del puente es la dirección de control de acceso medio (MAC) del puerto con el número más bajo en el momento de la inicialización. Este mandato se puede utilizar para alterar temporalmente la dirección por omisión y entrar la dirección exclusiva del usuario.

Entre *srb* o *tb* para especificar si la dirección del puente de direccionamiento en origen (srb) o del puente transparente (tb) se verá afectada.

Nota: Todos los puentes de la red deben disponer de una dirección exclusiva para que el protocolo de árbol de extensión funcione correctamente.

Atención: En los casos en los que una interfaz de línea serie (o túnel) sea el puerto con el número más bajo, es obligatorio utilizar este mandato a fin de que el puente disponga de una dirección exclusiva cuando se reinicie. Este proceso es necesario porque las líneas serie no disponen de su propia dirección MAC.

Entre en el indicador 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 mantendrá su valor anterior. Para devolver la dirección del puente al valor por omisión, entre una dirección con todo ceros.

Valores válidos: 12 dígitos hexadecimales

No utilice guiones ni dos puntos para separar cada octeto. Todos los puentes de la red deben disponer de una dirección exclusiva para que el protocolo de árbol de extensión funcione correctamente.

Valor por omisión: 000000000000

Ejemplo: **`set bridge`**

```
Bridge Address (in 12-digit hex)[]?
```

conversion-mode *modalidad*

Especifica la modalidad de conversión IPX como automática o manual.

modalidad

Cuando la modalidad de conversión se establece en automática, el tipo de trama IPX de cada estación final Ethernet/802.3 se averigua y se almacena en la base de datos de filtro y se utilizará en conversiones posteriores al formato MAC de Ethernet/802.3. El parámetro Ethernet Preference determina el tipo de trama IPX que se debe utilizar al convertir al formato MAC de Ethernet /802.3 MAC si todavía no se ha averiguado uno.

Cuando la modalidad de conversión se establece en manual, el valor del parámetro Ethernet Preference especifica en qué tramas IPX de Ethernet/802.3 se debe realizar la conversión.

Valores válidos de modalidad de conversión: automatic o manual

Valor por omisión de modalidad de conversión: automatic

Ejemplo: **`set conversion-mode manual`**

ethernet-preference *preferencia*

Especifica IEEE-802.3 o Ethernet como tipo de trama IPX preferida.

preferencia Cuando la modalidad de conversión se establece en automática, el tipo de trama IPX de cada estación final Ethernet/802.3 se averigua y se almacena en la base de datos de filtro y se utilizará en conversiones posteriores al formato MAC de Ethernet/802.3. El parámetro Ethernet Preference determina el tipo de trama IPX que se debe utilizar al convertir al formato MAC de Ethernet /802.3 MAC si todavía no se ha averiguado uno.

Cuando la modalidad de conversión se establece en manual, el valor del parámetro Ethernet Preference especifica en qué tramas IPX de Ethernet/802.3 se debe realizar la conversión.

Valores válidos de la preferencia de Ethernet: ieee-802.3 or ethernet

Valor por omisión de la preferencia de Ethernet: ieee-802.3

Ejemplo: `set ethernet-preference ethernet`

dmac-age *segundos*

Establece el tiempo al cabo del cual caducan las entradas RIF de la tabla RIF para direcciones MAC duplicadas. Este valor se utilizará sólo para las direcciones MAC duplicadas averiguadas. Para el resto de direcciones, se utilizará el valor que se haya especificado con el mandato **set age** para antigüedad.

Entre el valor que desee después de cada indicador y pulse **Intro**.

Valores válidos de antigüedad DMAC: 10 a 1000000

Valor por omisión de antigüedad 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 *tamaño-base_datos*

Establece el número de entradas que se pueden mantener en la base de datos de filtro de puentes.

Valor por omisión: 1024 veces el número de los puertos de puente.

Si desea obtener más información, consulte el mandato **list filtering** en la página 102.

Ejemplo: `set filtering`

```
database-size [2048]?
```

lf-bit-interpretation *modalidad-codificación*

Establece la interpretación de codificación de bits de las tramas más grandes (LF) si el direccionamiento en origen está habilitado en este puente.

Ejemplo: `set lf-bit-interpretation basic`

Encode-mode

Se entra como **basic** (básica) o **extended** (ampliada). En la modalidad básica sólo se utilizan 3 bits del campo de control de direccionamiento. Es la modalidad más común en los puentes de direccionamiento en origen que existen en la actualidad. En la modalidad ampliada, se utilizan 6 bits del campo de control de direccionamiento para representar la unidad máxima de datos a la que el puente da soporte. El valor por omisión es **extended** (ampliada). Los nodos ampliados y básicos son compatibles.

maximum-packet-size *núm-puerto tamaño-msdu*

Establece el tamaño más grande de la unidad de datos del servicio MAC para el puerto, si el direccionamiento en origen está habilitado en

este puerto. El valor MSDU no tiene ninguna repercusión en medios tradicionalmente transparentes. Un valor MSDU mayor que el tamaño del paquete configurado en el dispositivo será considerado un error.

Si este parámetro no se establece, el valor por omisión es el tamaño configurado como tamaño de paquete para esa interfaz.

Valores válidos: Especifique un entero del rango de 16 a 65535

Valor por omisión: el tamaño de paquete establecido para el puerto

Ejemplo: `set maximum-packet-size 1 4399`

multiaccess-age *segundos*

Establece el tiempo al cabo del cual caducan las entradas de la base de datos de multiacceso. La base de datos es explorada a la velocidad a la que se ha establecido el parámetro *resolución* 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*

Inicia la participación del puerto en el protocolo de árbol de extensión. Esto se consigue entrando el valor de estado “block”, lo que sitúa al puerto en un estado “bloqueado” como punto de partida. El protocolo de árbol de extensión determinará más tarde el estado real del puerto a medida que determina su topología. Si se entra el valor de estado “disable”, el puerto no participa en el árbol de extensión.

Ejemplo: `set port block`

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

protocol *bridge* **o** *port*

Modifica el puente de protocolo de árbol de extensión o los parámetros de puerto para una nueva configuración o ajusta los parámetros de configuración para que se adapten a una topología específica.

Entre “bridge” como opción para modificar parámetros de puente. Los parámetros relacionados con puentes que se pueden modificar con este mandato se describen a continuación.

Entre **srb** o **tb** para especificar si los parámetros del protocolo de árbol de extensión del puente de direccionamiento en origen (srb) o del puente transparente se verán afectados.

Al establecer estos valores, asegúrese de que existen las siguientes relaciones entre los parámetros o la entrada será rechazada:

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

La antigüedad máxima (periodo de tiempo) al cabo de la cual la información relacionada con el árbol de extensión excede el tiempo de espera.

Cuando este dispositivo de puente se selecciona como puente raíz en un árbol de extensión, el valor de este parámetro especifica el tiempo durante el que los puentes activos deben almacenar las unidades de datos de protocolos de puente (BPDU) de configuración que reciben. Cuando una BPDU alcanza su límite máximo de antigüedad sin que se la sustituya, los puentes activos de la red la descartan y presuponen que el puente raíz ha fallado. A continuación, se selecciona un nuevo puente raíz.

Dependencias

El valor de este parámetro puede verse afectado por el valor del parámetro Bridge Hello Time. Además, el valor de este parámetro puede afectar al valor del parámetro Bridge Forward Delay.

Valores válidos: 6 a 40 segundos

Valor por omisión: 20 segundos

Bridge Hello Timer

Intervalo de tiempo entre las BPDU Hello.

Cuando este dispositivo de puente se selecciona como puente raíz en un árbol de extensión, este parámetro especifica la frecuencia con la que este puente transmite unidades de datos de protocolos de puente (BPDU) de configuración. Las BPDU contienen información sobre la topología del árbol de extensión y reflejan los cambios en la topología.

Dependencias

El valor de este parámetro puede afectar el valor del parámetro Max age.

Valores válidos: 1 a 10 seconds

Valor por omisión: 2

Bridge Forward Delay

Intervalo de tiempo que transcurre antes de cambiar a otro estado (si este puente se convierte en raíz).

Cuando este dispositivo de puente se selecciona como puente raíz en un árbol de extensión, el valor de este parámetro especifica el tiempo durante el que los puertos activos de todos los puentes permanecen en un *estado de escucha*. Cuando finaliza el tiempo del reenvío, los puertos en estado de escucha entran en *estado de reenvío*. Se producen cambios de estado a consecuencia de los cambios en la topología del árbol de extensión, como pueden ser los producidos falla o se concluye un puente.

El puente raíz transmite este valor a todos los puentes. Este proceso garantiza que todos los puentes sean coherentes entre los cambios.

Dependencias

El valor de este parámetro puede verse afectado por el valor del parámetro SRB Bridge Max Age.

Valores válidos: 4 a 30 segundos

Valor por omisión: 15

Bridge Priority

Una dirección de puente de 2 octetos de orden alto que se encuentra en el identificador del puente - la dirección MAC obtenida a partir del puerto con el número más bajo o la dirección establecida por el mandato **Set Bridge**.

La prioridad del puente indica las posibilidades de que este puente se convierta en el puente raíz del árbol de extensión. Cuanto menor es el valor numérico de la prioridad del puente, mayor es la prioridad del puente y más probabilidades hay de que se seleccione. El algoritmo del árbol de extensión elige el puente con el valor numérico más pequeño de este parámetro para que sea el puente raíz.

Valores válidos: 0 a 65535

Valor por omisión: 32768

Entre **port** como opción para modificar los parámetros del puerto de protocolo de árbol de extensión. Entre el valor que desee en cada solicitud y pulse **Intro**.

Ejemplo: `set protocol port`

```
Port Number [1] ?
Port Path-Cost (0 for default) [0] ?   1
Port Priority [128] ?   1
```

Port Number

El número del puerto del puente; selecciona el puerto cuyos coste de vía de acceso y prioridad de puerto se cambiarán.

Path Cost

El coste asociado con el puerto que se utiliza para el coste posible de vía de acceso raíz.

Cada interfaz de puerto dispone de un coste de vía de acceso asociado, que es el valor relativo de la utilización del puerto para alcanzar el puente raíz en una red puenteada. El algoritmo de árbol de extensión utiliza el coste de vía de acceso para calcular una vía de acceso que minimice el coste desde el puente raíz hasta el resto de puentes de la topología de red.

Este parámetro especifica el coste asociado con las tramas pasajeras a través de la interfaz de este puerto, si este dispositivo de puente se convierte en puente raíz. Factorice este valor cuando

determine rutas de árbol de extensión entre dos estaciones cualesquiera. Un valor de 0 ordena al dispositivo de puente que calcule automáticamente un coste de vía de acceso para este puerto utilizando sus propias fórmulas.

Valores válidos: 1 a 65535

Valor por omisión: 0 (significa que el coste se calculará de manera automática)

Port Priority

Identifica la prioridad de puerto del puerto especificado. El algoritmo de árbol de extensión la utiliza al efectuar comparaciones para la selección de puertos (qué puerto ofrece el coste de vía de acceso más bajo al puente raíz) y para tomar decisiones de bloqueo.

Valores válidos: 0 a 255

Valor por omisión: 128

route-descriptor-limit *tipo-límite*

Permite al usuario asociar una longitud máxima de descriptor de ruta (RD) para las tramas exploradoras de ruta (ARE) o exploradoras del árbol de extensión (STE) reenviadas por el puente si el direccionamiento en origen está habilitado.

Ejemplo: `set route-descriptor-limit ARE`

Tipo-límite

Se entra como ARE o STE en función de si el valor del límite de RD se aplica a las tramas exploradoras de todas las rutas (ARE) o a las tramas exploradoras del árbol de extensión (STE). A continuación, se le solicitará un valor de límite de 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 de RD.

El recuento de saltos de cada trama es el número de puentes a través del que la trama ha viajado hasta ahora. Se añade un RD al campo de información de direccionamiento cada vez que la trama pasa por un puente. Por lo tanto, el número de RD equivale al número de saltos. Cuando el número de RD (saltos) supera al número de saltos que este parámetro permite, la trama es descartada.

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 apartado “Mandatos de configuración de túnel” en la página 117 si desea obtener una explicación de dichos mandatos.

Sintaxis:

tunnel

Mandatos de configuración de BAN

Esta sección describe todos los mandatos de configuración de BAN (nodos de acceso de límite). Estos mandatos le permite configurar BAN como una función añadida a los puentes ASRT o a DLSw.

Nota: Los mandatos de configuración de BAN no empiezan a tener efecto de manera inmediata. Quedan pendientes hasta que el dispositivo se reinicia o se vuelve a cargar.

Los mandatos de configuración se entran en el indicador `BAN config>`. A este indicador se accede entrando el mandato **ban** en el indicador `ASRT config>` o `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 de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Add	Añade un puerto de BAN.
Delete	Suprime un puerto de BAN.
List	Visualiza toda la información referente a 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 xxxi.

Respuesta a mandatos de configuración de BAN

Los mandatos de configuración de BAN (Talk 6) no empiezan a tener efecto de manera inmediata. Quedan pendientes hasta que se ejecuta el mandato **reload** o **restart**.

Add

Utilice el mandato **add** para añadir un puerto de BAN a la configuración de BAN. Si no proporciona con el mandato un número de puerto, 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 proporciona con el mandato un número de puerto, se le solicitará el número de puerto.

Sintaxis:

d**elete** *núm-puerto*

Ejemplo: `delete 3`

List

Utilice el mandato **list** para listar la información acerca de todos los puertos de BAN. La información que se visualiza incluye el número de puerto de BAN, la dirección MAC de la DLCI de BAN y si las tramas manejadas por el puerto se envían por puente o si el LLC ha sido interrumpido por DLSw.

Sintaxis: list

list

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 los parámetros de red de un túnel que transmite tramas de puente en IP.

Nota: Los mandatos de configuración de túnel no empiezan a tener efecto de manera inmediata. Debe reiniciar o volver a cargar el dispositivo antes de que empiecen a tener efecto.

Los mandatos de configuración de túnel se entran en el indicador `TNL config>`. A este indicador se accede entrando el mandato **tunnel** en el indicador `ASRT config>`. La Tabla 6 en la página 118 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 de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Add	Añade la dirección IP de los puentes de destino que participan en una configuración de direcciones de unidifusión o de multidifusión IP para puentes en IP.
Delete	Suprime la dirección IP de un puente de destino que participa en una configuración de direcciones de unidifusión o de multidifusión IP para puentes en IP.
Join	Configura el dispositivo como miembro de uno o más grupos de multidifusión.
Leave	Elimina el dispositivo como miembro de uno o más grupos de multidifusión.
List	Visualiza las direcciones IP de estaciones finales que participan en una configuración de direcciones de unidifusión o de multidifusión IP para puentes en IP. Visualiza también el tamaño (en número de bytes) de los paquetes de puente que se están direccionando a través de un túnel IP y si las direcciones de multidifusión están habilitadas o inhabilitadas.
Set	Establece una dirección IP para túneles de multidifusión 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 xxxi.

Respuesta a los mandatos de configuración de túnel

Los mandatos de configuración de túnel (Talk 6) no empiezan a tener efecto de manera inmediata. Quedan pendientes hasta que se ejecuta el mandato **reload** o **restart**.

Túneles y paquetes de multidifusión

Un túnel de puente se puede definir como túnel de unidifusión o túnel de multidifusión. Para definir un túnel de unidifusión, utilice el mandato **add** para configurar la dirección IP del punto final del túnel. Para definir un túnel de multidifusión, utilice los mandatos **set** y **join**. En el caso de configuraciones de túnel que implican paquetes de multidifusión, la dirección origen de los paquetes de multidifusión debe reposar en un segmento de red compatible con el protocolo de gestión de grupos de Internet (IGMP).

El IGMP no está definido en algunas interfaces como , X.25 y Frame Relay. Esto significa que, cuando se define un túnel de multidifusión en el dispositivo (por ejemplo, el túnel MOSPF), debe asegurarse de que se da una de las siguientes condiciones:

- EL origen es una de las direcciones de segmentos de la LAN.
- El origen es la dirección IP interna

Puede asegurarse de que la primera condición se da utilizando el mandato de configuración **set router-id** de IP. Puede asegurarse de que la segunda condición se da utilizando el mandato de configuración **set internal-ip-address** de IP.

En todo caso , es preferible la segunda opción y la primera debería utilizarse sólo si algunos de los dispositivos de la red no quieren direcciones de sistemas principales (esto puede pasar en redes de proveedores mezclados).

Add

Utilice el mandato **add** para añadir la dirección IP de estaciones finales que participan en una configuración de direcciones IP de unidifusión.

Para direcciones de unidifusión IP, la configuración de túnel requiere que el usuario proporcione las direcciones IP de los 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 de ruta origen en la dirección IP correspondiente del puente de destino. En el caso de tramas de 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 direcciones IP de unidifusión o de multidifusión.

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 establecer el dispositivo como miembro de uno o más grupos de multidifusión. Un grupo de túneles puede ser de uno de estos tres tipos: igual, cliente o servidor. El grupo de túneles se define mediante un identificador de enteros. Un puente sólo puede pertenecer a un tipo de grupo de cada distintivo. Un puente no puede pertenecer tanto al *grupo de iguales 1* como al *grupo de servidores 1*, por ejemplo.

Sintaxis:

j**oin** client-group *número-grupo*

peer-group *número-grupo*

server-group *número-grupo*

client-group *número-grupo*
Une el grupo de clientes con el número de grupo determinado.

Valores válidos: 0 a 64

Valor por omisión: 0

Ejemplo: `join client-group 3`

peer-group *número-grupo*
Une el grupo de iguales con el número de grupo determinado.

Valores válidos: 0 a 64

Valor por omisión: 0

Ejemplo: `join peer-group 5`

server-group *número-grupo*
Une el grupo de servidores con el número de grupo determinado.

Valores válidos: 0 a 64

Valor por omisión: 0

Ejemplo: `join server-group 7`

Leave

Utilice el mandato **leave** para eliminar el dispositivo como miembro de grupos de multidifusión.

Sintaxis:

l**eave**	server-group *número-grupo*
	client-group *número-grupo*
	peer-group *número-grupo*

server-group *número-grupo*
Deja al grupo de servidores con el número de grupo determinado.

Valores válidos: 0 a 64

Valor por omisión: 0

Ejemplo: `leave server-group 7`

client-group *número-grupo*
Deja al grupo de clientes con el número de grupo determinado.

Valores válidos: 0 a 64

Valor por omisión: 0

Ejemplo: `leave client-group 3`

peer-group *número-grupo*
Deja al grupo de iguales con el número de grupo determinado.

Valores válidos: 0 a 64

Valor por omisión: 0

Ejemplo: `leave peer-group 5`

List

Utilice el mandato de túnel **list** para visualizar las direcciones IP de los puertos que participan en una configuración de direcciones de unidifusión o de multidifusión IP para túneles en IP. Este mandato también se puede utilizar para visualizar el tamaño actual de los paquetes IP que se envían a través de los túneles y visualiza si IP está habilitado o inhabilitado.

Sintaxis:

list address

all

address Lista las direcciones IP de los puertos que participan en una configuración de direcciones de unidifusión o de multidifusión IP para túneles en 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 unidifusión, las direcciones de multidifusión configuradas y el tamaño de los paquetes de 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 establecer la dirección de multidifusión base del dispositivo.

En el caso de direcciones de multidifusión IP, la configuración de túnel requiere sólo que se reserve la dirección de multidifusión IP para los túneles. La encapsulación utiliza tres grupos de direcciones de multidifusión IP. El primer grupo es para enviar tramas exploradoras de todas las rutas (ARE), el segundo es para enviar tramas exploradoras del árbol de extensión (STE) y el tercero es para tramas direccionadas específicamente (SRF).

Sintaxis:

set base-multicast-address

base-multicast-address

Establece la dirección IP de multidifusión base para los túneles de multidifusión.

Valores válidos: cualquier dirección IP de clase D válida cuyos dos últimos bytes sean 0.

Valor por omisión: 224.186.0.0

Ejemplo: `set base-multicast-address 224.10.0.0`

Mandatos de Frame Relay

Para habilitar puentes en la interfaz Frame Relay, debe asociar un número de DLCI (denominado también número de circuito) con un puerto de puente. Esto se conoce como puerto de puente punto a punto de Frame Relay. Puede definir también un puerto de puente de multiacceso asociado con la propia interfaz Frame Relay. Si desea más información al respecto, consulte “Configuración de los puertos de puente multiacceso” en la página 56.

Una vez se ha configurado el puerto de puente, todas las funciones asociadas con los puertos de puentes, incluyendo el filtro de protocolos y el filtro de direcciones, están disponibles.

Debe especificar PVC o SVC para cada puerto de puente punto a punto de Frame Relay. En el caso del soporte de PVC, debe especificar el número de DLCI asociado. En el caso del soporte SVC, debe proporcionar el nombre del circuito SVC.

Respuesta a los mandatos de configuración de Frame Relay

Los mandatos de configuración de Frame Relay (Talk 6) no empiezan a tener efecto de manera inmediata. Quedan pendientes hasta que se ejecuta el mandato **reload** o **restart**.

En el indicador `ASRT config>`, utilice el siguiente mandato para habilitar puentes para 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 específico de puente exclusivo asociado con el circuito.

Rango válido: 1 a 254

Valor por omisión: ninguno

id-circuito
El número de DLCI del PVC en el que se va a habilitar el puente o el nombre de circuito del SVC en el que se va a habilitar el puente.

El mandato asocia un número de puerto con el PVC de Frame Relay identificado por el *número del circuito* o el SVC de Frame Relay identificado por el nombre del circuito y habilita la participación de dicho circuito en el puente transparente.

Ejemplo: añadir un puerto en una interfaz Frame Relay (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: añadir un puerto en una interfaz Frame Relay (SVC)

```
ASRT config> add port
Interface Number [0]? 5
Port Number [8]? 8
Use FR PVC? [Yes]: no
Frame Relay SVC Circuit Name []? 05svc020
```

Acceso al entorno de supervisión de ASRT

Para acceder al entorno de supervisión de 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. Dichos mandatos le permiten ver y modificar parámetros desde la supervisión activa. La información que modifique con los mandatos de supervisión se restablece a la configuración de la SRAM al reiniciar el dispositivo de puente.

Puede utilizar estos mandatos para modificar temporalmente la configuración sin perder información de configuración en la memoria de puentes. El indicador `ASRT>` se visualiza en todos los mandatos de supervisión de ASRT.

Los mandatos de supervisión de NetBIOS se entran en el indicador de supervisión `NetBIOS>`. El indicador NetBIOS es un subconjunto de los principales mandatos ASRT y se accede a él entrando el mandato ASRT **netbios** que se describe más adelante en este capítulo.

Los mandatos de supervisión de NetBIOS se entran en el indicador de supervisión `NetBIOS>`. El indicador NetBIOS-filtering es un subconjunto de los principales mandatos ASRT.

Nota: En el caso de mandatos para los que sea necesario entrar direcciones MAC, dichas direcciones se pueden entrar en los formatos siguientes:

orden de bits canónicos IEEE 802 00-00-00-12-34-56
orden de bits canónicos IEEE 802 (formato taquigráfico) 000000123456
orden de bits nativos de red en anillo IBM (no canónico) 00:00:00:12:34:56

La Tabla 7 muestra los mandatos de supervisión de ASRT.

Tabla 7 (Página 1 de 2). Resumen de los mandatos de supervisión de ASRT

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Add	Añade entradas de dirección permanentes (estáticas) a la base de datos permanente del dispositivo de puente.
BAN	Le permite acceder al indicador de supervisión del nodo de acceso de límite (BAN) para entrar mandatos de supervisión de BAN específicos. Consulte la Tabla 8 en la página 143 si desea obtener información detallada al respecto.
Cache	Visualiza las entradas de antememoria de un puerto especificado.

Tabla 7 (Página 2 de 2). Resumen de los mandatos de supervisión de ASRT

Mandato	Función
Delete	Suprime entradas de dirección MAC de la base de datos de dispositivos de puente.
Flip	Cambia la dirección MAC de orden de bits canónicos a 802.5 (no canónicos o IBM).
List	Visualiza información sobre la configuración de puentes completa o sobre las opciones de configuración seleccionadas.
NetBIOS	Visualiza 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 xxxi.

Add

Utilice el mandato **add** para añadir entradas de dirección estáticas y filtros de direcciones de destino a la base de datos del dispositivo de puente. Estas adiciones a la base de datos se pierden cuando se reinicia el dispositivo.

Sintaxis:

a**dd** destination-address-filter

static-entry

destination-address-filter *dirección_mac*

Añade un filtro de dirección de destino a la base de datos permanente del dispositivo de puente. 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 dirección a la base de datos permanente del dispositivo de puente. Entre el mandato seguido de la dirección MAC de la entrada estática y el número de puerto de entrada (se puede entrar también un número de puerto de salida opcional). 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 de acceso de límite). 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 los mandatos de supervisión específicos. Para volver al indicador `ASRT>` cuando lo desee, entre el mandato **exit**.

Cache

Utilice el mandato **cache** para visualizar el contenido de una antememoria de direccionamiento de puerto de puente seleccionada. Si el puerto no dispone de una antememoria, aparecerá el mensaje `Port X does not have a cache`.

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
La dirección MAC de 6 bytes de la entrada.

Entry Type
Especifica uno de los siguientes tipos de entradas de dirección:

Reserved - entradas reservadas por la norma IEEE 802.1d.

Registered - entradas que constan de direcciones de unidifusión que pertenecer a hardware de comunicaciones propietario conectado a la caja o de direcciones de multidifusión habilitadas por los reenviadores de protocolo.

Permanent - entradas que el usuario especifica en el proceso de configuración que permanecen después de apagar y encender el sistema o después de reinicializarlo.

Static - entradas que el usuario especifica en el proceso de supervisión que no permanecen después de encender o apagar el sistema o después de reinicializarlo y a las que no afecta el temporizador de antigüedad.

Dynamic - entradas “averiguadas” por el puente “dinámicamente” que no permanecen después de encender o apagar el sistema o después de reinicializarlo y que tienen una “antigüedad” asociada con la entrada.

Free - ubicaciones de la base de datos que se pueden rellenar con entradas de dirección.

Unknown - tipos de entradas que son desconocidas para el puente. Puede tratarse de errores bug y/o de direcciones no permitidas.

Age Antigüedad en segundos de cada entrada dinámica. La antigüedad disminuye con cada intervalo de resolución.

port(s) Especifica el número de puerto asociado con esta entrada y visualiza el nombre de la interfaz (éste siempre será el de la interfaz que dispone de la antememoria).

Delete

Utilice el mandato **delete** para suprimir entradas de dirección de estación (incluidas las MAC) 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 y no canónico al “cambiar” el orden de bits de direcciones. Este mandato es útil para convertir direcciones IEEE 802.5 en su formato no canónico habitual al formato canónico que la supervisión de puentes y ELS utilizan a nivel mundial (y vice-versa).

Sintaxis:

flip *dirección-MAC*

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 acerca de la configuración del dispositivo de puente o para visualizar información acerca de las opciones de puente o configuración seleccionadas.

Sintaxis:

list
- adaptive . . .
- bridge . . .
- conversion . . .
- database . . .
- dmac
- filtering . . .
- multiaccess-database . . .
- port
- source-routing . . .
- spanning-tree-protocol . . .
- transparent . . .
- tunnel . . .

adaptive *opción-grupo_datos [subopción]*

Lista toda la información general sobre el puente SR-TB que realiza conversiones de un tipo de puente a otro. Un cierto número de opciones de grupos de datos generales se pueden visualizar con **list adaptive**. Entre ellas se encuentran las siguientes:

- Config - Visualiza información general acerca del puente SR-TB.
- Counters - Visualiza todos los contadores del puente SR-TB.

- Database - Visualiza el contenido de la base de datos 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. Este valor se visualiza como Enabled (habilitado) o Disabled (inhabilitado).

Translation database size
Visualiza el estado actual del puente adaptable SR-TB, que contiene direcciones MAC y RIF asociadas para el dominio de direccionamiento en origen.

Aging time
Visualiza el valor del temporizador de antigüedad en segundos. Todas las entradas de la base de datos de RIF de SR-TB que superan este límite de tiempo se descartan.

Aging granularity
Visualiza la frecuencia con la que se exploran las entradas para saber su caducidad de acuerdo con el temporizador de antigüedad.

Port Visualiza el número de un puerto asociado con el puente de conversión.

Segment Visualiza el número del segmento de direccionamiento en origen asignado al puerto asociado con el puente de conversión.

Interface Identifica el dispositivo conectado a un segmento de red de puente de conversión.

State Indica el estado actual del puerto de puente de conversión.

MTU Especifica el tamaño máximo de trama (desde el final del RIF al principio del FCS) que el puente de conversión puede transmitir y recibir.

Ejemplo:

```
list adaptive counters
Hash collision count: 28
Adaptive database entry count: 0
Adaptive database overflow  count: 0
```

Hash Collision Count
Visualiza el número de direcciones que se han almacenado (con hash) en la misma ubicación de la tabla hash. Dicho número es acumulativo y refleja el número total de incidentes de colisión hash que se han producido. Si este número

aumenta, ello puede indicar un posible problema de tamaño de tabla.

Adaptive Database Entry Count
Visualiza el número de entradas almacenadas actualmente en la base de datos de puente adaptable.

Adaptive Database Overflow Count
Visualiza el número de veces que se ha sobreescrito una dirección al quedarse sin espacio la tabla de la base de datos de conversión.

La opción *database* del mandato **list adaptive** le permite seleccionar ciertas partes de la base de datos RIF del puente adaptable para visualizarlas. Ello es debido al tamaño potencial de la base de datos. Las opciones de visualización son las siguientes:

- Address - Visualiza la base de datos del puente de conversión relacionada con la dirección MAC específica.
- All - Visualiza toda la base de datos.
- Port - Visualiza todas las entradas de puente de conversión de un puerto específico.
- Segment - Visualiza todas las entradas de puente de conversión asociadas con el puerto que tiene el número de segmento especificado.

Los siguientes ejemplos ilustran cada una de las opciones de visualización de **list adaptive database**.

Nota: Sólo se pueden visualizar si el puente adaptable está habilitado.

Ejemplo: `list adaptive database address` ***dirección-mac***

Ejemplo: `list adaptive database all`

Ejemplo: `list adaptive database port` ***núm-segmento***

Example: `list adaptive database segment` ***núm-segmento***

Cada entrada se visualiza en dos líneas seguidas por una línea en blanco. Para cada entrada se visualiza la siguiente información:

Canonical address
Lista la dirección MAC del nodo que corresponde a esta entrada. Se visualiza en formato canónico IEEE 802 (hexadecimal).

Interface Visualiza el nombre de la interfaz de red que ha averiguado esta entrada.

Port Visualiza el número de puerto que ha averiguado esta entrada de direcciones.

Seg Visualiza el número del segmento que ha averiguado esta dirección.

Age Visualiza la antigüedad de la entrada en segundos.

RIF Type Visualiza el tipo de RIF como SRF, STE o ARE.

RIF Direction
Visualiza la dirección de RIF como Forward (adelante) o Reverse (atrás).

RIF Length
Visualiza la longitud de RIF en bytes.

RIF LF Visualiza el valor de trama más grande codificado en el RIF.

IBM MAC Address
Muestra la dirección MAC del nodo que corresponde a esta entrada. Se visualiza en el orden de bits no canónico “IBM” tal y como se etiqueta habitualmente en interfaces 802.5 y tal y como lo utilizan los protocolos IP/ARP, IPX y NetBIOS.

RIF Visualiza el campo de información de direccionamiento averiguado desde este nodo.

adaptive database duplicate
Lista la entrada de la base de datos de todas las direcciones MAC duplicadas. Lista los RIF primario y secundario de 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 referente a 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
El ID exclusivo que el algoritmo de árbol de extensión utiliza para determinar el árbol de extensión. Se asigna un identificador de puente exclusivo a cada puente de la red. La

prioridad del puente se visualiza en formato decimal seguida por la dirección hex.

Bridge State
Indica si el puente está habilitado o inhabilitado.

UB-Encapsulation
Indica si la encapsulación UB está habilitada o inhabilitada.

Bridge Type
Visualiza el tipo de puente configurado. Se visualiza como NONE (ninguno), SRB, TB, SRT, ADAPT, A/SRB, A/TB o ASRT.

Number of Ports
Visualiza el número de puertos configuradas para este puente.

STP Participation
Describe los tipos de protocolo de árbol de extensión en los que participa un puente.

IPX Conversion
Indica si la conversión IPX está habilitada o inhabilitada.

Conversion Mode
Indica la modalidad de conversión IPX como automática o manual.

Ethernet Preference
Indica el tipo de tramas de Ethernet preferibles utilizados para la conversión IPX Conversion como IEEE 802.3 o Ethernet.

Port Especifica un número definido por el usuario asignado a una interfaz mediante el mandato **add port**.

Interface Identifica dispositivos conectados a un segmento de red a través del puente.

State Indica el estado actual del puerto. Se visualiza como UP (activo) o DOWN (no activo).

MAC address
Visualiza la dirección MAC asociada con este puerto en orden de bits canónicos.

Modes Visualiza la modalidad de puente de ese puerto. T indica que es puente transparente. SR indica que es direccionamiento en origen. A indica que es puente adaptable.

MSDU Especifica el tamaño máximo de trama (unidad de datos), incluida la cabecera MAC pero no el campo FCS, que el puente puede transmitir y recibir en esta interfaz.

Segment Visualiza el número de segmento del puente de direccionamiento en origen asignado a este puerto (si lo hay).

SR bridge number
Visualiza el número de puente de direccionamiento en origen asignado por el usuario.

SR virtual segment
Visualiza el número de segmento virtual del puente de direccionamiento en origen asignado a este puerto (si lo hay).

Adaptive segment
Visualiza el número del segmento que se utiliza en el dominio de direccionamiento en origen para direccionar hacia el dominio transparente (mediante conversión).

conversion *opción-grupo_datos*

- Visualiza información general acerca de las normas del puente para la conversión de formatos de trama según el tipo de trama. Un cierto número de grupos de datos generales se pueden visualizar con el mandato **list conversion**. Entre ellos se encuentran los siguientes:
  - All - Visualiza todas las normas.
  - Ethertype - Visualiza normas para todos los tipos de Ethernet o para un tipo específico de Ethernet.
  - SAP - Visualiza normas para todos los identificadores de protocolos SAP o para un tipo de SAP 802.2 específico.
  - SNAP - Visualiza normas para todos los identificadores de protocolos SNAP o para un tipo de SNAP 802.2 específico.

  Los siguientes ejemplos desglosan cada una de las opciones de visualización del mandato list 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-grupo_datos*
Lista el contenido de las bases de datos de filtro transparente. Un cierto número de grupos de datos se pueden visualizar con el mandato list database. Entre ellos se encuentran los siguientes:

- All - Visualiza toda la base de datos de puente transparente.
- Dynamic - Visualiza todas las entradas de la base de datos de direcciones dinámicas (averiguadas).
- Dynamic - Visualiza todas las entradas de la base de datos de direcciones locales (reservadas).
- Permanent - Visualiza todas las entradas de la base de datos de direcciones permanentes.
- Port - Visualiza entradas de dirección de un puerto específico.
- Range - Visualiza un rango de entradas de base de datos de la base de datos total de direcciones de filtro de puente transparente.

Se determina una dirección MAC final y de inicio para definir el rango. Se visualizarán todas las entradas que se encuentren dentro de este rango.

- Static - Visualiza entradas estáticas de la base de datos de direcciones.

Los siguientes ejemplos desglosan las opciones de mandatos de bases de datos. El primer ejemplo muestra además 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 visualizan en todas las opciones del mandato **list database**.

MAC Address Especifica la entrada de direcciones en formato hex de 12 dígitos (orden de bits canónicos).

MC* Un asterisco después de una entrada de direcciones indica que la entrada se ha marcado como dirección de multidifusión.

Entry Type Especifica uno de los siguientes tipos:

Reserved
Entradas reservadas por la norma IEEE 802.1d.

Registered
Entradas que constan de direcciones de unidifusión que pertenecen a interfaces que parti-

cipan en las direcciones de puentes o de multidifusión habilitadas por reenviadores de protocolo.

Permanent
Entradas que el usuario especifica en el proceso de configuración que permanecen después de apagar y encender el sistema o después de reinicializarlo.

Static Entradas que el usuario especifica en el proceso de supervisión que no permanecen después de encender o apagar el sistema o después de reinicializarlo y que no caducan.

Dynamic Entradas “averiguadas” por el puente “dinámicamente” que no permanecen después de encender o apagar el sistema o después de reinicializarlo y que tienen una “antigüedad” asociada con la entrada

Si la conversión IPX está habilitada y se ha “averiguado” la entrada durante el proceso de reenvío de una trama IPX Novel, el tipo de trama Ethernet/802.3 (encapsulada) se visualiza también como:

- **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 se debería visualizar excepto en condiciones de “competición” ocasionales entre la supervisión y el puente.

Unknown Tipo de entrada desconocida. Puede tratarse de un error bug del software. Informe de este tipo de entrada hex al servicio de atención al cliente.

Age Hace referencia a la antigüedad (en segundos) de cada entrada dinámica. La antigüedad disminuye con cada intervalo de resolución.

Port(s) Especifica el(los) número(s) de puertos de salida de esta entrada. Se lista también el tipo de dispositivo para entradas de puerto únicas.

dmac Visualiza información acerca de las opciones configuradas para la función de direcciones MAC.

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-grupo_datos*

Visualiza información general acerca de las bases de datos de filtro de protocolos del puente. Un cierto número de grupos de datos generales se pueden visualizar con el mandato **list filtering**. Entre ellos se encuentran los siguientes:

- All - Visualiza todas las entradas de bases de datos de filtro.
- Ethertype - Visualiza las entradas de bases de datos de filtros de tipo de protocolo Ethernet.
- SAP - Visualiza las entradas de bases de datos de filtros de protocolos SAP.
- SNAP - Visualiza las entradas de bases de datos de filtros de identificadores de protocolo SNAP.

Los siguientes ejemplos desglosan cada una de las opciones de visualización del mandato list filtering.

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 que se utilizan para explicar la manera como se comunican los paquetes son:

- Routed - Describe los paquetes que han pasado al reenviador de direccionamiento y que se deben reenviar.
- Filtered- Describe los paquetes que se filtran administrativamente mediante los filtros de protocolo establecidos por el usuario.
- Bridged and routed - Describe un identificador de protocolo para el que existe una entidad de protocolo dentro del sistema que no es un reenviador. Por ejemplo, un protocolo de eco de nivel de enlace. Los paquetes de unidifusión de este protocolo se puentean o bien se procesan localmente si se envían a una dirección registrada. Los paquetes de multidifusión se reenvían y se procesan localmente para una dirección de multidifusión registrada.

Todos los descriptores arriba comentados también se aplican a paquetes ARP con este tipo de Ethernet.

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*

Visualiza el contenido de la base de datos de multiacceso. Esta base de datos correlaciona un número de segmento de direccionamiento en origen con un número de circuito de Frame Relay.

all-ports Especifica que todas las entradas de la base de datos se deben visualizar.

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* Visualiza entradas de base de datos de un puerto de puente específico.

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 las visualizaciones:

Segment Es el número del segmento de direccionamiento en origen de destino.

Age Es la entrada del tiempo de vida en segundos.

Port Es el número de puerto del puerto de puente de multiacceso que ha creado esta entrada.

Interface Es el nombre de la interfaz de red que ha creado esta entrada.

Circuit Es el número del circuito de Frame Relay que ha creado esta entrada.

port *núm-puerto*

Visualiza información del puerto.

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 asignado a una interfaz mediante el mandato **add port**.

Interface Identifica dispositivos conectados a un segmento de red a través del puente.

State Indica el estado actual del puerto. Se visualiza como UP (activo) o DOWN (no activo).

MAC address
Visualiza la dirección MAC asociada con este puerto en orden de bits canónicos.

Modes Visualiza la modalidad de puente de ese puerto. **T** indica que es puente transparente. **SR** indica que es direccionamiento en origen. **A** indica que es puente adaptable.

MSDU Especifica el tamaño máximo de trama (unidad de datos), incluida la cabecera MAC pero no el campo FCS, que el puente puede transmitir y recibir en esta interfaz.

Segment Visualiza el número de segmento del puente de direccionamiento en origen asignado a este puerto (si lo hay).

source-routing *opción-grupo_datos*
Visualiza información de configuración del puente de direccionamiento en origen. Un cierto número de opciones de grupos de datos generales se pueden visualizar con el mandato list source-routing. Entre ellas se encuentran las siguientes:

- Configuration - Visualiza información general acerca del puente SRB.
- Counters - Visualiza todos los contadores del puente SRB.
- State - Visualiza el contenido de todas las bases de datos del puente SR-TB relacionadas.

Los siguientes ejemplos ilustran cada una de las opciones de visualización de list 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 formato hexadecimal) asignado a este puente.

Bridge State
Indica si el puente está habilitado o inhabilitado.

Maximum STE hop count
El número máximo de saltos para las tramas exploradoras del árbol de extensión que transmiten desde el puente para una interfaz determinada asociada con el puente de direccionamiento en origen.

Maximum ARE hop count
El número máximo de saltos para las tramas exploradoras de todas las rutas que transmiten desde el puente para una interfaz determinada asociada con el puente de direccionamiento en origen.

Virtual segment
El número de segmento virtual asignado para puentes 1:N.

Port Los números de puertos asociados con el puente de direccionamiento en origen.

Segment Los números de segmentos asignados para los puertos asociados con el puente de direccionamiento en origen.

Interface Los nombres de interfaces asociadas. Para FR se muestra la DLCI.

State El estado actual del puerto (Enabled o Disabled, Habilitado o Inhabilitado).

MTU El tamaño de la MTU establecido para este puerto.

STE Forwarding
Indica si los exploradores de árbol de extensión recibidos en este puerto se reenvían (Yes, Sí) y su los STE de otros puertos salen de este puerto.

LNM Indica si los agentes de LAN Network Manager (LNM) están habilitados (ENA) o inhabilitados (DIS) en este puerto específico.

La opción de contadores dispone de más subgrupos de información que se pueden visualizar mediante el mandato list source-routing. Entre ellos se encuentran los siguientes:

- All-ports - Visualiza los contadores de todos los puertos.
- Port - Visualiza los contadores de un puerto específico.
- Segment - Visualiza los contadores del puerto correspondiente a un segmento específico.

Los siguientes ejemplos ilustran cada una de las opciones de visualización de list 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 el puente de direccionamiento en origen.

Segment Lista los números de segmentos de direccionamiento en origen en formato hex.

Interface Lista el nombre de la interfaz de red.

SRF Frames Received/Sent
Lista el número de tramas direccionadas de manera específica recibidas y enviadas en este puente.

STE Frames Received/Sent
Lista el número de tramas exploradoras del árbol de extensión recibidas y enviadas en este puente.

ARE Frames Received/Sent
Lista el número de tramas exploradoras de todas las rutas recibidas y enviadas en este puente.

SR Frames Sent as TB
Lista el número de tramas de direccionamiento en origen recibidas en esta interfaz que se han enviado como tramas de puente transparente.

TB Frames Sent as SR
Lista el número de tramas de puente transparente recibidas en esta interfaz que se han enviado como tramas de direccionamiento en origen.

Dropped, input queue overflow
Lista el número de tramas que llegan a esta interfaz que no se han enviado por puente por razones de control del flujo. La cola de entrada al reenviador se ha desbordado.

Dropped, source address filtering
Lista el número de tramas que llegan a esta interfaz que no se han enviado por puente porque la dirección origen ha coincidido con el filtro de direcciones origen de la base de datos de filtro.

Dropped, destination address filtering
Lista el número de tramas que llegan a esta interfaz que no se han enviado por puente porque la dirección de destino ha coincidido con el filtro de direcciones de destino de la base de datos de filtro.

Dropped, protocol filtering
Lista el número de tramas que llegan a esta interfaz que no se han enviado por puente porque su identificador de protocolo se está filtrando administrativamente.

Dropped, invalid RIF length
Lista el número de tramas que llegan a esta interfaz que se han eliminado porque la longitud del RIF es menos de 2 o más de 30.

Dropped, duplicate segment
Lista el número de tramas que llegan a esta interfaz que se han eliminado porque existe un segmento duplicado en el RIF. Esto es habitual en el caso de las tramas ARE.

Dropped, segment mismatch
Lista el número de tramas que llegan a esta interfaz que se han eliminado porque el número del segmento de salida de esta interfaz no coincide con ninguno de este puente.

Dropped, Duplicate LAN ID or tree error:
El número de ID de LAN duplicadas o de errores de árbol. Ayuda en la detección de problemas en redes que contienen puentes de direccionamiento en origen IBM más antiguos.

Dropped, STE hop count exceeded:
El número de tramas exploradoras que este puerto ha descartado porque el campo de información de direccionamiento ha superado la longitud máxima del descriptor de rutas.

Dropped, ARE hop count exceeded:
El número de tramas exploradoras que este puerto ha descartado porque el campo de información de direccionamiento ha superado la longitud máxima del descriptor de rutas.

Dropped, no buffer available to copy:
El número de veces que una trama no se ha reenviado en una interfaz porque no existía suficiente almacenamiento intermedio disponible para copiar la trama. (Es necesario que las tramas hacia destinos de multidifusión y hacia destinos desconocidos se copien para su transmisión en todos los puertos activos).

Dropped, MTU exceeded:

El número de tramas que este puerto ha descartado a causa de 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
çSTE 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-grupo_datos*

- Visualiza información del protocolo de árbol de extensión. El puente transparente utiliza el protocolo de árbol de extensión para crear una topología sin bucles. Un cierto número de opciones de grupos de datos generales se pueden visualizar con el mandato **list spanning-tree-protocol**. Entre ellas se encuentran las siguientes:
  - Configuration - Visualiza información referente al protocolo de árbol de extensión.
  - Counters - Visualiza los contadores del protocolo de árbol de extensión.
  - State - Visualiza información sobre el estado actual del protocolo de árbol de extensión.
  - Tree - Visualiza información sobre el estado actual del protocolo de árbol de extensión, incluyendo información de puertos, interfaces y coste.

  Los siguientes ejemplos ilustran cada una de las opciones de visualización del mandato list 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  ETH/1  32768/12-34-56-78-90-12    0 32768/12-34-56-78-90-12 90-01
2  ATM/0:0:48  0/00-00-00-00-00-00    0     0/00-00-23-45-00-00 80-00
```

transparent

Visualiza información de configuración del puente transparente. Un cierto número de opciones de grupos de datos generales se pueden visualizar con el mandato **list transparent**. Entre ellas se encuentran las siguientes:

- Configuration - Visualiza información referente al puente transparente.
- Counters - Visualiza los contadores del puente transparente. Puede utilizar **list transparent all-ports** para visualizar los contadores de todos los puertos o entrar el número específico del puerto después del mandato **list transparent** para visualizar los contadores de un puerto.
- State - Visualiza información del estado del puente transparente.

Los siguientes ejemplos ilustran cada una de las opciones de visualización del mandato **list transparent**.

Ejemplo: `list transparent configuration`

```
Filtering database size:    5141
Aging time:                 300 seconds
Aging granularity           5 seconds
Port  Interface   State     MTU
  4   Eth/1       Enabled   0
```

Ejemplo: `list transparent counters all-ports`

```
Counters for port 4, interface Eth/1:
Total frames received by interface:          25885
Frames submitted to bridging:                13732
Frames submitted to routing:                  6101
Dropped, source address filtering:               0
Dropped, dest address filtering:             12677
Dropped, protocol filtering:                     0
Counters for port 128, interface Tunnel:
 Total frames received by interface:              0
Frames submitted to bridging:                    0
Frames submitted to routing:                     0
Dropped, source address filtering:               0
Dropped, dest address filtering:                 0
Dropped, protocol filtering:                     0
Dropped, no buffer available to copy:            0
Dropped, input queue overflow:                   0
Dropped, source port blocked:                    0
Frames sent by bridging:                      5327
Dropped, dest port blocked:                      0
Dropped, transmit error:                         0
Dropped, too big to send on port:                0
```

Ejemplo: `list transparent counters port 4`

```
Counters for port 4, interface Eth/1:
Total frames received by interface:          25885
Frames submitted to bridging:                13732
Frames submitted to routing:                  6101
Dropped, source address filtering:               0
Dropped, dest address filtering:             12677
Dropped, protocol filtering:                     0
Dropped, no buffer available to copy:         6073
Dropped, input queue overflow:                 122
Dropped, source port blocked:                   31
Frames sent by bridging:                       388
Dropped, dest port blocked:                      0
Dropped, transmit error:                         0
Dropped, too big to send on port:                0
```

Ejemplo: `list transparent state`

```
Filtering database size:                      5141
Number of static entries:                        0
Number of dynamic entries:                      10
Hash collision count:                            1
Filtering database overflow count:               0
```

tunnel *opción-grupo_datos*

Visualiza información de configuración del túnel. Un cierto número de opciones de grupos de datos generales se pueden visualizar con el mandato list tunnel. Éstas pueden ser:

- Bridges - Visualiza información del puente del túnel.
- Config - Visualiza información referente a la configuración del túnel.

NetBIOS

Utilice el mandato **netbios** para acceder al indicador `NetBIOS>`. Los mandatos de configuración de NetBIOS se pueden entrar en el indicador `NetBIOS>`.

Consulte los “Mandatos de NetBIOS” en la página 174 si desea obtener información sobre los mandatos de supervisión de NetBIOS.

Sintaxis:

netbios

Acceso al indicador de supervisión de BAN

Utilice el mandato **ban** del 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>

   or

DLSw> ban
BAN>
```

Una vez haya accedido al indicador de supervisión de BAN, puede empezar a entrar los mandatos de supervisión específicos. Para volver al indicador de supervisión del que procede, 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 de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
List	Visualiza toda la información referente a 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 xxxi.

List

Utilice el mandato **list** para listar la información acerca de todos los puertos de BAN. La información que se visualiza incluye el número de puerto de BAN, la dirección MAC de la DLCI de BAN, si las tramas manejadas por el puerto se puentean o si el LLC ha sido interrumpido por DLSw, y el estado del puerto.

El estado del puerto tendrá uno de estos tres valores:

- Init Fail - Indica que existe un problema de configuración.
- Up - Indica que la DLCI de Frame Relay está activa y en funcionamiento.
- 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
```

Soporte de reconfiguración dinámica de puente ASRT

En este apartado se describe el modo en que la reconfiguración dinámica (DR) afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

El puente ASRT da soporte al mandato **delete interface** de CONFIG (Talk 6) sin restricciones.

Mandato activate interface de GWCON (Talk 5)

El puente ASRT da soporte al mandato **activate interface** de GWCON (Talk 5) con las matizaciones siguientes:

- La interfaz no puede activarse si está configurada como puerto de puente y el protolo de puente no estaba ya activo.
- La interfaz no puede activarse si está configurada como puerto de puente y la adición de este puerto provoca un cambio de personalidad de puente. Por ejemplo, no se puede añadir un puerto de puente de direccionamiento en origen (SR) a una configuración de puente que sólo tenga definidos puertos de puente transparente (TB). En el apartado “Matriz de configuración de ASRT” en la página 44 del “Métodos de puenteo” en la página 13 hallará información sobre la personalidad de puente.
- La interfaz no puede activarse si está configurada como puerto de puente y la adición de este puerto provoca un cambio en el segemento virtual interno de puente. Por ejemplo, no puede activarse si el direccionamiento en origen estaba inactivo y la adición del puerto recién activado provoca su activación, con lo que sería necesario el uso del circuito virtual interno.
- La interfaz no puede activarse si está configurada como puerto de puente y para el puerto se han configurado filtros por bytes o por nombre de NetBIOS.
- La interfaz no puede activarse si está configurada como puerto de puente y para el puerto se ha configurado LNM.

Todos los mandatos específicos de interfaz del puente ASRT están soportados por el mandato **activate interface** de GWCON (Talk 5).

Mandato reset interface de GWCON (Talk 5)

El puente ASRT da soporte al mandato **reset interface** de GWCON (Talk 5) con las matizaciones siguientes:

- La interfaz no puede restablecerse si acaba de configurarse como puerto de puente y el protolo de puente no estaba ya activo.
- La interfaz no puede restablecerse si la configuración de puente de la misma ha cambiado de manera que la adición o la supresión del puerto provoca un cambio de personalidad de puente. Por ejemplo, no se puede añadir un puerto de puente de direccionamiento en origen (SR) a una configuración de puente que sólo tenga definidos puertos de puente transparente (TB). En el apartado “Matriz de configuración de ASRT” en la página 44 del “Métodos de puenteo” en la página 13 hallará información sobre la personalidad de puente.
- La interfaz no puede restablecerse si la configuración de puente de la misma ha cambiado de manera que la adición o la supresión del puerto provoca un cambio del uso o valor del segmento virtual interno de puente.

- La interfaz no puede restablecerse si el puerto está configurado para puente y forma parte de un puente de dos puertos.
- La interfaz no puede restablecerse si la configuración de puente de la misma ha cambiado y se han configurado filtros por de bytes o por nombre de NetBIOS para el puerto que se añade o suprime.
- La interfaz no puede restablecerse si la configuración de puente de la misma ha cambiado y se ha configurado LNM para el puerto que se añade o suprime.

Todos los mandatos específicos de interfaz del puente ASRT están soportados por el mandato **reset interface** de GWCON (Talk 5).

Mandatos de cambio inmediato de CONFIG (Talk 6)

El puente ASRT da soporte a los mandatos de CONFIG que cambian de forma inmediata el estado operativo del dispositivo indicados más abajo. Los cambios se guardan y se conservan si se vuelve a cargar o iniciar el dispositivo o bien si se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
CONFIG, protocol asrt, enable dmac-addr
CONFIG, protocol asrt, enable dmac_load-balance
CONFIG, protocol asrt, disable dmac-addr
CONFIG, protocol asrt, disable dmac_load-balance

Soporte de reconfiguración dinámica de BAN

En este apartado se describe el modo en que la reconfiguración dinámica (DR) afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

BAN da soporte al mandato **delete interface** de CONFIG (Talk 6) sin restricciones.

Mandato activate interface de GWCON (Talk 5)

BAN da soporte al mandato **activate interface** de GWCON (Talk 5) con la matización siguiente:

Para que se pueda activar BAN para un puerto de puente (interfaz), se debe habilitar globalmente el puente SRT.

Todos los mandatos específicos de interfaz de BAN están soportados por el mandato **activate interface** de GWCON (Talk 5).

Mandato reset interface de GWCON (Talk 5)

BAN da soporte al mandato **reset interface** de GWCON (Talk 5) con la matización siguiente:

- Para que se pueda restaurar BAN para un puerto de puente (interfaz), se debe habilitar globalmente el puente SRT.

Todos los mandatos específicos de interfaz de BAN están soportados por el mandato **reset interface** de GWCON (Talk 5).

Mandatos no reconfigurables dinámicamente

Todos los parámtros de configuración de nodo de acceso de límites (BAN) pueden cambiarse dinámicamente.

Utilización de NetBIOS

Este capítulo describe la implementación de NetBIOS que efectúa IBM en redes puenteadas y en redes DLSw. Consta de los temas siguientes:

Acerca de NetBIOS

El protocolo NetBIOS ha sido diseñado para ser utilizado en una LAN de red en anillo. No es un protocolo direccionable, pero admite puentes o conmutación mediante DLSw. Ambos métodos de manejo del tráfico de NetBIOS están soportados.

NetBIOS confía en tramas de difusión para la mayoría de sus funciones, excepto para la transferencia de datos. Aunque ello puede no representar un problema en entornos de LAN, si no se controla, sí que puede fácilmente representar un problema en entornos WAN.

Las siguientes secciones describen los nombres NetBIOS y los diferentes tipos de comunicación de difusión de NetBIOS.

Nombres de NetBIOS

La clave de la comunicación entre las estaciones NetBIOS son los nombres NetBIOS. Se asigna un nombre NetBIOS a cada entidad NetBIOS. A fin de que un entidad NetBIOS se comunique con otra, se debe conocer su nombre NetBIOS. Los nombres se utilizan en tramas NetBIOS de difusión para indicar la entidad NetBIOS de origen de la trama y la entidad NetBIOS de destino que debe recibir la trama.

Todos los nombres de tramas NetBIOS son de 16 caracteres ASCII. Existen dos tipos de nombres NetBIOS:

Individual (o exclusivo)
Representa a un único cliente o servidor NetBIOS. Este nombre puede ser exclusivo dentro de la red NetBIOS.

Se utiliza para la comunicación con esta entidad NetBIOS concreta.

De grupo Representa un grupo de estaciones NetBIOS (un dominio de servidor de LAN de OS/2, por ejemplo). Dicho nombre no debe ser el mismo que ningún nombre individual NetBIOS de la red.

Se utiliza para que un grupo de entidades NetBIOS se puedan comunicar.

Una estación NetBIOS (una sola dirección MAC) puede disponer de varios nombres individuales y/o de grupo asociados a ella. La aplicación NetBIOS genera dichos nombres según el nombre o los nombres configurados en la estación NetBIOS por un administrador de la red.

Resolución de conflictos de nombres de NetBIOS

Cuando una entidad NetBIOS se prepara para utilizar un nombre individual NetBIOS como propio, comprueba la red para asegurarse de que ninguna otra estación NetBIOS ya ha utilizado ese nombre.

Comprueba el nombre NetBIOS difundiendo repetidamente una trama UI NetBIOS concreta a todas las estaciones NetBIOS. Si ninguna estación responde, se presupone que el nombre es único y que se puede utilizar. Si responde alguna estación, la nueva estación no debe intentar utilizar este nombre.

Procedimiento de configuración de una sesión de NetBIOS

Para establecer una sesión de NetBIOS con el fin de realizar operaciones de transferencia de datos de diferentes tipos, el cliente NetBIOS resuelve en primer lugar la dirección MAC del servidor NetBIOS y la ruta LLC hacia el servidor NetBIOS.

Lo hace difundiendo repetidamente un trama UI NetBIOS a todas las estaciones NetBIOS. Dicha trama contiene el nombre NetBIOS del servidor con cuyo cliente está estableciendo una sesión. Cuando el servidor recibe esta trama con su nombre NetBIOS dentro, el servidor responde con una trama UI NetBIOS correspondiente hacia el cliente. Cuando el cliente recibe la trama de respuesta, la trama contiene la dirección MAC y la ruta hacia el servidor NetBIOS.

En el caso de algunas aplicaciones NetBIOS, la búsqueda del servidor NetBIOS es un proceso consistente en varios pasos. Por ejemplo, el primer paso puede ser buscar un controlador de dominios que indique al cliente qué servidor de dominio debe utilizar. A continuación, el cliente busca dicho servidor de dominio.

Una vez se han encontrado la dirección MAC del servidor NetBIOS y la ruta hacia el servidor NetBIOS, el cliente NetBIOS puede efectuar 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 mediante tramas UI direccionadas de manera específica.

Flujos de datos de difusión NetBIOS

En el caso de aplicaciones NetBIOS, la difusión periódica de tramas de datos es una práctica habitual. Ello se puede realizar si una estación dispone de datos suficientes para una sola trama que se deben enviar a otra estación NetBIOS. Lo puede hacer difundiendo una trama UI NetBIOS concreta (que contenga el nombre de la estación NetBIOS de destino) a todas las estaciones NetBIOS.

Se da también el caso de estaciones NetBIOS pertenecientes a un grupo (o dominio) que necesitan comunicarse entre ellas. Lo pueden hacer difundiendo una trama UI NetBIOS concreta (que contenga el nombre del grupo NetBIOS de destino) a todas las estaciones NetBIOS. Es una práctica habitual.

Flujos de estado NetBIOS

Una de las funciones que menos se utilizan de NetBIOS es su capacidad para obtener el estado de cualquier estación NetBIOS. Se puede hacer difundiendo una trama NetBIOS concreta (que contenga el nombre de la estación NetBIOS de destino) a todas las estaciones NetBIOS. Cuando la estación NetBIOS de destino recibe esta trama, responde con una trama de respuesta NetBIOS de difusión correspondiente.

Tramas de difusión a todas las estaciones NetBIOS

Existen dos tipos de funciones NetBIOS que raramente se utilizan. Estas dos funciones implican la difusión de una trama NetBIOS a todas las estaciones NetBIOS. No existe ningún nombre NetBIOS en las tramas. Dichas dos funciones son:

- Función de difusión general NetBIOS – que envía una trama de datos a todas las estaciones NetBIOS de la red.
- Función de interrupción del rastreo de NetBIOS– que permite a un administrador de red interrumpir las funciones de rastreo de NetBIOS en todas las estaciones NetBIOS de la red desde un único punto. Se difunde una trama NetBIOS concreta 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 que se reenvía a través de las redes puentadas o conmutadas por DLSw. Ello se puede realizar de dos maneras:

- Filtrando tantas tramas NetBIOS de difusión como sea posible antes de enviarlas por puente o conmutarlas por DLSw.
- Reenviando tramas UI NetBIOS no filtradas en los menos puertos o sesiones TCP DLSw posibles.

La Tabla 9 lista los filtros que IBM proporciona.

Tabla 9. Filtros NetBIOS

Tipo de filtro	**Filtros**
Dirección MAC	Tramas por dirección MAC origen o de destino.
Bytes	Tramas por desplazamiento de bytes y longitud de campo dentro de una trama
Nombre	Tramas por nombres NetBIOS origen y de destino.
Trama duplicada	Tramas duplicadas.
Respuesta	Respuestas a las que el direccionador no ha reenviado una trama de difusión NetBIOS.

Después de que el direccionador filtre las tramas, las listas de nombres NetBIOS y la antememoria de nombres y de rutas NetBIOS controlan la manera en que se reenvían las tramas restantes. En los apartados “Filtro por bytes de NetBIOS” en la página 49 y “Filtro por nombre de sistema principal de NetBIOS” en la página 49 se describe los filtros por bytes y por nombre, respectivamente. En la publicación

Access Integration Services Guía del usuario de software se describe el filtro por dirección MAC.

Si desea obtener una introducción los filtros por nombre de sistema principal y los filtros por bytes, consulte “Filtros por nombre y por bytes de NetBIOS” en la página 48.

En las siguientes secciones se describen los filtros por tipo de trama, de tramas duplicadas y de tramas de respuesta; las listas de nombres de NetBIOS; y la antememoria de nombres y de rutas de NetBIOS.

Filtro por tipo de trama

El filtro por tipo de trama permite que ciertas categorías de tramas NetBIOS se filtren completamente para tráfico de puentes, tráfico DLSw o tanto para tráfico DLSw como para tráfico de puentes.

Las tres categorías de tramas NetBIOS que se pueden filtrar son:

- Tramas de resolución de conflictos de nombres

  Son las tramas NetBIOS de difusión utilizadas para garantizar que un nombre NetBIOS que se debe utilizar es exclusivo en la red.

  En redes NetBIOS, es muy importante que los nombres NetBIOS de estaciones para las que se establece una sesión NetBIOS (habitualmente los servidores NetBIOS) sean exclusivos. Normalmente también es muy importante que los nombres NetBIOS individuales de estaciones del mismo grupo (o dominio) sean exclusivos. Pero a menudo no es tan importante que los nombres NetBIOS de estaciones desde las que se configura una sesión NetBIOS (habitualmente clientes NetBIOS) sean exclusivos, especialmente en dominios.

  Por este motivo, las redes en las que se dispone de un buen control sobre los nombres pueden obtener muchas ventajas si filtran las tramas de resolución de conflictos de nombres. Lo anterior se da especialmente en las redes conmutadas por DLSw.

  Las tramas de resolución de conflictos de nombres NetBIOS son Add-Name-Query, Add-Group-Name-Query y Add-Name-Response.

- Tramas de difusión general

  Son las tramas NetBIOS de difusión utilizadas para enviar datos a todas las estaciones NetBIOS de una red. Este tipo de tramas se utilizan muy poco y habitualmente se filtran.

  La trama de difusión general NetBIOS es Datagram-Broadcast.

- Tramas de interrupción del rastreo

  Son las tramas NetBIOS de difusión utilizadas para interrumpir los rastreos NetBIOS en todas las estaciones NetBIOS de una red. Este tipo de tramas se utilizan muy poco y habitualmente se filtran.

  La trama de interrupción del rastreo NetBIOS es Terminate-Trace.

El valor por omisión es no filtrar ninguno de los tipos de tramas anteriores para el tráfico NetBIOS que circula por puente y filtrar todos los tipos de tramas anteriores para tráfico NetBIOS conmutado por DLSw. De todos modos, puede resultar bene-

ficioso filtrar los tipos de tramas anteriores si el tráfico NetBIOS circula por puente en enlaces de WAN.

En caso de utilizar puentes, entre **set filters bridge** para activar o desactivar el filtro por tipo de trama. En caso de utilizar DLSw, entre **set filters dlsw** para activar o desactivar el filtro por 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
```

Filtro de tramas duplicadas

Todas las tramas NetBIOS de difusión que pueden tener una respuesta son enviadas por la estación NetBIOS de origen un número fijo de veces (por omisión 6) a un intervalo fijo (por omisión 1/2 segundo). En la siguiente explicación, dichas tramas se denominan tramas de *mandato NetBIOS* y las posibles tramas de respuesta se denominan *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
- Las tramas de configuración de sesiones NetBIOS – Name-Query
- Las tramas de estado de NetBIOS – Status-Query

Las tramas de mandato se envían varias veces para aumentar las probabilidades de una entrega satisfactoria (dichas tramas son tramas sin conexión). Cada trama de respuesta se envía sólo una vez en respuesta a cada trama de mandato recibida.

En una red conmutada por DLSw, el reenvío de cada entrada por las sesiones WAN puede resultar muy costoso. Por lo tanto, cuando se recibe la primera trama de mandato, se reenvía al DLSw vecino y a los puertos de puente adecuados y se guarda una copia. Todos los reintentos de la misma trama de mandato NetBIOS recibida durante un periodo de tiempo configurable se descartan.

Existe un periodo de tiempo configurable para la red de puente y un periodo de tiempo configurable para la red DLSw.

El periodo de tiempo configurable de 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 de puente.
- **set general** (parámetro “Duplicate frame filter timeout value in seconds”)

Si está habilitado el filtro de tramas duplicadas, este valor especifica cuánto tiempo hay para descartar tramas de mandato NetBIOS duplicadas después de que se haya enviado por puente una trama de mandato NetBIOS.

Si se recibe una trama de mandato NetBIOS duplicada después de que se haya excedido el tiempo de espera, la trama se reenvía a la red de puente.

El periodo de tiempo configurable de la red DLSw se controla mediante un solo parámetro:

- **set cache-parms** (parámetro “Reduced search timeout value in seconds”)

  Este valor especifica cuánto tiempo hay para descartar tramas de mandato NetBIOS duplicadas después de que se haya reenviado una trama de mandato NetBIOS a la red DLSw.

  Si se recibe una trama de mandato NetBIOS duplicada después de que se haya excedido el tiempo de espera, la trama se reenvía a la red DLSw.

  Nota: El filtro de tramas de mandato NetBIOS a una red DLSw siempre está habilitado.

Cuando un vecino DLSw recibe una trama de mandato NetBIOS, la trama se reenvía a la red de puente y se guarda una copia. La función DLSw de vecino reenvía un reintento de la trama de mandato a la función de puente un número de veces configurable (por omisión 6) a un intervalo también configurable (1/2 segundo). 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 configurables se controlan mediante el mandato y los parámetros siguientes:

- **set general** (parámetros “Command frame retry count” y “Command frame retry timeout value in seconds”)

Existe un último parámetro que controla el tiempo durante el que se guarda la trama de mandato a fin de llevar a cabo el reenvío de red de puente y DLSw antes descrito:

- **set general** (parámetro "Duplicate frame detect timeout value in seconds")

  Este parámetro indica durante cuánto tiempo se guarda una trama de mandato recibida para el proceso de tramas duplicadas y de tramas de respuesta. Después de que se exceda el tiempo de espera, la trama de mandato se suprime y se cancelan el temporizador del filtro de tramas duplicadas y el temporizador de búsqueda reducida asociado a él. La primera trama de mandato duplicada recibida después de superar el tiempo de espera se considera la primera trama de mandato recibida. Todas las tramas de respuesta recibidas después de que se supere el tiempo de espera se descartan.

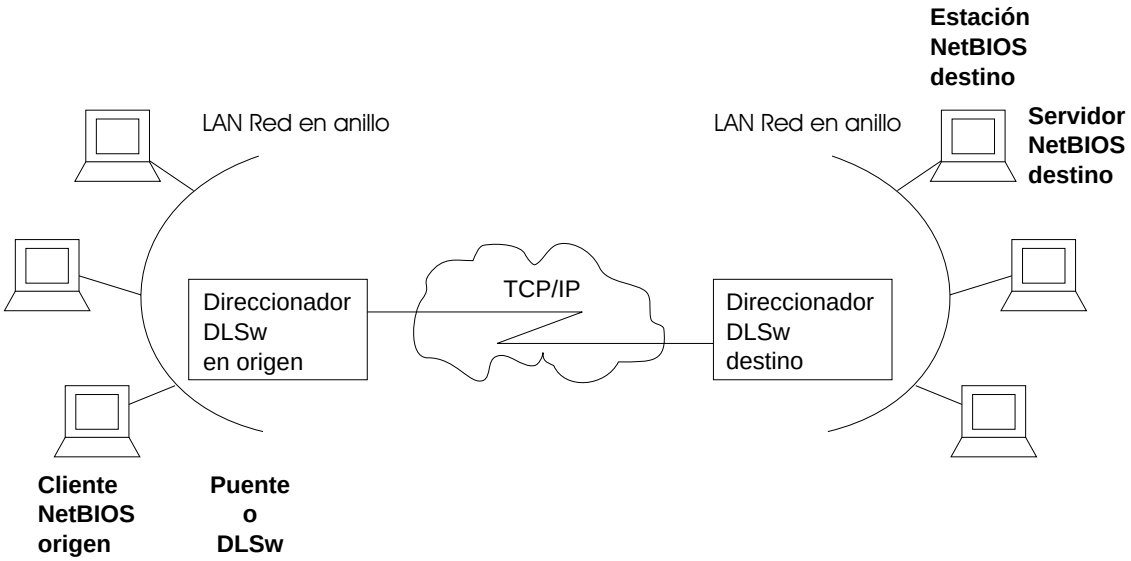
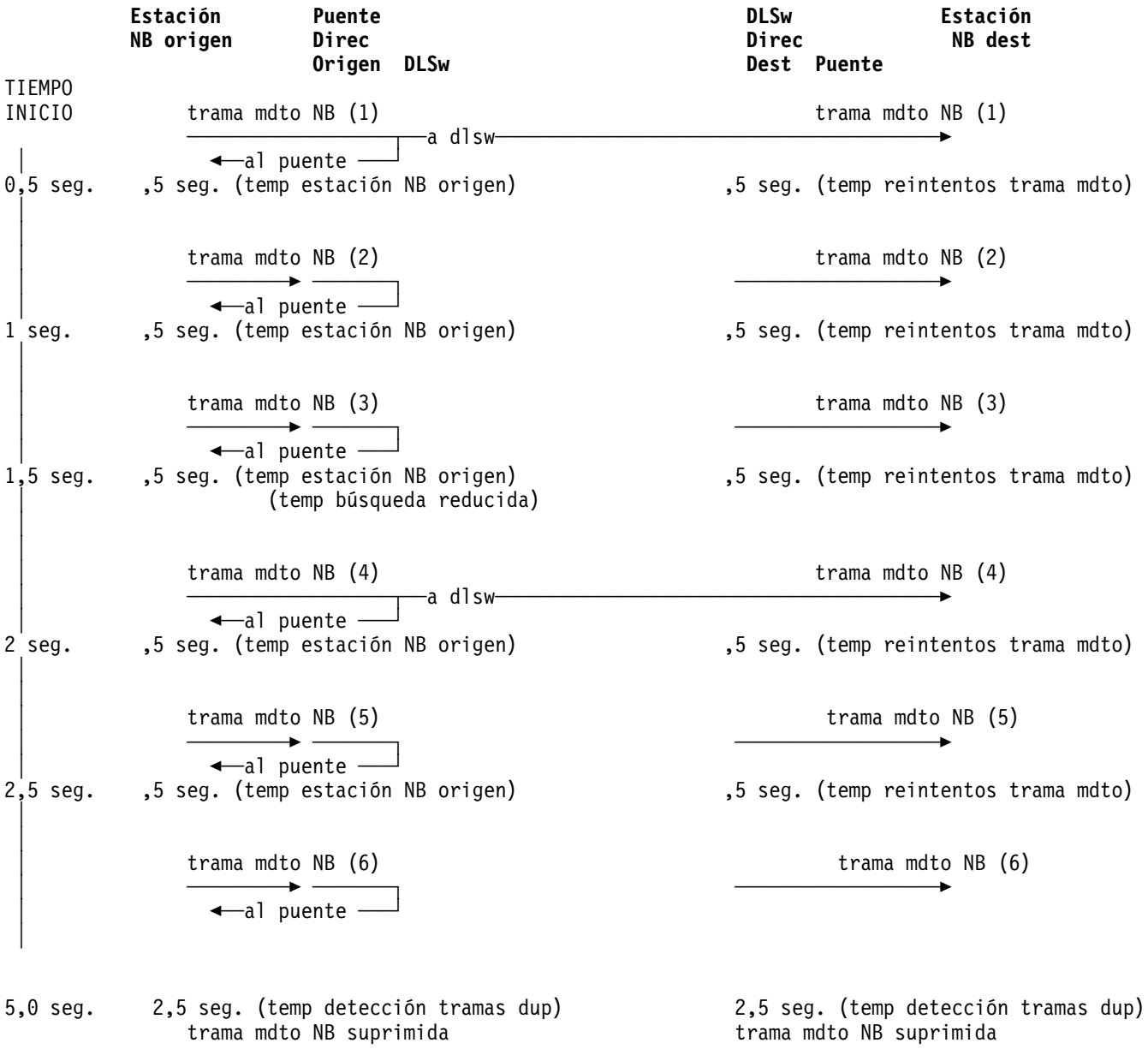


Figura 24. Configuración de una sesión NetBIOS en DLSw. El filtro de tramas duplicadas reduce el número de tramas de difusión reenviadas en la WAN de DLSw.

La Figura 24, junto con la siguiente secuencia, muestra el funcionamiento del proceso con los valores por omisión. Para que resulte más claro, se presupone que no se ha recibido 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 del direccionador DLSw de origen. Se guarda una copia de la trama de mandato NetBIOS. Puesto que los puentes están habilitados, la trama se reenvía a la red de puente. Como el filtro de tramas duplicadas de la red de puente está inhabilitado por omisión, el temporizador del filtro de tramas duplicadas no se inicia. Dado que NetBIOS DLSw está habilitado, la trama se reenvía a la red DLSw y el temporizador de búsqueda reducida se inicia (por omisión 1 - 1/2 segundos). El temporizador de detección de tramas duplicadas (por omisión 5 segundos) también se inicia.
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 los puentes están habilitados, la trama se reenvía a la red de puente. Como el filtro de tramas duplicadas de la red de puente está inhabilitado por omisión, el temporizador del filtro de tramas duplicadas no se inicia. El

temporizador de mandatos de reintento (por omisión 1/2 segundo) y el temporizador de detección de tramas duplicadas (por omisión 5 segundos) se inician.

3. En el direccionador de origen se recibe la segunda trama de mandato NetBIOS (primer reintento). Como el filtro de tramas duplicadas de la red de puente está inhabilitado por omisión, la trama se reenvía a la red de puente. Puesto que el tiempo de espera de la búsqueda reducida no ha finalizado, 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. Como el filtro de tramas duplicadas de la red de puente está inhabilitado por omisión, la trama se reenvía a la red de puente. El temporizador de mandatos de reintento (por omisión 1/2 segundo) se inicia.
5. En el direccionador de origen se recibe la tercera trama de mandato NetBIOS (segundo reintento).
6. En el direccionador de destino el segundo reintento de la trama de mandato NetBIOS se maneja igual que el primer reintento.
7. En el direccionador de origen se recibe la cuarta trama de mandato NetBIOS (tercer reintento). Como el filtro de tramas duplicadas de la red de puente está inhabilitado por omisión, la trama se reenvía a la red de puente. Puesto que el tiempo de espera de la búsqueda reducida ha finalizado, la trama se reenvía a la red DLSw. El temporizador de la búsqueda reducida se reinicia.
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. Como el filtro de tramas duplicadas de la red de puente está inhabilitado por omisión, la trama se reenvía a la red de puente. El temporizador de mandatos de reintento (por omisión 1/2 segundo) se inicia. El direccionador de destino recibe también la trama de mandato NetBIOS reenviada desde el direccionador de origen pero la descarta como si fuera duplicada.
9. En el direccionador de origen, la quinta trama de mandato NetBIOS (cuarto reintento) se maneja igual que la segunda trama de mandato NetBIOS.
10. En el direccionador de destino el cuarto reintento de la trama de mandato NetBIOS se maneja igual que el primer reintento.
11. En el direccionador de origen se recibe la sexta trama de mandato NetBIOS (quinto reintento). Como el filtro de tramas duplicadas de la red de puente está inhabilitado por omisión, la trama se reenvía a la red de puente. Puesto que el tiempo de espera de la búsqueda reducida no ha finalizado, 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. Como el filtro de tramas duplicadas de la red de puente está inhabilitado por omisión, la trama se reenvía a la red de puente. Puesto que se ha agotado el recuento de reintentos, el temporizador de reintentos de mandatos no se reinicia.
13. Después de 2 - 1/2 segundos más en el direccionador de origen, el temporizador de detección de tramas duplicadas finaliza y la trama de mandato NetBIOS guardada se suprime.

14. Después de 2 - 1/2 segundos más en el direccionador de destino, el temporizador de detección de tramas duplicadas finaliza y la trama de mandato NetBIOS guardada se suprime.

Filtro de tramas de respuesta

Tanto las tramas de mandato de configuración de una sesión NetBIOS como las tramas de mandato de estado NetBIOS esperan su correspondiente trama de respuesta. Si no se recibe ninguna trama de respuesta, se vuelve a intentar la trama de mandato como muestra el ejemplo anterior.

Cuando se recibe la primera trama de respuesta NetBIOS en la red de puente del direccionador de destino, ésta se reenvía de vuelta al direccionador origen y la trama de mandato NetBIOS guardada se suprime. Todas las tramas de respuesta posteriores que se reciban en el direccionador de destino se descartan porque no se ha encontrado ninguna trama de mandato NetBIOS correspondiente.

En el direccionador origen, la trama de respuesta recibida se reenvía a la red de puente y la trama de mandato NetBIOS guardada se suprime. Todas las tramas de respuesta posteriores recibidas en el direccionador de origen (desde la red DLSw o de puente) se descartan.

Las tramas de mandato de conflictos de nombres NetBIOS pueden generar una trama de respuesta NetBIOS correspondiente aunque no la necesitan. Así mismo, se utilizan todas las trama recibidas (para determinar si existe más de un conflicto).

Por lo tanto, todas las tramas de conflictos de nombres NetBIOS recibidas se reenvían pero la trama de mandato NetBIOS no se suprime hasta que finaliza el temporizador de detección de tramas duplicadas.

Listas de nombres de NetBIOS

La listas de nombres NetBIOS es un vehículo exclusivo de DLSw para limitar el número de asociados de DLSw a los que se reenvía una trama UI NetBIOS.

Se puede configurar una lista de nombres NetBIOS local en cada direccionador. Esta lista de nombres representa todos los nombres NetBIOS conectados a la red puenteada 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. Dichos asociados utilizan la lista para limitar el tráfico NetBIOS que el asociado envía a este direccionador.

Las listas de nombres NetBIOS son útiles en entornos en los que se dispone de un buen control sobre los nombres NetBIOS; especialmente los entornos a los que se debe acceder remotamente a través de DLSw.

Configuración de listas de nombres de NetBIOS locales

Una lista de nombres NetBIOS es un conjunto de entradas de lista de nombres NetBIOS . La configuración de la lista de nombres NetBIOS local implica:

- La adición de un máximo de 30 entradas en una lista de nombres
- La configuración de esta lista como representativa de todos los nombres NetBIOS a los que pueden acceder los asociados de DLSw del direccionador.

Configure las entradas de la lista de nombres en el indicador `NetBIOS config>` con el mandato *add name-list*. Cada entrada consta de la siguiente información:

calificador de nombres

Un calificador de nombres representa uno o más nombres NetBIOS. Cada calificador de nombres puede tener hasta 16 caracteres. Se pueden representar varios nombres NetBIOS utilizando comodines (un ? incorporado o un * al final) dentro del nombre.

El ? (signo de interrogación) significa que el carácter situado en esa posición del nombre NetBIOS puede tener cualquier valor.

El * (asterisco) como último carácter de un nombre significa que el resto de caracteres del nombre NetBIOS pueden tener cualquier valor.

Nota: En la mayoría de aplicaciones NetBIOS de cliente/servidor, los únicos nombres necesarios de las listas de nombres son los de servidores o dominios. No es necesario configurar nombres de clientes individuales en listas de nombres.

tipo de calificador de nombres

Los nombres NetBIOS pueden ser nombres individuales o nombres de grupos. Cada calificador de nombres representa un conjunto de nombres NetBIOS individuales o un conjunto de nombres NetBIOS de grupo. El tipo de calificador de nombres especifica el tipo de nombres NetBIOS (individuales o de grupo) al que representa el calificador de nombres correspondiente.

Como norma general, los nombres de dominio son nombres de grupo y los nombres de clientes o servidores son nombres individuales.

La propia lista de nombres dispone de un atributo que se configura en el indicador `NetBIOS config>` mediante el mandato SET NAME-LIST. Dicho atributo es *name list exclusivity.*

El atributo indica si el conjunto de las entradas de la lista de nombres representa todos los nombres a los que pueden acceder los asociados de DLSw del direccionador (exclusiva) o representa algunos pero no necesariamente a todos los nombres NetBIOS a los que pueden acceder los asociados de DLSw del direccionador (no exclusiva).

Las listas de nombres exclusivas son las que mejor limitan el tráfico DLSw NetBIOS de la red. Sólo las tramas destinadas a un nombre NetBIOS representado por la lista de nombres exclusiva de un direccionador se reenvían a dicho direccionador.

Las listas de nombres no exclusivas ayudan a limitar el tráfico NetBIOS DLSw de la red aunque no lo hacen tan bien como las listas de nombres exclusivas. Las tramas destinadas a un nombre NetBIOS representado por la lista de nombres no exclusiva de un direccionador se enviarán primero a dicho direccionador.

Si el direccionador recibe una trama destinada a un nombre NetBIOS no representado por ninguna lista de nombres del direccionador, éste reenvía la trama a todos los direccionadores con listas de nombres no exclusivas.

Se puede controlar la utilización por parte de un direccionador concreto de su lista de nombres NetBIOS local y de las listas de nombres recibidas de los asociados de 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 habilita use local NetBIOS name list, el direccionador envía la lista de nombres NetBIOS local configurada en el direccionador a todos los asociados de DLSw.

Si inhabilita use local NetBIOS name list, el direccionador no envía la lista de nombres NetBIOS local configurada en el direccionador a todos los asociados de 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 habilita use remote NetBIOS name lists, el direccionador utiliza todas las listas de nombres NetBIOS que recibe de los asociados de DLSw del direccionador para determinar cómo se deben reenviar ciertas tramas NetBIOS.

Si inhabilita use remote NetBIOS name lists, el direccionador ignora todas las listas de nombres NetBIOS recibidas de los asociados DLSw del direccionador.

Confirmación de cambios en las listas de nombres de NetBIOS

Puede cambiar todos los parámetros de las listas de nombres NetBIOS permanentemente en el indicador `NetBIOS config>` o temporalmente en el indicador `NetBIOS>`.

Puesto que cada cambio efectuado obliga al direccionador a enviar información a cada asociado de DLSw, deberá indicar que los cambios en la lista de nombres están preparados para ser utilizados entrando el mandato **set name-list** en el indicador `NetBIOS>`.

Utilización de las listas de nombres de NetBIOS

El direccionador utiliza las listas de nombres para determinar cómo se deben reenvía las siguientes tramas NetBIOS:

- Trama de mandato de configuración de sesión NetBIOS (Name-Query)
- Trama de mandato de estado NetBIOS (Status-Query)
- Trama de transferencia de datos sin conexión (Datagram)

Utilización de las listas de nombres de NetBIOS exclusivas de manera efectiva: Configure listas de nombres NetBIOS exclusivas siempre que sea posible. Si configura y envía una lista de nombres exclusiva a todos los asociados de DLSw, las únicas tramas NetBIOS que se recibirán desde los asociados de DLSw serán las tramas cuyo nombre de destino coincida con una de las entradas de la lista de nombres.

Una lista de nombres NetBIOS exclusiva útil es la lista de nombres NetBIOS vacía. Si un direccionador concreto no dispone de servidores NetBIOS a los que debe acceder alguno de sus asociados DLSw, deberá utilizar una lista de nombres exclusiva vacía.

Utilización de las listas de nombres de NetBIOS no exclusivas: Si un direccionador dispone de muchos asociados de DLSw que pertenecen todos a diferentes redes de puente, puede utilizar listas de nombres no exclusivas. Las entradas de la lista de nombres se pueden configurar para los servidores que se utilizan más a menudo a fin de que el tráfico que se destina a dichos servidores vaya primero a este direccionador. Si especifica la lista de nombres como no exclu-

siva, el tráfico podrá ir a servidores utilizados con menos frecuencia sin tener que configurar los servidores en la lista de nombres. Utilice esta configuración en una red que no disponga de un control muy estricto sobre los nombres NetBIOS; en especial los servidores a los que se debe acceder remotamente a través de DLSw.

Las listas de nombres NetBIOS no exclusivas se pueden utilizar también en configuraciones que contienen vías de acceso a DLSw paralelas entre redes de puente. Si dos direccionadores se encuentran en la misma red de puente, un direccionador puede configurar una lista de nombres NetBIOS que represente un conjunto de servidores a los que se deba acceder remotamente a través de DLSw en la red de puente y el otro direccionador puede configurar una lista de nombres NetBIOS que represente un conjunto diferente de servidores. Cuando ambos direccionadores están activos, el tráfico NetBIOS se distribuye entre los dos direccionadores. Si un direccionador está inactivo, todo el tráfico de NetBIOS irá a través del otro direccionador porque dispone de una lista no exclusiva.

La lista de nombres por omisión es una lista de nombres NetBIOS no exclusiva. Ello indica que un direccionador desea que sus asociados DLSw le envíen todo el tráfico NetBIOS que no se puede reenviar.

Antememoria de nombres y antememoria de rutas NetBIOS

La antememoria de nombres NetBIOS es la función del direccionador que clasifica el tipo de nombres NetBIOS y la información necesaria para llegar al nombre NetBIOS. Dicha información se utiliza para determinar mejor la manera de reenviar tramas NetBIOS no filtradas al menor número posible de vecinos DLSw y de puertos de puente. Los posibles tipos de nombres NetBIOS y la información que se guarda de cada uno son:

Individual remote
Es un nombre NetBIOS al que se puede acceder a través de una sesión concreta de TCP de DLSw. Se guardan las mejores sesiones de TCP.

Individual local
Es un nombre NetBIOS al que se puede acceder localmente a través de la red de puente. Se guarda la dirección MAC asociada con el nombre. Si la antememoria de rutas está habilitada, también se guarda la mejor ruta LLC entre el direccionador y la estación NetBIOS.

Group
Es un nombre NetBIOS de grupo. Se puede acceder a él remota y/o localmente y puede representar varias estaciones NetBIOS. No se guarda ninguna otra información.

Unknown
No se ha encontrado aún información acerca de este nombre NetBIOS, lo que indica que no ha finalizado su búsqueda. No se guarda ninguna otra información.

Cuando se reciben tramas de configuración de una sesión NetBIOS o tramas de transferencia de datos sin conexión, se utiliza la antememoria de nombres para determinar cómo se debe reenviar la trama. Si se recibe una de estas tramas en la red de puente de un direccionador, debe llevarse a cabo alguna de las siguientes acciones:

- Si el nombre de destino de la trama NetBIOS no se encuentra en la antememoria de nombres NetBIOS del direccionador, se busca uno coincidente en todas las listas de nombres de los asociados de DLSw.

  Si se encuentra alguna coincidencia con los calificadores de nombres de grupo, se crea una entrada de antememoria de nombres NetBIOS con el tipo de nombre *group*. La trama se reenvía a todos los puertos de puente y a todos los asociados de DLSw con listas de nombres no exclusivas o listas de nombres exclusivas que dispongan de una entrada de lista de nombres coincidente.

  Si se encuentran coincidencias con calificadores de nombres individuales, se crea una entrada de antememoria de nombres con el tipo de nombre *individual remote*. La trama se reenvía a cada asociado de DLSw que disponga de una entrada de lista de nombres coincidente.

  Si no se encuentran coincidencias, se crea una entrada de antememoria de nombres NetBIOS con el tipo de nombre *unknown*. La trama se reenvía a todos los puertos y a todos los asociados de DLSw que dispongan de listas de nombres no exclusivas.

- Si el nombre de destino de la tramas NetBIOS se encuentra en la antememoria de nombres NetBIOS del direccionador y se ha clasificado como individual remote, la trama se reenvía a la mejor sesión de TCP de DLSw averiguada.

  Si se averiguan sesiones de TCP igualmente óptimas, se utilizarán de forma alterna en diferentes tramas de configuración de sesión NetBIOS.

- Si el nombre de destino de la trama NetBIOS se encuentra en la antememoria de nombres NetBIOS del direccionador y se ha clasificado como individual local, la dirección MAC guardada sustituirá a la dirección MAC de destino de la trama NetBIOS.

  Si la antememoria de rutas está inhabilitada, la información de direccionamiento de la trama NetBIOS se descarta y la trama se reenvía a todos los puertos de puente.

  Si la antememoria de rutas está habilitada, 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 se encuentra en la antememoria de nombres NetBIOS del direccionador y está clasificado como group o unknown, la trama se reenvía a todos los puertos de puente o a todos los vecinos de DLSw.

Averiguar nombres de NetBIOS

Los nombres NetBIOS se averiguan y se clasifican a partir de la información de las tramas de configuración de sesión NetBIOS (Name-Query y Name-Recognized).

Configuración de las entradas de antememoria de nombres de NetBIOS

Se pueden configurar nombres NetBIOS remotos individuales y asociarlos con una sesión concreta de TCP de DLSw. Ello puede reducir en gran medida los gastos generales. Para mejorar el rendimiento, se recomienda configurar los servidores

NetBIOS remotos a los que acceden habitualmente clientes NetBIOS en la red de puente local del direccionador.

No se pueden configurar nombres NetBIOS locales y asociarlos con una dirección MAC y una ruta concreta.

Existen tres tipos de entradas de antememoria de nombres NetBIOS:

- Las entradas permanentes, que son las que se añaden en el indicador de configuración de NetBIOS (`NetBIOS config>`). El direccionador guarda las entradas permanentes en su configuración cuando el direccionador se reinicia.

  Entre **add cache-entry** en el indicador `NetBIOS config>` para añadir una entrada permanente. Se le solicita que entre el nombre NetBIOS y la dirección IP asociada.

- Las entradas estáticas, que son las que se añaden en el indicador de supervisión de NetBIOS (`NetBIOS>` console). El direccionador no guarda entradas estáticas cuando se reinicia el direccionador.

  Entre **add cache-entry** en el indicador de consola `NetBIOS>` para añadir una entrada estática. Se le solicita que entre el nombre NetBIOS y la dirección IP asociada.

- Las entradas dinámicas, que son las que ***no*** se añaden ni en el indicador de configuración ni en el indicador de supervisión de NetBIOS sino que se averiguan de manera dinámica a partir de las tramas de configuración de sesión NetBIOS. El direccionador no guarda entradas dinámicas cuando se reinicia el direccionador.

Configuración de los parámetros de la antememoria de nombres

Para evitar que un tipo de nombre NetBIOS llene toda la antememoria de nombres, existen dos límites de antememoria de nombres NetBIOS configurables:

- El número máximo de entradas de antememoria de nombres locales especifica el número máximo de entradas de antememoria de nombres NetBIOS locales individuales que se pueden almacenar en antememoria de una sola vez. Las nuevas entradas alteran temporalmente a las entradas que hace más tiempo que se han utilizado.
- El número máximo de entradas de antememoria de nombres remotas especifica el número combinado de entradas de antememoria de nombres NetBIOS individuales remotas, de grupo y desconocidas que se pueden almacenar en antememoria de una sola vez. Las nuevas entradas alteran temporalmente a las entradas que hace más tiempo que se han utilizado.

Si no se referencia una entrada durante un periodo de tiempo de espera configurable, ésta se suprime automáticamente. Dicho periodo de tiempo de espera es el valor de tiempo de espera de la entrada no referenciada.

La asociación de un nombre NetBIOS con una sesión de TCP o una dirección MAC y una ruta se realiza en un momento determinado. Como las redes cambian y la mejor vía de acceso a un nombre NetBIOS puede cambiar, la asociación entre un nombre NetBIOS y una sesión de TCP o una dirección MAC y una ruta se guarda sólo durante un periodo de tiempo configurable. Después de dicho periodo, se averigua una nueva asociación de vía de acceso óptima. El parámetro que con-

trola este periodo de tiempo configurable es best path aging timeout value (valor de tiempo de espera de la antigüedad de la mejor vía de acceso) .

Otro parámetro útil de configuración es reduced search timeout value (valor de tiempo de espera de la búsqueda reducida). Además de controlar durante cuánto tiempo las tramas de mandato duplicadas se filtran a la red DLSw, controla también cuánto tiempo se debe esperar antes de ampliar la búsqueda de un nombre NetBIOS. Si se recibe una trama se configuración de sesión NetBIOS y el nombre NetBIOS de destino se encuentra en la antememoria de nombres NetBIOS del direccionador como trama remota individual, la trama se reenvía a la sesión TCP correspondiente. Si no se recibe respuesta alguna a esta trama, puede ser debido a que ya no se puede acceder al nombre a través de esta vía de acceso. La primera trama de configuración de sesión NetBIOS recibida después de que finalice el temporizador de búsqueda reducida se reenvía a todas las sesiones de TCP de DLSw, con lo cual se amplía la búsqueda de una vía de acceso mejor.

El último parámetro, caracteres significativos en el nombre, controla cuántos de los 16 caracteres de un nombre NetBIOS son necesarios para considerarlo como un nombre NetBIOS exclusivo. Algunas aplicaciones NetBIOS utilizan el 16 carácter del nombre para distinguir ciertas entidades asociadas con un sólo nombre NetBIOS (por ejemplo, servidor de impresión o servidor de archivos). En tal caso, es mejor especificar el parámetro de caracteres significativos en el nombre como 15. Esto hace que cualquier trama en la que los primeros 15 caracteres del nombre NetBIOS de destino coincida con los primeros 15 caracteres de la entrada de antememoria de nombres NetBIOS del direccionador se reenvíe según la información de la entrada de antememoria de nombres. Por lo tanto, varios nombres NetBIOS se pueden representar con una sola entrada de antememoria de nombres NetBIOS.

Todos los anteriores parámetros relacionados de la antememoria de nombres NetBIOS se pueden configurar mediante el mandato **set cache-parms** de la manera siguiente.

```
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 “Mandatos de NetBIOS” en la página 174 si desea obtener más información sobre el mandato **set cache-parms**.

Visualización de las entradas de antememoria

El direccionador proporciona los siguientes mandatos que le permiten ver las entradas de antememoria. Desde el indicador de configuración de NetBIOS, puede utilizar los mandatos **list cache** que aparecen en la Tabla 10 en la página 163.

Tabla 10. Mandatos de configuración list cache de NetBIOS	
Mandato	**Visualiza . . .**
list cache all	Todas las entradas permanentes. No muestra entradas estáticas ni dinámicas.
list cache entry-number	Una entrada de antememoria permanente según su número de entrada.
list cache NetBIOS-name	Una entrada de antememoria permanente de un nombre NetBIOS específico.
list cache ip-address	Una entrada de antememoria permanente de una dirección IP específica.

Desde el indicador de supervisión de NetBIOS, puede utilizar los mandatos list cache de la Tabla 11.

Tabla 11. Mandatos de supervisión list cache de NetBIOS	
Mandato	**Visualiza . . .**
list cache active	Todas las entradas activas de la antememoria de nombres del direccionador, incluidas las permanentes, las estáticas y las dinámicas.
list cache config	Las entradas estáticas y permanentes. No muestra entradas dinámicas.
list cache group	Las entradas que existen en nombres de grupos NetBIOS.
list cache local	Las entradas de antememoria locales. Las entradas de antememoria locales son las que el direccionador averigua en la red puenteada.
list cache name	Una entrada de antememoria de un nombre NetBIOS específico.
list cache remote	Las entradas de antememoria remotas. Son las entradas que el direccionador averigua en la WAN de DLSw.
list cache unknown	Entradas en las que el tipo de entrada NetBIOS es desconocido. El direccionador considera a todas las entradas como desconocidas hasta que averigua el tipo de entrada.

Procedimientos de configuración de filtro por nombre de sistema principal y por bytes de NetBIOS

Las siguientes secciones proporcionan ejemplos sobre cómo configurar el filtro de NetBIOS. El primero explica cómo crear un filtro por nombre de sistema principal. El segundo demuestra cómo configurar un filtro por bytes. Si desea más información sobre los mandatos utilizados en estos ejemplos, consulte “Mandatos de NetBIOS” en la página 174.

Para crear un filtro por nombre 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>
```

Creación de un filtro por nombre de sistema principal

Utilice el siguiente mandato para crear un filtro por nombre de sistema principal.

1. Cree una lista de filtro por nombre vacía.

   ```
   NetBIOS Filter config>create name-filter-list
   Handle for Name Filter List []? boston
   ```

2. Añada los elementos de filtro a la lista de filtro por nombre.

   Entre **update** para acceder al indicador de esa lista de filtro específica. Desde dicho indicador, puede añadir elementos a la lista de filtro.

   ```
   NetBIOS Filter config>update
   Handle for Filter List []? boston
   Name Filter List Configuration
   NetBIOS Name boston config>
   ```

3. Añada elementos de filtro a la lista de filtro con el mandato **add**. El modo en que están configurados los elementos de filtro determina qués paquetes NetBIOS que envían por puente y cuáles que se eliminan. Configure elementos de filtro por nombre de sistema principal con los siguientes parámetros entrados en este orden:

   - *Inclusive* (enviado por puente) o *Exclusive* (eliminado).
   - *ASCII* o *HEX* - según esté representado el nombre del sistema principal.
   - *nombre-sistema-principal* - el nombre real del sistema principal representado como serie ASCII o hex (consulte “Mandatos de NetBIOS” en la página 174 si desea conocer su sintaxis).

     Nota: Esta entrada es sensible a mayúsculas y minúsculas.

   - <*ÚLTIMO-número-hexadecimal*> - un parámetro opcional para utilizarlo con series ASCII que contienen menos de 16 caracteres.

   En el siguiente ejemplo, se añade un elemento de filtro a la lista de filtro por nombre de sistema principal **boston**, lo que permite que los paquetes que contengan el nombre de sistema principal **westboro** (una serie ASCII) se envíen por el puente (configurados como *inclusive*). No se ha configurado el parámetro <*LAST-hex-number*> 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 desea que se le hagan solicitudes. Asegúrese de que deja un espacio entre cada parámetro.

4. Verifique la entrada de elementos de filtro.

   Escriba **list** para verificar 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 filtro.

   Repita los primeros cuatro pasos para añadir más elementos de filtro a la lista de filtro. El orden en que se entren los elementos de filtro es importante porque determina la manera 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 se entran los elementos de filtro más habituales en primer lugar el proceso de filtro será más eficaz porque es más probable 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 filtro. Puede cambiar la condición por omisión de la lista entrando **default inclusive** o **default exclusive** en el indicador de configuración de la lista de filtro. Por ejemplo:

   ```
   NetBIOS Name boston config> default exclusive
   ```

6. Cuando haya acabado de añadir elementos de filtro a la lista de filtro, entre **exit** para volver al indicador `NetBIOS Filter config>`.

   ```
   NetBIOS Name boston config>exit
   NetBIOS Filter config>
   ```

7. Añada el filtro a la configuración.

   La lista de filtro que contiene los elementos de filtro se puede añadir ahora como un filtro a la configuración dedireccionador de puente. Para ello, utilice el mandato **filter-on**. Configure filtros por nombre de sistema principal con los siguientes parámetros (entrados en este orden):

   - *Input* (para filtrar todos los paquetes NetBIOS recibidos en este puerto) o output (para filtrar todos los paquetes NetBIOS transmitidos en este puerto).
   - *Núm-puerto*, que es el número de puerto de puente configurado que desea en el direccionador.
   - *Lista-filtro*, que es el nombre de la lista de filtro (que contiene los elementos de filtro) que se desean incluir en este filtro.
   - Un operador opcional entrado como AND u OR en mayúsculas. Si hay presente un operador, debe ir seguido por un nombre de la lista de filtro. Los filtros con más de una lista de filtro se denominan filtros complejos.

   El siguiente ejemplo añade un filtro por nombre de sistema principal que afectará a la entrada de paquetes en el puerto número 3. Comprende la lista de filtro por nombre de sistema principal **boston**. Todos los paquetes que entren en el puerto número 3 se evalúan de acuerdo con las normas proporcionadas por los elementos de filtro contenidos en la lista de filtro **boston**. Esto significa que todos los paquetes que entren en el puerto número 3 y contengan el nombre de sistema principal **westboro** se enviarán por el puente.

```
NetBIOS Filter config>filter-on input
Port Number [1]? 3
Filter List []? boston
```

8. Verifique el filtro recién creado.

   Entre **list** para verificar 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. Habilite globalmente el filtro de NetBIOS.

   Utilice el mandato **enable** para habilitar globalmente el filtro de NetBIOS en el direccionador.

```
NetBIOS Filter config>enable NetBIOS-filtering
```

10. Reinicie el direccionador para activar todos los cambios de configuración del filtro de NetBIOS.

    Entre **exit** seguido por **Ctrl-P** para volver al indicador *. Desde este indicador, entre **restart** para activar todos los cambios de software efectuados durante el proceso de configuración del filtro de NetBIOS.

```
NetBIOS Filter config>exit
ASRT config>exit
Config> Ctrl-P
* restart
```

Creación de un filtro por byte

Utilice el siguiente procedimiento como pauta para crear un filtro por 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 filtro 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 filtro por bytes.

   Entre **update** para obtener el indicador de esa lista de filtro específica. Desde dicho indicador puede añadir elementos de filtro a la lista de filtro.

```
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 filtro con el mandato **add**. El modo en que están configurados los elementos de filtro determina qués paquetes NetBIOS que envían por puente y cuáles que se eliminan. Los elementos de filtro por bytes se configuran con los siguientes parámetros (entrados en este orden):

- Inclusive (enviado por puente) o Exclusive (eliminado).
- Byte Offset - el número de bytes (en formato decimal) a desplazar al paquete que se está filtrando. El desplazamiento empieza 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 los bytes que empiezan en el desplazamiento de bytes de la cabecera NetBIOS. Consulte “Mandatos de NetBIOS” en la página 174 si desea conocer las reglas de sintaxis.
- Hex mask - (si se encuentra presente) debe tener la misma longitud que el patrón hexadecimal y se une por medio del operador AND lógico a los bytes de desplazamiento del comienzo del paquete antes de que el resultado se compare con el patrón hexadecimal para comprobar su equivalencia. Si se omite el argumento *hex-mask*, se considera que todos son binarios.

En el siguiente ejemplo, se añade un elemento de filtro a la lista de filtro por bytes **westboro** que permite que los paquetes con el patrón hexadecimal 0x12345678 con un desplazamiento de bytes de 0 se envíen por puente (configurados como Inclusive). No hay ninguna máscara hexadecimal presente.

```
NetBIOS Byte westport config>add inclusive
Byte Offset [0]? 0
Hex Pattern []? 12345678
Hex Mask (<CR> for no mask) []?
```

3. Verifique la entrada de elementos 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 filtro.

   Repita los primeros tres pasos para añadir más elementos de filtro a la lista de filtro.

5. Cuando haya acabado de añadir elementos de filtro a la lista de filtro, escriba **exit** para volver al indicador `NetBIOS Filter config>`.

```
NetBIOS Byte westport config>exit
NetBIOS Filter config>
```

   El orden en que se entren los elementos de filtro es importante porque determina la manera 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 se entran los elementos de filtro más habituales en primer lugar el proceso de filtro será más eficaz porque es más probable que el software encuentre

una coincidencia al principio de la lista que no al tener que comprobar toda la lista antes de 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 filtro. Puede cambiar la condición por omisión de la lista entrando **default inclusive** o **default exclusive** en el indicador de configuración de la lista de filtro. Por ejemplo:

```
NetBIOS Byte westport config> default exclusive
```

6. Añada el filtro a la configuración.

   La lista de filtro que contiene los elementos de filtro se puede añadir ahora como un filtro a la configuración de direccionador de puente. Para ello, utilice el mandato **filter-on**. Configure filtros por nombre de sistema principal con los siguientes parámetros (entrados en este orden):

   - *Input* (para filtrar todos los paquetes recibidos en este puerto) o output (para filtrar todos los paquetes transmitidos en este puerto).
   - *Núm-puerto* - el número de puerto de puente configurado.
   - *Lista-filtro* - el nombre de la lista de filtro (que contiene los elementos de filtro) que se desean incluir en este filtro.
   - Un operador opcional entrado como AND u OR en mayúsculas. Si hay presente un operador, debe ir seguido por un nombre de la lista de filtro. Los filtros con más de una lista de filtro se denominan filtros complejos. Dichos filtros se describen con más detalle en “Acerca de los mandatos de configuración y supervisión de NetBIOS” en la página 171.

   El siguiente ejemplo añade un filtro por nombre de sistema principal que afectará a la salida de paquetes en el puerto número 3. Comprende la lista de filtro por nombre de sistema principal **westboro**. La salida de todos los paquetes en el puerto número 3 se evalúa de acuerdo con las normas que proporcionan los elementos de filtro contenidos en la lista de filtro **westboro**.

```
NetBIOS Filter config>filter-on output
Port Number [1]? 3
Filter List []? westboro
```

7. Verifique el filtro recién creado.

   Entre **list** para verificar 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. Habilite globalmente el filtro de NetBIOS.

Entre **enable** para habilitar globalmente el filtro NetBIOS en el direccionador de puente.

```
NetBIOS Filter config>enable NetBIOS-filtering
```

9. Reinicie el direccionador para activar todos los cambios de configuración del filtro de NetBIOS.

   Entre **exit** seguido por **Ctrl-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 la supervisión de NetBIOS por parte de IBM en redes puenteadas y en redes DLSw. Consta de los temas siguientes:

Acerca de los mandatos de configuración y supervisión de NetBIOS

Los mandatos de configuración de NetBIOS se pueden utilizar en el indicador `ASRT/DLSW config>`. Los cambios que se efectúen en la configuración del direccionador no son efectivos de manera inmediata. Entran a formar parte de la memoria de configuración del direccionador cuando éste se reinicia. Este capítulo denomina permanentes a los cambios de configuración.

Los mandatos de supervisión de NetBIOS se pueden utilizar en el indicador `ASRT/DLSW>`. Los mandatos de supervisión empiezan a tener efecto de manera 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, dichos cambios son temporales. La memoria de configuración del direccionador los sobreescribe cuando se reinicia el direccionador. Este capítulo denomina estáticos a los cambios que se efectúan en el indicador de supervisión.

Acceso al entorno de configuración de NetBIOS

Puede visualizar el indicador `NetBIOS config>` desde el entorno de configuración de ASRT o desde el entorno de configuración de DLSw. Los cambios que se efectúan en el indicador `NetBIOS config>` afectan tanto a los puentes como a DLSw.

Nota: Los mandatos de configuración NetBIOS no empiezan a tener efecto de manera inmediata. Debe reiniciar o volver a cargar el dispositivo antes de que empiecen a tener efecto.

Para visualizar el indicador `NetBIOS config>` desde el entorno de configuración de 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 de DLSw:

```
Config>protocol dls
DLSw protocol user configuration
DLSw config>NetBIOS

NetBIOS Support User Configuration

NetBIOS config>
```

Acceso al entorno de supervisión de NetBIOS

Puede visualizar el indicador NetBIOS> desde el entorno de supervisión de ASRT o el entorno de supervisión de DLSw.

Los cambios que se efectúan en el indicador de supervisión NetBIOS> afectan tanto a los puentes como a DLSw.

Para visualizar el indicador de supervisión NetBIOS> desde el entorno de supervisión de ASRT:

```
+ protocol asrt
ASRT>NetBIOS

NetBIOS Support User Console

NetBIOS>
```

Para visualizar el indicador NetBIOS> desde el entorno de supervisión de DLSw:

```
+ protocol dls
DLSw>NetBIOS

NetBIOS Support User Console

NetBIOS>
```

Configuración de NetBIOS para DLSw

Si está enviando tráfico NetBIOS en DLSw, utilice este procedimiento en el indicador DLSw config>:

- Abra SAP de NetBIOS.
- Establezca una prioridad para sesiones SNA y NetBIOS.
- Establezca el tamaño máximo de trama de NetBIOS.
- Establezca el número de bytes a asignar a tramas UI NetBIOS.

Abrir SAP de NetBIOS

Abra SAP de NetBIOS a ambos lados del enlace para que DLSw puede transmitir 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
```

Establecer de una prioridad para sesiones SNA y NetBIOS

Puede dar prioridad al tráfico SAN y NetBIOS para evitar que un tipo de sesión utilice demasiado ancho de banda disponible cuando la red está congestionada. Para hacerlo, entre **priority** para establecer una prioridad para sesiones SNA y sesiones NetBIOS. Puede establecer también una asignación de mensajes que corresponda a una prioridad de la sesión.

Utilice el mandato **set priority** tal y como muestra 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 de 4/3/2/1 proporciona la siguiente asignación a las sesiones:

4 - Critical
3 - High
2 - Medium
1 - Low

El direccionador utiliza la prioridad y la asignación de mensajes para limitar de manera selectiva la longitud de las ráfagas de tipos de tráfico específicos. Por ejemplo:

- Si asigna al tráfico SNA una prioridad Critical (totalmente prioritario) y las sesiones Critical (totalmente prioritarias) tienen una asignación de mensaje 4

  y

- Si asigna al tráfico NetBIOS una prioridad Medium (media) y las sesiones Medium (media) tienen una asignación de mensaje 2

el direccionador procesa cuatro tramas SNA antes de procesar dos tramas NetBIOS. Después de que el direccionador procese dos tramas NetBIOS, procesa cuatro tramas SNA y así sucesivamente.

En esta situación, el direccionador emplea dos tercios del ancho de banda disponible al tráfico SNA (una proporción de 4 a 2). Observe que el direccionador cuenta las tramas en lugar de los bytes cuando asigna ancho de banda de acuerdo con las prioridades que el usuario determina.

Puede cambiar la asignación de mensajes para sesiones que por omisión es 4/3/2/1. Debe entrar siempre cuatro dígitos, del 9 al 1, siempre en orden descendente. Por ejemplo, si la prioridad SNA es Critical y el tráfico NetBIOS es Medium y cambia la asignación de mensajes a 8/7/6/5, el direccionador procesa ocho tramas SNA antes de procesar seis tramas NetBIOS.

Establecer el tamaño máximo de trama NetBIOS

Puede utilizar también el mandato **set priority** de DLSw para cambiar el tamaño máximo de trama NetBIOS. Por omisión es 2052. Establezca este parámetro en el tamaño de trama más grande que crea que va a poder necesitar y no en un tamaño mayor a éste. Si se establece un tamaño mayor al necesario, se reducirá el número de almacenamientos intermedios disponibles.

Establecer asignación de memoria para tramas UI NetBIOS

Utilice el mandato **set memory** de DLSw para establecer el número de bytes que el direccionador asigna como almacenamiento intermedio para tramas UI NetBIOS. Si el almacenamiento intermedio de transmisión de TCP se llena, el direccionador utiliza dicho almacenamiento intermedio para tramas UI NetBIOS.

Observe que el número de bytes asignados para NetBIOS es global y 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 lista los mandatos de configuración y de supervisión de NetBIOS.

Tabla 12. Mandatos de configuración y de supervisión de NetBIOS

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Add	Añade entradas de antememoria a la antememoria de nombres del direccionador, y añade entradas de lista a la lista local de nombres del direccionador.
Delete	Suprime las entradas de antememoria o las entradas de lista de nombres que se han añadido mediante el mandato **add**.
Disable	Inhabilita el filtro de tramas duplicadas, la antememoria de rutas y la utilización de listas locales y remotas de nombres NetBIOS.
Enable	Habilita el filtro de tramas duplicadas, la antememoria de rutas y la utilización de listas locales y remotas de nombres NetBIOS.
List	Visualiza información diversa sobre la configuración de las listas de nombres y de la antememoria de nombres NetBIOS en función de si se encuentra en el indicador de configuración o en el indicador de supervisión.
Set	Configura parámetros para antememoria de nombres, filtro de tramas duplicadas, filtro por tipo de trama y listas de nombres. Visualiza también el indicador `NetBIOS Filter config>`.
Test	Este mandato está disponible sólo en el indicador de supervisión y prueba un nombre concreto NetBIOS contra la antememoria de nombres y las listas de nombres NetBIOS actuales.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Respuesta a los mandatos de configuración de NetBIOS

Los mandatos de configuración de NetBIOS (Talk 6) no empiezan a tener efecto de manera inmediata. Quedan pendientes hasta que se ejecuta el mandato **reload** o **restart**.

Add

Añade una nueva entrada de antememoria de nombres a la configuración permanente o estática del direccionador o añade una entrada de lista de nombres NetBIOS que se utiliza para limitar el acceso de estaciones remotas a DLSw locales. Sólo puede añadir entradas de antememoria de nombres sólo para vecinos de DLSw. El direccionador ignora las entradas que se añaden para tráfico ASRT.

Sintaxis:

add 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 indicador le solicita el 16 carácter en formato hexadecimal sólo si ha indicado a través de **set cache-parms** que los 16 caracteres son relevantes en un nombre NetBIOS.

Se pueden añadir varias entradas con diferentes direcciones IP para un solo nombre NetBIOS. Ello permite que se pueda acceder al nombre a través de varios vecinos de DLSw.

Nota: El nombre NetBIOS es sensible a mayúsculas y minúsculas y debe coincidir en mayúsculas y minúsculas con 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. Este cambio no empieza a tener efecto hasta que se reinicia 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. Este cambio no empieza a tener efecto hasta que se confirma desde el indicador `NetBIOS>` mediante el mandato **set name-list**. Este cambio se pierde cuando se reinicia el direccionador.

El calificador de nombres NetBIOS representa uno o más nombres NetBIOS a los que se puede acceder en la red puenteada localmente de este direccionador y a los que otros direccionadores deben poder acceder a través de DLSw.

El calificador de nombres NetBIOS puede contener los siguientes dos tipos de caracteres comodín:

? (signo de interrogación)
Indica que un carácter concreto del nombre NetBIOS real puede ser cualquier valor.

*** (asterisco)**
Al final de un calificador de nombres indica que el resto de caracteres de un nombre NetBIOS real puede ser cualquier valor.

Notas:

1. Si no aparece un asterisco al final de un calificador de nombres, el resto del calificador de nombres hasta un máximo de 16 caracteres se rellena con caracteres nulos (ceros hex).
2. El calificador de nombres NetBIOS es sensible a mayúsculas y minúsculas y debe coincidir en mayúsculas y minúsculas con 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 antememoria de nombres o entradas de listas de nombres NetBIOS.

Sintaxis:

de**lete**	cache-entry
	name-list

cache-entry

Desde el indicador de configuración, suprime las entradas de antememoria de nombres de la configuración permanente del direccionador. El direccionador le solicita un número de registro, que es el número de registro de la entrada que desea suprimir. Para ver una lista de números de entradas, entre el mandato **list cache all**.

Desde el indicador de supervisión, suprime las entradas de antememoria de nombres de la configuración estática o de la antememoria activa del direccionador. El direccionador le solicita un nombre de entrada de antememoria. Para ver una lista de entradas, entre **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 local de nombres del direccionador.

Desde el indicador de configuración, suprime una entrada de lista de nombres permanente. El direccionador le solicita un número de registro,

que es el número de la entrada que desea suprimir. Para ver una lista de números de entradas, entre el mandato **list name-list all**. Este cambio no empieza a tener efecto hasta que se reinicia el direccionador o se confirma el cambio desde el indicador de supervisión utilizando el mandato **set name-list**.

Desde el indicador de supervisión, suprime temporalmente una entrada de lista de nombres. El direccionador le solicita un número de registro, que es el número de la entrada que desea suprimir. Para ver una lista de números de entradas, entre el mandato **list name-list config**. Este cambio no empieza a tener efecto hasta que se confirma el cambio desde el indicador de supervisión mediante el mandato **set name-list**. El cambio se pierde si se reinicia 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

Inhabilita el filtro de tramas duplicadas, el uso de listas de nombres NetBIOS o la antememoria de rutas.

Sintaxis:

disable duplicate-filtering
name-list local
name-list remote
route-caching

duplicate-filtering

Inhabilita el filtro de tramas duplicadas para los puentes. No se puede inhabilitar el filtro de tramas duplicadas para el tráfico DLSw.

Ejemplo: `disable duplicate-filtering`

```
Duplicate frame filtering is          OFF
```

name-list local

Inhabilita la utilización de la lista local de nombres. Las entradas de la lista local de nombres no se enviarán a ningún asociado de DLSw.

Desde el indicador de configuración, inhabilita de manera permanente la utilización de la lista local de nombres. Este cambio no empieza a tener efecto hasta que se reinicia el direccionador o se confirma el cambio desde el indicador de supervisión utilizando el mandato **set name-list**.

Desde el indicador de supervisión, inhabilita temporalmente la utilización de la lista local de nombres. Este cambio no empieza a tener efecto hasta que se confirma el cambio desde el indicador de supervisión mediante el mandato **set name-list**. El cambio se pierde si se reinicia 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

Inhabilita la utilización de las listas remotas de nombres. No se utilizan las listas de nombres NetBIOS recibidas de asociados DLSw.

Desde el indicador de configuración, inhabilita de manera permanente la utilización de las listas remotas de nombres. Este cambio no empieza a tener efecto hasta que se reinicia el direccionador o se confirma el cambio desde el indicador de supervisión utilizando el mandato **set name-list**.

Desde el indicador de supervisión, inhabilita temporalmente la utilización de las listas remotas de nombres. Este cambio no empieza a tener efecto hasta que se confirma el cambio desde el indicador de supervisión mediante el mandato **set name-list**. El cambio se pierde si se reinicia 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

Inhabilita la antememoria de rutas para los puentes y DLSw. La antememoria de rutas es el proceso de convertir tramas de difusión en tramas direccionadas de manera específica (SRF) mediante las entradas de la antememoria de nombres NetBIOS.

Ejemplo: `disable route-caching`

```
Route caching is                    OFF
```

Enable

Habilita el filtro de tramas duplicadas, el uso de listas de nombres NetBIOS o la antememoria de rutas.

Sintaxis:

en**able**	duplicate-filtering name-list local name-list remote route-caching

duplicate-filtering

Habilita el filtro de tramas duplicadas para los puentes. El filtro de tramas duplicadas para DLSw siempre está habilitado. Puede habilitarlo e inhabilitarlo.

Ejemplo: `enable duplicate-filtering`

```
Duplicate frame filtering is           ON
```

name-list local

Habilita la utilización de la lista local de nombres. Las entradas de la lista local de nombres se enviarán a todos los asociados de DLSw.

Desde el indicador de configuración, habilita de manera permanente la utilización de la lista local de nombres. Este cambio no empieza a tener efecto hasta que se reinicia el direccionador o se confirma el cambio desde el indicador de supervisión utilizando el mandato **set name-list**.

Desde el indicador de supervisión, habilita temporalmente la utilización de la lista local de nombres. Este cambio no empieza a tener efecto hasta que se confirma el cambio desde el indicador de supervisión mediante el mandato **set name-list**. El cambio se pierde si se reinicia 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

Habilita la utilización de las listas remotas de nombres. Se utilizan todas las listas de nombres NetBIOS recibidas de asociados DLSw.

Desde el indicador de configuración, habilita de manera permanente la utilización de las listas remotas de nombres. Este cambio no empieza a tener efecto hasta que se reinicia el direccionador o se confirma el cambio desde el indicador de supervisión utilizando el mandato **set name-list**.

Desde el indicador de supervisión, habilita temporalmente la utilización de las listas remotas de nombres. Este cambio no empieza a tener efecto hasta que se confirma el cambio desde el indicador de supervisión mediante el mandato **set name-list**. El cambio se pierde si se reinicia 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

Habilita la antememoria de rutas para los puentes y DLSw. La antememoria de rutas es el proceso de convertir tramas de difusión en tramas direccionadas de manera específica (SRF) mediante la antememoria de nombres NetBIOS.

Ejemplo: `enable route-caching`

```
Route caching is                    ON
```

List (mandato de configuración)

Visualiza todas las entradas de antememoria o visualiza las entradas de antememoria por tipo de entrada. Visualiza información de configuración de filtros o información de configuración general. Visualiza entradas de listas de nombres NetBIOS locales.

Sintaxis:

list
- cache all
- cache entry-number
- cache name
- cache ip-address
- filters all
- filters bridge
- filters dlsw
- general
- name-list all

name-list *número-entrada*

cache all Visualiza todas las entradas permanentes de la antememoria de nombres del direccionador. No visualiza entradas estáticas o 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*
Visualiza una entrada de antememoria según su número de entrada. Entre **list cache all** para ver una lista de números de entrada.

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*
Visualiza una entrada de antememoria de un nombre NetBIOS específico. Puede utilizar los siguientes comodines para simplificar la búsqueda:

***** (asterisco) que representa cero o más apariciones de cualquier carácter. Por ejemplo, San* puede generar:

- San Francisco
- Santa Fe
- San Juan

? (signo de interrogación) que representa cualquier carácter.

$ (símbolo del dólar) sólo tiene efecto cuando el número de caracteres de nombres NetBIOS significativos no es 16 y cuando el argumento de búsqueda no empieza con un asterisco (*).

Puede utilizar tantos comodines como desee hasta el número máximo de caracteres de un nombre NetBIOS (15 o 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 un dirección IP específica.

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 Visualiza si el filtro por tipo de trama está activo o inactivo tanto para los puentes como para DLSw. Utilice los mandatos **set filters bridge** para activar o 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

Visualiza si el filtro por tipo de trama está activo o inactivo para los puentes. Utilice **set filters bridge** para activar o 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

Visualiza si el filtro por tipo de trama está activo o inactivo para DLSw. Utilice **set filters dlsw** para activar o 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 Visualiza la antememoria NetBIOS y la configuración de filtro actuales.

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

Visualiza todas las entradas de listas de nombres NetBIOS locales configuradas de manera permanente. No visualiza las entradas estáticas.

Ejemplo:

```
list name-list all
Entry  Name Qualifier    Type
-----  ----------------  ----------
  1    NY_SERV*          INDIVIDUAL
  2    NY_DOMAIN*             GROUP
```

name-list *número-entrada*

Visualiza una entrada concreta de listas de nombres NetBIOS locales configurada de manera permanente.

Ejemplo:

```
list name-list entry-number
Enter name list record number [1]? 1

Entry  Name Qualifier    Type
-----  ----------------  ----------
  1    NY_SERV*          INDIVIDUAL
```

List (mandato de supervisión)

Visualiza información diversa sobre tipos de entradas de antememoria, configuración de filtros, configuración general, listas de nombres NetBIOS o estadísticas sobre otros aspectos.

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

Visualiza todas las entradas activas de la antememoria de nombres del direccionador.

El número entre paréntesis angulares es el 16 carácter del nombre NetBIOS. Dicho carácter, que se puede entrar en formato hexadecimal si crea la entrada de antememoria, lo utilizan algunas aplicaciones NetBIOS para fines especiales.

Si el campo Name Type (tipo de 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

Visualiza todas las entradas de antememoria de nombres estáticas y permanentes. No muestra entradas dinámicas.

El número entre paréntesis angulares es el 16 carácter del nombre NetBIOS. Dicho carácter, que se puede entrar en formato hexadecimal si crea la entrada de antememoria, lo utilizan algunas aplicaciones NetBIOS para fines 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

Visualiza entradas de antememoria que existen para 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

Visualiza entradas de antememoria locales. Las entradas de antememoria locales son las que el direccionador averigua a través de la red de puente local.

En el caso de clientes NetBIOS el Local Path State (estado de la vía de acceso local) siempre es Unknown (desconocido) y los campos MAC address (dirección MAC) Y Routing information (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 El número de la entrada de antememoria.

NetBIOS Name
El nombre NetBIOS de la entrada.

Loc Path State
El estado de la vía de acceso local.

MAC Address
Si la entrada es un servidor, visualiza la dirección MAC del servidor.

Routing Information
Visualiza la información RIF estándar.

cache name *nombre*

Visualiza una entrada de antememoria de un nombre NetBIOS específico. Puede utilizar los siguientes comodines para simplificar la búsqueda:

***** (asterisco) que representa cero o más apariciones de cualquier carácter. Por ejemplo, San* puede generar:

- San Francisco
- Santa Fe
- San Juan

? (signo de interrogación) que representa cualquier carácter.

$ (símbolo del dólar) sólo tiene efecto cuando el número de caracteres de nombres NetBIOS significativos no es 16 y cuando el argumento de búsqueda no empieza con un asterisco (*).

Puede utilizar tantos comodines como desee hasta el número máximo de caracteres de un nombre NetBIOS (15 o 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

Visualiza las entradas de antememoria que el direccionador averigua en la WAN de 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 El número de la entrada de antememoria.

NetBIOS Name
El nombre NetBIOS de la entrada.

Rem Path State
El estado de la vía de acceso remota. Los estados posibles son:

Best Found
: El direccionador ha encontrado la mejor ruta hasta esta estación.

Unknown
: El direccionador no ha encontrado aún la mejor ruta hasta esta estación.

Group
: El direccionador no busca la mejor vía de acceso para nombres de grupo.

Search Limited
: El direccionador está llevando a cabo una búsqueda limitada de este nombre NetBIOS. Consulte el mandato **set cache-parms** si desea obtener más información sobre búsquedas reducidas.

Search All
El direccionador está llevando a cabo una búsqueda completa. Cuando finaliza 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, visualiza la dirección o direcciones IP asociadas con el DLSw vecino que puede acceder a la estación NetBIOS.

cache unknown
Visualiza entradas de antememoria en las que el tipo de nombre NetBIOS es desconocido. El direccionador entra todas las entradas dinámicas como Unknown (desconocidas) hasta que averigua el tipo de nombre. Cuando lo ha averiguado, las marca 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

Visualiza si el filtro por tipo de trama está activo o inactivo tanto para los puentes como para DLSw.

Utilice los mandato **set filters bridge** y **set filters dlsw** para activar o 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
Visualiza si el filtro por tipo de trama está activo o inactivo para los puentes. Utilice el mandato **set filters bridge** para activar o 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
Visualiza si el filtro por tipo de trama está activo o inactivo para DLSw. Utilice el mandato **set filters dlsw** para activar o 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 Visualiza la antememoria NetBIOS y la configuración de filtro actuales.

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

Visualiza todas las entradas de lista de nombres NetBIOS actualmente activas tanto locales como remotas. Si no se han confirmado las entradas de la lista de nombres local o la utilización de las listas de nombres locales está inhabilitada, las entradas de listas de nombres locales no aparecerán en la lista. Si la utilización de las listas de nombres remotas está inhabilitada, las entradas de lista de nombres remota no aparecerá 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

Visualiza todas las entradas de listas de nombres NetBIOS locales configuradas permanentemente y temporalmente.

El campo de origen puede tener uno de los siguientes valores:

PERMANENT
Entradas configuradas de manera permanente.

STATIC Entradas configuradas temporalmente.

El campo LastMod puede tener uno de los siguientes valores:

ADDED Se ha añadido la entrada de la lista local de nombres pero no se ha confirmado el cambio.

DELETED
Se ha suprimido la entrada de la lista local de nombres pero no se ha confirmado el cambio.

UNCHANGED
Se ha añadido la entrada de la lista local de nombres y se ha confirmado el cambio.

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

Visualiza todas las entradas de listas de nombres NetBIOS locales activas actualmente. Si las entradas de listas locales de nombres no se han confirmado o la utilización de listas locales de nombres está inhabilitada, las entradas de listas locales de nombres 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

Visualiza todas las entradas de listas remotas de nombres NetBIOS actualmente activas de un asociado de DLSw concreto. Si la utilización de listas remotas de nombres está inhabilitada, 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 de 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 de antememoria de nombres para los puentes.

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 de antememoria de nombres para 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

Visualiza recuentos de tramas para los puentes.

Ejemplo: `list statistics general bridge`

```
Frames received                    1339
Frames discarded                      0
Frames forwarded to bridge         1339
Frames forwarded to DLS            1339
```

statistics general dlsw

Visualiza recuentos de tramas para DLSw.

Ejemplo: `list statistics general dlsw`

```
Frames received                    1339
Frames discarded                      0
Frames forwarded to bridge         1339
```

Set

Establece los parámetros de antememoria de nombres, activa o desactiva el filtro por tipo de trama para los puentes o DLSw, ajusta los temporizadores de filtro de tramas duplicadas y los temporizadores de reintentos de tramas y establece los parámetros de listas de nombres NetBIOS. Visualiza también el indicador de filtro por nombre y por bytes NetBIOS.

Sintaxis:

set cache-parms
filters bridge
filters byte
filters dlsw
filters name
general
name-list

cache-parms

Establece parámetros de antememoria de nombres que se aplican a los puentes 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 considera 15 o 16 caracteres cuando consulta el nombre NetBIOS. Si entra 15, el direccionador ignora

el 16 carácter. Si selecciona 16, el direccionador incluye el 16 carácter cuando consulta las entradas de antememoria.

Por omisión es 15.

Best path aging timeout
La cantidad de tiempo que el direccionador considera la dirección y la ruta de una entrada de antememoria de nombres a la mejor vía de acceso a esta estación. Cuando este temporizador finaliza, el direccionador suprime la entrada de la antememoria de nombres e intenta descubrir una nueva vía de acceso óptima para el nombre NetBIOS.

Para determinar la mejor vía de acceso, el direccionador considera el tiempo de transmisión entre los nodos de todas las posibles rutas que los conectan, así como el tamaño más grande de trama. El direccionador considera que una vía de acceso no es adecuado si no puede dar cabida en ella a la trama NetBIOS más grande que se pueda transmitir en dicha vía.

Por omisión son 60 segundos. El rango de valores posibles es de 1,0 a 100000,0 seconds.

Reduced search timeout
Cuando el direccionador recibe una trama Name-Query, Status-Query o Datagram durante el tiempo de espera, lleva a cabo una búsqueda según la información actual de antememoria de nombres NetBIOS.

Si el direccionador recibe una trama duplicada después de que finalice el temporizador, presupone que la ruta anterior ya no es válida y amplía la búsqueda. El direccionador reenvía la trama duplicada tanto a los puentes como a DLS. DLS difunde el mensaje SSP correspondiente a todos los asociados DLS posibles.

Por omisión es 1,5 segundos. El rango de valores posibles es de 1,0 a 100,0 segundos.

Unreferenced entry timeout
El direccionador conserva un nombre que no está referenciado en su antememoria durante este tiempo antes de suprimirlo. Si la antememoria se llena, el direccionador elimina antes las entradas.

Por omisión son 5000 minutos. El valor está comprendido entre 1 y 100 000 minutos.

Max nbr local name cache entries
El número máximo de entradas averiguadas localmente que el direccionador guarda en la antememoria de nombres.

Por omisión es 500. El rango de valores posibles es de 100 a 30 000. Puede reducir este valor para ahorra memoria al direccionador. A fin de optimizar la utilización de memoria, la utilización del procesador y la cantidad de tráfico de difusión, establezca un número de entradas de antememoria de nombres locales que se acerque lo más posible al número total de estaciones NetBIOS (servidores y clientes) que están activos en la red de puente local de este direccionador.

Max nbr remote name cache entries

El número máximo de entradas averiguadas remotamente, de entradas de nombres de grupo y de entradas desconocidas que el direccionador guarda en la antememoria de nombres.

Por omisión es 100. El rango de valores posibles es de 100 a 30 000. Puede reducir este valor para ahorra memoria al direccionador. A fin de optimizar la utilización de memoria, la utilización del procesador y la cantidad de tráfico de difusión, establezca un número de entradas de antememoria de nombres remotas que sea igual al número de servidores NetBIOS remotos a los que deben acceder los clientes NetBIOS de la red de puente local de este direccionador, más aproximadamente un 25%.

filters bridge

Activa o desactiva el filtro por tipo de trama para los puentes.

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>`, visualiza el indicador de configuración de filtro NetBIOS (`NetBIOS Filter config>`). La configuración del filtro NetBIOS se describe en “Configuración y supervisión de filtro de NetBIOS” en la página 195.

Desde el indicador de supervisión `NetBIOS >`, visualiza el indicador de supervisión del filtro NetBIOS (`NetBIOS Filter>`). La supervisión del filtro NetBIOS se describe en “Supervisión de filtro de NetBIOS” en la página 206.

Este parámetro le permite acceder al filtro por bytes de NetBIOS.

Ejemplo: `set filters byte`

```
NetBIOS Filtering configuration
NetBIOS Filter config>
```

filters dlsw

Establece los filtros por tipo 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>`, visualiza el indicador de configuración de filtro NetBIOS (`NetBIOS Filter config>`). La configuración del filtro NetBIOS se describe en “Configuración y supervisión de filtro de NetBIOS” en la página 195.

Desde el indicador de supervisión `NetBIOS >`, visualiza el indicador de supervisión del filtro NetBIOS (`NetBIOS Filter>`). La supervisión del filtro NetBIOS se describe en “Supervisión de filtro de NetBIOS” en la página 206.

Este parámetro le permite acceder al filtro por nombre de NetBIOS.

Ejemplo: `set filters name`

```
NetBIOS Filtering configuration
NetBIOS Filter config>
```

general Establece el tiempo de espera de las tramas duplicadas, el tiempo de espera de la detección de tramas y el recuento y el tiempo de espera de los reintentos de las tramas de mandato. Consulte “Filtro de tramas duplicadas” en la página 151 si desea obtener más información sobre el funcionamiento de 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 habilitado, el software también le solicita:

```
Command frame retry count [5]?
Command frame retry timeout value in seconds [0.5]?
```

Duplicate frame filter timeout
Se aplica sólo al tráfico que circula por puente si el filtro de tramas duplicadas está habilitado. Durante este tiempo de espera, el direccionador filtra todas las tramas duplicadas que recibe.

El rango de valores posibles es de 0,0 a 100,0 segundos. Cero inhabilita la comprobación de tramas duplicadas. Por omisión es 1,5 segundos.

Duplicate frame-detect timeout
Se aplica tanto al tráfico que circula por puente como al tráfico DLSw. Es la cantidad de tiempo durante la que el direccionador guarda entradas en su base de datos de filtro de tramas duplicadas. Cuando el temporizador finaliza, el direccionador crea nuevas entradas para las nuevas tramas que recibe.

El rango de valores posibles es de 0,0 a 100,0 segundos. Por omisión son 5 segundos.

Command frame retry count
Se aplica sólo a tráfico DLSw.

El número de tramas UI NetBIOS duplicadas que el direccionador DLSw de destino envía a su LAN conectada localmente. Dichas tramas se envían a intervalos especificados por el tiempo de espera de reintentos de tramas de mandato.

El rango de valores posibles es de 0 a 10. Por omisión son 5.

Command frame retry timeout
Se aplica sólo a tráfico DLSw. Se trata del intervalo al que un direccionador DLSw vecino reintenta el envío de tramas UI NetBIOS duplicadas a su red de puente local.

El rango de valores posibles es de 0,0 a 10,0 segundos. Por omisión son 0.5 segundos.

name-list Establece los parámetros relacionados con la lista local de nombres NetBIOS. Actualmente el único parámetro relacionado de lista local de nombres NetBIOS es la exclusividad de la lista local de nombres NetBIOS.

Desde el indicador de configuración, establece de manera permanente los parámetros de la lista local de nombres NetBIOS. Este cambio no empieza a tener efecto hasta que se reinicia el direccionador o se confirma el cambio desde el indicador de supervisión utilizando el mandato **set name-list**.

Desde el indicador de supervisión, este mandato establece temporalmente los parámetros de la lista local de nombres NetBIOS. El mandato confirma también todos los cambios en las listas de nombres NetBIOS que se hayan efectuado desde los indicadores de configuración o de supervisión.

Test (sólo supervisión)

Permite probar nombre NetBIOS reales contra la antememoria NetBIOS o la lista de nombres NetBIOS actuales.

Sintaxis:

test cache
name-list

test cache

Visualiza una lista de los asociados de DLSw actuales a los que se reenviará una trama DLSw con un nombre de destino NetBIOS determinado y el modo en que la trama se reenviará.

Ejemplo (no corresponde a una entrada de 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 (corresponde a una entrada de antememoria de 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

Visualiza una lista de entradas de lista de nombres (local o remota) que coincide con el nombre NetBIOS determinado.

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
```

Soporte de reconfiguración dinámica de NetBIOS

En este apartado se describe el modo en que la reconfiguración dinámica (DR) afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

NetBIOS no da soporte al mandato **delete interface** de CONFIG (Talk 6).

Mandato activate interface de GWCON (Talk 5)

El mandato **activate interface** de GWCON (Talk 5) no es aplicable a NetBIOS. No existen parámetros de NetBIOS que sean específicos de interfaz.

Mandato reset interface de GWCON (Talk 5)

El mandato **reset interface** de GWCON (Talk 5) no es aplicable a NetBIOS. No existen parámetros de NetBIOS que sean específicos de interfaz.

Mandatos de cambio temporal de GWCON (Talk 5)

NetBIOS da soporte a los mandatos de GWCON que cambian de forma temporal el estado operativo del dispositivo indicados más abajo. Los cambios se pierden cada vez que se vuelve a cargar o iniciar el dispositivo o que se ejecuta un mandato reconfigurable dinámicamente.

Los mandatos relacionados a continuación no afectan a las funciones de NetBIOS ya activas en el momento de emitirse el mandato, salvo que se indique lo contrario. Los cambios sí que se aplican al tráfico y a todas las operaciones de NetBIOS posteriores.

Mandatos
GWCON, protocol asrt, netbios, add cache-entry
GWCON, protocol asrt, netbios, add name-list
GWCON, protocol asrt, netbios, delete cache-entry
GWCON, protocol asrt, netbios, delete name-list
GWCON, protocol asrt, netbios, disable duplicate-filtering
GWCON, protocol asrt, netbios, disable name-list local
GWCON, protocol asrt, netbios, disable name-list remote
GWCON, protocol asrt, netbios, disable route-caching
GWCON, protocol asrt, netbios, enable duplicate-filtering
GWCON, protocol asrt, netbios, enable name-list local
GWCON, protocol asrt, netbios, enable name-list remote
GWCON, protocol asrt, netbios, enable route-caching
GWCON, protocol asrt, netbios, set cache-parms
GWCON, protocol asrt, netbios, set filters bridge
GWCON, protocol asrt, netbios, set filters dlsw
GWCON, protocol asrt, netbios, set general
GWCON, protocol asrt, netbios, set name-list

Mandatos no reconfigurables dinámicamente

Todos los parámetros de configuración de NetBIOS pueden cambiarse dinámicamente.

Configuración y supervisión de filtro de NetBIOS

Este capítulo describe los mandatos de configuración de filtro de NetBIOS. Estos mandatos permiten configurar el filtrado de NetBIOS como una característica añadida al establecimiento de puentes de ARST. Puede accederse a los mandatos de configuración desde el indicador de mandatos `NetBIOS config>`.

Incluye las secciones siguientes:

- "Acceso a los entornos de configuración de ASRT y DLSW"
- "Mandatos de configuración de filtro de NetBIOS"

Acceso a los entornos de configuración de ASRT y DLSW

Para visualizar el indicador de mandatos de filtro de NetBIOS desde el entorno ASRT, entre los mandatos tal como se muestra en el ejemplo siguiente:

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

ASRT config> netbios
NetBIOS Support User Configuration

NetBIOS config> set filters name or byte
NetBIOS filtering configuration

NetBIOS filter config>
```

Para visualizar el indicador de mandatos `NetBIOS config>` desde el entorno de configuración de DLSw:

```
Config> protocol dls
DLSw protocol user configuration

DLSw config> netbios
NetBIOS Support User Configuration

NetBIOS config> set filters name or byte
NetBIOS filtering configuration

NetBIOS filter config>
```

La Tabla 13 muestra los mandatos de configuración de filtro de NetBIOS.

Mandatos de configuración de filtro de NetBIOS

Nota: Los mandatos de configuración de filtro de NetBIOS no surten efecto inmediatamente. Antes, debe rearrancar o volver a cargar el dispositivo.

Tabla 13 (Página 1 de 2). Mandatos de configuración de filtro de NetBIOS

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado "Cómo obtener ayuda" en la página xxx.
Create	Crea listas de filtro por bytes y de filtro por nombre de sistema principal para el filtrado de NetBIOS.

Tabla 13 (Página 2 de 2). Mandatos de configuración de filtro de NetBIOS

Mandato	Función
Delete	Suprime las listas de filtro por bytes y de filtro por nombre de sistema principal para el filtrado de NetBIOS.
Disable	Inhabilita el filtrado de NetBIOS en el direccionador de establecimiento de puente.
Enable	Habilita el filtrado de NetBIOS en el direccionador de establecimiento de puente.
Filter-on	Asigna un filtro creado a un puerto específico. Este filtro puede aplicarse a todos los paquetes de NetBIOS de entrada ***o*** de salida en el puerto especificado.
List	Visualiza toda la información relativa a los filtros que se han creado.
Update	Añade o suprime información información en una lista de filtro por bytes o de filtro por nombre 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 xxxi.

Respuesta a los mandatos de configuración de NetBIOS

Los mandatos de configuración de NetBIOS (Talk 6) no surten efecto inmediatamente. Permanecen pendientes hasta que se emitan los mandatos **reload** o **restart**.

Create

Utilice el mandato **create** para crear una lista de filtro por bytes o una lista de filtro por nombre de sistema principal.

Sintaxis:

create byte-filter-list *lista-filtro*
name-filter-list *lista-filtro*

byte-filter-list *lista-filtro*

Crea un nombre de lista de filtro por bytes para el filtrado de NetBIOS. Pueden utilizarse hasta 16 caracteres para identificar la lista que se crea. *Lista-filtro* debe ser un nombre exclusivo que no se haya utilizado previamente con el mandato **create byte-filter-list** o **create name-filter-list**.

Ejemplo: `create byte-filter-list newyork`

name-filter-list *lista-filtro*

Crea un nombre de lista de filtro por nombre de sistema principal para el filtrado de NetBIOS. Pueden utilizarse hasta 16 caracteres para identificar la lista de filtro por nombre que se crea. *Lista-filtro* debe ser un nombre exclusivo que no se haya utilizado previamente con el mandato **create byte-filter-list** o **create name-filter-list**.

Ejemplo: `create name-filter-list atlanta`

Delete

Utilice el mandato **delete** para suprimir listas de filtro por bytes, listas de filtro por nombre de sistema principal y filtros creados con el mandato **filter-on input** o **filter-on output**. El mandato elimina toda la información asociada con las listas de filtro por bytes y por nombre de sistema principal. También libera la serie definida por el usuario como nombre para una nueva lista de filtro.

Sintaxis:

d**elete**	byte-filter-list *lista-filtro* name-filter-list *lista-filtro* filter input *núm-puerto* filter output *núm-puerto*

byte-filter-list *lista-filtro*

Suprime una lista de filtro por bytes creada para el filtrado de NetBIOS. *Lista-filtro* es la serie definida por el usuario que se utiliza para identificar la lista de filtro por bytes que se suprime.

Ejemplo: `delete byte-filter-list newyork`

name-filter-list *lista-filtro*

Suprime una lista de filtro por nombre de sistema principal creada para el filtrado de NetBIOS. *Lista-filtro* es la serie definida por el usuario que se utiliza para identificar la lista de filtro por nombre que se suprime.

Ejemplo: `delete name-filter-list atlanta`

filter input *núm-puerto*

Suprime un filtro que se ha creado utilizando el mandato **filter-on input**. El mandato elimina toda la información asociada con el filtro y rellena cualquier agujero resultante en los números de filtro.

Ejemplo: `delete filter input 2`

filter output *núm-puerto*

Suprime un filtro que se ha creado utilizando el mandato **filter-on output**. El mandato elimina toda la información asociada con el filtro y rellena cualquier agujero resultante en los números de filtro.

Ejemplo: `delete filter output 2`

Disable

Utilice el mandato **disable** para inhabilitar globalmente el filtrado NetBIOS de nombres y de bytes en el direccionador.

Sintaxis:

d**isable**	netbios-filtering

Ejemplo: `disable netbios-filtering`

Enable

Utilice el mandato **enable** para habilitar globalmente el filtrado NetBIOS de nombres y de bytes en el direccionador.

Sintaxis:

enable netbios-filtering

Ejemplo: `enable netbios-filtering`

Filter-on

Este mandato asigna una o más listas de filtro previamente configuradas a la entrada o la salida de un puerto específico.

Sintaxis:

filter-on input *núm-puerto lista-filtro <operador lista-filtro. . . >*
output *núm-puerto lista-filtro <operador lista-filtro. . . >*

input *núm-puerto lista-filtro <operador lista-filtro . . . >*

Este mandato asigna una o más listas de filtro a paquetes de entrada en un puerto determinado. El filtro resultante se aplica a todos los paquetes de entrada de 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** si desea ver una lista de números de puerto. Lista-filtro es una serie que se ha entrado previamente con el mandato **create**. Para añadir a este puerto listas de filtro adicionales, debe entrarse AND u OR con mayúsculas, seguidas del nombre de la lista de filtro.

Nota: Puede utilizarse más de un operador para crear un filtro complejo. Si se entran múltiples operadores, deben entrarse todos al mismo tiempo en la misma línea de mandatos.

El filtro que se ha creado con este mandato se aplica a todos los paquetes NetBIOS de entrada en el puerto especificado. Cada lista de filtro en la línea de mandatos se evalúa de izquierda a derecha junto con cualquier operador que esté presente. Una evaluación Inclusiva de una lista de filtro equivale a una condición de Verdadero, mientras que una evaluación Exclusiva equivale a una condición de Falso. Si el resultado de la evaluación de las listas de filtro es Verdadero, el paquete pasa por el puente. En caso contrario, el paquete es filtrado (descartado).

Si el paquete no es ninguno de los tipos que soporta el filtrado de NetBIOS, entonces todas las listas de filtro por nombre de sistema principal para este filtro se señalan como “Inclusivas” (Verdaderas). Si ya existe un filtro de entrada para el número de puerto que se especifica, aparece un mensaje de error.

Ejemplo: `filter-on input 2 newyork AND boston`

output *núm-puerto lista-filtro <operador lista-filtro . . . >*

Este mandato asigna uno o más filtros a paquetes de salida en un puerto. Este filtro se aplica a todas las salidas de paquetes de NetBIOS en ese puerto.

Núm-puerto es un número de puerto de puente configurado en el direccionador. El número de puerto identifica este filtro. Entre **list** si desea ver una lista de números de puerto. Lista-filtro es una serie que se ha entrado previamente con el mandato create. Los operadores opcionales tales como AND u OR deben entrarse utilizando las letras mayúsculas. Si se encuentra presente un operador, debe ir seguido de un nombre de lista de filtro. El número de puerto se utiliza para identificar este filtro.

Nota: Pueden utilizarse diversos operadores. Ello crea un filtro complejo. Si se encuentran presentes uno o más operadores, deben entrarse todos al mismo tiempo en la misma línea de mandatos.

El filtro que se ha creado con este mandato se aplica a todos los paquetes NetBIOS de salida en el número de puerto especificado. Cada lista de filtro en la línea de mandatos se evalúa de izquierda a derecha junto con cualquier operador que esté presente. Una evaluación Inclusiva de una lista de filtro equivale a una condición de Verdadero, mientras que una evaluación Exclusiva equivale a una condición de Falso. Si el resultado de la evaluación de las listas de filtro es Verdadero, el paquete pasa por el puente. En caso contrario, el paquete es filtrado (descartado).

Si el paquete no es ninguno de los tipos que soporta el filtrado de NetBIOS, entonces todas las listas de filtro por nombre de sistema principal para este filtro se señalan como “Inclusivas” (Verdaderas). Si ya existe un filtro de salida para el número de puerto que se especifica, aparece un mensaje de error.

Ejemplo: `filter-on output 2 newyork OR boston`

List

Utilice el mandato de filtro de NetBIOS **list** para visualizar toda la información relativa a los filtros que se han creado.

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
```

NetBIOS Filtering:
Visualiza si el filtrado de NetBIOS está habilitado o inhabilitado.

NetBIOS Filter Lists

Visualiza el nombre definido por el usuario (handle) las listas de filtro configuradas. En la columna Type, “Name” indica que se trata de una lista de filtro por nombre de sistema principal y “Byte” que se trata de una lista de filtro por bytes.

NetBIOS Filters

Visualiza el número de puerto asignado y la dirección (entrada o salida) de cada filtro. Filter List Handles visualiza los nombres de las listas de filtro que forman el filtro.

Update

Utilice el mandato **update** para añadir o suprimir información en las listas de filtro por nombre de sistema principal o por bytes. La lista de filtro es una serie que se ha entrado previamente mediante el indicador de mandato de crear lista de filtro por bytes (o por nombre). Este mandato remite al usuario al indicador de mandatos `NetBIOS Byte (or Name) filter-list Config>`, que permite ejecutar tareas de actualización en la lista de filtro que se especifique. En este indicador de mandatos el usuario puede añadir, suprimir, enumerar o mover elementos de filtro de listas de filtro por bytes y por nombre de sistema principal. En este indicador también puede establecerse el valor por omisión de cada lista de filtro a Inclusiva (Inclusive) o Exclusiva (Exclusive).

La utilización del submandato add crea un elemento de filtro dentro de la lista de filtro. Al primer elemento de filtro que se crea se le asigna el número 1, al siguiente el número 2, etcétera. Después de entrar satisfactoriamente un submandato add, el direccionador muestra el número del elemento de filtro que se acaba de añadir.

Nota: Añadir más elementos de filtro a las listas de filtro aumenta el tiempo de proceso (debido al tiempo empleado en evaluar cada elemento de filtro de la lista) y puede afectar el rendimiento si hay gran volumen de tráfico de NetBIOS.

El orden en que se especifican los elementos de filtro para una lista de filtro determinada es importante, puesto que determina el modo en que se aplican los elementos de filtro a un paquete. La primera coincidencia que se produzca hace parar la aplicación de elementos de filtro y la lista de filtro se evalúa entonces como Inclusiva o Exclusiva (dependiendo de la designación como Inclusivo o Exclusivo del elemento de filtro coincidente). Si no se produce ninguna coincidencia con los elementos de filtro de una lista de filtro, entonces se devuelve la condición por omisión (Inclusiva o Exclusiva) de la lista de filtro.

El submandato delete especifica el número de un elemento de filtro que ha de suprimirse de la lista de filtro. En caso de efectuar el submandato delete, se reordena la lista con el fin de evitar los agujeros creados. 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 pasará a ser el 3.

El submandato default permite cambiar el valor por omisión de la lista de filtro a Inclusiva o Exclusiva. Si una lista de filtro es evaluada como inclusiva, entonces el paquete pasa por el puente. En caso contrario, el paquete es filtrado.

El submandato move renumera elementos de filtro dentro de una lista de filtro. El primer argumento del submandato move es el número de la lista de filtro que debe

moverse. El segundo argumento del submandato move es el número de la lista de filtro detrás de la que deberá trasladarse la primera lista de filtro.

Sintaxis:

update byte-filter-list . . .
name-filter-list . . .

byte-filter-list *lista-filtro*

Actualiza información perteneciente a una lista de filtro por bytes. El parámetro lista-filtro es una serie que se ha entrado previamente mediante el mandato **create byte-filter-list**. Este mandato remite al usuario al siguiente nivel de mandatos `NetBIOS BYTE filter-list Config>` (véase el ejemplo). En este nivel el usuario puede ejecutar tareas de actualización para la lista de filtro especificada.

Ejemplo: **`update byte-filter-list newyork`**

```
NetBIOS Byte newyork Config>
```

En este nivel pueden ejecutarse diversos mandatos. El apartado "**Update Byte-Filter-List** (opciones del mandato)" contiene una relación de los mandatos disponibles.

name-filter-list *lista-filtro*

Actualiza información perteneciente a una lista de filtro por nombre. Este mandato es idéntico al mandato byte-filter-list, excepto que, en lugar de una lista de filtro por bytes, especifica una lista de filtro por nombre. El parámetro de lista de filtro es una serie que se ha entrado previamente utilizando el mandato create en el indicador de lista de filtro por nombre name-filter-list. Este mandato remite al usuario al siguiente nivel de mandatos `NetBIOS Name filter-list Config>` (véase el ejemplo). En este nivel el usuario puede ejecutar tareas de actualización para la lista de filtro especificada.

Ejemplo: **`update name-filter-list accounting`**

```
NetBIOS Name accounting Config>
```

En este nivel pueden ejecutarse diversos mandatos. El apartado "**Update Name-Filter-List** (opciones del mandato)" contiene una relación de los mandatos disponibles.

Update Byte-Filter-List (opciones del mandato)

Esta sección enumera las opciones de mandatos disponibles para el mandato **update byte-filter-list**:

add inclusive *desplazamiento-bytes patrón-hexadecimal* <*máscara hexadecimal*>

Añade un elemento de filtro a la lista de filtro por bytes. Si el elemento de filtro por bytes que se añade coincide con un paquete de NetBIOS, la lista de filtro a la que pertenece se evaluará como Inclusiva (Verdadera).

- Desplazamiento-bytes especifica el número de bytes (en notación decimal) de desplazamiento que aparecen al principio en el paquete que se filtra. Esto empieza en la cabecera NetBIOS del paquete.
- Patrón-hexadecimal es un número hexadecimal que se utiliza para compararlo con los bytes de la cabecera de NetBIOS, empezando a partir del desplazamiento. Las reglas de sintaxis para el patrón

hexadecimal no incluyen ningún 0x delante, tienen un máximo de 32 números y un número par de dígitos hexadecimales.

- La máscara hexadecimal, si se encuentra presente, debe tener la misma longitud que el patrón hexadecimal y se une por medio del operador AND lógico a los bytes de desplazamiento del comienzo del paquete antes de que el resultado se compare con el patrón hexadecimal para comprobar su equivalencia. Si se omite el argumento de la máscara hexadecimal, se considera que consta de unos (1) binarios.

Si los bytes de desplazamiento y el patrón de un elemento de filtro por bytes representan bytes que no existen en un paquete de NetBIOS (esto es, si el paquete es más corto de lo que se pretendía al establecer una lista de filtro por bytes), entonces el elemento de filtro no se aplicará al paquete y el paquete no se filtrará. Si se utiliza una serie de elementos de filtro por bytes para establecer una sola lista de filtro de NetBIOS, entonces un paquete no se comprobará para filtrado si cualquiera de los elementos de filtro por bytes en la lista de filtro de NetBIOS representa bytes que no existen en el paquete de NetBIOS.

Ejemplo: `add inclusive`

```
Byte Offset  [0] ?
Hex Pattern  [] ?
Hex Mask (<CR> for no mask)  [] ?
```

add exclusive *desplazamiento-bytes patrón-hexadecimal <máscara hexadecimal>*

Añade un elemento de filtro a la lista de filtro por bytes. Este mandato es idéntico al mandato add inclusive, excepto que si el resultado de la comparación entre el elemento de filtro y un paquete de NetBIOS da una coincidencia como resultado, entonces la lista de filtro se evalúa como Exclusiva (Falsa). Puede especificarse que los paquetes de difusión por datagrama sean eliminados utilizando este mandato con un desplazamiento de bytes de 4 y un patrón de bytes de 09.

- Desplazamiento-bytes especifica el número de bytes (en notación decimal) de desplazamiento que aparecen al principio en el paquete que se filtra. Esto empieza en la cabecera NetBIOS del paquete.
- Patrón-hexadecimal es un número hexadecimal que se compara con los bytes de la cabecera de NetBIOS, empezando a partir del desplazamiento. Las reglas de sintaxis para el patrón hexadecimal no incluyen ningún 0x delante, tienen un máximo de 32 números y un número par de dígitos hexadecimales.
- La máscara hexadecimal, si se encuentra presente, debe tener la misma longitud que el patrón hexadecimal y se une por medio del operador AND lógico a los bytes de desplazamiento del comienzo del paquete antes de que el resultado se compare con el patrón hexadecimal para comprobar su equivalencia. Si se omite el argumento de la máscara hexadecimal, se considera que consta de unos (1) binarios.

Si los bytes de desplazamiento y el patrón de un elemento de filtro por bytes representan bytes que no existen en un paquete de NetBIOS (esto es, si el paquete es más corto de lo que se pretendía al establecer una lista de filtro por bytes), entonces el elemento de filtro no se aplicará al paquete y el paquete no se filtrará. Si se utiliza una serie de elementos de filtro por bytes para establecer una sola lista de filtro de

NetBIOS, entonces un paquete no se comprobará para filtrado si cualquiera de los elementos de filtro por bytes en la lista de filtro de NetBIOS representa bytes que no existen en el paquete de 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 filtro a “inclusiva (inclusive).” Este mandato indica que si no hay ningún elemento de filtro de la lista de filtro que coincida con el contenido del paquete que se está evaluando para filtrado, la lista de filtro se evaluará como Inclusiva. Éste es el valor por omisión.

default exclude
Cambia el valor por omisión de la lista de filtro a “exclusiva (exclusive).” Este mandato indica que si no hay ningún elemento de filtro de la lista de filtro que coincida con el contenido del paquete que se está evaluando para filtrado, la lista de filtro se evaluará como Exclusiva.

delete *elemento-filtro*
Suprime un elemento de filtro de la lista de filtro.

Elemento-filtro es un número decimal que se creó previamente mediante el mandato add.

list Visualiza información relacionada con elementos de filtro de la lista de filtro 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*
Reordena los elementos de filtro dentro de la lista de filtro. El elemento de filtro cuyo número está especificado por elemento-filtro1 se desplaza y se le asigna un nuevo número justo detrás de elemento-filtro2.

exit Sale al nivel anterior de indicador de mandatos.

Update Name-Filter-List (opciones del mandato)

La sección siguiente enumera las opciones de mandatos disponibles para el mandato update name-filter-list:

add inclusive *nombre-sistema-principal ASCII <ÚLTIMO-número-hexadecimal>*
Añade un elemento de filtro a la lista de filtro por nombre de sistema principal. Con este mandato, los campos del nombre de sistema principal de los paquetes NetBIOS se comparan con el nombre de sistema principal que se da en este mandato. La lista siguiente muestra cómo se hacen estas comparaciones :

- ADD_GROUP_NAME_QUERY: Se examina el campo de nombres NetBIOS de origen
- ADD_NAME_QUERY: Se examina el campo de nombres NetBIOS de origen
- DATAGRAM: Se examina el campo de nombres NetBIOS de destino

- NAME_QUERY: Se examina el campo de nombres NetBIOS de destino

Si se produce una coincidencia (teniendo en cuenta designaciones comodín en este mandato), la lista de filtro será considerada Inclusiva. Si no, el siguiente elemento de filtro de la lista de filtro del filtro (si hay alguno) se aplica al paquete. Si el paquete no es ninguno de los cuatro tipos que soporta el filtrado de nombres de NetBIOS el paquete pasa por el puente.

- Nombre-sistema-principal es una serie ASCII de 16 caracteres como máximo de longitud. Puede utilizarse un interrogante (?) en el nombre de sistema principal para indicar un comodín de un solo carácter. Puede utilizarse un asterisco (*) como carácter final del nombre de sistema principal para indicar un comodín para el resto del nombre. Si el nombre de sistema principal contiene menos de 15 caracteres, se rellena hasta el carácter número 15 con espacios ASCII. El nombre de sistema principal puede contener cualquier carácter excepto los siguientes:

  . / \ [ ] : | < > + = ; , <espacio>

  Nota: Nombre-sistema-principal es sensible a mayúsculas y minúsculas

- Puede usarse ÚLTIMO-número-hexadecimal si el nombre de sistema principal contiene menos de 16 caracteres. Es un número hexadecimal (sin 0x al comienzo) que indica el valor que se utilizará para el último carácter. Si no se especifica el ÚLTIMO argumento en un nombre de sistema principal de menos de 16 caracteres, entonces se proporciona un carácter comodín “?” para el carácter número 16.

add inclusive HEX *serie-hex*

Añade un elemento de filtro a la lista de filtro por nombre de sistema principal. Este mandato es funcionalmente el mismo que el mandato add inclusive ASCII. Sin embargo, la representación del nombre de sistema principal es diferente. Este mandato proporciona el nombre de sistema principal como una serie de números hexadecimales (sin 0x delante).

- Serie-hex debe consistir en un número par de números hexadecimales. Si no se proporciona un número completo con los 32 caracteres, se acaban de rellenar los números en las posiciones 29 y 30 con espacios en blanco ASCII y se proporciona un comodín para los números en posición 31 y 32 (byte número 16). Puede especificarse un comodín para un solo byte con **??**.

add exclusive ASCII *nombre-sistema-principal <ÚLTIMO-número-hexadecimal>*

Añade un elemento de filtro a la lista de filtro por nombre de sistema principal. Este mandato es idéntico al mandato add inclusive ASCII, excepto en que los paquetes que coinciden con este elemento de filtro producen el resultado Exclusive para la lista de filtro.

- Nombre-sistema-principal es una serie ASCII de 16 caracteres como máximo de longitud. Puede utilizarse un interrogante (?) en el nombre de sistema principal para indicar un comodín de un solo carácter. Puede utilizarse un asterisco (*) como carácter final del nombre de sistema principal para indicar un comodín para el resto del nombre. Si el nombre de sistema principal contiene menos de 15 caracteres, se rellena hasta el carácter número 15 con espacios ASCII. El nombre de sistema principal puede contener cualquier carácter excepto los siguientes:

  . / \ [ ] : | < > + = ; , <espacio>

- Puede usarse ÚLTIMO-número-hexadecimal si el nombre de sistema principal contiene menos de 16 caracteres. Es un número hexadecimal (sin 0x al comienzo) que indica el valor que se utilizará para el último carácter. Si no se especifica el ÚLTIMO argumento en un nombre de sistema principal de menos de 16 caracteres, entonces se proporciona un carácter comodín **?** para el carácter número 16.

add exclusive HEX *serie-hex*

Añade un elemento de filtro a la lista de filtro por nombre. Este mandato es funcionalmente el mismo que el mandato add inclusive hex, excepto en que los paquetes que coinciden con este elemento de filtro producen el resultado Exclusive para la lista de filtro.

- Serie-hex debe consistir en un número par de números hexadecimales. Si no se proporciona un número hexadecimal completo de 32 caracteres, se acaban de rellenar los números en las posiciones 29 y 30 con espacios en blanco ASCII y se proporciona un comodín para los números en posición 31 y 32 (byte número 16). Puede especificarse un comodín para un solo byte con **??**.

default include

Cambia el valor por omisión de la lista de filtro a “inclusiva (inclusive).” Este mandato indica que si no hay elementos de filtro de la lista de filtro que coincidan con el contenido del paquete que se está evaluando para filtrado, la evaluación de la lista de filtro dará como resultado Inclusiva. Éste es el valor por omisión.

default exclude

Cambia el valor por omisión de la lista de filtro a “exclusiva (exclusive).” Este mandato indica que si no hay ningún elemento de filtro de la lista de filtro que coincida con el contenido del paquete que se está evaluando para filtrado, la evaluación de la lista de filtro dará como resultado Exclusiva.

delete *elemento-filtro*

Suprime un elemento de filtro de la lista de filtro.

- Elemento-filtro es un número decimal que se creó previamente mediante el mandato add.

list

Visualiza información relacionada con elementos de filtro de la lista de filtro 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*

Reordena los elementos de filtro dentro de la lista de filtro. El elemento de filtro cuyo número está especificado por elemento-filtro1 se desplaza y se le asigna un nuevo número justo detrás de elemento-filtro2.

exit

Sale al nivel anterior de indicador de mandatos.

Supervisión de filtro de NetBIOS

Esta sección describe los mandatos de supervisión de filtro de NetBIOS. Estos mandatos permiten al usuario supervisar y visualizar la información de filtro de NetBIOS como característica añadida al establecimiento de puentes ASRT. Los mandatos de supervisión se entran en el indicador de mandatos de supervisión `NetBIOS >`.

Los cambios que se hagan en el indicador de mandatos de supervisión `NetBIOS>` afectan tanto al establecimiento del puente como al DLSw.

Acceso a los entornos de supervisión de filtro de NEtBIOS ASRT y DLSw

Para visualizar el indicador de mandatos de supervisión `NetBIOS>` desde el entorno de supervisión de ASRT, entre el mandato **netbios** en el indicador ASRT>:

```
+ protocol asrt

ASRT> netbios
NetBIOS Support User monitoring

NetBIOS monitoring> set filters name or byte

NetBIOS filter>
```

Para visualizar el indicador de mandatos de supervisión `NetBIOS>` desde el entorno de supervisión de DLSw:

```
+ protocol dls
DLSw> netbios
NetBIOS Support User monitoring

NetBIOS Console> set filters name or byte
NetBIOS filtering

NetBIOS filter>
```

Mandatos de supervisión de filtro de NetBIOS

La Tabla 14 enumera los mandatos de filtro de NetBIOS.

Tabla 14. Resumen de los mandatos de supervisión de filtro de NetBIOS

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
List	Visualiza toda la información relativa a los filtros que se han creado.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

List

Utilice el mandato de filtro de NetBIOS **list** para visualizar toda la información relativa a los filtros que se han creado.

Sintaxis:

list byte-filter-lists
filters

name-filter-lists

byte-filter-lists

Visualiza información relacionada con elementos de filtro de la lista de filtro por 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 del elemento de filtro. Los elementos de filtro se evalúan en orden numérico al determinar el estado Inclusivo/Exclusivo de la lista de filtro.

Inc/Ex Especifica el estado por omisión del elemento de filtro.

Byte-offset

Especifica el número de bytes (en notación decimal) de desplazamiento al principio del paquete que se filtra. Esto empieza en la cabecera NetBIOS del paquete.

Pattern El número hexadecimal que se utiliza para comparación con los bytes de comienzo del desplazamiento de bytes de la cabecera de NetBIOS. Las reglas de sintaxis para el patrón hexadecimal no incluyen ningún 0x delante, tienen un máximo de 32 números y un número par de dígitos hexadecimales.

Mask Si se encuentra presente, debe tener la misma longitud que el patrón hexadecimal y se une por medio del operador AND lógico a los bytes de desplazamiento del comienzo del paquete antes de que el resultado se compare con el patrón hexadecimal para comprobar su equivalencia. Si se omite el argumento de la máscara hexadecimal, se considera que consta de unos (1) binarios.

filters Visualiza 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

Visualiza información relacionada con elementos de filtro de la lista de filtro por nombre 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 del elemento de filtro. Los elementos de filtro se evalúan en orden numérico al determinar el estado Inclusivo/Exclusivo de la lista de filtro.

Inc/Ex Especifica el estado por omisión del elemento de filtro.

Type “ASCII” indica un elemento de filtro por nombre de sistema principal añadido como caracteres ASCII. “Hex” indica un elemento de filtro por nombre de sistema principal añadido como números hexadecimales.

Host-name

Serie ASCII de hasta 16 caracteres de longitud. Puede utilizarse un interrogante (?) en el nombre del sistema principal para indicar un comodín de un solo carácter. Puede utilizarse un asterisco (*) como carácter final del nombre de sistema principal para indicar un comodín para el 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 de sistema principal puede contener cualquier carácter excepto los siguientes:

. / \ [ ] : | < > + = ; , <espacio>

Last char

Puede usarse si el nombre de sistema principal contiene menos de 16 caracteres. Es un número hexadecimal (sin 0x al comienzo) que indica el valor que se utilizará para el último carácter. Si no se especifica el ÚLTIMO argumento en un nombre de sistema principal de menos de 16 caracteres, entonces se proporciona un carácter comodín “?” para el carácter número 16.

Utilización de LAN Network Manager (LNM)

Este capítulo describe LAN Network Manager (LNM) ASRT de IBM. Incluye las secciones siguientes:

Acerca de LNM

Utilice LNM para gestionar redes en anillo interconectadas mediante puentes de direccionamiento en origen. Permite supervisar el funcionamiento de anillos, puentes y estaciones de anillo individuales.

La información recogida por los agentes de software en el puente está disponibles en las estaciones de gestión LNM. En concreto, los agentes de LNM reenvían la información recogida mediante otro agente denominado LAN Reporting Mechanism (LRM), un protocolo exclusivo de IBM. El reenvío de la información se hace a través de una conexión LLC2 hacia una estación de LAN Network Manager.

Agentes y funciones de LNM

Los agentes de LNM y sus funciones son los siguientes:

- Configuration Report Server (CRS) - informa a LNM de cambios en la topología del anillo y del estado de la estación de anillo.
- Ring Parameter Server (RPS) - proporciona servicio a las peticiones de estaciones de anillo para obtener información de parámetros del anillo incluyendo el número de anillo, el valor del temporizador del informe de errores temporales y la ubicación física.
- Ring Error Monitor (REM) - recoge los informes de error de las estaciones de anillo y los analiza. Si se exceden los valores umbrales, REM puede reenviar la información de error a LNM.
- LAN Reporting Mechanism (LNM) - controla el establecimiento de enlaces de informes desde estaciones LNM a los agentes de puente. También gestiona la transferencia de información a y desde los otros agentes pasando por estos enlaces.

La Figura 25 en la página 210 ilustra la conexión entre el puente IBM, los agentes de LNM y la estación LNM IBM.

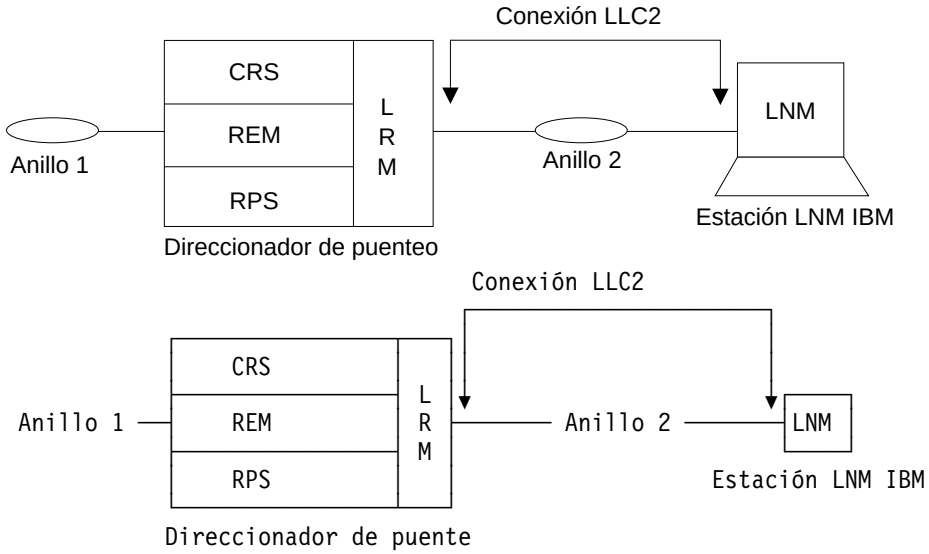


Figura 25. Estación LNM y agentes

Las secciones siguientes describen con más detalle cada agente LNM.

Configuration Report Server (CRS)

A petición de LNM, CRS obtiene y reenvía a LNM información sobre el estado de la estación de anillo. Utilice CRS para establecer los parámetros de la estación de anillo y eliminar una estación del anillo.

La información de configuración generada por las estaciones de anillo se reenvía a LNM. Cuando LNM pide el estado de una estación de anillo, CRS crea y envía tramas MAC a la estación para obtener la información. A continuación CRS envía las tramas siguientes a la estación de anillo:

- Trama MAC de petición de dirección de la estación de anillo
- Trama MAC de petición de estado de la estación de anillo
- Trama MAC de petición de conexiones de la estación de anillo

Cuando la estación de anillo contesta, CRS pone la información en una trama LLC2 formateada adecuadamente y la reenvía a LNM.

CRS también puede eliminar una estación del anillo a petición de LNM. Para eliminar una estación de anillo, CRS envía al anillo una trama MAC de eliminación de estación. CRS devuelve una respuesta a LNM indicando el éxito o bien el error de la eliminación.

Cuando CRS recibe una trama MAC de informe de nuevo monitor activo, reenvía la información a LNM. Cuando se recibe una trama MAC de informe de cambio de NAUN (vecino ascendente activo más próximo), también se notifica esta información. El agente CRS tiene su propia dirección funcional, que las capas MAC de la estación de anillo pueden utilizar para reenviar tramas MAC a CRS.

Ring Parameter Server (RPS)

RPS inserta estaciones de anillo en el anillo. Cuando se inserta por primera vez en el anillo una estación de anillo, sucede lo siguiente:

- La nueva estación envía a RPS una trama MAC de petición de inicialización para este anillo. La trama MAC incluye información sobre la estación.
- RPS responde con una trama MAC de inicialización de estación de anillo, que contiene el número de anillo y el intervalo de tiempo de espera entre el envío de tramas MAC de informe de errores temporales. La información recogida desde la trama de petición de inicialización se pasa a LNM, de modo que éste pueda mantener una base de datos de todas las estaciones del anillo.
- RPS también responde a peticiones de estado de LNM. El número de anillo, la información de versión RPS y valor del temporizador de informe de errores temporales se devuelven a LNM.

La función RPS tiene asociada una dirección funcional para recibir las tramas MAC que le envían otras estaciones de anillo.

Atención: Si una estación intenta insertarse en un anillo, envía una trama MAC de petición de inicialización al servidor de parámetros de anillo (RPS) para ese anillo. Si RPS copia con éxito esta trama, la estación entonces espera recibir a su vez una trama MAC de inicialización de estación de anillo de RPS. Si no se recibe esta trama, la estación no se insertará en el anillo.

Es posible que una estación no consiga insertarse en el anillo si el dispositivo está configurado para LNM, pasa a ser el servidor de parámetros del anillo y entra en un estado de congestión que impide el envío de la trama MAC de inicialización de estación de anillo. La solución a este problema consiste en inhabilitar RPS en el puerto afectado. Si RPS está inhabilitado y ningún servidor copia la trama de petición de inicialización, la estación emisora no espera ninguna respuesta y se insertará en el anillo.

Ring Error Monitor (REM)

REM observa el funcionamiento de la red en anillo conectada buscando errores permanentes y temporales. A continuación informa de éstos a LRM y ayuda a aislar la causa de los errores. Durante la detección de errores permanentes hace lo siguiente:

- Los errores permanentes se detectan en el anillo mediante la recepción de tramas MAC de baliza.
- Las estaciones del dominio defectuoso intentan corregir el problema eliminándose a ellas mismas del anillo.
- REM determina si la condición de error permanente está o no corregida y entonces informa de los resultados a LNM.

REM supervisa los errores de soft como sigue:

- Periódicamente las estaciones del anillo envían a REM tramas MAC de error temporal para informarle del número de veces que tienen lugar diversos errores intermitentes, como por ejemplo errores de CRC y errores de frecuencia.
- Si el número de errores temporales de una estación pasa de un umbral determinado, REM informa de ello a LNM.

- REM también supervisa las tramas MAC de informes de errores temporales en circunstancias de congestión del receptor. La congestión del receptor indica que una estación del anillo ha eliminado tramas debido a la escasez de almacenamientos intermedios para la recepción.
- Si el número de veces que una estación informa de congestión en la recepción pasa de cierto umbral, REM informa de esta circunstancia a LNM. Cuando el estado de congestión de recepción vuelve a ser normal, se notifica a LNM que ha finalizado el estado de congestión de recepción.

LAN Reporting Mechanism (LRM)

LRM controla la conexión entre LNM y los agentes. LRM establece enlaces de informes entre él mismo y cada LNM conectado. Un *enlace de informe* es una conexión LLC2 entre LNM y LRM.

Todas las comunicaciones entre LNM y los agentes se hace a través de un enlace de informe. LRM pasa datos de gestión desde y hacia los agentes pertinentes hacia los enlaces de informe. Se soportan hasta cuatro enlaces de informes. Uno de ellos se denomina *enlace de control* y los otros tres se denominan *enlaces de observación*.

Un LNM conectado a través del enlace de control puede ejecutar todas las funciones disponibles. Las LNM conectadas por enlaces de observación solamente pueden ejecutar un subconjunto limitado de las operaciones disponibles.

Restricciones de configuración de LNM

IBM 2212 da soporte a configuraciones multipuerto de red en anillo y dos configuraciones de red en anillo.

El agente LNM y la estación LNM siempre suponen que los mensajes se pasan según un modelo consistente en dos partes. Sin embargo, LNM está habilitado según un criterio de un puerto por cada puente, para ser coherente con la configuración existente.

En una configuración multipuerto, LNM puede estar habilitado en cualquier puerto de puente de direccionamiento en origen para red en anillo. Se crea una instancia de LNM para cada puerto sobre el que está habilitado LNM.

En una configuración de dos redes en anillo, el otro puerto siempre se denomina según una pseudo-dirección. Ello se conoce como puente multipuerto. Puede corresponder a un anillo virtual o a una interfaz de línea serie.

Solamente si el puente IBM 2212 tiene dos puertos de red en anillo de direccionamiento en origen, el otro puerto del puente de dos puertos será una red en anillo con una dirección real.

Para obtener las direcciones MAC que se necesitan para configurar LNM Manager, entre **`list lnm ports`** en el indicador de mandatos `ASRT>`.

LAN Bridge Server (LBS) puede proporcionar información estadística sobre datos de ejecución de reenvío de paquetes y eliminación de paquetes cuando el gestor de estaciones así lo solicita. Las actualizaciones de configuración remota desde el gestor de estaciones no están soportadas.

Soporte de enlace lógico de clase 2

En las LAN, la capa de enlace de datos comprende dos subcapas: MAC (control de acceso al medio) y LLC (control de capa de enlace). LLC proporciona dos tipos de servicio:

- LLC1 (Tipo 1) - un servicio sin conexión sin acuse de recibo
- LLC2 (Tipo 2) - un conjunto de servicios orientados a la conexión

LAN Network Manager (LNM) requiere servicios LLC2 orientados a conexión. LLC2 proporciona posibilidades para:

- Iniciar nuevas conexiones de enlaces de datos
- Gestionar conexiones de enlaces de datos
- Intercambiar datos en orden secuencial (de manera segura)
- Ejecutar un nivel de control de flujo en las conexiones establecidas
- Terminar conexiones de enlace a petición del usuario del servicio o por errores de enlace no recuperables.

La subcapa LLC sigue el estándar IEEE 802.5.

Configuración y supervisión de LNM

Este capítulo describe la implementación para ASRT de LNM de IBM. Incluye las secciones siguientes:

Configuración de LNM

Esta sección resume el procedimiento para hacer una configuración básica de la característica LNM en el direccionador de puentes.

1. Obtenga la dirección MAC que se requiere para el software de gestión de red.

   Entre el mandato **list lnm ports** en el indicador de mandatos `ASRT>` para obtener las direcciones MAC requeridas por el software de gestión de red que se ejecuta en la estación gestora de 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
   ```

   Las direcciones MAC visualizadas (que en el ejemplo se muestran en negrita) son utilizadas por el gestor de red para configurarlo según los agentes de LNM presentes en el direccionador.

   Nota: Estas direcciones deben entrarse exactamente igual como aparecen en la salida del mandato, puesto que en caso contrario LNM no se configurará correctamente.

2. Habilite los agentes de LNM existentes en el direccionador. Teclee **`enable lnm`** en el indicador de mandatos `LNM config>` para habilitar los agentes de LNM en el puerto del direccionador de puentes que se escoja. Por ejemplo:

   ```
   LNM config>enable lnm
   Port Number [1]? 1
   ```

   Por omisión, todos los agentes de LNM están habilitados.

3. Compruebe la configuración mediante la visualización de los agentes de LNM habilitados. Teclee **`list port`** en el indicador de mandatos `LNM config>` para visualizar los agentes de LNM que están habilitados 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 supervisión de LNM. Estos mandatos permiten configurar y supervisar parámetros de red para LNM.

Nota: Los mandatos de configuración de LNM no surten efecto inmediatamente. Antes, debe rearrancar o volver a cargar el dispositivo.

Entre los mandatos de configuración en el indicador de mandatos `LNM config>`. El acceso al indicador de mandatos es de la forma siguiente:

```
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 de mandatos `LNM>`. Visualice este indicador tal como sigue:

```
+protocol asrt
ASRT>lnm
LNM>
```

La Tabla 15 enumera los mandatos de LNM.

Tabla 15. Resumen de los mandatos de LNM

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Disable	Inhabilita todos los agentes de LNM en un determinado puerto o bien agentes de LNM concretos (RPS, CRS o REM) en el puerto que se especifique. Inhabilita el establecimiento de ciertos parámetros de LNM desde la aplicación LNM remota enlazada con el puente. Se aplica globalmente a todas las instancias de LNM dentro del puente. Este mandato se utiliza sólo para la configuración.
Enable	Habilita todos los agentes de LNM en un determinado puerto, o bien agentes de LNM concretos (RPS, CRS o REM) en el puerto que se especifique. Habilita el establecimiento de ciertos parámetros de LNM desde la aplicación remota de LNM enlazada con el puente. Se aplica globalmente a todas las instancias de LNM dentro del puente. Este mandato se utiliza sólo para la configuración.
List	Visualiza los agentes de LNM que se hayan habilitado para el puerto que se especifica. Visualiza las contraseñas configuradas para el puente. Este mandato se utiliza tanto para configuración como para seguimiento.
Set	Establece la contraseña para el número de enlace de información especificado. Este mandato se utiliza sólo 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 xxxi.

Respuesta a los mandatos de configuración de LNM

Los mandatos de configuración de LNM (Talk 6) no son efectivos inmediatamente. Permanecen pendientes hasta que se emitan los mandatos **reload** o **restart**.

Disable

Utilice el mandato **disable** para inhabilitar todos los agentes de LNM (RPS, CRS o REM) de un puerto específico.

Este mandato también inhabilita el establecimiento de contraseñas de enlaces de información desde la aplicación LNM remota enlazada con el puente.

Sintaxis:

disable — agent *núm-puerto* | lnm . . . | configuration-remote-change

agent *núm-puerto*

Inhabilita el agente de LNM especificado (RPS, CRS o REM) en el puerto especificado. Si el puerto no está configurado, se visualizará el mensaje `LNM not configured for port XX`, y el mandato no tendrá efecto.

Ejemplo: **`disable REM 1`**

lnm Inhabilita LNM en el puerto especificado. Si el puerto no está configurado para LNM, se visualizará el mensaje `LNM not configured for port XX` y el mandato no tendrá efecto.

Ejemplo: **`disable lnm`**

```
Port number [1]? 1
LNM not configured for Port 1
```

configuration-remote-change

Inhabilita el establecimiento de las contraseñas de enlace de información desde la aplicación LNM remota enlazada con el puente. Este mandato se aplica globalmente a todas las instancias de LNM dentro del puente.

Ejemplo: **`disable configuration-remote-change`**

```
CONFIGURATION-REMOTE-CHANGE: disabled
```

Enable

Habilita todos los agentes de LNM en un puerto específico o bien habilita determinados agentes de LNM (CRS, REM o RPS) en un puerto específico.

Si la interfaz no es una red en anillo, se visualiza el mensaje `Port number XX is not token-ring` y el mandato no surte efecto.

Si el puerto no está configurado, aparece el mensaje `Port number XX does not exist` y el mandato no surte efecto.

Si el agente que se especifica ya está habilitado para el puerto específico, se visualiza el mensaje `Already enabled`.

Este mandato también habilita el establecimiento de contraseñas de enlace de información desde la aplicación LNM remota enlazada con el puente.

Sintaxis:

enable agent *núm-puerto*
lnm . . .
configuration-remote-change

agent *núm-puerto*
Habilita el agente de LNM especificado (RPS, CRS o REM) en el puerto especificado.

Ejemplo: **`enable CRS 1`**

lnm *núm-puerto*
Habilita todos los agentes de LNM en el puerto especificado.

Ejemplo: **`enable lnm`**

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

configuration-remote-change
Habilita el establecimiento de las contraseñas del enlace de información desde la aplicación remota de LNM enlazada con el puente. Por omisión, el establecimiento de parámetros de configuración de LNM de forma remota está inhabilitado.

Este mandato se aplica globalmente a todas las instancias de LNM dentro del puente.

Ejemplo: **`enable configuration-remote-change`**

```
CONFIGURATION-REMOTE-CHANGE: Enabled
```

List (mandato de configuración)

Visualiza los agentes de LNM habilitados para el puerto especificado y visualiza también las contraseñas que se han configurado para el puente. El mandato puede entrarse desde el indicador de mandatos ASRT>.

Sintaxis:

list password
port . . .

password
Visualiza las contraseñas que se han configurado para los enlaces de información del puente. Visualiza si las contraseñas pueden cambiarse mediante la aplicación de LNM remota.

Ejemplo: **`list password`**

```
Reporting Link     Password
0             87654321
1             MADRAS
2             ABC1234
3             123ABC
CONFIGURATION-REMOTE-CHANGE: Disabled
```

port *núm-puerto*
Visualiza los agentes de LNM habilitados para el puerto especificado si el puerto es un puerto de red en anillo que soporta el establecimiento de puentes de direccionamiento en origen.

Ejemplo: **`list port`**

```
Port Number [1]? 1
LNM Agents Enabled: RPS CRS REM
```

List (mandato de supervisión)

Visualiza información acerca del estado de la configuración de LNM. El mandato puede entrarse desde el indicador de mandatos ASRT>.

Sintaxis:

list bridge
lnm ports
source-routing configuration

bridge Visualiza si LNM está habilitado en un puerto específico.

Ejemplo: **`list bridge`**

lnm ports

Visualiza información acerca de la configuración de LNM habilitado en el direccionador de puenteo.

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

Visualiza si LNM está habilitado en un puerto específico.

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

Establece la contraseña para el número de enlace de información especificado. El número de enlace puede ser 0, 1, 2 ó 3. El enlace 0 se utiliza para el enlace de control. Los enlaces 1, 2 y 3 se utilizan para los enlaces de observación.

La contraseña debe consistir en una serie de seis a ocho caracteres y debe coincidir con la contraseña utilizada por LNM cuando establece un enlace de información con el puente. Si la contraseña no está establecida para un enlace, pasa a ser por omisión la serie 00000000.

Sintaxis:

set password *núm-enlace contraseña*
Ejemplo: **`set password`**

Ejemplo: **`set password`**

```
Link Number [0]? 1
Enter new password :  [ABCDEFGH]? guesswho
```

Soporte de reconfiguración dinámica de LAN Network Manager

En este apartado se describe el modo en que la reconfiguración dinámica (DR) afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

LAN Network Manager (LNM) da soporte al mandato **delete interface** de CONFIG (Talk 6) sin restricciones.

Mandato activate interface de GWCON (Talk 5)

LNM no da soporte al mandato **activate interface** de GWCON (Talk 5).

Mandato reset interface de GWCON (Talk 5)

LNM no da soporte al mandato **reset interface** de GWCON (Talk 5).

Configuración y supervisión de TCP/IP Host Services

En este capítulo se describe cómo configurar el protocolo TCP/IP Host Services (TCP/IP Host) y utilizar sus mandatos de configuración. Consta de los siguientes apartados:

En el apartado "TCP/IP Host Services (gestión sólo de puentes)" en la página 47 hallará más información sobre los motivos por los que interesa utilizar TCP/IP Host Services.

No utilice este capítulo si está configurando el dispositivo para direccionamiento IP; en este caso, consulte el "Utilización de IP" en la página 235.

Nota: Para configurar TCP/IP Host Services, no puede haber ninguna dirección IP configurada en las interfaces. El dispositivo no puede configurarse como direccionador para IP. TCP/IP Host Services es únicamente para el establecimiento de puentes.

Acceso al entorno de configuración de TCP/IP Host

Para acceder al entorno de configuración de TCP/IP Host, entre el mandato siguiente en el indicador de mandatos `Config>`:

```
Config> protocol hst
TCP/IP-Host Services user configuration
TCP/IP-Host Config>
```

Procedimientos básicos de configuración

En los apartados que siguen se describen los procedimientos básicos de configuración para habilitar TCP/IP Host Services en el 2212.

Establecimiento de la dirección IP

Para establecer una configuración mínima de TCP/IP Host Services, asigne al 2212 una dirección IP con el mandato **set ip-host**. Esta dirección IP se asocia con el 2212 en su conjunto, en lugar de estar asociada a una sola interfaz.

Habilitación de TCP/IP Host Services

Utilice el mandato **enable services** para habilitar TCP/IP Host Services.

Adición de una pasarela por omisión

El 2212 utiliza su propia pasarela por omisión para comunicarse con sistemas principales y pasarelas que no se encuentran en la red puenteada a la que 2212 está directamente conectado. El 2212 puede averiguar dinámicamente su pasarela por omisión utilizando o bien el descubrimiento de direccionador ICMP (véase el mandato **enable router-discovery** en este capítulo) o RIP (véase el mandato **enable rip-listening** en este capítulo). También puede especificarse de forma estática una o más pasarelas por omisión con el mandato **add default gateway**. El 2212 utiliza solamente una pasarela por omisión cada vez; cualquier pasarela por omisión adicional se utiliza como reserva.

Para guardar la dirección IP asignada y la información de la pasarela por omisión, debe hacerse lo siguiente:

1. Salga del indicador de mandatos `TCP/IP-Host config>` para ir al indicador de mandatos `Config>`.
2. Utilice el mandato **write** en el indicador de mandatos `Config>` para grabar la configuración actual en la memoria.
3. Entre **CTRL-P** para llegar al indicador OPCON y utilice el mandato **reload** o **restart** de OPCON para cargar una nueva copia del software.
4. Una vez reiniciado o recargado el 2212, vuelva al indicador `TCP/IP-Host config>`.

Mandatos de configuración de TCP/IP Host

En este apartado se describen los mandatos de configuración de TCP/IP Host. Los mandatos de configuración de TCP/IP permiten especificar parámetros de red para el puente de TCP/IP Host. Rearranque el dispositivo para activar los mandatos de configuración.

Nota: Los mandatos de configuración de TCP/IP Host no surten efecto inmediatamente. Permanecen pendientes hasta que se rearranque o recargue el dispositivo.

Entre los mandatos de configuración de TCP/IP Host en el indicador de mandatos `TCP/IP-Host config>`. La Tabla 16 en la página 223 muestra los mandatos.

Tabla 16. Resumen de los mandatos de configuración de TCP/IP Host

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Add	Añade una pasarela por omisión.
Delete	Suprime una pasarela por omisión.
Disable	Inhabilita TCP/IP Host Services, los procesos de descubrimiento de direccionador y la escucha RIP.
Enable	Habilita TCP/IP Host Services, los procesos de descubrimiento de direccionador y la escucha RIP.
List	Enumera la configuración actual de TCP/IP Host.
Set	Establece la dirección IP del 2212.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Respuesta a los mandatos de configuración de TCP/IP Host

Los mandatos de configuración de TCP/IP Host (Talk 6) no surten efecto inmediatamente. Permanecen pendientes hasta que se emitan los mandatos **reload** o **restart**.

Add

Utilice el mandato **add** para añadir pasarelas por omisión (esto es, direccionadores) a la configuración.

Las pasarelas por omisión se utilizan al intentar enviar paquetes a destinos IP que quedan fuera de la subred local. Entonces se crea la tabla de direccionamiento mediante los procesos de redireccionamiento. Se intentan detectar los direccionadores que desaparecen. Si el 2212 ha arrancado a través de la red (mediante TFTP/BootP), la pasarela por omisión se configura con la información del proceso de arranque.

Sintaxis:

a**dd** default-gateway *dirección-IP-por-omisión-pasarela*

Ejemplo: `add default-gateway`

```
Default-Gateway address [0.0.0.0]?  123.45.67.89
```

Delete

Utilice el mandato **delete** para suprimir pasarelas por omisión de la configuración del 2212. Entre la dirección IP de la pasarela por omisión que se desea suprimir después del mandato **delete**.

Sintaxis:

de**lete** default-gateway *dirección-IP-por-omisión-pasarela*

Ejemplo: `delete default-gateway`

```
Enter address to be deleted [0.0.0.0]?  123.45.67.89
```

Disable

Utilice el mandato **disable** para inhabilitar las siguientes funciones de TCP/IP:

- TCP/IP Host Services
- Procesos de descubrimiento de direccionador
- Escucha RIP

Sintaxis:

disable rip-listening
router-discovery
services

rip-listening
Inhabilita la creación de entradas de la tabla de direccionamiento que se han recogido mediante la escucha del protocolo RIP. Por omisión, la escucha RIP está inhabilitada.

Ejemplo: `disable rip-listening`

router-discovery
Inhabilita la capacidad de averiguar pasarelas por omisión mediante la recepción de mensajes de descubrimiento de direccionador de ICMP. Por omisión, el proceso de descubrimiento de direccionador está habilitado.

Ejemplo: `disable router-discovery`

services Inhabilita el protocolo TCP/IP Host Services. Si el direccionamiento IP no está habilitado, el protocolo TCP/IP Host Services está habilitado por omisión.

Ejemplo: `disable services`

Enable

Utilice el mandato **enable** para habilitar las siguientes funciones de TCP/IP:

- TCP/IP Host Services
- Procesos de descubrimiento de direccionador
- Escucha RIP

Sintaxis:

enable rip-listening
router-discovery
services

rip-listening
Habilita la creación de las entradas de la tabla de direccionamiento recogidas por el puente a partir de la “escucha” del protocolo RIP. La escucha RIP está inhabilitada por omisión.

Ejemplo: `enable rip-listening`

router-discovery
Habilita la averiguación de pasarelas por omisión mediante la recepción de mensajes de descubrimiento de direccionador de ICMP. Por omisión, el proceso de descubrimiento de direccionador está habilitado.

Ejemplo: `enable router-discovery`

services Habilita el protocolo TCP/IP Host Services. Si el direccionamiento IP no está habilitado, el protocolo TCP/IP Host Services está habilitado por omisión.

Ejemplo: `enable services`

List

Utilice el mandato **list** para visualizar información acerca de la configuración actual de TCP/IP Host.

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	Visualiza si TCP/IP Host SERVICES está habilitado o inhabilitado.
IP-HOST Address	Visualiza la dirección actual de IP-HOST.
IP-HOST Mask	Visualiza la máscara de IP-HOST actual.
DEFAULT-GATEWAY Address	Visualiza la dirección actual de DEFAULT-GATEWAY.
RIP-LISTENING	Visualiza si RIP-LISTENING está habilitado o inhabilitado.
ROUTER DISCOVERY	Visualiza si ROUTER DISCOVERY está habilitado o inhabilitado.

Set

Utilice el mandato **set** para establecer la dirección IP del 2212. Debe asignarse una dirección IP al 2212 antes de habilitar TCP/IP Host Services.

Nota: Si la dirección IP no está todavía configurada se establece (por omisión) utilizando información de arranque. Este proceso solamente se aplica si el 2212 es un sistema principal de red que opera como un sistema principal IP.

Sintaxis:

set ip-host address *dirección-IP-sistema-principal*

Ejemplo: `set ip 123.45.67.89`

```
Address mask [255.255.0.0]?
IP-Host Address set.
```

Supervisión de TCP/IP Host Services

En este apartado se describe cómo supervisar TCP/IP Host Services en IBM 2212.

Acceso al entorno de supervisión de TCP/IP Host

Para acceder al entorno de supervisión de TCP/IP Host, entre el mandato siguiente en el indicador + (GWCON):

```
+ protocol hst
   TCP/IP-Host>
```

Mandatos de supervisión de TCP/IP Host

En este apartado se describen los mandatos de supervisión de TCP/IP Host. Estos mandatos permiten visualizar parámetros y entrar peticiones de información desde el terminal activo. Entre estos mandatos en el indicador de mandatos `TCP/IP-Host>`. La Tabla 17 muestra los mandatos.

Tabla 17. Resumen de los mandatos de supervisión de TCP/IP Host

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
dump	Visualiza la tabla de direccionamiento IP actual. Se presenta una línea por cada destino.
Interface	Visualiza la dirección IP de IBM 2212.
ping	Continuamente sondea un destino dado, imprimiendo una línea por cada respuesta que se reciba.
Traceroute	Visualiza la ruta hacia un destino determinado salto por salto.
Routers	Visualiza la lista de todos los direccionadores IP que conoce el 2212.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

dump

Utilice el mandato **dump** para visualizar la tabla de direccionamiento IP actual. Se imprime una línea por cada destino. Muchas de las entradas que se visualizan 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	El tipo de ruta indica cómo se ha obtenido la ruta: RIP - La ruta se ha averiguado a través del protocolo RIP. Stat - Indica una ruta configurada estáticamente. Dir - Indica una red o subred conectada directamente.
Dest net	Visualiza la dirección IP de la red/subred de destino.
Mask	Visualiza la máscara de dirección IP.
Cost	Visualiza el coste de la ruta.
Age	Para las rutas RIP visualiza el tiempo, en segundos, desde que se renovó la ruta. Para otros tipos de rutas visualiza el tiempo, en segundos, desde que se instaló la ruta.
Next Hop	Visualiza la dirección IP del siguiente dispositivo en la ruta hacia el sistema principal de destino. También se visualiza el tipo de interfaz que utiliza el dispositivo de envío para reenviar el paquete.
Default gateway	Visualiza la dirección IP de la pasarela por omisión junto con información sobre el tipo de ruta, el coste, la edad y el salto siguiente asociados con esa entrada.
Routing table size	Visualiza el tamaño actual (en redes y bytes) de la tabla actual. También identifica el número de redes conocidas por el sistema principal.

Interface

Utilice el mandato **interface** para visualizar la dirección IP de IBM 2212. Cuando TCP/IP Host Services se ejecuta a través del puente, en el terminal se visualiza una única dirección como Bridge/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	Visualiza el tipo de interfaz. Para TCP/IP Host Services, la interfaz es siempre BDG/0, lo que denota el puente.
IP Address	Visualiza la dirección IP de la interfaz de TCP/IP Host Services.
Mask	Visualiza la máscara de subred de la dirección IP.

Ping

Utilice el mandato **ping** para que el dispositivo envíe peticiones de eco ICMP a una dirección determinada una vez por segundo (“hacer ping”) y esté atento a una respuesta. Este mandato puede utilizarse para aislar un problema en un entorno de interred.

Este proceso se realiza de forma continuada, incrementando el número de secuencia ICMP con cada paquete adicional. Se informa de las respuestas de eco ICMP que se reciban coincidentes, junto con su número de secuencia y el tiempo de ida y vuelta. La granularidad (resolución de tiempo) del cálculo del tiempo de ida y vuelta es específico de cada plataforma y suele ser de unos 20 milisegundos.

Para detener el proceso de ping, teclee cualquier carácter en el terminal. En ese momento se visualizará un resumen de información sobre pérdida de paquetes, tiempos de ida y vuelta y número de destinos ICMP a los que no se puede acceder.

Cuando se proporciona una dirección de multidifusión como destino, puede que se impriman varias respuestas para cada paquete enviado, una para cada miembro del grupo. Cada una de las respuestas devueltas aparece con la dirección de origen de la que se recibe la respuesta.

El tamaño de ping (número de bytes de datos en el mensaje ICMP, excluyendo la cabecera ICMP), el valor de TTL y la velocidad de ping pueden configurarse por el usuario. Los valores por omisión son: un tamaño de 56 bytes, un TTL de 64 y una velocidad de 1 ping por segundo.

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 toda la ruta que conduce a un destino concreto, salto a salto. Para cada salto sucesivo, el mandato traceroute envía por omisión tres sondas e imprime la dirección IP del emisor de la respuesta, junto con el tiempo de ida y vuelta que conlleva la respuesta. Si una determinada sonda no recibe ninguna respuesta, se visualiza un asterisco (*). Cada línea que se visualiza hace referencia a este conjunto de tres sondas, con el número situado más a la

izquierda indicando la distancia desde el dispositivo que ejecuta el mandato (en términos de saltos de dispositivo).

El rastreo de rutas se completa al alcanzar el destino, cuando se recibe el mensaje de ICMP de destino no accesible o cuando la longitud de la ruta alcanza 32 saltos de dispositivo de red.

Sintaxis:

t**raceroute** *destino origen tamaño sondas 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
```

Se visualiza:

TRACEROUTE	Visualiza la dirección del área de destino y el tamaño del paquete que se envía a esa dirección.
1	El primer rastreo que muestra el NSAP del destino y el tiempo de ida y vuelta que ha utilizado el paquete para llegar al destino y volver. El paquete se rastrea tres veces.
Destination unreachable	Indica que no hay disponible ninguna ruta hacia el destino.
1 * * * 2 * * *	Indica que el dispositivo espera algún tipo de respuesta desde el destino, pero el destino no responde.

Cuando una sonda recibe un resultado inesperado (véase el ejemplo anterior) pueden aparecer varios indicadores. Éstos se explican en la tabla siguiente.

!N	Indica que se ha recibido un mensaje de ICMP de destino no accesible (red no accesible).
!H	Indica que se ha recibido un mensaje de ICMP de destino no accesible (sistema principal no accesible).
!P	Indica que se ha recibido un mensaje de ICMP de destino no accesible (protocolo no accesible).
!	Indica que se ha alcanzado el destino, pero que la respuesta enviada por el destino se ha recibido con un TTL de 1. Esto habitualmente indica un error en el destino, común en algunas versiones de UNIX, por el cual un destino inserta el TTL de la sonda en sus respuestas. Desafortunadamente, ello conduce a a la existencia de un número de líneas que consisten únicamente en asteriscos antes de alcanzar finalmente el destino.

Routers

Utilice el mandato **routers** para visualizar la lista de todos los direccionadores IP que conoce IBM 2212. Se puede averiguar dónde hay direccionadores mediante:

- Una configuración estática (utilizando el mandato **add default-gateway** que se explica en “Add” en la página 223).
- Redirecciones ICMP recibidas
- Mensajes ICMP de descubrimiento de direccionador (si está configurado)
- Actualizaciones RIP (si está configurado)

Cada direccionador aparece en la lista con su origen, prioridad (utilizada al seleccionar la ruta por omisión) y su tiempo de vida (el número de segundos que transcurren antes de que se considere al direccionador como no válido, a no ser que vuelva a recibirse información de él.

Sintaxis:

r**outers**

Ejemplo: `routers`

Soporte de reconfiguración dinámica de TCP/IP Host Services

En este apartado se describe el modo en que la reconfiguración dinámica (DR) afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

TCP/IP Host Services (HST) no da soporte al mandato **delete interface** de CONFIG (Talk 6).

Mandato activate interface de GWCON (Talk 5)

El mandato **activate interface** de GWCON (Talk 5) no es aplicable a TCP/IP Host Services (HST). TCP/IP Host Services no tiene ningún parámetro de configuración que sea específico de interfaz.

Mandato reset interface de GWCON (Talk 5)

El mandato **reset interface** de GWCON (Talk 5) no es aplicable a TCP/IP Host Services (HST). TCP/IP Host Services no tiene ningún parámetro de configuración que sea específico de interfaz.

Mandatos no reconfigurables dinámicamente

En la tabla siguiente figuran los mandatos de configuración de TCP/IP Host Services (HST) que no pueden cambiarse dinámicamente. Para activar estos mandatos, es necesario volver a cargar o a arrancar el dispositivo.

Mandatos
CONFIG, protocol hst, add default-gateway
CONFIG, protocol hst, delete default-gateway
CONFIG, protocol hst, disable rip-listening
CONFIG, protocol hst, disable router-discovery
CONFIG, protocol hst, disable services
CONFIG, protocol hst, enable rip-listening
CONFIG, protocol hst, enable router-discovery
CONFIG, protocol hst, enable services
CONFIG, protocol hst, set ip-host address

Configuración y supervisión de los protocolos de direccionador

Utilización de IP

Este capítulo describe cómo configurar el protocolo IP (Internet Protocol). Incluye las secciones siguientes:

Procedimientos básicos de configuración

Esta sección esboza los pasos necesarios que se requieren para que el protocolo IP esté listo para funcionar. Los detalles acerca de más cambios de configuración se encuentran en otras secciones de este capítulo. Los detalles acerca de los mandatos para configuraciones individuales se tratan en la sección de este capítulo sobre mandatos. La siguiente lista resume las tareas iniciales de configuración para arrancar IP en el direccionador. Después de completar estas tareas, debe reiniciarse el direccionador para que surta efecto la nueva configuración.

1. Acceso al entorno de configuración de IP. (Consulte "Acceso al entorno de configuración de IP" en la página 269.)
2. Asignación de direcciones IP a las interfaces de red. (Consulte "Asignación de direcciones IP a las interfaces de red".)
3. Habilitación del direccionamiento dinámico. (Consulte "Habilitación del direccionamiento dinámico" en la página 239.)
4. Adición de información de direccionamiento estático, si fuera necesario.(Consulte "Adición de información de direccionamiento estático" en la página 241.)
5. Habilitación del direccionamiento de subred ARP, si fuera necesario. (Consulte "Habilitación del direccionamiento de subred ARP" en la página 244.)
6. Establecimiento de parámetros ARP, si fuera necesario. (Consulte "Establecer una configuración ARP" en la página 244.)
7. Salir del proceso de configuración de IP.
8. Proceso de rearranque del direccionador para activar los cambios de configuración.

Asignación de direcciones IP a las interfaces de red

Utilice el mandato de configuración de IP **add address** para asignar direcciones IP a las interfaces de red. Los argumentos de este mandato incluyen el número de interfaz (obtenido del mandato `Config>` **list devices**) y la dirección IP con su máscara de dirección asociada.

En el ejemplo siguiente, 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 el establecimiento de subredes).

```
IP config> add address 2 128.185.123.22 255.255.255.0
```

Puede asignarse más de una dirección IP a una sola interfaz de red.

Por omisión, las direcciones IP asignadas a las interfaces de red deben encontrarse en una red o subred distinta. El mandato **enable same-subnet** suprime esta restricción.

IP permite utilizar una interfaz de línea serie para el tráfico de IP sin asignar una dirección IP real a la línea. Sin embargo, todavía resulta necesario asignar una pseudo dirección IP a cada línea serie; esta dirección es utilizada por el direccionador para hacer referencia a la interfaz, pero nunca se usa externamente. 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 (de nuevo, éste se obtiene a partir del mandato `Config>` **list devices**). Este formato de dirección informa al direccionador que la interfaz en cuestión es una *línea serie no numerada*.

Para habilitar IP en la interfaz de línea serie número dos sin asignar una dirección IP a la interfaz, utilice el siguiente mandato:

```
IP config> add address 2 0.0.0.2
```

Utilización de una dirección dinámica

Puede utilizarse una dirección dinámica para identificar una interfaz que averigua su dirección IP a partir del extremo remoto de un enlace PPP utilizando el protocolo IPCP (Internet Protocol Control Protocol). Debe añadirse primero la interfaz, como una línea serie no numerada (0.0.0.n). En el momento en que se complete IPCP, IP será informado y la dirección IP negociada se instalará en la interfaz especificada. Para habilitar la dirección dinámica, haga los pasos siguientes:

- PPP debe configurarse como sigue para que solicite una dirección IP:

```
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 configurarse en la interfaz 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 habilitar 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
```

Asignación de direcciones IP a la interfaz de red de puente

El 2212 direcciona paquetes IP en las interfaces de red a las que se han asignado direcciones IP (*interfaces de direccionamiento*) y establece puentes para paquetes IP en las interfaces de red en las que el establecimiento de puentes está configurado, pero en las que no se ha asignado ninguna dirección IP (*interfaces de puenteo*). El 2212 puede recibir datagramas IP de las interfaces de puenteo, enviar datagramas IP a las interfaces de puenteo, y direccionar paquetes IP entre las interfaces de puenteo y las interfaces de direccionamiento. Estas funciones pueden habilitarse en el 2212 añadiendo una o más direcciones IP a la interfaz de red de puente. Ésta es una interfaz lógica que conecta IP a la red puenteada a la está conectado el 2212.

Para añadir direcciones IP a la interfaz de red de puente, utilice el mandato **add address**, especificando **bridge** como interfaz de red:

```
IP config> add address bridge dirección-ip máscara-dirección-ip
```

Este mandato no asigna una dirección IP a una interfaz de puenteo individual sino en realidad a todas las interfaces de puenteo.

La asignación de direcciones IP a la interfaz de red de puente permite liberar una de las interfaces de red físicas (puertos físicos) del 2212. Para comprender esto mejor, examine la Figura 26, que ejemplifica un interred IP con dispositivos separados que ejecutan las funciones de direccionador y de puente. Las redes LAN 2 y LAN 3 están conectadas por el puente para formar una red puenteada; para el direccionador, la red puenteada es una sola subred IP que está definida por la dirección IP 9.67.5.1 y la máscara 255.255.255.0.

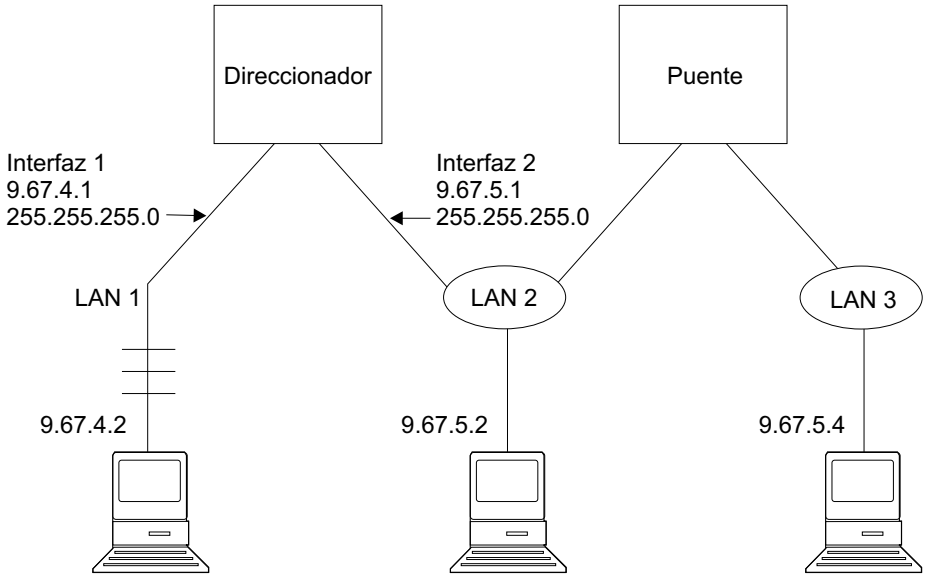


Figura 26. Direccionamiento hacia una red puenteada. Posibilidad 1

La Figura 27 en la página 238 ejemplifica la misma interred con las funciones de direccionador y de puente unidas en un solo dispositivo. En esta ilustración, el direccionador tiene todavía su propia interfaz de red física (Interfaz 2) hacia la red puenteada.

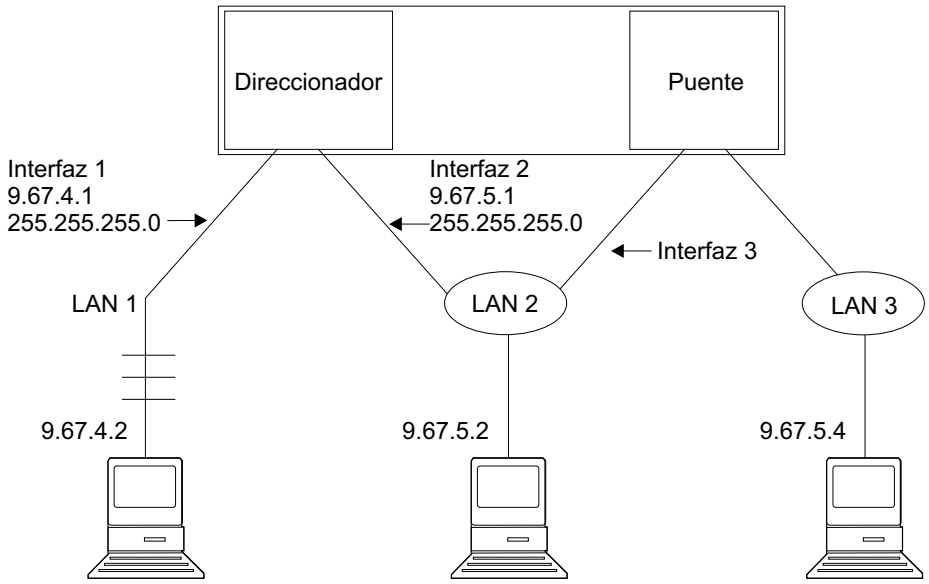


Figura 27. Direccionamiento hacia una red puenteada. Posibilidad 2

Finalmente, en la Figura 28, la interfaz física de red del direccionador con la red puenteada se sustituye por la interfaz de red de puente, que es una interfaz interna. Ésta es la misma interred que se ejemplifica en las Figuras 26 y 27, pero el direccionador ya no necesita tener su propia interfaz física de red con la red puenteada.

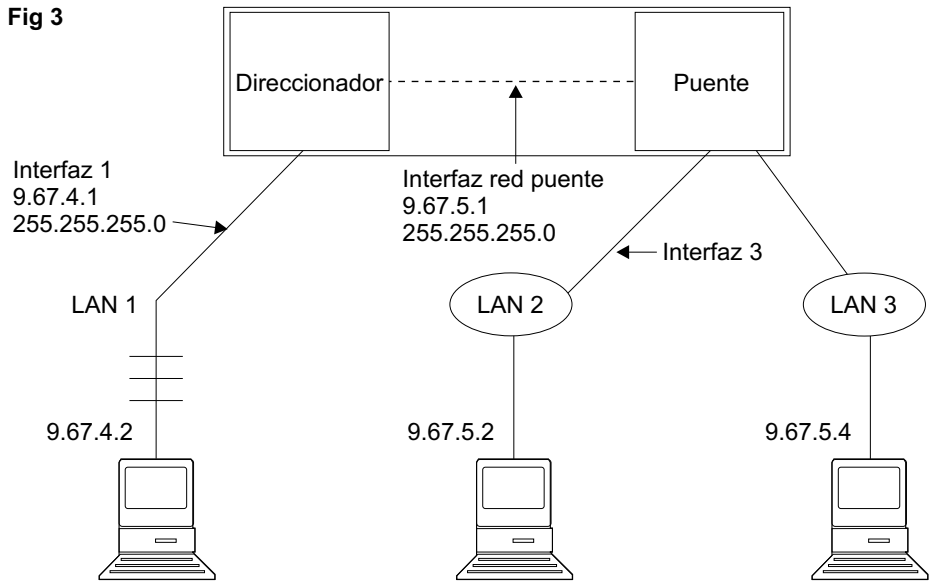


Figura 28. Direccionamiento hacia una red puenteada. Posibilidad 3

Nota: Si se configuran direcciones IP en la interfaz de red de puente, no se pueden configurar direcciones IP en una interfaz de red en anillo en la que esté configurado el puenteo de ruta en origen.

Establecimiento de la dirección IP interna

Ésta es una dirección IP que no depende del estado de ninguna interfaz y se establece sin hacer referencia a ninguna de ellas. Algunas configuraciones de IP la necesitan. Vea el mandato **set internal-IP-address** en la página 325 si desea más información.

Habilitación del direccionamiento dinámico

Utilice los siguientes procedimientos para habilitar el direccionamiento dinámico en el direccionador. El software del direccionador da soporte a OSPF, RIPv1 y RIPv2 como protocolos de pasarela interior (IGP), así como a BGP, que es un protocolo de pasarela externa.

Todos los protocolos de direccionamiento pueden ejecutarse de forma simultánea. Sin embargo, la mayor parte de direccionadores probablemente se ejecutarán únicamente con un solo protocolo de direccionamiento (uno de los IGP). Se recomienda el protocolo OSPF por su robustez y por las características de IP adicionales (tales como subredes multivía de igual coste y subredes de longitud variable) a las que da soporte.

Establecimiento del tamaño de la tabla de direccionamiento

El tamaño de la tabla de direccionamiento determina el número de entradas en la tabla de direccionamiento de todos los orígenes, incluyendo los protocolos de direccionamiento dinámico y las rutas estáticas. El tamaño por omisión es de 768 entradas.

Para cambiar el tamaño de la tabla de redireccionamiento, utilice el mandato **set routing table-size**. Si se establece un tamaño demasiado pequeño para la tabla de direccionamiento, como resultado algunas rutas son descartadas. Si se establece un tamaño demasiado grande, se produce un uso no eficiente de los recursos de memoria. Después de realizar la operación, utilice el mandato de consola **dump** para visualizar el contenido de la tabla y ajustar a continuación el tamaño según sea necesario, dejando un espacio para la expansión.

Habilitación del protocolo OSPF

La configuración de OSPF se hace a través de su propia consola de configuración (a la cual se entra a través del mandato `Config>` **protocol ospf**). Para habilitar OSPF, utilice el siguiente mandato:

```
OSPF Config> enable OSPF
```

Después de habilitar el protocolo OSPF, se le solicitará estimaciones de tamaño para la base de datos de estado de enlaces. Ello proporciona al direccionador una idea de la cantidad de memoria que debe reservarse para OSPF. Deben proporcionarse los dos valores siguientes, que se utilizarán para estimar el tamaño de la base de datos de estado de enlaces de OSPF:

- Número total de rutas externas importadas al dominio de direccionamiento de OSPF.
- Número total de direccionadores OSPF en el dominio de direccionamiento.

Debe entrar estos valores cuando se le solicite lo siguiente (se proporcionan valores de muestra)

```
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 participará en el redireccionamiento OSPF. Para configurar una interfaz IP para OSPF, utilice el mandato siguiente:

```
OSPF Config> set interface
```

Se le solicitará que entre una serie de parámetros de funcionamiento. A cada interfaz se le asigna un coste, además de otros parámetros de funcionamiento de OSPF.

Al ejecutar otros protocolos de direccionamiento IP además de OSPF, es posible que desee habilitar el intercambio de rutas entre OSPF y los otros protocolos. Para hacer esto, utilice el mandato siguiente:

```
OSPF Config> enable AS-boundary-routing
```

Si desea más información sobre el proceso de configuración de OSPF, vea el “Utilización de OSPF” en la página 363.

Habilitación del protocolo RIP

Esta sección describe como configurar inicialmente el protocolo RIP. Al configurar el protocolo RIP, se puede especificar el conjunto de rutas que el direccionador anuncia y/o acepta en cada interfaz IP.

RIP no está soportado en interfaces de red X.25 . Para estos tipos de interfaces, utilice OSPF en lugar de RIP para un protocolo de pasarela interior (IGP).

En primer lugar, habilite el protocolo RIP con el mandato siguiente:

```
IP config> enable RIP
```

Cuando RIP esté habilitado, se establece el siguiente comportamiento por omisión:

- El direccionador incluye todas las rutas de red y subred en las actualizaciones RIP que se envían a cada una de las direcciones IP configuradas. No incluye las rutas por omisión ni las rutas estáticas.
- El direccionador procesa todas las actualizaciones de RIP recibidas en cada una de las interfaces IP que tiene configuradas.
- RIP no prevalecerá sobre las rutas por omisión y las rutas estáticas.

Si se desea cambiar cualquiera de los comportamientos de envío/recepción, utilice los siguientes mandatos de configuración de IP, que están definidas para cada 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 están configuradas las políticas de direccionamiento IP. Véase “Filtrado de rutas con políticas” en la página 253 para obtener más información.

Habilitación del protocolo BGP

El protocolo BGP se habilita desde su propio indicador de mandatos de configuración, `BGP Config>`. Si desea obtener más información sobre la configuración de BGP, consulte la explicación de la utilización y la configuración de BGP4 que se da en la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 1*.

Adición de información de direccionamiento estático

Este procedimiento es necesario sólo para direccionar información que no pueda obtenerse de ninguno de los protocolos de direccionamiento dinámico mencionados anteriormente. La información de direccionamiento estático persiste aunque se produzcan interrupciones de la alimentación, y se utiliza para rutas que nunca cambian o que no pueden ser averiguadas de forma dinámica.

El destino de una ruta estática está descrito por una dirección IP, (*dir-dest*) y una máscara de dirección IP, (*másc-dest*). La máscara indica el rango de direcciones IP a las 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 que van desde 10.0.0.0 hasta 10.255.255.255. La ruta hacia el destino viene dada por la dirección IP del direccionador de salto siguiente (*salto-siguiente*) y el coste de reenviar un paquete por esta ruta (*coste*). Se pueden definir cuatro rutas estáticas como máximo por destino IP. Las rutas estáticas que van a un destino dado pueden tener el mismo coste, en cuyo caso IP podrá utilizarlas simultáneamente, o bien un coste diferente, en cuyo caso IP utilizará la ruta con menor coste que funcione.

Para crear, modificar o suprimir una ruta estática, utilice los mandatos siguientes: :

```
IP config>add route dir-dest másc-dest salto-siguiente coste
IP config>change route dir-dest másc-dest salto-siguiente coste
IP config>delete route dir-dest másc-dest
```

Estos mandatos surten efecto inmediatamente sin que haya necesidad de volver a arrancar el direccionador.

Regla de la coincidencia más larga

Dado que el destino de una ruta incluye la máscara de dirección IP, es posible que haya más de una ruta que coincida con una dirección IP concreta; por ejemplo, para la dirección IP 10.1.2.3, una ruta con dirección IP 10.0.0.0 y máscara 255.0.0.0 y una ruta con dirección IP 10.1.0.0 y máscara 255.255.0.0 coinciden. Para determinar qué ruta se utilizará, se aplica la regla de la coincidencia más larga. Se utiliza la ruta con la máscara más larga (en este caso, la ruta con dirección IP 10.1.0.0 y máscara 255.255.0.0).

Rutas por omisión, de red, de subred y de sistema principal

Las rutas pueden clasificarse como rutas *por omisión (default)*, *de red (network)*, *de subred (subnet)* o *de sistema principal (host)*, según su dirección y máscara de destino IP.

Una ruta *por omisión* tiene una dirección/máscara IP 0.0.0.0/0.0.0.0. Esta ruta coincide con todas las direcciones de destino IP, pero, a causa de la regla de coinci-

dencia más larga, sólo se utiliza si no hay ninguna otra ruta coincidente. El mandato siguiente crea una ruta estática por omisión:

```
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 estática por omisión también puede establecerse con el mandato **set default network-gateway**; sin embargo, este mandato no surte efecto inmediatamente, permitiendo definir una sola ruta estática por omisión. El ejemplo siguiente crea la misma ruta estática por omisión que el mandato anterior **add route**:

```
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, especificada por las clases de dirección IP definidas en el documento RFC 791:

Clase de dirección 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 valor de máscara por omisión. El mandato siguiente 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>
```

También puede establecerse una ruta de red estática con el mandato **set default subnet-gateway**; sin embargo, este mandato no surte efecto inmediatamente y sólo permite definir una única ruta estática por destino. El ejemplo siguiente crea la misma ruta de red estática que el mandato anterior **add route**:

```
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 que es mayor que la máscara de red para la dirección IP de destino de la ruta. El mandato siguiente crea una ruta estática de subred:

```
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 hacia una dirección IP específica; tiene una máscara 255.255.255.255. El mandato siguiente crea una ruta estática de sistema principal:

```
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 averiguadas dinámicamente a través de los protocolos OSPF y RIP pueden prevalecer sobre las rutas estáticas. Para el protocolo RIP, este comportamiento de prevalencia puede desactivarse. Véase la sección sobre RIP de este capítulo referente a los mandatos **enable/disable override static-routes**

Tanto OSPF como RIP pueden configurarse para anunciar rutas estáticas configuradas a través de interfaces donde están habilitados estos protocolos dinámicos.

Para configurar RIP para que anuncie rutas estáticas, entre el mandato siguiente en el indicador de mandatos `IP config>`

```
IP config> enable sending static-routes dirección-ip-interfaz
```

Para configurar OSPF para que anuncie rutas estáticas, entre el mandato siguiente en el indicador de mandatos `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]?
```

Conocimiento del salto siguiente

La opción de conocimiento del salto siguiente permite al direccionador detectar si un direccionador vecino funciona o no. Cuando esta opción está habilitada, el direccionador determina con más detalle si una ruta estática que utiliza el direccionador vecino como su salto siguiente va a funcionar. También permite que el direccionador establezca sobre qué interfaz de red el salto siguiente de una ruta estática puede alcanzarse cuando este salto está en una subred IP definida en más de una interfaz de red.

Para habilitar esta opción en una interfaz IP concreta, entre el mandato siguiente en el indicador de mandatos de configuración de IP:

```
IP config> enable nexthop-awareness dirección-ip-interfaz
```

Para inhabilitar la opción de conocimiento del salto siguiente en una interfaz IP concreta, entre el mandato siguiente en el indicador de mandatos de configuración de IP:

```
IP config> disable nexthop-awareness dirección-ip-interfaz
```

Sólo se da soporte a la opción de conocimiento del salto siguiente en las redes frame relay donde los direccionadores vecinos soportan ARP inverso.

Establecer una configuración ARP

El protocolo ARP (Address Resolution Protocol) se utiliza para correlacionar direcciones de protocolo con direcciones de hardware antes de que el direccionador remita un paquete. ARP siempre está activo en el direccionador, así que no es necesario hacer ninguna configuración adicional para habilitarlo con sus características adicionales. Sin embargo, si hace falta alterar cualquiera de los parámetros de configuración de ARP (tales como **enable auto-refresh** o **set refresh-timer**, que modifica el temporizador de renovación por omisión), o si es necesario añadir, modificar o suprimir correlaciones de direcciones permanentes, lea el “Utilización de ARP” en la página 637.

Si la emulación de LAN está configurada en una interfaz, se aplican los valores por omisión. Puede utilizarse efectivamente el protocolo ARP sin efectuar ningún cambio.

Habilitación del direccionamiento de subred ARP

Si hay sistemas principales en redes de subredes conectadas que no dan soporte a las subredes IP, utilice el direccionamiento de subred de ARP (que se describe en el documento RFC 1027). Cuando el direccionador está configurado para el direccionamiento de subred de ARP, responderá por proxy a las peticiones de ARP para destino (es decir, fuera de la LAN si el direccionador es él mismo la mejor ruta para el destino y éste está en la misma red natural que el origen). Para funcionar correctamente, todos los direccionadores conectados a una LAN que contenga sistemas principales que no reconocen las subredes deberán configurarse para un direccionamiento de subred ARP.

Si se desea habilitar el direccionamiento de subred ARP, utilice el mandato siguiente:

```
IP config> enable arp-subnet-routing
```

Habilitación del direccionamiento de red ARP

Algunos sistemas principales IP utilizan ARP para todos sus destinos, tanto si el destino está en la misma red natural que el origen como si no lo está. Para estos servidores el direccionamiento de subred ARP no resulta suficiente, pero puede configurarse el direccionador para que responda por proxy a cualquier petición ARP siempre y cuando el destino pueda alcanzarse a través del direccionador y no se encuentre en el mismo segmento de red local que el origen.

Para habilitar el direccionamiento de red ARP, utilice el siguiente mandato::

```
IP config> enable arp-network-routing
```

Filtrado IP

El filtrado permite especificar ciertos criterios que utiliza el direccionador para controlar la emisión de paquetes. Los principales tipos de filtrado que se relacionan a continuación se proporcionan como ayuda para alcanzar sus objetivos administrativos y de seguridad:

- Control de acceso
- Función de políticas (consulte Utilización de la función de políticas en la publicación *Utilización y configuración de las funciones*)
- Filtrado de rutas

Nota: Para IPv4, ahora existe la opción de configurar las reglas de control de acceso en una base de datos de política para designar el control de acceso y determinar cómo se filtran los paquetes IP. Para obtener información más detallada, consulte “Utilización de políticas” en la publicación *Utilización y configuración de las funciones*.

Control de acceso

El control de acceso permite al direccionador IP controlar el proceso de paquetes individuales, basándose en los parámetros siguientes:

- dirección IP de origen
- dirección IP de destino
- número de protocolo IP
- número de puerto de origen TCP o UPD
- número de puerto de destino TCP o UPD
- bits SYN y ACK de TCP
- tipo y código ICMP
- filtrado de preferencia y de tipo de servicio (TOS)

El control de acceso puede limitar la capacidad de un conjunto concreto de sistemas principales y servicios de IP para comunicarse entre sí.

Se pueden definir los controles de acceso configurando listas de control de acceso. Pueden especificarse una lista global y dos listas para cada interfaz. La lista global se aplica al direccionador en su conjunto. Las listas de interfaz, que se conocen también como filtros de paquetes, tienen nombres asignados y se aplican solamente a la interfaz designada. Para cada interfaz se aplica una lista a los paquetes de entrada, mientras que la otra lista se aplica a los paquetes de salida. Las listas se aplican con independencia una de otra. Un paquete podría *pasar* una lista de interfaz de entrada, pero podría ser *descartado* por la lista global.

La Figura 29 ejemplifica la serie de listas de control de acceso por las que debe pasar un paquete antes de reenviarlo.

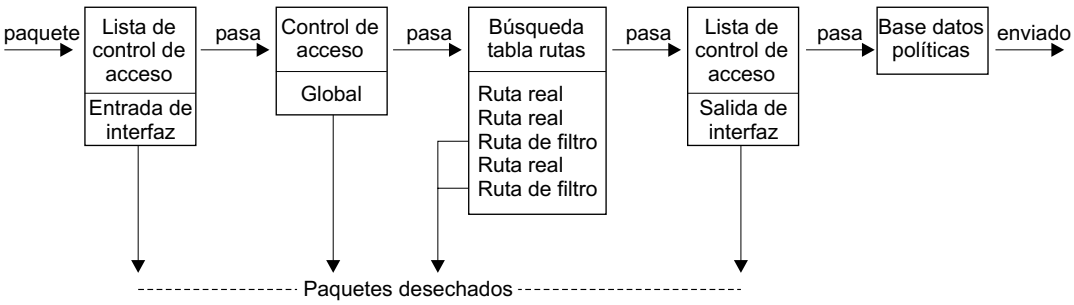


Figura 29. Listas de control de acceso de la vía de reenvío de paquetes

Reglas de control de acceso

Cada lista de control de acceso consiste en una o más reglas de control de acceso que establecen los criterios de filtrado. Algunas reglas de control de acceso definen los filtros globales que afectan todas las interfaces en el direccionador, mientras que otras definen las listas de control de acceso específicas de la interfaz (también denominadas filtros de paquetes). Las reglas globales de control de acceso se configuran con el mandato **add access** en el indicador de mandatos `IP config>`. Los filtros de paquetes se establecen mediante dos mandatos en el indicador de man-

datos `IP config>`: el mandato **add packet-filter** define el filtro, mientras que el mandato **update packet-filter** lo configura.

A medida que los paquetes IP circulan por el direccionador, los campos del paquete 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 concuerda con una regla y el tipo de filtro de la regla es inclusivo, el paquete *pasa*. Si el tipo de filtro de la regla es exclusivo, el paquete se *descarta* y deja de ser procesado por el direccionador. Si, después de pasar por toda la lista, no hay reglas que coincidan, también se descarta el paquete.

Cuando se definen registros en listas de control de acceso, es importante recordar la información siguiente:

- Es importante el orden de los registros de una lista. Se proporcionan mandatos de configuración para cambiar el orden de los registros de una lista.
- Por cada lista que incluya al menos una regla de control de acceso, debe existir una regla inclusiva para que un paquete que no coincida con ninguna de las reglas de control de acceso pase la lista. Un método para permitir que pasen todos los paquetes que no coincidan con las reglas especificadas es incluir la siguiente regla comodín como última regla de la lista :

```
IP config> add access-control
Enter type [E]? i
```

Habilitación del control de acceso

El control de acceso IP (incluido el control de acceso global y de interfaz) se habilita mediante el mandato **set access-control on** y se inhabilita con el mandato **set access-control off**. Pueden utilizarse los mandatos **enable packet-filter** y **disable packet-filter** para habilitar y inhabilitar filtros de paquetes específicos cuando el control de acceso IP está habilitado.

Si el control de acceso IP está habilitado, debe irse con cuidado con los paquetes que el direccionador origina y recibe. Asegúrese de no descartar los paquetes RIP o OSPF que se envíen o reciban a través del direccionador. El modo más fácil de hacerlo es añadiendo una regla comodín inclusiva que aparezca en último lugar de la lista de control de acceso. Como alternativa, también pueden añadirse reglas específicas para RIP y OSPF, quizás con direcciones y máscaras restrictivas. Nótese que algunos paquetes OSPF se envían a las direcciones multidifusión de Clase D 224.0.0.5 y 224.0.0.6, lo que es importante si se realizan comprobaciones de dirección para protocolos de direccionamiento. Véase el mandato **add** para obtener más información sobre el control de acceso.

Definición de la lista global de control de acceso

La lista global de control de acceso se define cuando se añaden reglas en el indicador de mandatos `IP config>` :

```
IP config>  add access-control...
```

Las reglas globales de control de acceso se pueden listar, mover o suprimir mediante los mandatos **list**, **move** o **delete**. Consulte estos mandatos si desea más información sobre ello.

Definición de filtros de paquetes

Para definir filtros de paquetes, que son específicos de la interfaz, utilice el mandato **add packet-filter** en el indicador de mandatos `IP config>`. El direccionador le solicitará el nombre del filtro, la dirección (de entrada o de salida) y el número de interfaz a que se aplica.

```
IP config> add packet filter
Packet-filter nombre [ ]? test
Filter incoming or outgoing traffic? [IN]? in
Which interface is this filter for [0]? 1
```

Puede utilizarse el mandato **list packet-filter** para obtener una lista de todas las listas de control de acceso específicas de interfaz que estén configuradas en el direccionador.

Configuración de reglas de control de acceso para filtros de paquetes

Deben definirse reglas de control de acceso para cada lista definida (filtro de paquetes). De otro modo, los filtros de paquetes definidos no tendrían efecto en el tráfico de entrada o de salida. Utilice el mandato **update packet-filter** en el indicador de mandatos `IP config>` para definir las reglas de control de acceso. El direccionador primero le solicitará el nombre del filtro de paquetes que desea actualizar. Entonces el indicador de mandatos `IP config>` cambia a `Packet-filter 'nombre' Config>`, donde 'nombre' es el nombre de lista que proporciona el usuario.

```
IP config>  update packet-filter
Packet-filter nombre [ ]?  test
Packet-filter 'test' Config>
```

Desde este indicador, se pueden emitir los mandatos **add**, **disableenablelist**, **move** y **delete**. Estos mandatos son similares a aquellos 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 consisten en múltiples parámetros. Algunos de ellos pueden especificarse en todas las reglas de control de acceso, mientras que otros sólo pueden especificarse en las reglas de filtros de paquetes. Los siguientes parámetros pueden especificarse en todas las reglas de control de acceso:

- Tipo (regla inclusiva, exclusiva)
- Dirección de origen y máscara IP
- Dirección de destino y máscara IP
- Rango de números de protocolo IP
- Rango de números de puerto de destino TCP/UDP
- Rango de números de puerto de origen TCP/UDP
- Filtrado de TCP SYN
- Tipo y código de mensaje ICMP
- Soporte de precedencia y de filtrado de TOS
- Direccionamiento basado en una política (seleccionando la pasarela del salto siguiente)
- Opción de recurso de SysLog
- Opciones de anotaciones de seguridad
- Compression-bypass
- Encryption-bypass

Los siguientes parámetros son únicamente para filtros de paquetes:

- Nombre del filtro de paquetes
- Verificación de la dirección de origen

Tipos adicionales:

- Conversión de direcciones de red (NAT)

Tipo: La designación de tipo de una regla de control de acceso determina cómo afecta a los paquetes que coincidan con ella del modo siguiente::

- Una regla *exclusiva* (E) descarta los paquetes.
- Una regla *inclusiva* (I) permite que el direccionador continúe procesando los paquetes.
- Una regla de *conversión de direcciones de red*, o NAT (N), pasa los paquetes a NAT para la conversión de la dirección.

Las reglas de NAT sólo son válidas en filtros de paquetes y únicamente cuando se especifican en combinación con reglas inclusivas (IN). Utilice el programa de configuración para especificar primero reglas inclusivas y, a continuación, para especificar reglas de NAT.

Direcciones y máscaras de origen y de destino IP: Cada regla tiene un par formado por una dirección y una máscara IP para las direcciones IP de origen y las de destino. Cuando un paquete IP se compara con una regla de control de acceso, la dirección IP del paquete se une por medio del operador AND lógico con la máscara de la regla, y el resultado se compara con la dirección de la regla. Por ejemplo, una dirección de origen 26.0.0.0 con una máscara 255.0.0.0 en una regla de control de acceso coincidirá con cualquier dirección de origen IP que tenga 26 en el primer byte. Una dirección de destino 192.67.67.20 con una máscara 255.255.255.255 coincidirá solamente con la de sistema principal de destino IP 192.67.67.20. Una dirección 0.0.0.0 con una máscara 0.0.0.0 es un comodín que coincide con cualquier dirección IP.

Rango de números de protocolo IP: Cada registro también puede tener un rango de números de protocolo IP. Este rango se compara con el byte de protocolo de la cabecera IP; un valor de protocolo que se encuentre dentro del rango especificado por la regla de control de acceso coincidirá (incluyendo los números primero y último del rango). Si se especifica un rango de entre 0 y 255, cualquier protocolo coincidirá. Los números de protocolo habitualmente más utilizados son 1 (ICMP), 6 (TCP), 17 (UDP) y 89 (OSPF).

Rango de números de puerto de origen y de destino TCP/UDP: Si el rango de números de protocolo IP incluye el 6 (TCP) o el 17 (UDP), los rangos de números de puertos TCP/UDP también pueden especificarse en una regla de control de acceso, tanto para los puertos de origen como los de destino. Estos rangos se comparan con el campo del número de puerto de la cabecera TCP o UPD del paquete IP; un valor de número de puerto que se encuentre dentro del rango especificado (incluyendo los números primero y último) coincidirá. Estos campos se ignoran para paquetes IP que no son paquetes TCP o UDP. Si se especifica un rango de 0 a 65535, coincidirá cualquier número de puerto. Los números de puerto que se utilizan habitualmente son 21 (FTP), 23 (Telnet), 25 (SMTP), 513 (rlogin) y 520 (RIP). Consulte el documento RFC 1700 (Assigned Numbers) si desea una lista de los números de protocolo y los números de puerto IP.

Filtrado del establecimiento de conexión TCP (SYN): Si el rango de números de protocolo incluye el 6 (para TCP) y el tipo de filtro es exclusivo, puede definirse un filtrado de establecimiento de conexión TCP. Cuando el filtrado de establecimiento de conexión TCP está habilitado, la regla de control de acceso se aplica a un paquete TCP sólo si ese paquete establece una conexión TCP. (Éstos son los paquetes en que el bit de TCP SYN es 1 y el bit de ACK es 0.)

Tipo y código de mensaje ICMP: Si el rango de números de protocolo incluye el 1 (para ICMP), puede especificarse el tipo y código de mensaje ICMP. Por omisión, se aplica la regla de control de acceso a todos los tipos y códigos de mensaje ICMP.

Precedencia y soporte de filtrado TOS: El direccionador que da soporte a TOS identifica ciertas rutas que proporcionan los niveles de servicio requerido. El direccionador envía paquetes por las rutas según la configuración de sus bits de TOS.

TOS en IP no garantiza ningún tipo concreto de servicio, sino una petición al direccionador que proporcione servicio del nivel requerido. Por ejemplo, un paquete con un campo TOS que requiera una productividad máxima puede ser enviado a través de varios saltos que tengan distintos anchos de banda. Obtendrá un servicio normal- ningún tratamiento especial (si pasa a través de un salto gestionado por un direccionador que no soporta TOS). Véase el mandato **add access-controls** en la página 270 si se desea obtener descripciones de estos parámetros.

También pueden establecerse filtros para proporcionar QoS (Calidad de Servicio) utilizando la característica de Reserva de ancho de banda (Bandwidth Reservation System o BRS). BRS se utiliza con interfaces PPP y frame relay. Consulte los capítulos “Utilización de la reserva de ancho de banda y la cola prioritaria” y “Configuración y supervisión del ancho de banda” en la publicación*Utilización y configuración de las funciones*.

Parámetros para soporte de direccionamiento basado en TOS: Con el fin de habilitar el direccionador para que interprete los bits de TOS y direccione los paquetes según esos bits, se crea una regla de control de acceso desde la cual el direccionador recibirá los paquetes de TOS para filtrado y direccionamiento de Tipo de Servicio. Esta regla de control de acceso se aplica a todas las interfaces del direccionador. Los siguientes parámetros se utilizan para definir los bits de TOS que comparará el direccionador:

- Valor de comienzo de rango para los bits del byte de TOS
- Valor de final de rango para los bits del byte de TOS
- Máscara de filtro para determinar cuáles de los bits del byte de TOS se incluyen en el rango

Modificación de los bits de TOS: Con el fin de habilitar el direccionador para que modifique los bits TOS de paquetes de entrada, se crea una regla de control de acceso desde la cual el direccionador recibirá los paquetes de TOS que deben modificarse. La modificación del valor de los bits de TOS es una actividad separada de la actividad de interpretarlos y dirigir el paquete. Si están configuradas tanto la interpretación como la modificación, ésta se hará después de la interpretación. Los parámetros siguientes de utilizan para definir los bits de TOS que van a modificarse:

- Un valor nuevo para los bits de TOS
- Una máscara de modificación para determinar cuáles de los bits del byte de TOS se cambiarán

Direccionamiento basado en una política (selección de la pasarela de salto siguiente): Los paquetes de entrada pueden filtrarse para dirigirlos a una dirección de pasarela de próximo salto seleccionada manualmente (esto se conoce como direccionamiento basado en una política). Para hacer esto, debe crearse una regla de control de acceso de entrada inclusiva sea global, para el direccionador, o bien para una interfaz concreta, y proporcionar los parámetros siguientes:

- Utilización o no de un direccionamiento basado en una política.
- La dirección IP de la pasarela para el salto siguiente
- Si se envía o no el paquete usando la tabla normal de direccionamiento en el caso de que el salto siguiente no esté disponible

Opción de recurso de SysLog: SysLog es una opción de anotaciones que genera un mensaje de SysLog para un servidor de anotaciones remoto. Si SysLog está habilitado, la opción de recurso de SysLog especifica qué recurso de SysLog se utiliza para anotaciones remotas. Esta opción, cuyo valor por omisión es *User*, define el archivo de anotaciones remoto donde pueden almacenarse y posteriormente analizarse los mensajes de SysLog. La opción de recurso de SysLog se visualiza tanto en el programa de configuración como en la interfaz de línea de mandatos.

Opciones de anotaciones de seguridad: Si se habilitan las anotaciones de seguridad, puede especificarse parte o la totalidad de de estas opciones de anotaciones:

- Mensajes de ELS
- Condiciones de excepción de SNMP
- SysLog

También puede especificarse si los mensajes de ELS y SysLog pueden utilizar un formato de mensaje *corto* o *largo*. Las condiciones de excepción de SNMP pueden estar *habilitados* o *inhabilitados*. Si Si no se especifica ninguna opción de anotaciones, las anotaciones de seguridad estarán inhabilitadas.

También puede configurarse el nivel de prioridad de SysLog. Éste especifica el nivel del mensaje de error que se visualizará, como por ejemplo *Emergency* o *Information*. El valor por omisión es el valor por omisión del sistema del direccionador. Los niveles de prioridad de SysLog se visualizan tanto en el programa de configuración como en la interfaz de la línea de mandatos.

Los mensajes SysLog se envían a un servidor remoto y se guardan en los archivos de SysLog de la opción de recurso de SysLog actual.

Nombre de filtro de paquetes: Este parámetro específico de la interfaz puede consistir en cualquier nombre. Puede tener hasta 16 caracteres de longitud, pudiendo incluir guiones (-) y guiones de subrayado (_). Pueden configurarse hasta dos listas de registro de control de acceso para cada nombre de filtro de paquetes, una para paquetes de salida y otra para paquetes de entrada.

Verificación de dirección de entrada: Esta opción de filtro de paquetes de entrada verifica si la dirección IP de origen de un paquete de entrada es coherente con la interfaz para la cual se ha recibido el paquete, basándose en la tabla de direccionamiento IP. Esta opción ayuda a impedir el reenvío de paquetes desde un sistema principal IP con un comportamiento erróneo que esté utilizando una dirección de origen IP que no le pertenece, comportamiento que se conoce como *usurpación*.

Ejemplos: El ejemplo siguiente permite a cualquier sistema principal enviar paquetes al socket de SMTP TCP en 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 ejemplo siguiente impide a un sistema principal en la subred 1 de la red de Clase B 150.150.0.0 enviar paquetes a sistemas principales en la subred 2 de la red de Clase B 150.150.0.0 (suponiendo 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 global de control de acceso. Se entran valores que habiliten la interpretación de los bits de TOS de paquetes que lleguen desde la dirección IP 9.1.2.3 y cambien los valores de estos bits antes de enviar los paquetes. Léase “Add” en la página 270 para obtener una explicación del significado de los parámetros que crean el filtrado de TOS y el direccionamiento basado en una política.

```
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]):
```

Filtrado de rutas sin políticas

El filtrado de rutas afecta el reenvío de paquetes, ya que incfluye en el contenido de la tabla de direccionamiento. En general, el filtrado de rutas es más eficaz pero menos flexible que el control de acceso. El filtrado basado en campos del paquete que no sea la dirección IP de destino puede hacerse utilizando el control de acceso, que se describe más arriba, o bien utilizando políticas de filtrado de ruta como las descritas en “Filtrado de rutas con políticas” en la página 253.

Los métodos siguientes se utilizan en este direccionador para influir en el contenido de la tabla de direccionamiento.

- Rutas de filtro
- filtros de entrada de RIP
- filtrado de tablas de rutas

Definición de rutas de filtro

Se 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 referente a ellos no se anunciará. Las rutas de filtro ***no*** se recomiendan cuando se utiliza OSPF en la red; las rutas internas averiguadas por OSPF prevalecen sobre las rutas filtradas en la tabla de direccionamiento.

Para configurar una ruta de filtrado, entre el mandato siguiente en el indicador de mandatos `IP config>`:

```
IP config>  add filter  dest-IP-address  address-mask
```

Las rutas de filtro aparecerán enumeradas como una entrada del tipo *fltr* cuando se utilice el mandato **dump** para ver la tabla de direccionamiento de IP.

Nota: Si está disponible una ruta más específica, los paquetes se reenviarán allí. Por ejemplo, si se define una ruta de filtrado para la red 9.0.0.0 (máscara 255.0.0.0), pero se averigua una ruta para una subred de la red (por ejemplo 9.1.0.0, máscara 255.255.0.0), entonces los paquetes se reenviarán a la subred 9.1.0.0 pero no a otras subredes de esa red.

Definición de filtros de entrada de RIP

Cuando se utiliza RIP como el protocolo de direccionamiento dinámico, pueden configurarse algunas interfaces para que se ignoren rutas en las actualizaciones de RIP.

El mandato siguiente tiene como resultado que se ignoran todas las actualizaciones de RIP recibidas en una interfaz:

```
IP config>  disable receiving rip  dirección-ip-interfaz
```

Los mandatos siguientes tienen como resultado que se ignoren algunos tipos de rutas recibidas en una interfaz:

```
IP config> disable receiving dynamic nets dirección-ip-interfaz
IP config> disable receiving dynamic subnets dirección-ip-interfaz
IP config> disable receiving dynamic host dirección-ip-interfaz
```

Si se requiere un filtrado de rutas de RIP menos fino, pueden utilizarse las políticas de ruta que se describen en el mandato siguiente:

```
IP config> add accept-rip-route dirección-ip-red/subred/sistema-principal
```

Definición de filtrado de tablas de rutas

Cuando está habilitado el filtrado de tablas de ruta y se han definido filtros de ruta, se realiza una comprobación antes de añadir rutas a la tabla de direccionamiento de IP. Si la ruta a añadir coincide con un filtro de ruta inclusivo, se añadirá a la tabla de direccionamiento de IP. Si coincide con un filtro de ruta exclusivo, no se añadirá a la tabla de direccionamiento de IP. Las rutas directas y estáticas nunca serán filtradas.

Esta función puede utilizarse para impedir que se añadan rutas a la tabla de direccionamiento de IP en situaciones donde el administrador de la red no desea

que todas las rutas se anuncien, haciendo disponibles los protocolos de direccionamiento. Esta función puede utilizarse en el entorno de un proveedor de servicios para impedir que los clientes tengan acceso a las redes de los demás.

Filtrado de rutas con políticas

Las políticas de filtros de rutas son definiciones que describen una ruta o conjunto de rutas. Una política de filtros de rutas consiste en el nombre de la política de filtros de la ruta y al menos una entrada que defina una dirección o rango de direcciones para que se filtre la ruta. Cada entrada incluye instrucciones que incluyen o excluyen las rutas definidas en esa entrada de la tabla de direccionamiento. Las políticas de filtros de rutas pueden usarse para filtrar las rutas que RIP y OSPF instalan en la tabla de reenvíos IP y anuncian desde la tabla de reenvíos de IP.

Una política de filtros de rutas se identifica con una serie de 15 caracteres ASCII, como por ejemplo *ospf-import*. Después de nombrar la política de filtros de rutas, es necesario configurar como mínimo una entrada que se asocie con esa política de filtros de rutas. Utilice el mandato **add route-policy** en el indicador de mandatos `IP config>` para añadir la política, el mandato **change route-policy** para provocar la aparición del indicador de mandatos `IP Route Policy Config>` y, finalmente, el mandato **add entry** en el indicador de mandatos `IP Route Policy Config>` para definir cada entrada de la política.

Es necesario que se asigne un número de índice a cada entrada el configurar ésta. Este número se utiliza para identificar la entrada para establecer coincidencias.

El emparejamiento se realiza mediante *coincidencia lineal* o mediante *búsqueda de la coincidencia más larga*. Puede seleccionarse uno de estos métodos al utilizar el mandato **add route policy** para crear la política de filtros de rutas. Si se escoge la coincidencia lineal, la ruta que se filtre se comparará con las entradas de la lista, una después de la otra, basándose en el número de índice. Cuando se encuentra una coincidencia, se filtra la ruta. Si se escoge la búsqueda por coincidencia más larga, la ruta que se filtra se compara con las entradas de filtro según la búsqueda de coincidencia más larga. Si hay más de una entrada que especifique la misma dirección y máscara IP, entonces la ruta que se filtra se compara siguiendo un orden ascendente, según el número de índice.

Por ejemplo, supongamos que se desea excluir las direcciones para la red 9.8.0.0 con la máscara 255.255.0.0, pero desea incluirse la dirección de sistema principal 9.8.1.8 con la máscara 255.255.255.255. Según el método de filtrado de búsqueda de la coincidencia más larga, el usuario 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. Entonces, de entre todas las direcciones de esa subred, sólo se incluirá 9.8.1.8.

Para obtener el mismo resultado utilizando la coincidencia lineal, tendría que asignarse un número de índice más bajo al filtro inclusivo que al filtro exclusivo. Por ejemplo, la dirección 9.8.1.8 con la máscara 255.255.255.255 requiere un número de índice más bajo que la dirección 9.8.0.0 con la máscara 255.255.0.0. De otro modo, 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 cómo se procesará la máscara de dirección para la entrada. Si este parámetro es *exacto*, el software hará coincidir la ruta sólo en la dirección y máscara exactas especificadas por la entrada y no tendrá en cuenta la dirección como un rango. Si el tipo de coinci-

dencia es *rango*, el direccionador leerá la dirección y la máscara como un rango y coincidirá con la ruta si ésta se encuentra dentro del rango.

Además de las entradas, también pueden configurarse acciones y condiciones de coincidencia asociadas con cada entrada. Las acciones son cambios efectuados en la ruta antes de que se anuncie, como establecer una métrica en una ruta. Las condiciones de coincidencia hacen cambiar las reglas según las cuales se selecciona la ruta. Cuando se encuentra una coincidencia basada en la dirección de destino, la condición de coincidencia establece entonces más limitaciones a la coincidencia. Por ejemplo, si la condición de coincidencia es el protocolo BGP, las rutas no coinciden a no ser que coincida la dirección de entrada y además el paquete pertenezca al protocolo BFP. Éstas son las condiciones de coincidencia:

- Protocolo, tal como RIP, OSPF o BGP
- número de AS (sistema autónomo)
- Dirección de pasarela para el salto siguiente de la ruta
- Número de red para el salto siguiente de la ruta
- Rango métrico
- La pasarela de origen, que puede aplicarse sólo a la política de recepción de RIP

Las acciones y condiciones de coincidencia, que ayudan a refinar el proceso de filtrado de la entrada, son opcionales.

Políticas de filtros de direccionamiento de límites de AS para OSPF

Si se utiliza una política de filtros de rutas para controlar las tablas de direccionamiento de OSPF, la configuración se hace durante la configuración de OSPF. Véase el mandato **enable** en la página 390 si se desea más información.

Políticas de filtros de envío y recepción para RIP

Pueden utilizarse políticas de filtros de rutas para definir qué rutas enviará o recibirá RIP. Estas políticas de filtros de rutas pueden configurarse globalmente, para todas las interfaces IP del direccionador o para cada interfaz IP. Si se habilita una política de filtros de rutas de envío, todas las rutas que sean conformes a la política se anunciarán, ignorándose los valores para *default-routes*, *host-routes*, *net-routes*, *subnet-routes* y *static-routes*. Los valores para las rutas *poison-reverse-routes*, *ripv1-only routes* y *outage-only* no se ven afectados por la política de filtros de rutas de envío. Si el envío *all-routes* está inhabilitado, no se anunciarán rutas, aunque se haya especificado una política global de envío.

Si se configura una política de filtros de rutas de recepción y está habilitada la recepción de RIP, la política configurada sustituirá cualquier tipo de rutas dinámicas, tanto si están habilitadas como si están inhabilitadas. En otras palabras, se aceptarán todas las rutas incluidas en la política de filtros de rutas conformes con las restricciones del protocolo RIP.

Agregación de ruta

Para reducir la proliferación de información de direccionamiento en las tablas de direccionamiento de los direccionadores limítrofes, el 2212 ofrece la agregación de ruta. Esta posibilidad permite utilizar una dirección IP y una máscara de subred para definir un rango de subredes pertenecientes a diferentes dominios de direccionamiento.

En todos los direccionadores se produce un cierto nivel de agregación, puesto que generan las rutas con clase correspondientes a cada conjunto de rutas de subred. Esta agregación automática puede inhabilitarse habilitando el soporte de direccionamiento sin clase mediante la configuración IP. Por ejemplo, un direccionador generará la ruta 10.0.0.0/255.0.0.0 siempre y cuando haya rutas de subred dentro de la red 10. A continuación, los protocolos que no dan soporte a las subredes de longitud variable (por ejemplo, RIPv1) pueden anunciar dicha ruta.

Si se configura la agregación de ruta en el direccionador, se puede sustituir los dos rangos de direcciones por una dirección agregada nueva que identifique los dominios RIPv2 y OSPF. La ruta agregada definida en el ejemplo es 10.0.0.0 y tiene la máscara de subred 255.254.0.0. Esta única dirección agregada se anuncia a los dominios RIPv2 y OSPF. Éste es un ejemplo sencillo. Dependiendo de las circunstancias, una ruta agregada puede servir para representar varios dominios y no sólo dos.

Las rutas agregadas pueden configurarse para que se generen incondicionada o condicionadamente. Si la generación es incondicionada, se generarán tanto si hay rutas de componente como si no. Si una ruta agregada es incondicionada, se debe configurar un valor de métrica.

Si una ruta agregada se genera condicionadamente, la métrica derivará de su política o de la política de una ruta de componente. Las rutas agregadas generadas condicionadamente deben estar obligatoriamente asociadas a una política de filtros de rutas. Para ello, se debe proporcionar un identificador de política de ruta para la ruta agregada. En este caso, la ruta agregada se anuncia sólo cuando una ruta de componente queda disponible. Las rutas de componente cumplen dos requisitos:

- Tienen una dirección de destino que está comprendida en el rango definido por la ruta agregada.
- Cumplen todas las condiciones definidas por la política de filtros de rutas asociada.

Por ejemplo, la ruta cuya dirección de destino es 10.3.34.216 constituye una ruta de componente de la ruta agregada 10.0.0.0/255.252.0.0 si la política de filtros de rutas que se ha asociado a esta ruta agregada no tiene ninguna otra condición más que el rango de direcciones. En el apartado “Filtrado de rutas con políticas” en la página 253 hallará más información sobre las políticas de filtros de rutas.

Utilización de la agregación de ruta en RIP y OSPF

RIP y OSPF son dos de los protocolos que importan y exportan información de direccionamiento. La agregación de ruta se utiliza en el contexto de protocolos como éstos que anuncian la información de direccionamiento mediante la red IP. En los siguientes párrafos se explica el modo de implementar la agregación de ruta para RIP y OSPF.

Para el mandato de configuración de IP **enable**, se da soporte a una opción nueva, **enable sending aggregate-routes**. Esta opción permite a RIP determinar si ha de anunciar o no las rutas agregadas. En el caso de RIPv1, no se anunciarán las rutas agregadas a menos que se adhieran a las restricciones de las políticas RIPv1.

Para la política de límites de AS OSPF, se da soporte a una pregunta nueva sobre rutas agregadas para el mandato **enable as boundary routing**. La pregunta es si

se han de importar las rutas agregadas en OSPF como rutas externas OSPF. Esta pregunta no se visualiza si se configura una política de filtros de rutas.

Las políticas de filtros de rutas sirven para filtrar las rutas agregadas que enviará RIP o que importará OSPF. Para identificar una entrada de política de filtros de rutas que se utilizará para filtrar rutas agregadas, se ha añadido una condición de coincidencia nueva a la configuración de políticas de filtros de rutas. Se trata del protocolo *Aggregate*. Cuando una entrada de política de filtros de rutas tiene esta condición de coincidencia, la política de filtros de rutas se aplica sólo a las rutas agregadas.

El ejemplo siguiente muestra el modo de utilizar una política de filtros de rutas para filtrar las rutas agregadas que envía RIP.

Ejemplo:

Primero, se añade una política de ruta que permita las agregadas. La segunda entrada de este ejemplo de configuración es opcional. No es necesario excluir las rutas que no coinciden con la entrada 1 porque el comportamiento por omisión de una política de filtros de rutas es excluir aquellas rutas que no coincidan con ninguna de las entradas de política de ruta.

```
IP config>add route-policy
Route Policy Identifier [1-15 characters] []? all-aggregates
Use strictly linear policy? [No]:
IP config>change route-policy
Route Policy Identifier [1-15 characters] []? all-aggregates
all-aggregates IP Route Policy Configuration
IP Route Policy Config>add entry 1
IP Address [0.0.0.0]?
IP Mask [0.0.0.0]?
Address Match (Range/Exact) [Range]?
Policy type (Inclusive/Exclusive) [Inclusive]?
IP Route Policy Config>
IP Route Policy Config>add entry
Route Policy Index [1-65535] [0]? 2
IP Address [0.0.0.0]?
IP Mask [0.0.0.0]?
Address Match (Range/Exact) [Range]?
Policy type (Inclusive/Exclusive) [Inclusive]? exclusive
```

Se añade una condición de coincidencia para el protocolo Aggregate. Este parámetro permite que la política de filtros de rutas procese únicamente las rutas agregadas.

```
IP Route Policy Config>add match-condition protocol aggregate
 Route Policy Index [1-65535] [0]? 1
Route policy entry match condition updated or added
IP Route Policy Config>exit
```

Se elabora un listado de la política de filtros de rutas:

```
IP config>list route-policy all-aggregates

                Route Policy: all-aggregates (0x3904)


IP Address      IP Mask           Match  Index  Type
-----------------------------------------------------
0.0.0.0         0.0.0.0           Range  1      Include
    Match Conditions:  Protocol: Aggregate
0.0.0.0         0.0.0.0           Range  2      Exclude
```

Se anuncian las agregadas en RIP por medio de la política *all-aggregates*.

```
IP config>enable sending policy global
Route Policy Identifier [1-15 characters] [ ]? all-aggregates
```

Se activa la política por medio de la consola (Talk 5) restableciendo IP dinámicamente. Se visualiza el estado de ejecución de RIP mediante la consola.

```
IP>reset ip
IP>RIP
                                RIP Interfaces

Interface-Addr  Interface-Mask  Version  In Out  Send-Flags       Receive-Flags
10.69.1.1       255.255.255.0      1      1   0  OFF              N,S
153.2.2.25      255.255.255.240    1      1   0  Global,D,P       N,S,H
10.2.1.1        255.255.255.0      1      1   0  Global,P         N,S
Send Flags: A=Aggr N=Network S=Subnet H=Host St=Static D=Default O=Outage-Only
            P=PoisonReverse Policy=Send-Policy Global=Global-Send-Policy
Recv Flags: N=Network S=Subnet H=Host OSt=Override-Static OD=Override-Default
            Policy=Receive-Policy Global=Global-Receive-Policy

        RIP Policy

Interface-Address  Send Policy        Receive-Policy
10.69.1.1          all-aggregates     Not-Applicable
153.2.2.25         all-aggregates     Not-Applicable
10.2.1.1           all-aggregates     Not-Applicable
RIP global receive policy: NONE
RIP global send policy: all-aggregates
```

RIP siempre origina el valor por omisión con coste 5.

Configuración del proceso de reenvío BOOTP/DHCP

BOOTP (descrito en los documentos RFC 951 y RFC 1542) es un protocolo de arranque que se utilizan las estaciones de trabajo sin disco para averiguar su dirección IP, la ubicación del archivo de arranque y el nombre del servidor de arranque. El protocolo DHCP (Dynamic Host Configuration Protocol), descrito en el documento RFC 2131, se utiliza para asignar de un servidor direcciones de red reutilizables y parámetros de configuración específicos del sistema principal.

Los términos siguientes son de utilidad al tratar el proceso de reenvío de BOOTP/DHCP:

- *Cliente* - la estación de trabajo que requiere los servicios BOOTP/DHCP.
- *Servidor* - el sistema principal de arranque (con UNIX daemon bootpd, una versión de DOS disponible desde sofware FTP o OS/2) o cualquier otro ser-

vidor DHCP/BOOTP que proporcione estos servicios. El direccionador puede proporcionar la función de servidor DHCP/BOOTP. Consulte el apartado "Utilización del servidor DHCP" de la publicación *Utilización y configuración de las funciones*.

- *Agente de retransmisión BOOTP* o *reenviador BOOTP* - dispositivo que reenvía las peticiones/respuestas intercambiadas entre el cliente y el servidor. Este direccionador puede proporcionar la función de agente de retransmisión.

A continuación se esbozan un ejemplo de los pasos a seguir en el proceso de reenvío de BOOTP. (los intercambios DHCP funcionan de manera similar):

1. El cliente copia su dirección Ethernet (o una dirección MAC apropiada) en un paquete BOOTP y la difunde en la LAN local. BOOTP se ejecuta encima de UDP.
2. El agente de retransmisión local de BOOTP recibe el paquete y comprueba que su formato sea correcto y que el número máximo de saltos de aplicación no ha expirado. También comprueba que el intento del cliente tiene una duración mínima.

   Nota: Si se requiere más de un salto antes de alcanzar el agente de BOOTP, el paquete es direccionado normalmente vía IP. Los otros direccionadores no examinan el paquete para determinar si es o no un paquete de BOOTP.
3. El agente local de BOOTP reenvía una petición BOOTP separada a cada uno de los servidores añadidos. La petición BOOTP es la misma que la que fue enviada inicialmente por el cliente, excepto en que tiene una nueva cabecera IP con la dirección IP del agente de retransmisión copiada en el cuerpo de la petición BOOTP.
4. El servidor recibe la petición y efectúa una búsqueda de la dirección del hardware del cliente (por ejemplo, Ethernet) en su base de datos. Si se encuentra, da formato a una respuesta de 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 entonces al agente de retransmisión de BOOTP.
5. El agente de retransmisión de BOOTP recibe la respuesta y hace una entrada en su tabla de ARP para el cliente, reenviando a continuación la respuesta al cliente.
6. El cliente entonces continúa rearrancando utilizando TFTP con la información del paquete de respuesta de BOOTP.

Habilitación/inhabilitación de reenvíos de BOOTP

Para habilitar o inhabilitar el reenvío de BOOTP en una interfaz IP concreta, entre el siguiente mandato en el indicador de mandatos de configuración de IP (habilite el reenvío de BOOTP para permitir que el direccionador reenvíe peticiones y respuestas de BOOTP y/o DHCP entre clientes y servidores de segmentos distintos de la red.)

```
IP config> enable/disable bootp
```

Nota: La función de servidor DHCP que se describe en el apartado "Utilización del servidor DHCP" de la publicación *Utilización y configuración de las funciones* y este proceso de reenvío de BOOTP no deberían estar habilitados

en el mismo direccionador. Si ambos están habilitados, el dispositivo de servidor de DHCP prevalecerá y el reenvío de BOOTP no tendrá lugar.

Al habilitar BOOTP, se le solicitarán los valores siguientes:

- Número máximo de saltos de aplicación por los que se desea que pase la petición de BOOTP. Éste es el número máximo de agentes de retransmisión de BOOTP que pueden reenviar el paquete. ***No*** es el número máximo de saltos IP al servidor. Un valor típico para este parámetro es 1.
- El número de segundos que se desea que el cliente reintente antes de reenviar la petición de BOOTP. *Este parámetro no se utiliza habitualmente.* Un valor típico de este parámetro es 0.

Después de aceptar una petición de BOOTP, el direccionador reenvía la petición de BOOTP a cada servidor de BOOTP. Si hay más de un servidor configurado para BOOTP, el direccionador replica el paquete.

Adición de un servidor BOOTP/DHCP

Para añadir un servidor de BOOTP o DHCP a la configuración del agente de relay del direccionador , entre el mandato siguiente en el indicador de mandatos de configuración de IP:

```
IP config> add bootp-server dirección-IP-servidor
```

Puede configurarse más de un servidor. Además, si solamente se conoce el número de red del servidor o bien si hay más de un servidor que resida en el mismo segmento de red, puede configurarse una dirección de difusión para el servidor.

Integración de IP y SNA

Puede utilizarse TN3270E para integrar IP y SNA. Consulte el capítulo titulado “Utilización de APPN” en la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 2* y el capítulo titulado “Configuración y supervisión de APPN” en la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 2* si desea obtener más información acerca de TN3270E.

Configuración de reenvío de UDP

El protocolo UDP, descrito en el documento RFC 768, es un protocolo de capa de transporte que proporciona servicio sin conexión utilizando el protocolo IP. Con el reenvío de UPD, los paquetes de UPD que se reenvían localmente (como UDP difundido en una LAN IBM 2212 conectada a 2212) puede reenviarse a un destino IP concreto o bien a una red de destino como difusión dirigida.

Por ejemplo, NetBIOS utiliza difusiones de UDP en algunas aplicaciones de cliente-servidor para difundir los paquetes Name-Query. A no ser que se haya configurado el reenvío de UDP, el direccionador descarta estos paquetes; de este modo el direccionador no reenviará los paquetes difundidos más allá de la red local.

Para configurar el reenvío de UDP es necesario seguir estos pasos:

1. Añadir un número de puerto de destino y dirección IP para UDP. El direccionador correlaciona esta dirección IP con el puerto UDP.

```
IP config> add udp-destination
UDP port number [-1] 36
Destination IP address [0.0.0.0] 20.1.2.2
```

2. Habilitar el Reenvío de UDP.

```
IP config>enable udp-forwarding
For which UDP port number [-1] 36
```

En este ejemplo, el direccionador reenvía los paquetes que recibe para el puerto de UDP 36 a la dirección IP 20.1.2.2.

Entre **list udp-forwarding** para ver la configuración de Reenvío de UDP.

Habilitación/inhabilitación de reenvío de UDP

Para habilitar o inhabilitar el reenvío de UDP en el direccionador, entre el mandato en el indicador de mandatos de configuración de IP. (Habilítese el reenvío de UDP para permitir al direccionador reenviar los paquetes de Difusión por UDP a una dirección determinada según el criterio de un puerto por UDP.

```
IP config> enable/disable udp-forwarding número de puerto
```

Adición de un destino UDP

Los destinos de reenvío de UDP se añaden especificando la dirección IP a la que tienen que reenviarse los paquetes, seguida del número de puerto. Para añadir un destino de UDP, entre el mandato siguiente en el indicador de mandatos de configuración de IP:

```
IP config> add udp-destination port-number dest-ip-address
```

Configuración del protocolo VRRP (Virtual Router Redundancy Protocol)

El uso de una ruta por omisión configurada estáticamente es una práctica habitual en las configuraciones IP de sistema principal. Minimiza el nivel de actividad general derivado de la configuración y el proceso, y está soportado por prácticamente todas las implementaciones IP. Es más probable que se dé esta modalidad de funcionamiento cuando se despliegan protocolos de configuración dinámica de sistema principal, ya que éstos normalmente proporcionan configuración para una dirección IP de sistema principal final y una pasarela por omisión. Sin embargo, esto crea un único punto de error. La pérdida del direccionador por omisión tiene un resultado catastrófico al provocar el aislamiento de todos los sistemas principales finales incapaces de detectar una vía alternativa disponible.

El protocolo VRRP (Virtual Router Redundancy Protocol) está diseñado para eliminar este único punto de error inherente al entorno de direccionamiento por omisión estático. VRRP especifica un protocolo de elección que, de forma dinámica, permite que un conjunto de direccionadores se respalden mutuamente. El direccionador VRRP que controla una o más direcciones IP se denomina direccionador maestro, y reenvía los paquetes enviados a estas direcciones IP. El proceso de elección proporciona una función dinámica de conmutación por anomalía, respecto a quién debe hacerse cargo del reenvío, si por alguna razón el direccionador maestro dejase de estar disponible. En ese caso, los sistemas principales finales pueden utilizar cualquiera de las direcciones IP de un direccionador virtual como direccionador de primer salto por omisión. La ventaja de utilizar VRRP es que se consigue una vía por omisión con un mayor grado de disponibilidad, sin

tener que configurar el direccionamiento dinámico ni protocolos de descubrimiento de direccionador en cada sistema principal final.

Para utilizar y configurar, VRRP primero debe definirse un ID de direccionador virtual (VRID) en cada segmento de LAN en el que se ejecute VRRP. El VRID es un número comprendido entre 1 y 255. Identifica los direccionadores que se respaldarán mutuamente. Por lo tanto, todos los direccionadores VRRP que sean dispositivos de reserva entre sí deben tener el mismo VRID. Para cada segmento VRRP, existe un direccionador, denominado direccionador maestro, que es el propietario de la dirección IP por omisión configurada para los sistemas principales del segmento de LAN. Mientras el direccionador maestro está disponible, responde a las peticiones ARP dirigidas a dicha dirección y reenvía los paquetes. Uno de los direccionadores de reserva ocupa el lugar del direccionador maestro, si éste deja de estar disponible. Cuando un direccionador de reserva toma el control, se puede acceder a él en la dirección IP por omisión y, de esta forma, los sistemas principales lo utilizarán como direccionador maestro.

El VRID representa una dirección MAC virtual de unidifusión o de multidifusión. Puede configurar los direccionadores de reserva con una dirección MAC virtual o bien puede configurar cada uno de los direccionadores VRRP de manera que utilice la dirección MAC de hardware exclusiva que tiene estampada. Si utiliza la opción de multidifusión, no puede utilizar la dirección MAC de hardware. Si utiliza la dirección MAC de hardware, los sistemas principales que se comunican con el direccionador VRRP deben dar soporte a los ARP gratuitos. La utilización de la dirección MAC de hardware puede aportar una mejora de rendimiento a la red.

El ejemplo siguiente sirve de ilustración de una topología VRRP muy simple. En él, se utiliza la dirección MAC virtual. Si se utilizase la dirección MAC de hardware, el direccionador maestro y el de reserva utilizarías sus respectivas direcciones MAC de hardware.

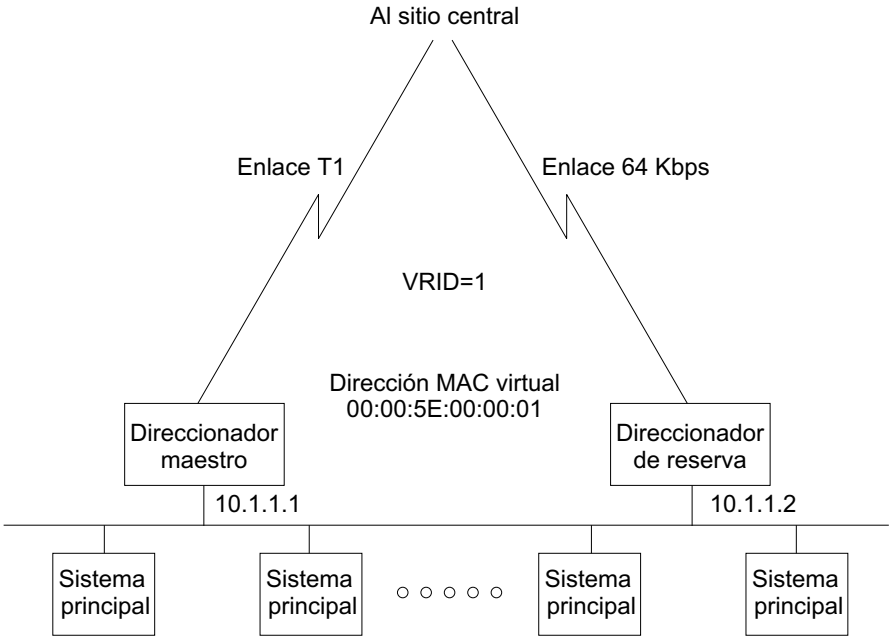


Figura 30. Ethernet LAN con subred 10.1.1.0/255.255.255.0. Todos los sistemas principales están configurados con la pasarela por omisión 10.1.1.1

1. Todos los sistemas principales están configurados con la pasarela por omisión 10.1.1.1
2. El direccionador maestro contestará todas las peticiones de ARP para 10.1.1.1 con la dirección virtual MAC 00:00:5E:00:00:01.
3. El direccionador maestro reenviará paquetes dirigidos a la dirección virtual MAC.
4. Si el direccionador maestro no está disponible, el direccionador de reserva determina este hecho dada la ausencia de anuncios de VRRP y empezará a recibir paquetes dirigidos a la dirección virtual MAC. El direccionador de reserva también contestará las peticiones de ARP para 10.1.1.1.

Una topología complicada sería una en la cual hay múltiples direccionadores de VRRP y se desea equilibrar la carga entre ellos, aunque conservando las capacidades de reserva completas. En este caso haría falta definir 2 VRID y cada direccionador sería el maestro de un VRID y la reserva para el otro. A modo de ejemplo:

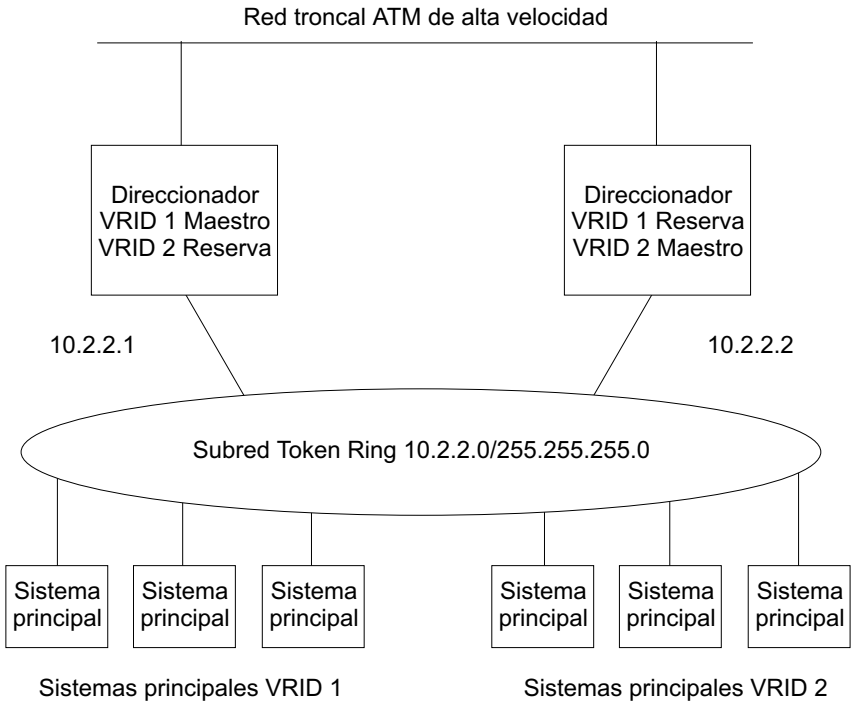


Figura 31. Direccionadores VRRP múltiples

1. Todos los sistemas principales VRID1 se configurarán con la dirección de pasarela por omisión 10.2.2.1.
2. Todos los sistemas principales VRID2 se configurarán con la dirección de pasarela por omisión 10.2.2.2.
3. El direccionador maestro VRID1 responderá peticiones ARP para la dirección 10.2.2.1 con la dirección virtual MAC C0:00:00:10:00:00. También recibirá y reenviará paquetes dirigidos a la dirección virtual MAC C0:00:00:10:00:00.
4. El direccionador maestro VRID 2 responderá peticiones ARP para la dirección 10.2.2.2 con la dirección MAC virtual C0:00:00:20:00:00. También recibirá y reenviará paquetes dirigidos a la dirección virtual MAC C0:00:00:20:00:00.

5. Si alguno de los dos direccionadores no se encuentra disponible, el otro se hará cargo.
6. Si lo que le sucede a un direccionador no es que no esté disponible, sino que pierde su conectividad externa, redirigirá el tráfico a través del otro servidor con redireccionamientos ICMP (suponiendo que los 2 direccionadores están intercambiando rutas a través de un protocolo de direccionamientos como RIP o OSPF).

Se da soporte a VRRP en Ethernet, Fast Ethernet, y Red en anillo.

El VRRP de multidifusión no está soportado en las redes de puente cuando las LAN con direccionamiento en origen forman parte de la red puenteada. Esta restricción sólo se aplica en topologías donde IP está configurado en la red de puente.

Configuración de la pasarela IP por omisión redundante

Esta sección esboza los pasos a seguir para configurar pasarelas IP por omisión redundantes en una ELAN. La configuración de una pasarela redundante permite que las estaciones finales con pasarelas por omisión configuradas manualmente continúen pasando tráfico a otras subredes en el caso de que su pasarela primaria se desactive.

Para configurar un dispositivo con una pasarela primaria 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 esté utilizada por ninguna interfaz en la ELAN. Para determinar qué direcciones MAC se utilizan, consulte “Database List” en el capítulo “Supervisión de los servicios de emulación de LAN” en la publicación *Guía del usuario de software*.
3. Seleccione un dispositivo para que tenga la pasarela primaria. Este dispositivo debe tener una interfaz LEC en la ELAN de la estación final.
4. Seleccione un dispositivo o conjunto de dispositivos para la pasarela de reserva. Este dispositivo o conjunto de dispositivos deben tener una interfaz LEC en la ELAN de la estación final.
5. Configure una pasarela redundante en cada dispositivo, utilizando la opción“Add” para IP.

Nota: La pasarela primaria y la pasarela de reserva deben tener la misma dirección MAC

Soporte multidifusión IP

La multidifusión IP es una extensión de multidifusión de LAN a una Internet de TCP/IP. Es la capacidad que tiene un sistema principal IP para enviar un solo datagrama (denominado datagrama de multidifusión IP) a múltiples destinos. Los datagramas de multidifusión IP se identifican como aquellos paquetes cuyos destinos son direcciones IP de Clase D (es decir, cuyo primer byte se encuentra en el rango de 224 a 239). Cada dirección de Clase D define un grupo de multidifusión.

Las extensiones que se requiere que tenga un sistema principal IP para participar en multidifusión IP se especifican en el documento RFC 1112 (Host Extensions for IP Multicasting). Este documento define un protocolo, IGMP (Internet Group Management Protocol), que permite que los sistemas principales se unan a un grupo de multidifusión o lo dejen. Este direccionador implementa las funciones del protocolo IGMP que le permitan hacer el seguimiento de la pertenencia a un grupo IP en las LAN físicas locales o en sus LAN emuladas mediante el envío de consultas IGMP de pertenencia a sistemas principales y la recepción de Informes IGMP de pertenencia a sistemas principales.

Un direccionador también debe ser capaz de direccionar datagramas de multidifusión IP entre los sistemas de origen y de (múltiples) destino(s). Este direccionador soporta el protocolo MOSPF (Multicast Open Shortest Path First) tal como está definido en el documento RFC 1584 (Multicast Extensions to OSPF) y el protocolo DVMRP (Distance Vector Multicast Routing Protocol).

Un direccionador de MOSPF distribuye la información de ubicación de grupo por todo el dominio de direccionamiento mediante el uso extenso de un nuevo tipo de anuncio de estado de enlace, el LSA de pertenencia a grupo (group-membership-LSA) (tipo 6). Esto, a su vez, permite que los direccionadores de MSPF reenvíen del modo más eficiente un datagrama de multidifusión a sus múltiples destinos: cada direccionador calcula la vía del datagrama de multidifusión a modo de árbol, cuya raíz es el origen del datagrama y cuyas ramas terminales son LAN que contienen miembros del grupo. Si desea obtener más información, consulte “OSPF multidifusión” en la página 365.

DVMRP es un protocolo de direccionamiento multidifusión que deriva del protocolo RIP (Routing Information Protocol). Este direccionador proporciona soporte para DVMRP, de manera que puede intercambiarse información de direccionamiento multidifusión con otras entidades de direccionamiento que no dan soporte a MOSPF. La implementación de DVMRP de este direccionador también permite el tunelado de información de DVMRP a través de una red capacitada para MOSPF y a través de una red IP no capacitada para multidifusión.

Este direccionador también permite “incorporar” el direccionador mismo como miembro de uno o más grupos de multidifusión. Como miembro de un grupo de multidifusión, el direccionador responderá a “pings” y a consultas de SNMP dirigidos a la dirección del grupo (puede utilizarse un solo mandato para consultar a múltiples direccionadores).

Además, el soporte multidifusión IP del dispositivo se utiliza para establecer y administrar grupos de DLSw (Data Link Switching), lo que reduce la configuración necesaria para DLSw. Si desea información adicional, consulte “Utilización de DLSw” en la página 535.

Configuración del direccionador para multidifusión IP

Para habilitar el direccionador para que rastree pertenencias a grupos de multidifusión IP y reenvíe datagramas IP, debe habilitarse MOSPF, DVMRP o ambos

Habilitación de DVMRP

Para habilitar DVMRP:

1. Habilite DVMRP en el direccionador

   ```
   DVMRP config> dvmrp on
   ```

2. Establezca en qué interfaces de LAN se ejecutará DVMRP

   ```
   DVMRP config> phyint
   dirección-interfaz métrica umbral
   ```

El 2212 da soporte a IVMP versión 2 y DVMRP versión 3. IGMP puede configurarse para que opere en el modo de versión 1.

Consulte la parte que trata de la configuración de DVMRP en *Configuración y supervisión de protocolos - Manual de consulta, volumen 1* si desea obtener informacuón detallada sobre éstos y otros mandatos de configuración utilizados para establecer la interacción entre DVMRP y MOSPF cuando ambos están activos en el direccionador.

Incorporación del direccionador en grupos de multidifusión IP

Si el direccionador mismo va a unirse a uno o más grupos de multidifusión, se utilizan los mandatos siguientes join/leave:

- **join multicast-group-address**
- **leave multicast-group-address**

Puede accederse a estos mandatos **join** y **leave** desde el indicador de mandatos `OSPF Config` y desde el indicador de mandatos de supervisión `OSPF`. También se encuentran disponibles desde la consola de supervisión de DVMRP.

Tenga en cuenta que estos mandatos no son necesarios para que el direccionador ejecute las funciones de seguimiento de grupos de IGMP o de reenvío de multidifusión IP, sino que se utilizan para añadir el direccionador a grupos, de modo que pueda responder a “pings” y a consultas SNMP dirigidas a estos grupos.

Utilización del acceso simple a Internet

El acceso simple a Internet es un modo de configurar rápidamente muchas de las opciones que se requieren para dar acceso a Internet a un grupo de clientes DHCP. Todo lo que se necesita para configurar IP es habilitar esta opción y añadir una interfaz de LAN. Cuando se combina con una interfaz PPP configurada para acceder a una cuenta de un proveedor de servicios Internet (ISP), varios clientes DHCP pueden acceder a Internet con una sola dirección IP pública. Esto se consigue utilizando la función de servidor DHCP y la conversión de direcciones de red (NAT).

Nota: Esta opción sólo está disponible en cargas de software de direccionador que incluyen las funciones DHCP y NAT. Si se necesita una conectividad a Internet similar en cargas que no incluyen la función de servidor de DHCP pero sí NAT, debe utilizarse la dirección dinámica (consulte el apartado “Utilización de una dirección dinámica” en la página 236) con una configuración similar a la que se muestra en el ejemplo.

Ejemplo:

- Si PPP está configurado para pedir una dirección IP en la interfaz 3 del modo siguiente:

```
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]?
```

- El acceso simple a Internet puede habilitarse de esta forma:

```
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 automáticamente los siguientes filtros de paquetes en 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 automáticamente 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 automáticamente la siguiente ruta estática en la configuración de IP:

```
IP config>list routes

route to 0.0.0.0        ,0.0.0.0         via 0.0.0.3         cost 1
```

- Se generará automáticamente la siguiente configuración de NAT:[1]

```
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.
```

- La siguiente configuración del servidor DHCP se generará automáticamente: [1]

```
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
```

[1] Si ya se ha configurado el servidor DHCP antes de habilitar el acceso simple a Internet en IP, no se generará ni modificará ninguna configuración DHCP. Las subredes DHCP existentes se utilizarán como rangos de conversión para la configuración de NAT.

Configuración y supervisión de IP

Este capítulo describe los mandatos de configuración y supervisión de IP. Incluye las secciones siguientes:

Acceso al entorno de configuración de IP

Para acceder al entorno de configuración de IP, entre el mandato siguiente en el indicador de mandatos `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 permiten modificar el comportamiento de protocolo IP y ajustarse a las necesidades concretas del usuario. Para obtener un direccionador de IP totalmente funcional, es necesario realizar algunos ajustes de configuración. Entre los mandatos de configuración de IP en el indicador de mandatos `IP config>`.

Tabla 18. Resumen de los mandatos de configuración de IP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Add	Añade información de configuración de IP. Pueden añadirse direcciones de interfaz, así como controles de acceso, filtros y filtros de paquetes.
Change	Modifica la información que se entró en un principio con el mandato **add**.
Delete	Suprime información de IP que se había entrado con el mandato **add**.
Disable	Inhabilita determinadas características de IP que habían sido activadas con el mandato **enable**.
Enable	Habilita características de IP tales como el direccionamiento de subred ARP, reenvío UDP, originar por omisión, difusión dirigida, BOOTP, diversos distintivos de RIP que controlan el envío y recepción de información de RIP, diffserv, elusión de la compresión y el cifrado de capa 2 en los registros de control de acceso, y filtrado de tabla de direccionamiento.
List	Visualiza los elementos de configuración de IP.
Move	Cambia el orden de los registros de control de acceso.
Set	Establece los modos de configuración de IP, tales como el uso de control de acceso y el formato de las direcciones de difusión. También establece parámetros de IP como TTL (time-to-live) de los paquetes originados por el direccionador, el tamaño de la tabla de direccionamiento de IP, el tamaño de la antememoria y la métrica de la interfaz RIP y establece los parámetros de configuración de IGMP.
Update	Utilizado 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 xxxi.

Add

Utilice el mandato **add** para añadir información de IP a la configuración.

Sintaxis:

add
- accept-rip-route . . .
- access-control . . .
- address . . .
- aggregate . . .
- 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 el filtrado de RIP de entrada de una interfaz está habilitado. Puede obtenerse la lista de redes y subredes que ya se han entrado con el mandato **list rip**. El filtrado de entrada de rutas RIP puede habilitarse según un criterio de filtrado por interfaz IP. Ello se hace por separado para las rutas de 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 habilitar el filtrado de entrada de rutas en una interfaz IP, utilice los mandatos **disable receiving dynamic nets**, **disable receiving dynamic subnets** o **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] [syn-tcp] [tipo-icmp código-icmp] [máscara-tos inf-rango-tos sup-rango-tos máscara-mod-tos nuevo-valor-tos direccionamiento-basado-política pasarela-salto-siguiente usar-ruta-omisión] [anotar els captura-snmp syslog nivel-syslog]*

Desde el indicador de mandatos `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 al final de la lista de control de acceso del filtro de paquetes. El control de acceso permite definir categorías de paquetes a enviar, descartar o procesar con la conversión de direcciones de red, basándose en 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 el rendimiento del reenvío de IP.

Nota: El mandato **add access-control** configura reglas de control de acceso, pero no habilita automáticamente el control de acceso; véase el mandato **set access-control**.

tipo Indica qué hacer con los paquetes que coinciden con los parámetros de la regla de control de acceso.

E Exclusivo; los paquetes que coinciden se descartan.

I Inclusivo; los paquetes que coincidan continúan siendo procesados por el direccionador.

N Conversión de direcciones de red (NAT); los paquetes coincidentes se pasan a NAT para la conversión de las direcciones. Este tipo solamente es válido cuando se especifica en combinación con inclusivo, como por ejemplo *IN*. Este parámetro sólo es válido en la consola de configuración de filtro de paquetes (a la que se accede con el mandato**update packet-filter**).

origen-IP máscara-origen

Dirección IP y máscara de origen. La máscara de origen se une por medio del operador AND lógico con la dirección IP de origen recibida para que la regla haga coincidir un rango de direcciones IP de origen. Si los bits de la máscara de origen son 0, los bits correspondientes de la dirección IP de origen también deben ser 0.

Valores válidos: de 0.0.0.0 a 255.255.255.255

Valores por omisión: 0.0.0.0 para la dirección IP de origen. El valor por omisión de máscara-origen se basa en la dirección de IP-origen configurada.

dest-IP máscara-dest

Dirección IP y máscara de destino. La máscara de destino se une por medio del operador AND lógico con la dirección IP de destino recibida para que la regla haga coincidir un rango de direcciones IP de destino. Si los bits de la máscara de destino son 0, los bits correspondientes de la dirección de destino IP también deben ser 0.

Valores válidos: de 0.0.0.0 a 255.255.255.255

Valor por omisión: 0.0.0.0 para la dirección IP de destino. El valor por omisión de máscara-dest se basa en la dirección de IP-dest.

primer-protocolo último-protocolo

Rango de números de protocolo IP.

Algunos de los números de protocolo IP más 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 puerto de destino TCP/UDP. Estos parámetros solamente son válidos si el rango de números de protocolo IP incluye el 6 (para TCP) o el 17 (para UDP). Estos parámetros se ignoran para paquetes en que el número de protocolo IP no sea 6 ni 17.

Algunos de los números de puerto más comúnmente utilizados son:

21 para FTP
23 para Telnet
25 para SMTP
513 para rlogin
520 para RIP

Valores válidos: 0 - 65535

Valor por omisión: 0 para el primer puerto de destino y 65535 para el último puerto de destino

primero-puerto-origen último-puerto-origen
Un rango de números de puerto de origen TCP/UDP. Estos parámetros solamente son válidos si el rango de números de protocolo IP incluye el 6 (para TCP) o el 17 (para UDP). Estos parámetros se ignoran para paquetes en que el número de protocolo IP no sea 6 ni 17. Véase la descripción de *first-dest-port last-dest-port* para una lista de números de puerto TCP/UDP que se utilizan más comúnmente.

Valores válidos: 0 - 65535

Valor por omisión: 0 para el primer puerto de origen y 65535 para el último puerto de origen

syn-tcp Este parámetro hace coincidir dos paquetes TCP que establecen conexiones TCP (esto es, paquetes TCP en los que el bit SYN es 1 y el bit ACK es 0). Este parámetro solamente es válido si el rango de números de protocolo IP incluye el 6 (para TCP) y el tipo de regla es exclusiva. Este parámetro no es válido para los tipos IPSec y NAT, que siempre son inclusivos. Este parámetro se ignora para paquetes en que el número de protocolo IP no es 6.

Valores válidos: Yes o No

Valor por omisión: No

tipo-icmp Este parámetro, que define el tipo de ICMP, solamente es válido si el rango de números de protocolo IP incluye el 1 (para ICMP). El valor de este parámetro define el tipo de ICMP de la regla de acceso. Los paquetes de ICMP pueden coincidir con la regla solamente si el tipo de ICMP del paquete coincide con el tipo de ICMP de la regla de acceso. Si se especifica el valor por omisión -1, todos los valores de tipo de ICMP se tratan como si coincidieran con la regla de acceso. Este parámetro se ignora para paquetes en que el número de protocolo IP no es 1.

Valores válidos: -1 to 255

Valor por omisión: -1 (todos los tipos de ICMP)

código-icmp
Este parámetro, que define el tipo de código ICMP, solamente es válido si el rango de números de protocolo IP incluye el 1 (para ICMP). El valor de este parámetro define el código de ICMP de la regla de acceso. Los paquetes de

ICMP solamente pueden coincidir con la regla de acceso si el código de ICMP del paquete coincide con el código de ICMP de la regla de acceso. Si se especifica el valor por omisión -1, todos los valores de código de ICMP se tratan como si coincidieran. Este parámetro se ignora para paquetes en que el número de protocolo IP no es 1.

Valores válidos: -1 to 255

Valor por omisión: -1 (todos los códigos de ICMP)

máscara-tos, inf-rango-tos, sup-rango-tos

Si se establece *máscara-tos* a un valor que no sea cero, se habilita el filtrado según los bits del byte de TOS. *Máscara-tos* identifica los bits del byte de TOS/precedencia que deben filtrarse. Por ejemplo, si *máscara-tos* es X'E0' (B'11100000'), el filtrado se aplica solamente a los 3 bits de precedencia del byte de TOS (los 3 bits más significativos del byte de TOS).

Inf-rango-tos y *sup-rango-tos* definen el rango de valores consecutivos dentro de los bits seleccionados. Si se desea filtrar todos los 8 valores de los bits de precedencia (decimales 0 - 7), *inf-rango-tos* es X'00' (B'00000000') y *sup-rango-tos* es X'e0' (B'11100000', que define el decimal 7 dentro de los 3 bits que se seleccionan para filtrado). Si se desean filtrar los valores binarios B'000', B'001', B'010' y B'011' (decimal 0 - 3) de los 3 bits de precedencia, *inf-rango-tos* es X'00' (B'00000000') y *sup-rango-tos* es X'60' (B'01100000').

Si se necesitan filtrar patrones de bits que no forman una secuencia de valores consecutivos, tendrá que definirse una regla de control de acceso separada para cada rango que se desea. Por ejemplo, para filtrar los dos valores de bit de precedenciaB'001' (decimal 1) y B'011' (decimal 3) sin filtrar B'010' (decimal 2), tiene que definirse la primera regla de control de acceso con *máscara-tos* igual a X'e0' e *inf-rango-tos* y *sup-rango-tos* ambos iguales a X'20'. Entonces tendría que definirse la segunda regla de control de acceso con *máscara-tos* igual a X'e0' e *inf-rango-tos* y *sup-rango-tos* ambos iguales a X'60'.

Valores válidos para *máscara-tos*: X'00' - X'FF'

Valor por omisión: 0, que significa ninguna

Valores válidos para *inf-rango-tos*: X'00' - X'FF'

Valor por omisión: 0

Valores válidos para *sup-rango-tos*: X'00' - X'FF'

Valor por omisión: El *inf-rango-tos* configurado.

nuevo-valor-tos, máscara-mod-tos

El establecimiento de estos parámetros capacita al direccionador para modificar bits específicos en el byte de TOS. *Máscara-mod-tos* identifica los bits dentro del byte de TOS que deben cambiarse. *Nuevo-valor-tos* define el nuevo

valor para los bits seleccionados. Por ejemplo, si *máscara-mod-tos* es X'1e' y *nuevo-valor-tos* es X'00', los 4 bits del campo TOS (identificados dentro del byte por el valor X'1e' [B'00011110'] de *máscara-mod-tos*) se establecen en B'0000'. Para establecer los bits de TOS en el valor de máximo rendimiento (B'0100'), utilice la *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, que significa ninguna

Valores válidos para *nuevo-valor-tos*: X'00' - X'FF'

Valor por omisión: 0

direccionamiento-basado-política, pasarela-salto-siguiente, usar-ruta-omisión
Estos parámetros habilitan el direccionamiento basado en una política, que consiste en la capacidad de especificar la pasarela de salto siguiente a través de la que se enviarán los paquetes filtrados. Si se establece el parámetro *direccionamiento-basado-política* en Yes, se indica la intención de que los paquetes filtrados se envíen a la pasarela de salto siguiente definida. *Pasarela-salto-siguiente* es la dirección de la pasarela de salto siguiente a la que se enviarán estos paquetes.

Si se establece *usar-ruta-omisión* en Yes, se habilita el direccionador para que direccione el paquete utilizando la tabla de direccionamiento normal en el caso de que la pasarela definida no esté disponible. Si este parámetro se establece en No, el paquete se descartará si la pasarela definida no está disponible, y se enviará el mensaje *unreachable* de ICMP a la dirección de origen del paquete descartado.

Valores válidos para *direccionamiento-basado-política*: Yes o No

Valor por omisión: No

Valor válido para *pasarela-salto-siguiente*: una dirección válida IP

Valor por omisión: ninguno

Valor válido para *usar-ruta-omisión*: Yes o No

Valor por omisión: Yes

anotar Habilita las anotaciones.

Valores válidos: Yes o No

Valor por omisión: No

els Si están habilitadas las anotaciones, els habilita los mensajes de ELS para esta regla de control de acceso.

Valores válidos: No, short o long

Valor por omisión: No

captura-snmp
Si están habilitadas las anotaciones, captura-snmp habilita el envío de capturas de SNMP para esta regla de control de acceso.

Valores válidos: Yes o No

Valor por omisión: No

syslog Si están habilitadas las anotaciones, syslog habilita SysLog para esta regla de control de acceso. SysLog remite los mensajes del sistema a una estación de trabajo conectada remota.

Valores válidos: No, short, or long

Valor por omisión: No

nivel-syslog
Si SysLog está habilitado, especifica el nivel de los mensajes de SysLog

Valores válidos: Sys Def, Emerg, Alert, Crit, Error, Warn, Notice, Info, o Debug

Valor por omisión: valor por omisión de sistema del direccionador

Ejemplo:

```
IP config> add access-control
Enter 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]?
Enter starting protocol number ([CR] for all) [-1]?
Enter starting destination port number ([CR] for all) [-1]?
Enter starting source port number ([CR] for all) [-1]?
Enter ICMP Type ([CR] for all) [-1]? 3
Enter ICMP Code ([CR] for all) [-1]?
TOS/Precedence filter mask (00-FF - [0] for none) [0]? CD
TOS/Precedence start value (00-FF) [0]?
TOS/Precedence end value [0]?
TOS/Precedence modification mask (00-FF - [0] for none) [0]? FA
New TOS/Precedence value (00-FF) [0]?
Next hop gateway address [ ]? 8.8.8.2
Use default route if next hop gateway unreachable? [Yes]:
IP config>
```

address *número-interfaz dirección-IP máscara-dirección*
Asigna una dirección IP a una de las interfaces de red hardware del direccionador. Una interfaz de red hardware no recibirá ni transmitirá paquetes IP si no tiene al menos una dirección IP. Debe especificarse una dirección IP junto con su máscara de subred. Por ejemplo, si la dirección está en una red de clase B, utilizando el tercer byte para subredes, la máscara sería 255.255.255.0. Utilice el mandato **list devices** para obtener el número de interfaz de mandatos apropiado. Las líneas serie no necesitan direcciones. Estas líneas se denominan no numeradas. Sin embargo, deben también habilitarse para el tráfico IP con el mandato**add address**. La dirección que entonces 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 2212, especifíque **bridge** como *número de interfaz*. Consulte el apartado “Asignación de direcciones IP a la interfaz de red de puente” en la página 237 si desea obtener más información.

Debe especificarse una dirección IP junto con su máscara de subred. Por ejemplo, si la dirección está en una red de clase B, utilizando el tercer byte para subredes, la máscara sería 255.255.255.0. Utilice la opción **List Devices** para obtener el número de interfaz adecuado.

número-interfaz

Valores válidos: cualquier número de interfaz que se defina, o **bridge**

Valor por omisión: ninguno

dirección-IP

Valores válidos:

El rango de la clase A es de 1.0.0.1 a 126.255.255.254
El rango de la clase B es de 128.0.0.1 a 191.255.255.254
El rango de la clase C es de 192.0.0.1 a 223.255.255.254
Para las interfaces de línea serie no numeradas, 0.0.0.n, donde*n* es el número de interfaz

Valor por omisión: ninguno

máscara-dirección

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`

aggregate *dirección-IP-agregada máscara-IP-agregada agregada-incondicionada IP-política-ruta métrica*

Añade una ruta agregada a la configuración IP. La agregación de ruta permite utilizar una dirección IP y una máscara de subred para definir un rango de subredes pertenecientes a diferentes dominios de direccionamiento. En el apartado “Agregación de ruta” en la página 254 hallará más información.

dirección-IP-agregada

Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

máscara-IP-agregada

Valores válidos: cualquier máscara IP válida

Valor por omisión: ninguno

agregada-incondicionada

Si la respuesta a esta pregunta es **yes**, con ello se indica que la ruta agregada se genera incondicionadamente. En tal caso, se anunciará cuando sea necesario. Las rutas agregadas incondicionadas tienen asociado un valor de métrica.

Si la respuesta a esta pregunta es **no**, con ello se indica que la ruta agregada se genera condicionadamente. En tal caso, se generará sólo cuando la dirección de destino que ha de procesarse coincida con el rango especificado por la ruta

agregada y, además, cumpla las condiciones de una política de filtros de rutas especificada.

Valores válidos: Yes o no

Valor por omisión: No

identificador-política-ruta
Se trata del identificador de la política de filtros de rutas que está asociada con la ruta agregada. Este parámetro se aplica sólo cuando la ruta agregada es condicionada.

Valores válidos: un identificador de política de filtros de rutas válido (de 1 a 15 caracteres ASCII)

Valor por omisión: ninguno. Este parámetro es obligatorio cuando se especifica *No* o se toma el valor por omisión para agregada-incondicionada.

métrica Este parámetro sirve para medir el coste de la ruta agregada en relación con el coste de las demás rutas agregadas. Se aplica sólo a rutas agregadas incondicionadas.

Valores válidos: de 1 a 65535

Valor por omisión: 1

Ejemplo:

```
IP config> add aggregate
IP Address [ ]? 10.0.0.0
IP Mask [ ]? 255.0.0.0
Aggregate Route Always Generated? [No]:yes
Metric value [1-16777215] [1]?
Route aggregate 10.0.0.0/255.0.0.0 added or modified.
```

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 apartado “Configuración del proceso de reenvío BOOTP/DHCP” en la página 257 si desea obtener más información.

dirección-IP-servidor
Valores válidos: cualquier dirección IP de un servidor Bootp válida

Valor por omisión: ninguno

Ejemplo: **`add bootp-server 128.185.123.22`**

filter *dirección-IP-dest máscara-dirección*
Designa un destino IP para que sea filtrado. Los paquetes IP no se reenviarán a destinos filtrados, ni se diseminará información de direccionamiento relativa a estos destinos. Los paquetes a destinos filtrados son simplemente descartados. Un destino filtrado debe especificarse como una dirección IP con su máscara de subred. Por ejemplo, para filtrar una subred de una red de clase B, utilizando el tercer byte para subred, la máscara debería ser 255.255.255.0. La utilización del mecanismo de filtro es más eficiente que los controles de acceso IP, aunque no tan flexible. A diferencia de los controles de acceso, los filtros también afectan el funcionamiento de los protocolos de direccionamiento IP. Las redes/subredes filtradas prevalecen si se averiguan utilizando el protocolo de direccionamiento ISPF.

El efecto de este mandato es inmediato; no hace falta rearrancar el direccionador para que surta efecto.

dirección-IP-dest

Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

máscara-dirección

Valores válidos: de 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 paquetes en la configuración del direccionador.

nombre-filtro

Valores válidos: cualquier nombre de 16 caracteres.

Pueden incluirse guiones (-) y guiones de subrayado (_) en el nombre.

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 **bridge** para la interfaz de red de puente

Valor por omisión: ninguno

Example: `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-subred dirección-MAC pasarela-primaria*

Añade una dirección IP de pasarela redundante por omisión a la configuración.

número-interfaz

Especifica el número de red de las interfaces LEC en 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 usadas 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 primaria y la pasarela de reserva deben tener la misma dirección MAC

Valores válidos: cualquier dirección MAC válida que no esté utilizada por otras interfaces en la ELAN

Valor por omisión: 00.00.00.00.00.00

pasarela-primaria
Especifica si la pasarela se utiliza como pasarela primaria o pasarela de reserva.

Esta consulta pregunta si la pasarela de este dispositivo es la pasarela primaria activa durante el funcionamiento normal de la red o si la pasarela de reserva que está activa cuando la interfaz LEC que contiene la pasarela primaria no está operativa. Una contestación de **Yes** configura una pasarela primaria. Tiene que haber una única pasarela primaria por ELAN.

Valores válidos Yes o No

Valor por omisión: No

Ejemplo: `add redundant`

```
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 *dir-dest máscara-dest salto-siguiente1 coste1 [salto-siguiente2 coste2 [salto-siguiente3 coste3 [salto-siguiente4 coste4]]]*
Añade de 1 a 4 rutas estáticas a la configuración IP del dispositivo. Cuando la información de direccionamiento dinámico no está disponible para un destino en concreto, entonces se utilizan rutas estáticas.

El destino se especifica mediante una dirección IP (*dir-dest*) junto con una máscara de dirección (*máscara-dest*). Si la dirección IP de destino es una dirección de red, entonces máscara-dest debe ser una máscara de red. Si la dirección IP de destino es una dirección de subred, entonces máscara-dest debe ser una máscara de subred. Finalmente, si la dirección IP de destino es una dirección de sistema principal, entonces máscara-dest debe ser una máscara de sistema principal (lo que quiere decir que el único valor válido es 255.255.255.255). Máscara-dest debe ser precisa; si no, no se aceptará la ruta estática.

Se puede definir un máximo de cuatro rutas estáticas por destino, cada una de las cuales tendrá la dirección IP de su salto siguiente (salto-siguiente) y el coste (coste) de direccionar un paquete al destino. El salto siguiente debe estar en la misma (sub)red que una de las interfaces del direccionador directamente conectadas. Las rutas estáticas que van a un destino dado pueden tener el mismo coste, en cuyo caso IP podrá utilizarlas simultáneamente, o bien un coste diferente, en cuyo caso IP utilizará la ruta con menor coste que funcione.

Las rutas averiguadas a través de OSPF prevalecen siempre sobre las rutas estáticas. Por omisión, las rutas averiguadas a través de RIP también prevalecen sobre las rutas estáticas; no obstante, esto puede cambiarse con el mandato **enable/disable override static-routes**. El mandato **add route** surte efecto de forma inmediata; no es necesario rearrancar el direccionar.

dir-dest **Valores válidos**: cualquier dirección IP válida

Valor por omisión: ninguno

máscara-dest

Valores válidos: de 0.0.0.0 a 255.255.255.255

Valor por omisión: ninguno

salto-siguiente1, salto-siguiente2, salto-siguiente3, salto-siguiente4

Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

coste1, coste2, coste3, coste4

Valores válidos: un entero en el rango de 0 a 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-ruta usar-política-estrictamente-lineal*

Añade una política de filtros de rutas. Una política de filtros de rutas consta de entradas que definen un conjunto de rutas que pueden filtrarse para ser incluidas o excluidas de la tabla de direccionamiento de un protocolo de direccionamiento externo tal como OSPF o RIP.

identificador-política-ruta

Una serie que identifica una política de filtros de rutas.

Valores válidos: cualquier serie de 1 a 15 caracteres ASCII

Valor por omisión: ninguno

usar-política-estrictamente-lineal

Yes indica que la coincidencia se establecerá basándose estrictamente en la secuencia de números de índice de las entradas de la política de filtros de rutas. Se procesará en primer lugar la entrada con el número de índice más bajo.*No* indica que se establecerá la coincidencia utilizando la coinci-

dencia más larga. Se escogerá la entrada con el número de índice más bajo únicamente cuando hay más de una entrada con la misma dirección y la misma 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 tablas de rutas para las rutas especificadas. Cuando está habilitado **route-table-filtering** el filtro de tablas de rutas se hará coincidir con las rutas añadidas a la tabla de direccionamiento de IP. El orden en que se aparecen en la tabla de direccionamiento no es relevante. En cambio, se escogerá el filtro de tablas de rutas con la coincidencia más específica. Si no se encuentra ninguna coincidencia, la ruta se añade a la tabla de direccionamiento. Cuando se especifica **exact**, para que se produzca una coincidencia el destino y la máscara de la ruta deben ser exactamente los mismos que el destino y la máscara del filtro de tablas de rutas. Cuando se especifica **more-specific** el destino de ruta y la máscara deben ser parte del rango incluido por el destino y la máscara del filtro de tablas de rutas. Al especificar **both** se especifica el superconjunto de "both" y "more-specific" (esto es, se producirá una coincidencia en el caso tanto de una coincidencia exacta como una coincidencia más específica). Si el filtro de tablas de rutas indica **include**, se añadirá la ruta a la tabla de direccionamiento de IP. Si el filtro de tablas de rutas indica **exclude**, no se añadirá la ruta a la tabla de direccionamiento de IP. Las rutas estáticas y directas nunca se excluyen de la tabla de direccionamiento de 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 entrarse una dirección IP de difusión o de unidifusión.

Repita este mandato para añadir más de una dirección IP para el mismo puerto UDP. Esto hace que el direccionador reenvíe el datagrama UDP a cada una de las direcciones IP.

número-puerto

Valores válidos: de 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... Añade una definición de ID de direccionador virtual para un direccionador VRRP en un segmento de LAN.

Interface IP address
Indica la interfaz IP para la cual se define este VRID.

Valores válidos: Cualquier interfaz IP configurada.

Valor por omisión: ninguno

VRID El identificador del direccionador virtual. La combinación de *ip-interface-address* y *vrid* otorgan una definición única al VRID. Puede utilizarse el mismo *vrid* en más de una interfaz física. Si el VRID ya existe, será modificado.

Valores válidos: 1-255

Valor por omisión: ninguno

Advertisement interval
Intervalo entre anuncios de VRRP.

Valores válidos: 1-255

Valor por omisión: 1

Backup router
Indica si este direccionador es el direccionador maestro o bien el direccionador de reserva para este VRID.

Valores válidos: Yes o No

Valor por omisión: No

Backup IP address
Indica la primera dirección IP de reserva este VRID. Pueden añadirse más direcciones con el mandato *add vr-address* para segmentos de LAN que dan soporte a más de una subred. No es aplicable si se ha configurado **No** para *Backup router*.

Valores válidos: Cualquier dirección IP válida.

Valor por omisión: ninguno

Priority Indica la prioridad de VRRP para los direccionadores de reserva. Si un direccionador de reserva asume las funciones del direccionador primario, usará esta prioridad en sus anuncios de VRRP. No es aplicable si se ha configurado **No** para *Backup router*. Un direccionador maestro siempre anunciará una prioridad de 255.

Valores válidos: de 1 a 254

Valor por omisión: 100

Preempt mode
Indica que un direccionador VRRP de reserva tendrá preferencia ante un VRRP de reserva cuya prioridad sea inferior. Tener preferencia significa asumir las funciones del direccionador que da soporte a reenvíos para VRID. No es aplicable si se ha configurado **No** para *Backup router*. Un direccionador maestro siempre tiene preferencia ante un direccionador de reserva que ha asumido temporalmente las responsabilidades del VRID.

Valores válidos: Yes o No

Valor por omisión: Yes

Hardware MAC mode
Indica si se utiliza o no la dirección MAC de hardware como dirección MAC virtual de VRID. Todos los direccionadores configurados para este VRID deben tener el mismo valor en este parámetro para que VRRP funcione correctamente. Si se ha entrado **Yes** para este parámetro, *Functional/group mode* toma por omisión el valor **No** y no se visualiza.

Functional/group mode
Indica si una dirección de multidifusión MAC se utiliza o no como la dirección MAC virtual de VRID. Todos los direccionadores configurados para este VRID deben tener el mismo valor en este parámetro para que VRRP funcione correctamente. Este parámetro toma por omisión el valor **No** y no se visualiza si *Hardware MAC mode* está configurado como **Yes**.

Valores válidos: Yes o No

Valor por omisión: No

Authentication type
Indica el tipo de autenticación usado para los anuncios de VRRP. Los posibles valores para los tipos de autenticación son el 1, que indica una simple contraseña o bien 0, que indica que no se usa ninguna autenticación.

Valores válidos: none (ninguno), simple

Valor por omisión: ninguno

Authentication key
Es el parámetro que define la contraseña para este VRID. Cuando se usa la autenticación mediante contraseña, sólo se aceptarán los paquetes con la clave de autenticación correcta. *authentication key* no es aplicable cuando se especifica *none* para *authentication type* o bien es el valor por omisión.

Valores válidos: Cualquier serie de 1 a 8 caracteres.

Valor por omisión: Una serie nula.

Require network for master eligibility
Indica si se supervisará el estado de funcionamiento (activo o inactivo) de una red con el fin de determinar la elegibilidad de maestro. Si el valor de este parámetro es **yes**, cuando la red deje de estar activa y el direccionador sea el maestro VRRP, el direccionador renunciará a su estado de maestro y se elegirá uno nuevo.

Valores válidos: Yes o No

Valor por omisión: No

Required network
La red que se supervisará para determinar la elegibilidad de maestro. Esta pregunta no es aplicable si se ha especificado **No** para *Require network for master eligibility*.

Valores válidos: de 1 al número de redes configuradas

Valor por omisión: No

Required route destination

El destino de ruta que se supervisará para determinar la elegibilidad de maestro. Esta pregunta no es aplicable si se ha especificado **No** para *Require route for master eligibility*.

Valores válidos: cualquier dirección IP válida

Valor por omisión: 0.0.0.0

Required route mask

El máscara de ruta que se supervisará para determinar la elegibilidad de maestro. Esta pregunta no es aplicable si se ha especificado **No** para *Require route for master eligibility*.

Valores válidos: Cualquier máscara IP válida

Valor por omisión: 0.0.0.0

Ejemplo:

```
IP config>add vrid
IP Interface []? 153.2.2.1
VRID (1-255) [0]? 1
Advertisement Interval (1-255) [1]?
Backup Virtual Router? [No]:
Use Hardware MAC Address? [No]: yes
Authentication Type (0 - None, 1 - Simple) [0]?
Require network for master eligibility? [No]:
Require route for master eligibility? [No]:
VRID 153.2.2.25/1 added/modified successfully
```

vr-address ...

Añade una dirección secundaria a la definición de un ID de direccionador virtual (VRID) configurado. Las direcciones secundarias se incluirán en los anuncios de VRRP para el VRID. Las direcciones secundarias son necesarias en las LAN físicas que den soporte a más de una subred IP. Cada dirección designa la dirección de pasarela por omisión para esa subred. Si el direccionador es un direccionador maestro, las direcciones que se añadan mediante el mandato *add vr-address* serán anunciadas además de la *dirección de interfaz IP* del VRID. Si el direccionador es un direccionador de reserva para el VRID, las direcciones que se añadan con el mandato *add vr-address* se anunciarán además de la *dirección IP de reserva*.

Interface IP address

La interfaz IP del VRID.

Valores válidos: Cualquier interfaz IP configurada.

Valor por omisión: ninguno

VRID El identificador del direccionador virtual. La combinación de *dirección de interfaz IP* y *VRID* define el VRID de manera exclusiva. El VRID debe estar configurado para que se añadan direcciones a su definición. El direccionador maestro y los direccionadores de reserva deben estar configurados todos ellos con el mismo VRID.

Valores válidos: de 1 a 255

Valor por omisión: ninguno

IP address

La dirección IP adicional se incluirá en los anuncios de VRRP para el 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 cambiar un elemento de configuración de IP previamente instalado mediante el mandato **add**. En general, debe especificarse el elemento que se desea cambiar del mismo modo en que se especificó este 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] [syn-tcp] [tipo-icmp código-icmp] [máscara-tos inf-rango-tos sup-rango-tos máscara-mod-tos nuevo-valor-tos direccionamiento-basado-política pasarela-salto-siguiente usar-ruta-omisión] [anotar els captura-snmp syslog nivel-syslog]*

Modifica un registro global de control de acceso existente. Utilice el mandato **list access-control** para visualizar todos los registros existentes y obtener el número de regla. Véase el mandato de talk 6 **Add** si se desea obtener 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 interface IP del direccionador. Debe especificarse cada dirección nueva junto con la máscara de subred de ésta. Este mandato también puede utilizarse para cambiar la máscara de subred de una dirección ya existente.

Direcciones IP válidas:

- El rango de la clase A es de 1.0.0.1 a 126.255.255.254
- El rango de la clase B es de 128.0.0.1 a 191.255.255.254
- El rango de la clase C es de 192.0.0.1 a 223.255.255.254
- Para las interfaces serie no numeradas, 0.0.0.n, donde n es el número de interfaz de hardware

Para interfaces de línea serie :

- 0.0.0.n, donde n es el número de interfaz de hardware.

dirección-antigua

Valor válido: una interfaz IP que esté actualmente configurada address

Valor por omisión: ninguno

dirección-nueva

Valor válido: cualquier dirección IP válida

Valor por omisión: ninguno

nueva-máscara

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 *dir-dest máscara-dest nuevo-salto-siguiente1 nuevo-coste1 [nuevo-salto-siguiente2 nuevo-coste2 [nuevo-salto-siguiente3 nuevo-coste3 [nuevo-salto-siguiente4 nuevo-coste4]]]*

Modifica o bien los saltos siguientes o bien los costes asociados a las rutas estáticas configuradas al destino específico. El efecto de este mandato es inmediato; no hace falta rearrancar el direccionador para que surta efecto.

dir-dest **Valores válidos**: cualquier dirección IP válida

Valor por omisión: ninguno

máscara-dest

Valores válidos: de 0.0.0.0 a 255.255.255.255

Valor por omisión: ninguno

nuevo-salto-siguiente1, nuevo-salto-siguiente2, nuevo-salto-siguiente3, nuevo-salto-siguiente4

Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

nuevo-coste1, nuevo-coste2, nuevo-coste3, nuevo-coste4

Valores válidos: un entero en el rango de 0 a 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-ruta*

Utilice este mandato para cambiar una política de filtros de rutas ya existente que se creó con el mandato **add route-policy**. Se utiliza el mandato **change route-policy** para configurar las entradas, acciones y condiciones de coincidencia asociadas a la política de filtros de rutas. El mandato **change route-policy** hace aparecer el indicador de mandatos `IP Route Policy Config>`.

identificador-política-ruta

Valores válidos: la serie de 1 a 15 caracteres ASCII que identifica una política de filtros de rutas existente

Valor por omisión: ninguno

Delete

Utilice el mandato **delete** para suprimir un elemento de configuración IP previamente instalado mediante el mandato **add**. En general, debe especificarse el elemento que se desea suprimir del mismo modo en que se especificó este elemento con el mandato **add**.

Sintaxis:

de**lete** accept-rip-route . . .
access-control . . .
address . . .
aggregate . . .
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 siempre acepta.

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. list.

Ejemplo: `delete access-control 2`

address *dirección-interfaz-ip*
Suprime una de las direcciones de interfaz IP del direccionador.

Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

Ejemplo: `delete address 128.185.123.22`

aggregate *dirección-ip máscara-ip*
Suprime una de las rutas agregadas del direccionador; está definido por la dirección IP y la máscara de IP de la ruta agregada que se va a suprimir.

dirección-ip
Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

máscara-ip
Valores válidos: Cualquier máscara IP válida

Valor por omisión: ninguno

bootp-server *dirección-IP-servidor*
Elimina un servidor BOOTP de una configuración IP.

Valores válidos: cualquier dirección IP configurada de un servidor BOOTP

Valor por omisión: 0.0.0.0

Ejemplo: `delete bootp-server 128.185.123.22`

default network/subnet-gateway *[dirección-ip-red]*

Suprime o bien la pasarela por omisión o la pasarela de subred por omisión para 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 *dir-dest máscara-dest*

Suprime una de las redes del direccionador filtradas. El efecto de este mandato es inmediato; no hace falta rearrancar el direccionador para que surta efecto.

dir-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 paquetes especificado de la configuración del direccionador.

Valores válidos: cualquier nombre de 16 caracteres.

Pueden incluirse guiones (-) y guiones de subrayado (_) en el nombre.

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 *dir-dest máscara-dest [suprimir-salto-siguiente1 [suprimir-salto-siguiente2 [suprimir-salto-siguiente3 [suprimir-salto-siguiente4]]]]*

Suprime una de las rutas estáticas configuradas del dispositivo. El efecto de este mandato es inmediato; no hace falta rearrancar el direccionador para que surta efecto.

dir-dest **Valores válidos**: cualquier dirección IP válida

Valor por omisión: ninguno

máscara-dest

Valores válidos: cualquier máscara IP válida

Valor por omisión: ninguno

suprimir-salto-siguiente

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-ruta suprimir-entradas-política-rutas*

Suprime de la configuración una política de filtros de rutas existente. Existe la opción de suprimir todas las entradas de la política de filtros de rutas asociadas a la política de filtros de rutas. Si las entradas no se han suprimido, al reconfigurar la política de filtrado de la ruta suprimida, se reintegran las entradas asociadas a esa política de filtros de rutas. Utilice el mandato **add route-policy** para reconfigurar una política de filtros de rutas suprimida.

identificador-política-ruta

Valores válidos: la serie de 1 a 15 caracteres ASCII que identifica una política de filtros de rutas configurada.

Valor por omisión: ninguno

suprimir-entradas-política-rutas

Yes suprime las entradas correspondientes de 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 direccionamiento añadidos con**add route-table-filter.** Véase “route-table-filter (filtro de tablas de rutas)” en la página 282 para las definiciones de las extensiones de los mandatos.

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 que se configuró mediante el mandato **add udp-destination**. Como resultado, los datagramas UDP entregados localmente que se reciban en el puerto especificado no serán reenviados a la dirección IP especificada.

número-puerto

Valores válidos: cualquier entero en el rango de 0 a 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 de ID de direccionador virtual para un direccionamiento 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* definen el VRID de forma exclusiva. Se utiliza para identificar el VRID que va a suprimirse.

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-interfaz*

Suprime una dirección secundaria de la definición de un ID de Direccionador virtual configurado.

dirección-ip-interfaz
La interfaz IP para el 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* definen el VRID de forma exclusiva. El VRID debe estar configurado para que se añadan direcciones a su definición.

Valores válidos: 1-255

Valor por omisión: ninguno

dirección-IP
Las direcciones IP adicionales que se suprimen de la definición de 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 **inhabilitar** para inhabilitar características IP previamente habilitadas con el mandato **enable**.

Sintaxis:

di**sable**
- arp-net-routing
- arp-subnet-routing
- bootp-forwarding
- classless
- compression-bypass
- directed-broadcast
- dynamic-address
- echo-reply
- encryption-bypass
- 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 habilitado, el direccionador responde por proxy a todas las peticiones ARP para destinos remotos a las que se accede con mayor facilidad desde el direccionador. Éste es el valor por omisión y el que se recomienda generalmente.

Ejemplo: `disable arp-net-routing`

arp-subnet-routing

Desactiva la característica de IP denominada direccionamiento de subred ARP o ARP proxy que, cuando se habilita, se encarga de los sistemas principales que no tengan soporte para subredes IP. Éste es el valor por omisión y el que se recomienda generalmente.

Ejemplo: `disable arp-subnet-routing`

bootp-forwarding

Desactiva la función de retransmisión de BOOTP/DHCP.

Ejemplo: `disable bootp-forwarding`

classless Inhabilita la supresión de rutas de red con clase. Estas rutas (por ejemplo, las rutas de clase A, B o C) se generarán automáticamente para su anuncio en protocolos que no anuncien la máscara de subred (como por ejemplo RIPv1).

compression-bypass *número-regla*

Inhabilita la elusión de la compresión de capa 2 para el control de acceso especificado por el *número-regla*, lo que hace que los paquetes

se compriman si la compresión está habilitada en la interfaz de red de salida. La elusión de compresión sólo puede inhabilitarse para los controles de acceso de tipo **include**.

Ejemplo: `disable compression-bypass 1`

directed-broadcast

Inhabilita el reenvío de paquetes IP cuyo destino es una dirección de difusión no local (por ejemplo, una LAN remota). El sistema principal de origen origina el paquete como una unidifusión, reenviándose entonces como unidifusión a una subred de destino donde "explota" como difusión broadcast. Estos paquetes pueden utilizarse para localizar servidores de red.

Nota: El reenvío y la explosión no pueden ser inhabilitados por separado.

Ejemplo: `disable directed-broadcast`

dynamic-address *0.0.0.n*

En la interfaz de red PPP especificada, impide al direccionador averiguar su dirección IP a partir del nodo remoto en la interfaz de red. Esta opción está inhabilitada por omisión.

Esta opción sólo es válida en una interfaz de red que se haya configurado como una interfaz de línea serie no numerada (la dirección IP asignada a la interfaz de red con el mandato **add address** es *0.0.0.n*, donde *n* es el número de la interfaz de red).

Ejemplo:

```
IP config> disable dynamic-address
Interface address []? 0.0.0.1
IP config>
```

echo-reply

Inhabilita la función ICMP Echo Reply del direccionador. De este modo, un ping que se envíe a cualquiera de las interfaces del direccionador no generará respuesta. La opción por omisión del direccionador es la habilitación para respuesta eco.

Ejemplo: `disable echo-reply`

encryption-bypass *número-regla*

Inhabilita la elusión del cifrado de capa 2 para el control de acceso especificado por el *número-regla*, lo que hace que los paquetes se cifren si el cifrado está habilitado en la interfaz de red. La elusión de cifrado sólo puede habilitarse para los controles de acceso de tipo **include**.

Ejemplo: `disable encryption-bypass 1`

fragment-offset-check

Inhabilita la comprobación del fragmento de desplazamiento de los paquetes IP recibidos. Cuando esta comprobación está habilitada, el direccionador comprueba cada fragmento para asegurarse que ningún fragmento secundario ha sustituido la información de los primeros 8 bytes de la carga útil del primer fragmento. Por omisión, esta comprobación está inhabilitada.

icmp-redirect *dirección-interfaz-ip*

Inhabilita el envío de mensajes de redirección ICMP del direccionador en la interfaz IP especificada. IP interface. Si no se entra ningún valor en el indicador de mandatos para la dirección de interfaz IP, el direccionador será inhabilitado para 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*

Inhabilita el conocimiento del salto siguiente 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 que recibe RIP no prevalecen sobre las rutas estáticas. Sin embargo, el mandato **enable override static-routes** habilita las rutas recibidas por RIP para que prevalezcan sobre las rutas estáticas. Una vez habilitadas las rutas RIP para que prevalezcan sobre las rutas estáticas, puede utilizarse el mandato **disable override default-route** o **disable override static-route** para volver a impedir que las rutas recibidas por RIP prevalezcan sobre las rutas estáticas. El mandato **disable override default-route** impide 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** impide que las rutas RIP recibidas en la interfaz *dirección-interfaz-ip* prevalezcan sobre cualquiera 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*

Inhabilita la lista de control de acceso determinada para una interfaz que se especifique (filtros de paquetes).

nombre-filtro

Valores válidos: cualquier nombre de 16 caracteres. Pueden incluirse guiones (-) y guiones de subrayado (_) en el nombre.

Valor por omisión: Ninguno

Ejemplo: `disable packet-filter pf-in-0`

per-packet-multipath
Si la multivía por paquete está inhabilitada, las rutas multivía de igual coste equilibrarán la carga según destino cuando éste se coloca en la antememoria de IP. Por omisión, esta función está inhabilitada.

receiving policy global/interface *dirección-interfaz-ip*
Inhabilita el uso de la política de determinación de las rutas que serán aceptadas por RIP. El mandato **disable receiving policy global** inhabilita el uso de la política global de recepción de filtros de rutas para todas las interfaces RIP que reúnan estas dos condiciones:

- No tienen configuradas políticas RIP de recepción de filtros de rutas a nivel de interfaz. Si una política RIP de recepción de filtros de rutas a nivel de interfaz está configurada en una interfaz, esa política continúa determinando qué rutas se aceptan.
- La recepción de rutas RIP no está inhabilitada.

Después de que se inhabilite la política global RIP de recepción de filtros de rutas, las interfaces RIP ya no se encontrarán afectadas por dicha política.

El mandato **disable receiving policy interface** *irección-interfaz-ip* inhabilita 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*
Impide que RIP procese las actualizaciones RIP que se reciban 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** garantiza que, para las actualizaciones RIP recibidas en la interfaz *dirección-interfaz-ip*, el direccionador aceptará sólo las rutas de nivel de red que se hayan entrado con el mandato **add accept-rip-route**. El mandato **disable receiving dynamic subnets** produce un comportamiento análogo para rutas de subred. El mandato **disable receiving dynamic host** produce un comportamiento análogo para rutas de sistemas principales.

dirección-interfaz-ip
Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

Ejemplo: `disable receiving dynamic nets 128.185.123.22`

record-route
Inhabilita al direccionador para la recepción o reenvío de paquetes IP que contengan una opción IP de ruta de registro. Por omisión, el direccionador recibe y reenvía estos paquetes.

rip Desactiva el protocolo RIP.

Ejemplo: `disable rip`

rip2 Inhabilita RIP2 en una interfaz IP en que previamente había estado habilitado.

dirección-interfaz-ip
Indica la interfaz IP en la que RIP2 está inhabilitado.

Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

Ejemplo: `disable rip2 128.185.123.22`

route-table-filtering
Inhabilita la aplicación de filtros de tabla de direccionamiento cuando se añaden rutas a la tabla de direccionamiento.

Ejemplo: `disable route-table-filtering`

same-subnet
Inhabilita la opción de misma subred. Al rearrancar el direccionador, no se permitirá que se instale más de una interfaz IP en la misma subred. Éste es el valor por omisión.

Ejemplo: `disable same-subnet`

sending policy global/interface *dirección-interfaz-ip*
Inhabilita el uso de la política de filtros de rutas para determinar las rutas que serán anunciadas por RIP. El mandato **disable sending policy global** inhabilita el uso de la política global de envío de filtros de ruta para todas las interfaces RIP que reúnan las dos condiciones siguientes:

- No tienen configurada una política RIP de filtros de rutas de envío a nivel de interfaz. Si está configurada una política RIP de filtros de rutas de envíos a nivel de interface, esa política continúa determinando qué rutas son anunciadas.
- El envío de rutas RIP no está inhabilitado.

Después de que se inhabilite la política global RIP de envíos de rutas, las interfaces RIP ya no se encontrarán afectadas por dicha política.

El mandato **disable sending policy interface** *dirección-interfaz-ip* inhabilita 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*
Impide que el direccionador anuncie el tipo de ruta que se especifica en las actualizaciones RIP que se envían utilizando la dirección de interfaz ip de la interfaz. Los otros distintivos que controlan las rutas RIP enviadas fuera de una interfaz son **host-routes**, **static-routes**, **net-**

routes y **subnet-routes**. Estos valores pueden desactivarse individualmente. Una ruta sólo se anuncia si está especificada por cualquiera de los distintivos habilitados.

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 sólo las rutas RIP en los paquetes multidifusión RIP2.

dirección-interfaz-ip

Valores válidos: cualquier dirección IP válida de una interfaz que tenga habilitado RIP2.

Valor por omisión: ninguno

Ejemplo: `disable sending rip1-routes-only 128.185.123.22`

sending outage-only *dirección-IP-interfaz*

Inhabilita el envío de de actualizaciones RIP dependientes de la presencia de la ruta especificada en el mandato de habilitación análogo. Cuando esta función se encuentra inhabilitada, los anuncios RIP se enviarán incondicionalmente.

dirección-IP-interfaz

Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

Ejemplo: `disable sending outage-only`

simple-internet-access

Esta opción inhabilita el acceso simple a Internet en la interfaz que se especifica.

source-addr-verification

Esta opción de filtro de paquetes de entrada verifica si la dirección IP de origen del paquete recibido es consistente, basándose en la tabla de direccionamiento IP, con la interfaz desde la cual se recibió. Esta opción sirve para impedir el reenvío de paquetes desde un sistema principal IP que esté utilizando una dirección IP de origen que no le pertenezca, una técnica conocida como *usurpación*. Este mandato sólo es válido en la consola de configuración de filtro de paquetes (a la que se accede con el mandato **update packet-filter**).

source-routing

Impide que el direccionador reenvíe los paquetes direccionados desde origen (esto es, paquetes IP que incluyan una opción de ruta de origen). Esta opción habilita el direccionamiento de origen por omisión.

Ejemplo: `disable source-routing`

tftp-server

Impide que el direccionador acepte peticiones TFTP GET o PUT desde la red. De este modo, no se produce una sustitución de información de archivos de configuración o imágenes de carga desde otro dispositivo. Sin embargo, el usuario podrá ejecutar operaciones de cliente TFTP

(GET y PUT) desde el direccionador a través de un terminal conectado directamente o una sesión Telnet.

timestamp
Inhabilita en el direccionador la recepción o el reenvío de paquetes IP que contengan una opción IP de indicación de la hora. Por omisión, el direccionador recibe y reenvía estos paquetes.

trace *número-regla*
Inhabilita el rastreo de paquetes IP que coincidan con el número de regla de control de acceso especificado. Esta opción está inhabilitada por omisión. Si se desea más información sobre el rastreo de paquetes IP, véase el mandato**enable trace**.

Ejemplo: `disable trace 1`

udp-forwarding *número-puerto*
Inhabilita el reenvío UDP de paquetes recibidos por el direccionador con el número de puerto de destino UDP especificado.

Por omisión, el envío UDP está inhabilitado para todos los números de puerto.

número-puerto
Valores válidos: cualquier entero en el rango de 0 a 65535

Valor por omisión: 0

Ejemplo: `disable udp-forwarding 36`

vrrp Inhabilita el protocolo VRRP.

Ejemplo: `disable vrrp`

Enable

Utilice el mandato **enable** para activar las características y capacidades IP y la información añadida a la configuración IP del usuario.

Sintaxis:

en**able** arp-net-routing
arp-subnet-routing
bootp-forwarding
classless
compression-bypass
directed-broadcast
dynamic-address
echo-reply
encryption-bypass
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 habilitado, el direccionador responde por proxy a todas las peticiones ARP para destinos remotos a las que se accede con mayor facilidad desde el direccionador. Utilice este mandato cuando hay sistemas principales en la LAN que realizan ARP para todos los destinos, en vez de (como sería lo más habitual) solamente los destinos locales.

Ejemplo: `enable arp-net-routing`

arp-subnet-routing

Activa la función de direccionamiento ARP de subred del direccionador (denominada también Proxy ARP). Esta función sólo se utiliza cuando hay sistemas principales que no tiene conocimiento de subredes adjuntas a subredes IP directamente conectadas. La red directamente conectada que tiene sistemas principales que no reconozcan subredes debe utilizar ARP para que esta característica sea útil.

El direccionamiento de subredes ARP funciona como sigue: Cuando un sistema principal que no reconozca subredes quiere enviar un paquete IP a un destino en una subred remota, no se da cuenta que tendría que enviar el paquete a un direccionador. Por tanto, el sistema principal que no reconoce subredes se limita a difundir una petición ARP. Esta petición ARP es recibida por el direccionador. Éste responde como si fuera el destino (de ahí el nombre de proxy, cuyo significado original es "apoderado") si el direccionamiento de subredes arp está habilitado y si el salto siguiente al destino está sobre una interfaz distinta que la interfaz que recibe la petición ARP.

Si no hay sistemas principales en la LAN del usuario que sean “reconocedores de subred”, no habilite el direccionamiento de subred ARP. Si en una LAN es necesario el direccionamiento de subred ARP, entonces deberá habilitarse en todos los direccionadores de la LAN.

Ejemplo: `enable arp-subnet-routing`

bootp-forwarding

Activa el reenvío de paquetes BOOTP/DHCP. Para utilizar el reenvío de BOOTP, también es necesario 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 saltos de direccionamiento)

Número máximo de agentes BOOTP disponibles que pueden reenviar una petición de BOOTP del cliente al Servidor (éste no es el número máximo de saltos IP al servidor).

Por omisión: 4

Minimum seconds before forwarding (mínimo de segundos antes del reenvío)

Este parámetro generalmente no se utiliza. Utilice cuando exista una vía redundante entre el cliente y el servidor y se desea usar la vía o vías secundarias como reserva.

Valor por omisión: 0

classless Indica que el direccionador funcionará en un entorno de direccionamiento IP sin clase. El IBM 2212 da soporte plenamente al direccionamiento CIDR tal como se describe en el RCF 1817 sin que esta opción esté habilitada. La habilitación de esta opción impide la generación automática de las rutas de red con clase (por ejemplo, las rutas de red de clase A, B o C) correspondientes a rutas añadidas a la

tabla de direccionamiento de IP. Si no se está ejecutando RIPv1, no hace falta la ruta de red con clase.

Ejemplo: `enable classless`

compression-bypass *número-regla*
Habilita la elusión de la compresión de capa 2 para el control de acceso especificado por el *número-regla*, lo que hace que los paquetes eludan la compresión aunque esté habilitada en la interfaz de red. La elusión de compresión sólo puede habilitarse para los controles de acceso de tipo **include**.

Ejemplo: `enable compression-bypass 1`

directed-broadcast
Habilita el reenvío de paquetes IP cuyo destino es una dirección de difusión dirigida por red o bien una dirección de difusión dirigida por subred. El sistema principal de origen origina el paquete como unidifusión y a continuación se reenvía como unidifusión a una subred de destino donde "explota" en una multidifusión. Estos paquetes pueden utilizarse para localizar servidores de red. Este mandato habilita el reenvío y la explosión de multidifusiones dirigidas. El reenviador de paquetes IP nunca reenvía difusiones/multidifusiones a nivel de enlace, a no ser que correspondan a direcciones IP de Clase D. (Véase el mandato de OSPF **enable multicast-routing**.) Por omisión, esta característica está habilitada.

Nota: El reenvío y la explosión no pueden implementarse por separado. Además, el direccionador no reenviará las difusiones IP de todas las subredes.

Ejemplo: `enable directed-broadcast`

dynamic-address *0.0.0.n*
En la interfaz de red PPP especificada, permite al direccionador averiguar su dirección IP a partir del nodo remoto en la interfaz de red. Esta opción está inhabilitada por omisión.

Esta opción sólo es válida en una interfaz de red que se haya configurado como una interfaz de línea serie no numerada (la dirección IP asignada a la interfaz de red con el mandato **add address** es *0.0.0.n*, donde *n* es el número de la interfaz de red).

Nota: Para que el direccionador averígüe su dirección IP desde el modo remoto, además de habilitar esta opción también debe configurarse IPCP en la interfaz de red PPP para pedir una dirección IP desde el modo 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

Habilita la creación y envío de una Respuesta Eco ICMP en respuesta a una Petición Eco ICMP.

Ejemplo: `enable echo-reply`

encryption-bypass *número-regla*

Habilita la elusión de la compresión de capa 2 para el control de acceso especificado por el *número-regla*, lo que hace que los paquetes eludan el cifrado aunque esté habilitado en la interfaz de red. La elusión de cifrado sólo puede habilitarse para los controles de acceso de tipo **include**.

Ejemplo: `enable encryption-bypass 1`

fragment-offset-check

Habilita la comprobación de los fragmentos de desplazamiento de los paquetes IP recibidos en los que el número de protocolo IP es 6 (eso es, TCP). Los paquetes con un fragmento de desplazamiento de 1 se descartan. Esta opción está inhabilitada por omisión.

Nota: Después de que haya sido habilitada, esta función puede activarse sin afectar otras funciones de IP. Véase el mandato **reset IP** de talk 5 si se desea obtener más información.

icmp-redirect *dirección-interfaz-ip*

Habilita al direccionador para que envía mensajes ICMP redirigidos en la interfaz IP especificada. Si no se entra ningún valor en el indicador de mandatos para la dirección de interfaz IP, el direccionador será habilitado para enviar mensajes redirigidos ICMP en todas las interfaces IP.

dirección-interfaz-ip

Valores válidos: cualquier dirección IP válida, o nada para todas las interfaces IP

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*

Habilita el conocimiento del salto siguiente en una interfaz IP.

dirección-interfaz-ip

Valores válidos: cualquier dirección IP válida

Valor por omisión: disabled (inhabilitado)

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*

Habilita la prevalencia de la información RIP sobre cualquier ruta por omisión instalada en la tabla de direccionamiento IP. Este mandato se invoca según el criterio de una interfaz por IP. Cuando se invoca el mandato **enable override default**, las rutas RIP por omisión recibidas en la dirección de interfaz ip prevalecen por encima de la ruta por omisión actual del direccionador, suponiendo que el coste de la nueva ruta 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*

Habilita la información RIP recibida para que prevalezca por encima de cierta información de direccionamiento configurada estáticamente. Este mandato se invoca según el criterio de una interfaz por IP. Cuando se invoca el mandato **enable override static-routes**, la información de direccionamiento TIP recibida en la dirección de interfaz ip de la interfaz prevalece por encima de rutas de red/subred configuradas estáticamente, 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*

Habilita la lista de control de acceso determinada para una interfaz que se especifique (filtros de paquetes)

nombre-filtro

Valores válidos: cualquier nombre de 16 caracteres. Pueden incluirse guiones (-) y guiones de subrayado (_) en el nombre.

Valor por omisión: ninguno

Ejemplo: `enable packet-filter pf-in-0`

per-packet-multipath

Si está habilitado y hay más de una vía de igual coste a un destino, entonces el direccionador reparte la carga entre las vías de igual coste para cada paquete siguiendo un proceso cíclico. Por omisión, esta característica está inhabilitada.

Ejemplo: `enable per-packet-multipath`

receiving policy global/interface *dirección-interfaz-ip identificador-política-ruta*

Habilita el uso de la política de filtros de rutas para determinar las rutas que aceptará RIP. El mandato **enable receiving policy global** *identificador-política-rutas* habilita el uso de la política global de recep-

ción de filtros de rutas para todas las interfaces RIP que reúnan estas dos condiciones:

- No tienen configurada una política RIP de filtros de rutas de recepción a nivel de interfaz. Si está configurada una política RIP de filtros de rutas de recepción a nivel de interface, esa política continúa determinando qué rutas son anunciadas.
- La recepción de rutas RIP no está inhabilitada.

Después de habilitar la política global de recepción de filtros de ruta, las interfaces RIP que reúnan estas condiciones aceptarán rutas tal como se definen en la política.

El mandato **enable receiving policy interface** *dirección-interfaz-ip identificador-política-ruta* habilita el uso de la política de filtros de rutas para determinar qué rutas se aceptan en una determinada interfaz RIP. Nótese que las redes, subredes y sistemas principales dinámicos no son aplicables si la política de recepción global o de interfaz está habilitada.

dirección-interfaz-ip

Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

identificador-política-ruta

Valores válidos: un identificador de política de rutas válido consistente en una serie de 1 a 15 caracteres ASCII.

Valor por omisión: ninguno

receiving rip *dirección-interfaz-ip*

Habilita el proceso de actualizaciones RIP que se reciben en una interfaz determinada. Este mandato tiene un mandato análogo de inhabilitación. (Véase el mandato **disable receiving**.) Por omisión, este mandato está habilitado.

Si se invoca el mandato **disable receiving rip**, no se aceptarán actualizaciones 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 interfaz determinada. Este mandato tiene un mandato análogo de inhabilitación. (Véase el mandato **disable receiving**.) Por omisión, este mandato está habilitado.

Si se invoca el mandato **disable receiving dynamic nets** para las actualizaciones RIP recibidas en la interfaz *ip-interface-address*, el direccionador no aceptará ninguna ruta a nivel de red, a no ser que se haya especificado con 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 interfaz determinada. Este mandato tiene un mandato análogo de inhabilitación. (Véase el mandato **disable receiving**.) Por omisión, este mandato está habilitado.

Si se 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 haya especificado con 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
Habilita al direccionador para la recepción y reenvío de paquetes IP que contengan una opción IP de ruta de registro. Éste es el valor por omisión.

Nota: Después de que haya sido habilitada, esta función puede activarse sin afectar otras funciones de IP. Véase el mandato **reset IP** de talk 5 si se desea obtener más información.

rip Habilita el proceso del protocolo RIP del direccionador.

Cuando RIP esté habilitado, se establece el siguiente comportamiento por omisión:

- El direccionador incluye todas las rutas de red y subred en actualizaciones RIP que se envían en cada una de las direcciones IP configuradas.
- El direccionador procesa todas las actualizaciones de RIP recibidas en cada una de las interfaces IP que tiene configuradas.

Si se desea cambiar cualquiera de los comportamientos de envío/recepción, utilice los mandatos de configuración de IP, que se definen según un criterio de interfaz-por-IP.

Ejemplo: `enable rip`

rip2 *dirección-interfaz-ip autenticación-RIP2 claves-autenticación*

Habilita RIP1 en una interfaz IP. Se envían anuncios RIP2 a la dirección de multidifusión 224.0.0.9. RIP2 está descrito en el documento RFC 1723.

dirección-interfaz-ip

Indica la interfaz IP en la que RIP2 está habilitado.**Valores válidos**: cualquier dirección IP válida

Valor por omisión: ninguno

autenticación-RIP2

Indica si se utilizará o no una simple clave no cifrada para la autenticación de RIP2. No se requiere la autenticación.**Valores válidos**: yes o no

Valor por omisión: yes

clave-autenticación

Define una contraseña no cifrada que se utilizará para la autenticación de RIP2. Sólo se solicita esta serie cuando se ha respondido **yes** a la pregunta “Set RIP-2 Authentication?” Cuando se usa la autenticación RIP2, sólo se aceptan los paquetes RIP2 con una contraseña que coincida.**Valores válidos**: una serie no cifrada ASCII

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 tablas de rutas a cualquier ruta que se añada a la tabla de direccionamiento. Los filtros de tablas de rutas se aplican basándose en la coincidencia más específica de las máscaras de destino y de red. Los filtros de tablas de rutas nunca se aplican a rutas directas o estáticas.

Ejemplo: `enable route-table-filtering`

same-subnet

Habilita la opción de misma subred. Al rearrancar el dispositivo, no se permitirá que se instale más de una interfaz IP en la misma subred. Las interfaces IP múltiples en la misma subred son útiles solamente bajo una de las condiciones siguientes:

- OSPF Punto-a-Multipunto está configurado en las interfaces IP.
- Nexthop Awareness está habilitado en las interfaces IP y están definidas rutas estáticas para las rutas que pasan por las interfaces IP.

Esta opción está inhabilitada por omisión.

Ejemplo: `enable same-subnet`

sending default-routes *dirección-interfaz-ip*

Determina los contenidos de actualizaciones RIP que se envían fuera de una interfaz determinada. Este mandato tiene un mandato análogo de inhabilitación. (Véase el mandato **disable sending**.) El efecto del mandato **enable sending** es aditivo. Cada mandato de habilitación de envíos especifica que debe anunciarse un determinado conjunto de reglas desde una interfaz concreta. Una ruta se incluye en una actualización RIP sólo si ha sido incluida por al menos uno de los mandatos de habilitación de envíos. El mandato **enable sending default-routes**

especifica que la ruta por omisión (si existe una) debe incluirse en las actualizaciones RIP enviadas de 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 enviará rutas de red, estáticas y de subred.

sending net-routes *dirección-interfaz-ip*

Determina los contenidos de actualizaciones RIP que se envían fuera de una interfaz determinada. Este mandato tiene un mandato análogo de inhabilitación. (Véase el mandato **disable sending**.)

El efecto del mandato **enable sending** es aditivo. Cada mandato **enable sending** especifica que debe anunciarse un determinado conjunto de reglas para una interfaz concreta. Una ruta se incluye en una actualización RIP sólo si ha sido incluida por al menos uno de los mandatos **enable sending**. El mandato **enable sending network-routes** especifica que todas las rutas a nivel de red deberían incluirse en actualizaciones RIP enviadas de la interfaz *dirección-interfaz-ip*. Una ruta a nivel de red es una ruta a una 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-suministro máscara-red-corte*

Habilita el envío de paquetes de actualización RIP en la interfaz especificada por *dirección-ip-interfaz* dependiendo de la presencia de la ruta IP especificada por *red-corte-suministro* y *máscara-red-corte*. Normalmente, las actualizaciones se envían incondicionadamente en interfaces configuradas para anunciar rutas RIP. Además, las actualizaciones RIP no se tienen en cuenta en una interfaz de sólo corte de suministro cuando está presente la ruta especificada. Esta función puede ser útil en contextos de reserva, cuando el circuito de marcación de reserva está configurado como circuito de marcación según demanda.

dirección-interfaz-ip

Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

red-corte-suministro

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 sólo se enviarán en la interfaz no numerada cuando la ruta 10.50.0.0/255.255.0.0 no aparece en la tabla de direccionamiento.

sending poisoned-reverse-routes *dirección-interfaz-ip*
Técnica utilizada por RIP para mejorar el tiempo de convergencia cuando cambian las rutas (si desea obtener información más detallada de esta técnica, consulte el documento RCF 1058). El uso de esta técnica incrementa el tamaño de los mensajes de actualización RIP. Es posible que resulte más conveniente minimizar la información extra de direccionamiento aceptando una convergencia un poco más lenta. El mandato **disable sending poisoned-reverse-routes** especifica que las rutas envenenadas no deben incluirse en las actualizaciones RIP enviadas en una interfaz especificada mediante el mandato **enable ip-interface-address**.

Por omisión: Habilitado

dirección-interfaz-ip
Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

sending policy global/interface *dirección-interfaz-ip identificador-política-ruta*
Habilita el uso de la política de filtros de rutas para determinar las rutas que anunciará RIP. El mandato **enable sending policy global** *identificador-política-ruta* habilita el uso de la política global de envío de filtros de ruta para las interfaces RIP que reúnan las dos condiciones siguientes:

- No tienen configurada una política RIP de envíos a nivel de interfaz. Si está configurada una política RIP de envíos a nivel de interfaz, continúa determinando qué rutas son anunciadas.
- El envío de rutas RIP no está inhabilitado.

Después de habilitarse la política global de envío de filtros de ruta, las interfaces RIP que reúnan estas dos condiciones anunciarán las rutas del modo que determine la política global de envío de filtros de rutas.

El mandato **enable sending policy interface** *dirección-interfaz-ip identificador-política-ruta* habilita el uso de la política de filtros de rutas para determinar qué rutas se anunciarán en la interfaz RIP especificada. La política de filtros de rutas sirve para filtrar rutas agregadas. En el apartado “Agregación de ruta” en la página 254 hallará más información.

dirección-interfaz-ip
Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

identificador-política-ruta
Valid Values: un identificador de política de rutas válido consistente en una serie de 1 a 15 caracteres ASCII.

Valor por omisión: ninguno

sending rip-routes-only *dirección-interfaz-ip*

Anuncia solamente las rutas RIP en los paquetes multidifusión RIP2.

dirección-interfaz-ip

Valores válidos: cualquier dirección IP válida de una interfaz que tenga habilitado RIP2.

Valor por omisión: ninguno

Ejemplo: `enable sending rip-routes-only 128.185.123.22`

sending subnet-routes *dirección-interfaz-ip*

Determina los contenidos de actualizaciones RIP que se envían fuera de una interfaz determinada. Este mandato tiene un mandato análogo de inhabilitación. (Véase el mandato **disable sending**.) El efecto del mandato **enable sending** es aditivo. Cada mandato **enable sending** especifica que un determinado conjunto de rutas deberían anunciarse fuera de una interfaz concreta. Una ruta se incluye en una actualización RIP sólo si ha sido incluida por al menos uno de los mandatos de habilitación de envíos. El mandato **enable sending subnet-routes** especifica que todas las rutas de subred deberían incluirse en las actualizaciones RIP enviadas desde la interfaz dirección-interfaz-ip. Sin embargo, una ruta de subred sólo se incluye si la dirección-interfaz-ip se conecta directamente a una subred de la misma red IP con subredes.

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 los contenidos de actualizaciones RIP que se envían fuera de una interfaz determinada. Este mandato tiene un mandato análogo de inhabilitación. (Véase el mandato **disable sending**.) El efecto del mandato **enable sending** es aditivo. Cada mandato **enable sending** por separado especifica que un determinado conjunto de rutas que reúnan otros criterios de envío deberían anunciarse fuera de una interfaz concreta. Una ruta se incluye en una actualización RIP sólo si ha sido incluida por al menos uno de los mandatos **enable sending**. El mandato **enable sending static-routes** especifica que todas las rutas configuradas estáticamente y conectadas directamente deberían incluirse en actualizaciones RIP enviadas fuera de 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 los contenidos de actualizaciones RIP que se envían fuera de una interfaz determinada. Este mandato tiene un mandato análogo **disable ...**. (Véase el mandato **disable sending**.) El efecto del mandato **enable sending** es aditivo. Cada mandato **enable sending** especifica que un determinado conjunto de rutas deberían anunciarse fuera de una interfaz concreta. Una ruta se incluye en una actualización RIP sólo si

ha sido incluida por al menos uno de los mandatos **enable sending**. El mandato **enable sending host-routes** especifica que todas las rutas de sistema principal deberían incluirse en actualizaciones RIP enviadas fuera de la interfaz dirección-interfaz-ip.

dirección-interfaz-ip

Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

simple-internet-access

Esta opción habilita el acceso simple a Internet en la interfaz que se especifique. Utilice el acceso simple a Internet para crear una configuración integrada que incluya una línea serie no numerada con la opción de dirección dinámica habilitada, filtros de paquetes IP (tanto de entrada como de salida), controles de acceso IP (tanto de entrada como de salida), una ruta por omisión, fondo común de reserva de NAT/NAPT y una subred de dirección privada en la característica de DHCP. Los usuarios que tengan requisitos adicionales para la configuración integrada deberían tener en consideración una configuración manual.

Nota: Esta opción sólo está disponible en imágenes que incluyan las características DHCP y NAT.

source-addr-verification

Esta opción de filtro de paquetes de entrada verifica si la dirección IP de origen del paquete recibido es consistente, basándose en la tabla de direccionamiento IP, con la interfaz desde la cual se recibió. Esta opción sirve para impedir el reenvío de paquetes desde un sistema principal IP que esté utilizando una dirección IP de origen que no le pertenezca, una técnica conocida como *usurpación*. Este mandato sólo es válido en la consola de configuración de filtro de paquetes (a la que se accede con el mandato **update packet-filter**).

source-routing

Permite al direccionador reenviar paquetes IP que contengan una opción de ruta de origen IP.

Ejemplo: `enable source-routing`

tftp-server

Permite al direccionador aceptar peticiones TFTP GET o PUT de la red para archivos de configuración o cargas de imagen.

Ejemplo: `enable tftp-server`

timestamp

Habilita en el direccionador la recepción o el reenvío de paquetes IP que contengan una opción IP de indicación de la hora. Éste es el valor por omisión.

Nota: Después de que haya sido habilitada, esta función puede activarse sin afectar otras funciones de IP. Véase el mandato **reset IP** de talk 5 si se desea obtener más información.

trace *número-regla*

Habilita el rastreo de paquetes IP que coincidan con el número de regla de control de acceso especificado. Esta opción está inhabilitada por omisión.

El rastreo de paquetes IP utiliza la función de rastreo de paquetes del sistema para el registro cronológico de sucesos. Consulte los mandatos **set trace** y **view** en el capítulo Configuración y supervisión del sistema para el registro cronológico de sucesos (ELS) de la publicación *Access Integration Services Guía del usuario de software* si desea obtener información detallada acerca de estos mandatos. Solamente se rastrean los paquetes IP que coincidan con una regla de control de acceso para la que está habilitado el rastreo. La regla de control de acceso podría 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 visualizar las reglas para las que se ha habilitado 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=17
                SMask =0.0.0.0    DMAask =0.0.0.0
                SPorts=5004-5511  DPorts=5004-5511
                       T/C=**/**  Log=N
                BypassComp BypassEncIP 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*

Habilita el reenvío UDP para los paquetes recibidos por el direccionador con el número de puerto de destino UDP especificado.

Por omisión, el envío UDP está inhabilitado para todos los números de puerto.

número-puerto

Valores válidos: cualquier entero en el rango de 0 a 65535

Valor por omisión: 0

Ejemplo: `enable udp-forwarding 36`

vrrp Habilita el protocolo VRRP.

Ejemplo: `enable vrrp`

List

Utilice el mandato **list** para visualizar distintos trozos de los datos de configuración IP, dependiendo del submandato que se invoque en cada caso.

Sintaxis:

list

all
access-control
addresses
aggregate
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 Visualiza toda la configuración IP.

Ejemplo: `list all`

access-control

Visualiza el modo de control de acceso configurado (habilitado o inhabilitado) y la lista de registros de control de acceso global configurados. Cada registro aparece con su número de registro. Este número de registro puede usarse para reordenar la lista con el mandato IP **move access-control**.

Ejemplo: `list access-control`

```
list access-control
1   Type=I   Source=0.0.0.0    Dest   =0.0.0.0     Prot=17
             SMask =0.0.0.0    DMAask =0.0.0.0
             SPorts=5004-5511  DPorts=5004-5511
                    T/C=**/**  Log=N
             BypassComp BypassEnc
```

addresses

Visualiza las direcciones de interfaz IP que se han asignado al direccionador, junto con sus formatos de difusión configurados. La interfaz identificada por *BDG/0* es la interfaz de puente.

Ejemplo: `list addresses`

aggregate

Visualiza todas las rutas agregadas configuradas.

Ejemplo:

```
IP config>list aggregate

                Aggregate Route Configuration

Address         Mask            Type           Policy/Metric
-----------------------------------------------------------------
10.1.0.0        255.255.0.0     Unconditional         12
10.2.0.0        255.255.0.0     Policy-Driven  EAST-REGION
```

bootp Indica si el reenvío BOOTP está habilitado o inhabilitado, además de la lista configurada de servidores BOOTP.

Ejemplo: `list bootp`

filters Relaciona las redes filtradas del direccionador configuradas.

icmp-redirect

Expresa en una lista si el envío de mensajes de redirección ICMP está habilitado o inhabilitado en cada interfaz IP.

igmp Visualiza la configuración 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 Enumera los valores MTU configurados.

nexthop-awareness

Enumera el establecimiento de conocimiento de salto siguiente para 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*

Enumera información sobre filtros de paquetes. Si se especifica un nombre, el mandato enumera la información de control de acceso configurada para el filtro. Si no se especifica un nombre de filtro, el mandato enumera los filtros de paquetes configurados. Si se ha configurado un filtro de paquetes en la interfaz de puente, ésta se identifica con *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=I   Source=0.0.0.0    Dest   =0.0.0.0     Prot=17
                SMask =0.0.0.0    DMAask =0.0.0.0
                SPorts=5004-5511  DPorts=5004-5511
                       T/C=**/**  Log=N
                BypassComp BypassEnc

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

Enumera los diversos 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

Visualiza el estado de configuración de los protocolos de direccionamiento IP, (OSPF, RIP, BGP), además de otros valores generales de configuración.

Ejemplo: `list protocols`

redundant default gateway

Visualiza la pasarela IP por omisión redundante de 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 Visualiza todos los parámetros de configuración de RIP. RIP puede configurarse para recibir y enviar rutas dinámicas o las rutas que pueden definirse mediante una política de filtros de rutas. Véanse los mandatos de configuración de IP **enable receiving dynamic nets/subnets/hosts** si se desea más información sobre el direccionamiento dinámico. Véase “Configuración de políticas de filtros de rutas” en la página 331 si se desea más información sobre políticas de filtros 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-ruta*

Visualiza información sobre la política de rutas configurada. Si se especifica una política de rutas concreta, se visualiza una lista detallada de esa política de rutas. Si no se especifica una política de rutas concreta, se visualiza 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

Visualiza la lista de filtro 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 Visualiza la lista de rutas estáticas que se han configurado.

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

Visualiza el número de interfaz del acceso simple a Internet.

sizes Visualiza el tamaño de la tabla de direccionamiento, el tamaño del almacenamiento de reserva de reensamblaje y el tamaño de antememoria de la ruta.

Ejemplo: `list sizes`

tags Visualiza los identificadores por interfaz que se asociarán con la información RIP recibida. Estos identificadores pueden utilizarse para agrupar rutas para un posterior reanuncio vía BGP, donde un identificador se tratará como si fuera un sistema autónomo (AS) de origen de la ruta. Los identificadores también se propagan mediante el protocolo de direccionamiento OSPF.

Ejemplo: `list tags`

udp-forwarding

Visualiza toda la información configurada para la función de reenvío UDP, incluyendo todos los puertos y todas las direcciones IP.

Ejemplo: `list udp-forwarding`

vrid Visualiza el estado del VRRP, VRID y direcciones VRID configurados. En este ejemplo, el parámetro *Preempt mode* y la opción *Hardware MAC address* son ambos **yes**, tal y como indica el campo Flags, en el que figura P y H.

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,H
```

Move

Utilice el mandato **move** para cambiar el orden de los registros en la lista global de control de acceso. Este mandato coloca el número de registro *núm-inicial* inmediatamente después del número de registro *núm-final*. Después de mover los registros, inmediatamente quedan renumerados según el nuevo orden.

El direccionador aplica los registros de control de acceso en una lista según el orden en que fueron creados. Para cada paquete que se reciba en una interfaz, el direccionador aplica cada registro de control de acceso por orden, hasta que encuentra una coincidencia. El primer registro que coincida con el paquete determina si éste será descartado o reenviado a su destino.

Esto hace que el orden de los registros de control de acceso sea muy importante. Si los registros se encuentran en un orden incorrecto, algunos paquetes podrían pasar, o bien ser bloqueados de modo contrario a las intenciones del usuario.

Por ejemplo, pongamos que el registro de control de acceso 1 hace cumplir la regla según la cual : *todos los paquetes de la red 10.0.0.0 serán bloqueados en esta interfaz.* Contrariamente a esto, el registro de control 2 especifica : *Los paquetes de la subred 10.5.5.0 en la red 10.0.0.0, destinados a la dirección 1.2.3.4, podrán pasar.* Según este orden, los registros bloquearán todo el tráfico de 10.0.0.0, incluso si el registro 2 permite explícitamente que pasen ciertos tipos de paquetes.

En este ejemplo, el registro 1 convierte el registro 2 en papel mojado. El registro 1 garantiza que el direccionador descarta todos los paquetes de 10.0.0.0, a pesar de que la intención del registro 2 es la de que se reenvíen algunos de los paquetes. La clave en solucionar este tipo de problemas reside en el orden de los registros de control de acceso. De este modo, los paquetes en la subred 10.5.5.0 destinados a la dirección 1.2.3.4 pasarán por la interfaz; el direccionador descartará todos los otros paquetes de 10.0.0.0, tal como se quería.

Sintaxis:

m**ove** a**ccess-control** *núm-inicial núm-final*

Ejemplo: `move 5 2`

Set

Utilice el mandato **set** para establecer determinados valores, rutas y formatos dentro de su configuración 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* **o bien** *off*

Permite configurar el direccionador para que habilite o inhabilite el control de acceso IP. El establecimiento del control de acceso en *on* habilita la lista global de control de acceso, además de las listas específicas de la interfaz. El establecimiento en *off* inhabilita todas listas, aunque no las suprime.

Ejemplo: `set access-control on`

access-control log-facility *recurso*

Establece el recurso de SysLog para el control de acceso. La opción del recurso de SysLog define el sistema en el que se visualizarán los mensajes de Syslog.

Nota: Después de que haya sido habilitada, esta función puede activarse sin afectar otras funciones de IP. Véase el mandato **reset IP** de talk 5 si se desea obtener más información.

recurso **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 IP que utiliza el direccionador al difundir paquetes fuera de una interfaz concreta. El direccionador utiliza más comúnmente las difusiones IP al enviar paquetes de actualización RIP.

El parámetro de estilo puede adoptar bien el valor local-wire o el valor network. Las direcciones difundidas local-wire constan o bien de todo unos (255.255.255.255) o bien de todo ceros (0.0.0.0). Las difusiones de estilo network empiezan por la parte de red y subred de la dirección-interfaz-ip.

El parámetro de patrón de relleno puede establecerse en 1 o bien 0. Ello indica si el resto de la dirección difundida (esto es, que no sea la parte de la red y la subred, si hay alguna) debe establecerse a todo unos o todo ceros.

Durante la recepción, el direccionador reconoce todas las formas de la dirección IP difundida.

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 un dirección de difusión de 255.255.255.255. El segundo ejemplo produce una dirección de difusión de 192.9.1.0, suponiendo que la red 192.9.1.0 no es una subred.

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 almacena información acerca de las direcciones IP específicas a las que el direccionador ha reenviado paquetes recientemente. La antememoria reduce el tiempo de proceso que se necesita para reenviar múltiples paquetes al mismo destino.

En contraste con esta antemrmoria, la *tabla* de direccionamiento IP almacena información acerca de todas las redes accesibles, pero no contiene ninguna dirección de destino IP específica. Utilice el mandato **set routing table-size** para configurar el tamaño de la tabla de direccionamiento IP.

Valores válidos: de 64 a 10000

Valor por omisión: 64

Ejemplo: `set cache-size 64`

default network-gateway *salto-siguiente coste*

Configura una ruta al direccionador autorizado (pasarela por omisión). Se supone que la pasarela por omisión del direccionador tiene una información de direccionamiento más completa que el direccionador mismo.

La ruta está especificada por la dirección IP del salto siguiente (salto-siguiente) y la distancia (coste) que media hasta la pasarela por omisión.

Todos los paquetes con destinos desconocidos se reenvían al direccionador autorizado (pasarela por omisión).

salto-siguiente **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 en el rango de 0 a 255

Valor por omisión: 1

Ejemplo: `set default network-gateway 192.9.1.10 10`

default subnet-gateway *red-con-subredes salto-siguiente coste*

Configura una ruta al direccionador autorizado (pasarela de subred por omisión). Puede configurarse una pasarela de subred por omisión separada para cada red con subredes.

La dirección IP del salto siguiente (salto-siguiente) y la distancia (coste) que media hasta la pasarela de subred por omisión especifican la ruta.

Todos los paquetes que se destinan a subredes desconocidas de una red conocida con subredes se reenvían al direccionador autorizado de la red con subredes (pasarela de subred por omisión).

red-con-subredes

Valores válidos: cualquier dirección IP válida

Valor por omisión: 0.0.0.0

salto-siguiente

Valores válidos: cualquier dirección IP válida

Valor por omisión: 0.0.0.0

coste

Valores válidos: un entero en el rango de 0 a 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 que se deben asignar a la antememoria de flujo DiffServ. Ésta se asigna si se cumple una de las condiciones siguientes:

- La función de servicios diferenciados (DiffServ o DS) está habilitada (consulte Configuración y supervisión de la función de servicios diferenciados en la publicación *Utilización y configuración de las funciones* si desea obtener información más detallada).
- La función de seguridad IP (IPSec) está habilitada (consulte Configuración y supervisión de la seguridad IP en la publicación *Utilización y configuración de las funciones* si desea obtener información más detallada).
- La función de políticas está habilitada (consulte Configuración y supervisión de la función de políticas en la publicación *Utilización y configuración de las funciones* si desea obtener información más detallada).

Valores válidos: de 64 a 8192

Valor por omisión: 1024

igmp ... Configura los parámetros IGMP. Pueden especificarse valores para los parámetros siguientes:

qu**ery interval** *red intervalo*
Cambia el intervalo entre consultas generales de IGMP.

red Especifica el número de red para que se configure la interfaz.

Valores válidos: cualquier máscara de red válida

Valor por omisión: ninguno

intervalo Especifica el número de segundos entre las transmisiones de consultas generales .

Valores válidos: de 1 a 3600

Valor por omisión: 125

re**sponse-interval** *red intervalo*
Cambia el tiempo máximo de respuesta insertado en consultas generales IGMP.

red Especifica el número de red para que se configure la interfaz.

Valores válidos: cualquier máscara de red válida

Valor por omisión: ninguno

intervalo Especifica el número de segundos entre las transmisiones de una consulta y un sistema principal enviando como respuesta un informe IGMP

Valores válidos: de 1 a 60

Valor por omisión: 10

ro**bustness-variable** *red variable*
Cambia la variable de robustez para una red.

red Especifica el número de red para que se configure la interfaz.

Valores válidos: cualquier máscara de red válida

Valor por omisión: ninguno

variable Especifica el número de paquetes IGMP enviados para evitar la pérdida de paquetes en una red.

Valores válidos: de 2 a 10

Valor por omisión: 2

le**ave-interval** *red intervalo*
Cambia el tiempo máximo de respuesta insertado en consultas específicas IGMP.

red Especifica el número de red para que se configure la interfaz.

Valores válidos: cualquier máscara de red válida

Valor por omisión: ninguno

intervalo Especifica el número de segundos permitidos entre las transmisiones de consultas específicas y un sistema principal enviando como respuesta un informe IGMP.

Valores válidos: de 1 a 60

Valor por omisión: 1

ve**rsion** *red núm-ver*

Cambia la versión de IGMP que se ejecuta en una red.

red Especifica el número de red para que se configure la interfaz.

Valores válidos: cualquier máscara de red válida

Valor por omisión: ninguno

núm-ver Especifica el número de versión a ejecutar en la red.

Valores válidos: 1 o 2

Valor por omisión: 2

internal-ip-address *dirección-ip*

Configura una dirección IP independiente del estado de cualquier interfaz. La dirección interna siempre se considera activa. El motivo principal para definir una dirección interna es proporcionar una dirección para una dirección TCP que no pasará a inactiva cuando lo haga una interfaz. Esta dirección se utiliza para la conmutación de enlace de datos (DLSw), permitiendo el uso de vías alternas con el fin de evitar conexiones DLSw alteradas cuando una interfaz se vuelva inactiva. Puesto que la dirección interna permanece activa y OSPF mantiene rutas IP activas a su destino, el direccionamiento IP puede conmutar el tráfico de DLSw en la vía alterna, sin hacer caer la conexión TCP o alterar las sesiones de SNA que se estén ejecutando por encima de DLSw.

La dirección IP interna también es de utilidad cuando se utilizan interfaces no numeradas. Es la primera dirección de origen que se escoge para los paquetes originados por este direccionador y transmitidos por encima de una interfaz no numerada. La estabilidad de esta dirección facilita el rastreo de estos paquetes. La posibilidad de que se produzca una confusión todavía se reduce más cuando se utiliza la misma dirección IP para el ID de direccionador y la dirección interna. Por lo tanto, el ID del direccionador tomará por omisión la dirección interna.

Cuando se define una dirección interna, se anunciará por OSPF como una ruta de sistema principal en todas las áreas directamente conectadas al direccionador. También aparecerá como una ruta de sistema principal y se anunciará en RIP si la configuración de envíos RIP de la interfaz lo permite.

Valores válidos: cualquier dirección IP válida.

Valor por omisión: ninguno

Ejemplo: `set internal-ip-address 142.82.10.1`

mtu Establece el valor de MTU para el protocolo IP en esta interfaz.

Valores válidos: 0, 68 - 65535

Valor por omisión: Como mínimo todas las MTU no-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 en la tabla de direccionamiento de este direccionador están determinadas por un número de protocolos.
- RIP es uno de estos protocolos.
- Como mucho, se importa información de direccionamiento parcial de los demás protocolos y es advertida por RIP.

El tráfico de la red RIP para los destinos que no son conocidos por RIP pueden seguir la vía por omisión a este direccionador. La información de direccionamiento más completa en la tabla de direccionamiento de este nodo puede utilizarse entonces para reenviar el tráfico por una vía apropiada hacia su destino. Puede configurarse el direccionador para originar solamente el valor por omisión cuando este direccionador conoce rutas que no se anunciarán en la red RIP.

Cuando el usuario emite este mandato, se le solicitará que indique si el direccionador siempre debería originar un valor RIP por omisión u originarlo solamente cuando las rutas desde otros protocolos no están disponibles)

Esta ruta por omisión dirigirá el tráfico de una red no RIP a un direccionador de límite. Originar una sola ruta por omisión significa que el direccionador de límite no tiene que distribuir la otra información de direccionamiento de la red a los otros nodos de la red.

From AS number

Valores válidos: cualquier entero en el rango de 0 a 65535

Valor por omisión: ninguno

To network number

Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

Default cost

Valores válidos: un entero en el rango de 0 a 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]?
```

- La respuesta “Yes” a la pregunta “Always originate” significa que siempre se origina una ruta por omisión.
- La respuesta “Yes” a la pregunta “BGP” origina un valor por omisión cuando hay rutas BGP en la tabla de direccionamiento.

- La respuesta “Yes” a la pregunta “if OSPF routes available” hace que el valor (valor, ruta, vía, mateix a l'anterior) RIP por omisión sea anunciada cuando haya rutas OSPF en la tabla de direccionamiento.
- Cuando el direccionador decide originar un valor RIP por omisión, utiliza el número de “original default cost”.
- Cuando se especifica 0 para el número de ruta AS (Sistema Autónomo) de BGP, una ruta que cumpla los criterios de red desde cualquier AS hará que se origine un valor RIP por omisión.
- Cuando se especifica 0.0.0.0 para los criterios de red BGP, cualquier ruta GBP que cumpla los criterios AS hará que se origine un valor RIP por omisión.

reassembly-size *bytes*

Configura el tamaño de los almacenamientos de reserva que se utilizan para el reensamblaje de 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 que se añada a las rutas RIP de una interfaz antes de la instalación en la tabla de direccionamiento.

dirección-interfaz-ip

Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

métrica **Valores válidos**: un entero en el rango de 1 a 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 que se añada 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 en el rango de 0 a 15

Valor por omisión: 0

Ejemplo: `set rip-out-metric 128.185.120.209 0`

router-id *dirección-ip*

Establece la dirección IP por omisión utilizada por el direccionador al originar varios paquetes IP. Esta dirección es particularmente importante en multidifusión y OSPF.

El ID del direccionador debe coincidir con una de las direcciones de interfaz IP del direccionador configuradas o con la dirección IP interna configurada. En caso contrario, se ignora. Si se ignora, o simplemente no se configura, la dirección IP por omisión del direccionador (y su ID

de direccionador OSPF) queda establecida en la dirección IP interna (si está configurada) o la primera dirección IP en 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*

Establece el tamaño de la tabla de direccionamiento IP del direccionador. El tamaño por omisión es de 768 entradas. Si se establece un tamaño para la tabla de direccionamiento demasiado pequeño, se eliminará información de direccionamiento dinámico. Si se establece para la tabla de direccionamiento un tamaño demasiado grande, se malgastan recursos de memoria del direccionador. Véase “Sizes” en la página 354 si se desea información adicional acerca de los tamaños de tablas.

Valores válidos: un número entero de entradas en el rango de 64 a 65535

Valor por omisión: 768 entradas

Ejemplo: `set routing table-size 1000`

tag Configura los identificadores por interfaz asociados con la información RIP recibida Estos identificadores pueden utilizarse para agrupar rutas para un posterior reanuncio vía BGP, donde un identificador se tratará como si fuera un número de sistema autónomo (AS) de origen de la ruta. (Si se desea más información sobre políticas de origen, envío y recepción, consulte el capítulo “Utilización y configuración de BGP” en la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 1*.) Los identificadores también se propagan mediante el protocolo de direccionamiento OSPF.

Valores válidos: cualquier entero en el rango de 0 a 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 número en el rango de 1 a 255

Valor por omisión: 64

Ejemplo: `set ttl 255`

Update

Utilice el mandato **update packet-filter** para configurar filtros de paquetes. Éste es un ejemplo del mandato:

```
IP config> update packet-filter
    Packet-filter name [ ]? pf-1-in
Packet-filter 'pf-1-in' Config>
```

Packet-filter name es cualquier nombre de filtro de paquetes que se haya creado con el mandato **add packet-filter** *nombre-filtro-paquetes* desde el indicador `IP`

config>. Para habilitar el filtro de paquetes se utiliza el mandato **set access-control on**. Desde el indicador Packet-filter '*nombre-filtro-paquetes*' Config> pueden entrarse los mandatos siguientes:

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** desde el indicador Packet-filter '*nombre-filtro*' Config>, consulte la descripción de los parámetros dada en el parámetro **access-control** que se visualiza en el indicador de mandatos IP config>. Por ejemplo, consulte **add access-control** si desea obtener una descripción de los parámetros del mandato **update packet-filter add access-control**.

Para los mandatos **disable** y **enable**, la palabra clave **source-addr-verification** únicamente puede configurarse desde el indicador Packet-filter '*nombre-filtro*' Config>.

Las secciones siguientes enumeran los parámetros exclusivos del mandato **update packet-filter**. Son parámetros que se aplican a filtros de paquetes, pero no a filtros de todo el ámbito del direccionador, y sólo se entran mediante el indicador Packet-filter '*nombre-filtro*' Config>.

add/change access-control *tipo*

Conversión de direcciones de red (NAT)

Este tipo de regla de control de acceso de filtro de paquetes hace pasar los paquetes a NAT para la conversión de direcciones. Este tipo solamente es válido en filtros de paquetes y sólo cuando se especifica en combinación con reglas inclusivas; por ejemplo, ***IN***. Consulte la descripción de la función NAT en la publicación *Access Integration Services Guía del usuario de software* si desea obtener más información. En el capítulo Utilización de la conversión de direcciones de red de la publicación *Utilización y configuración de las funciones* hallará un ejemplo de reglas de control de acceso para NAT.

Valor válido: N

Valor por omisión: ninguno

disable/enable source-addr-verification

Esta opción de filtro de paquetes de entrada verifica si la dirección IP de origen del paquete recibido es consistente, basándose en la tabla de direccionamiento IP, con la interfaz desde la cual se recibió. Esta opción sirve para impedir el reenvío de paquetes desde un sistema principal IP

que esté utilizando una dirección IP de origen que no le pertenezca, una técnica conocida como *usurpación*.

Ejemplo:

```
Packet-filter 'nombre-filtro' Config> enable source-addr-verification
```

disable/enable trace *número-índice-control-acceso*

Esta opción inhabilita o habilita el rastreo de paquetes para una regla específica de control de acceso. Para ver los paquetes rastreados, utilice el mandato **event** de GWON de Talk 5; y para visualizar los registros de rastreo, utilice el mandato **view** de ELS de Talk 5 con las opciones adecuadas para visualizar los registros de rastreo.

Nota: Para hacer activo el rastreo, entre el mandato de Talk 5 **reset IP**.

Ejemplo:

```
Packet-filter 'nombre-filtro' Config> enable trace 1
```

Ejemplos:

Los ejemplos siguientes muestran cómo configurar diversas reglas de control de acceso para filtros de paquetes. En el capítulo “Utilización de la conversión de direcciones de red” de la publicación Utilización y configuración de las funciones hallará un ejemplo de reglas de control de acceso para NAT.

Ejemplo 1—Regla de control de acceso de tipo Exclusiva

Este ejemplo muestra cómo excluir todos los paquetes de entrada que se originen desde la red 128.185.0.0 y se reciban 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 al mandato **list access-control** para encontrar 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 que se ha 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 los puertos de destino y *Sports* son los puertos de origen.

Ejemplo 3— List access-control command (mandato de enumeración de control de acceso)

Puede utilizarse el mandato **list access-control** para visualizar 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 utilizados para configurar políticas de filtros de rutas. Síganse los pasos siguientes para acceder a esta subconjunto de mandatos de configuración de IP:

1. Créese una política de filtro de rutas. Véase el mandato **add route-policy** en la página 281.
2. Utilice el mandato **change route-policy** para hacer aparecer el indicador de mandatos `IP Route Policy Config>`. El indicador de mandatos `IP Route Policy Config>` sólo se aplica a la política de rutas concreta que se ha identificado 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 filtro de rutas pueden utilizarse para determinar qué rutas se importan en OSPF y los detalles concretos de su anuncio, incluyendo el tipo externo OSPF, la métrica y el valor del identificador. Consulte el mandato **enable as boundary routing** en la página 390 si desea obtener información acerca del uso de políticas de filtros de rutas para configurar OSPF.

Las políticas de filtros de rutas también pueden utilizarse para controlar qué rutas se anuncian o aceptan cuando se utiliza RIP. Véanse los mandatos anteriormente descritos **enable receiving**, **enable sending**, **disable receiving** y **disable sending**.

Tabla 19. Resumen de los 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 filtros de rutas.
Delete	Suprime una acción, una entrada o una condición de coincidencia de una política de filtros de rutas.
List	Enumera las entradas de política de rutas, acciones y condiciones de coincidencia para la política de rutas que se está cambiando.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Add

Utilice al mandato **add** para añadir entradas de política de filtros de rutas a la política de filtros de rutas, añadir condiciones de coincidencia a entradas ya existentes o añadir acciones a entradas existentes.

Sintaxis:

add action . . .

entry . . .

match-condition . . .

action . . .

Añade una acción a una entrada de política de filtros de rutas ya existente. Añadir una acción a una política de filtros de rutas es opcional. Puede añadirse una acción a cada entrada. Si se necesita aplicar más de una acción a una dirección o rango de direcciones, especifique una segunda entrada para esa dirección o rango. A continuación, defínase la segunda acción para la segunda entrada. Éstas son las acciones que pueden especificarse:

Sintaxis:

auto-tag

set manual-tag

set metric

set route-type

auto-tag *índice-política-ruta*

Establece automáticamente el identificador para la ruta, utilizando un protocolo de direccionamiento heurístico específico. Esta opción está descrita en el documento 1745.

índice-política-ruta

Identifica la entrada a la que debe aplicarse la acción.

Valor válido: de 1 a 65535

Valor por omisión: ninguno

set manual-tag *índice-política-ruta identificador-manual*
Establece el identificador manual para la ruta al valor que se especifique. Este identificador habitualmente es el número de AS cuando el protocolo es OSPF.

índice-política-ruta
Identifica la entrada a la que debe aplicarse la acción.

Valor válido: de 1 a 65535

Valor por omisión: ninguno

identificador-manual

Valor válido: X'de 0' a X'FFFFFFFF'

Valor por omisión: ninguno

set metric *índice-política-ruta métrica*
Establece la métrica para la ruta al valor que se especifique.

índice-política-ruta
Identifica la entrada a la que debe aplicarse la acción.

Valor válido: de 1 a 65535

Valor por omisión: ninguno

métrica

Valor válido: de 1 a 255

Valor por omisión: ninguno

set route-type *índice-política-ruta tipo-ruta*
Establece el tipo de ruta OSPF externa. Esta acción se ignora para aplicaciones que no sean la importación OSPF de rutas limítrofes de AS.

índice-política-ruta
Identifica la entrada a la que debe aplicarse la acción.

Valor válido: de 1 a 65535

Valor por omisión: ninguno

tipo-ruta

Valor válido: 1 o 2

Valor por omisión: ninguno

entry *índice-política-ruta 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 cambia. Cada entrada dentro de una política de filtro de rutas se identifica con un número de índice propio que se configura manualmente. Si la entrada con el número de índice especificado ya existe, se cambia según los nuevos parámetros configurados.

Cuando se añade la política de filtro de rutas, se define el proceso de las entradas según el criterio de linealidad estricta o según la coincidencia más larga. Si el proceso de la política de filtro de rutas es estric-

tamente 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 la política de filtro de rutas se efectúa según la coincidencia más larga, las entradas de la política de filtro de rutas se procesan según la dirección y máscara IP con la coincidencia más larga. Si, al utilizar el criterio de coincidencia más larga, hay más de una entrada de política de filtro de rutas con las mismas direcciones y máscaras IP, entonces la coincidencia será según el orden ascendente del número de entradas entre las entradas que compartan la misma dirección y máscara IP.

índice-política-ruta
Identifica la entrada.

Valor válido: de 1 a 65535

Valor por omisión: ninguno

dirección-ip

Valor válido: cualquier dirección IP válida

Valor por omisión: ninguno

máscara-ip

Valor válido: cualquier dirección IP válida

Valor por omisión: ninguno

coincidencia-dirección exact/range
Si este valor es *exact*, la entrada de la política de filtro de rutas sólo coincidirá con una ruta que tenga las misma s dirección y máscara exactas. Si el valor es *range*, la entrada de la política de filtro de rutas coincidirá con cualquier ruta que se encuentre dentro del rango abarcado por la dirección y máscara, incluyendo la ruta exacta.

Valores válidos: 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 filtros de rutas se incluyen en la tabla de direccionamiento. Si el valor es *exclusive*, las rutas que coincidan con esta entrada de política de filtro de rutas se excluyen, esto es, no se entran en la tabla de direccionamiento. Incluso si se configuran acciones para una entrada de política de filtro de rutas que sea exclusiva, estas acciones no serán aplicables.

Valor válido: inclusive o exclusive

Valor por omisión: inclusive

match-condition . . .
Añade una condición de búsqueda a una entrada de política de filtro de rutas ya existente. Una condición de coincidencia, que es un parámetro opcional o un conjunto de parámetros, se aplica a una ruta con la que coincide una definición de entrada. La condición de coincidencia filtra el

paquete para condiciones concretas además de la dirección IP y la máscara IP. Sólo puede configurarse una condición de coincidencia por entrada. Si se desea utilizar dos condiciones de coincidencia para la misma dirección o rango de direcciones, puede añadirse una segunda entrada a la política de filtros de rutas y especificar la segunda condición de coincidencia para esa entrada. Éstas son las condiciones de coincidencia:

Sintaxis:

as

gateway

metric

net

protocol

source-gateway

as *índice-política-ruta número-as*
Coincide con la ruta según su número de AS. Este valor se interpreta sólo cuando la política de filtro de rutas se aplica a los direccionamientos de límite AS.

índice-política-ruta
Un entero que identifica la entrada con la que debe establecerse la coincidencia.

Valor válido: de 1 a 65535

Valor por omisión: ninguno

número-as

Valor válido: de 1 a 65535

Valor por omisión: ninguno

gateway *índice-política-ruta dirección-y-máscara-pasarela*
Hace coincidir la ruta con una pasarela de salto siguiente en el rango especificado.

índice-política-ruta
Identifica la entrada con la que debe establecerse la coincidencia.

Valor válido: de 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-ruta número-métrica-inferior número-métrica-superior*
Hace coincidir la métrica de la ruta con uno de los números de un rango de números de métrica. Se solicita al usuario dos números para identificar el rango de números de

métrica: uno para el límite inferior del rango y otro para el límite superior. Si se desea un solo número de métrica, debe especificarse el mismo número dos veces.

índice-política-ruta

Valor válido: de 1 a 65535

Valor por omisión: ninguno

número-métrica-inferior

Valor válido: de 1 a 65535

Valor por omisión: ninguno

número-métrica-inferior

Valor válido: de 1 a 65535

Valor por omisión: ninguno

net *índice-política-ruta número-red-inferior número-red-superior*

Hace coincidir las rutas que tienen un salto siguiente con un número de red de salida en el rango definido por los números de red inferior y superior. Se solicitan al usuario dos números para identificar el rango de los números de red de salida: uno para el límite inferior del rango y uno para el límite superior. Si se desea un solo número de red, especifique el mismo número dos veces.

índice-política-ruta

Identifica la entrada con la que debe establecerse la coincidencia.

Valor válido: de 1 a 65535

Valor por omisión: ninguno

número-red-inferior

El límite inferior del rango de números de red para redes de salida del salto siguiente coincidentes. Pueden visualizarse mediante el mandato **list devices** desde el indicador de mandatos `Config>`.

Valores Válidos: de 1 a 65536

Valor por omisión: ninguno

número-red-superior

El límite superior del rango de números de red para redes de salida del salto siguiente coincidentes.

Valores Válidos: de 1 a 65536

Valor por omisión: ninguno

protocol *protocolo índice-política-ruta*

Hace coincidir la ruta con un protocolo.

protocolo

Valores válidos:

Sintaxis:

aggregate

bgp

direct

natural-nets

ospf-intra

ospf-inter

ospf

ospf-all

ospf-ext

ospf-e1

ospf-e2

rip

static

Valor por omisión: ninguno. En la explicación del mandato **add aggregate** y en el apartado “Agregación de ruta” en la página 254 hallará más información sobre el protocolo aggregate.

índice-política-ruta
Un entero que identifica la entrada con la que debe establecerse la coincidencia.

Valor válido: de 1 a 65535

Valor por omisión: ninguno

source-gateway *índice-política-ruta dirección-y-máscara-ip*
Hace coincidir rutas que provienen de una pasarela de origen concreta o un rango de pasarelas de origen.

índice-política-ruta
Un entero que identifica la entrada con la que debe establecerse la coincidencia.

Valor válido: de 1 a 65535

Valor por omisión: ninguno

dirección-y-máscara-ip

Valores válidos: cualquier combinación válida de dirección y máscara IP

Valor por omisión: ninguno

Delete

Utilice el mandato **delete** para suprimir entradas de política de filtro de rutas, condiciones de coincidencia de entradas de política de filtro de rutas ya existentes, o acciones de entradas de política de filtro de rutas ya existentes. Véase el mandato**add** en esta sección para una descripción de los parámetros que pueden suprimirse.

List

Utilice el mandato **list** para enumerar las entradas de la política de filtro de rutas, coincidencias y acciones existentes para la política de filtro de rutas que se está cambiando.

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
```

Acceso al entorno de supervisión de IP

Utilice el procedimiento siguiente para acceder a los mandatos de supervisión de IP. Este proceso da acceso al proceso de *monitoring (supervisión)*.

1. En el indicador de mandatos de OPCON, entre **talk 5**. (Si desea obtener información más detallada sobre este mandato, consulte “El proceso y los mandatos de OPCON” en la publicación*Access Integration Services Guía del usuario de software*.)Por ejemplo:

   ```
       * talk 5
   +
   ```

   Después de entrar el mandato **talk 5** en el terminal se visualiza el indicador de mandatos de GWCON prompt (+). Si el indicador no aparece cuando se entra por primera vez la configuración, pulse **Intro** de nuevo.

2. En el indicador + , entre el mandato **protocol ip** que le llevará al indicador de mandatos IP> prompt.

   Ejemplo:

   ```
   + prot ip
   IP>
   ```

Mandatos de supervisión de IP

Esta sección describe los mandatos de supervisión de IP. Tabla 20 enumera los mandatos de supervisión de IP. Los mandatos permiten supervisar el proceso de envío IP del direccionador. Las posibilidades de supervisión incluyen lo siguiente: la visualización de parámetros configurados tales como la dirección de interfaz y las rutas estáticas y el estado actual de la tabla de direccionamiento IP y la enumeración de la cuenta de errores de direccionamiento IP.

Tabla 20 (Página 1 de 2). Resumen de los mandatos de supervisión de IP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Access controls	Enumera el modo actual de control de acceso IP, además de los registros del control de acceso configurado.
Aggregate	Visualiza rutas agregadas.
Aggr-policy	Visualiza el estado y la política de la ruta agregada especificada.
Cache	Visualiza una tabla de todos los destinos recientes redireccionados.
Counters	Enumera diversos datos estadísticos IP, incluyendo cuentas de errores de direccionamiento y paquetes descartados.
Dscache	Enumera las acciones, estadísticas y orden de antememoria de flujo DiffServ.
Dump routing tables	Enumera los contenidos de la tabla de direccionamiento IP.
IGMP	Visualiza contadores y parámetros IGMP
Interface addresses	Enumera las direcciones de interfaz IP del direccionador.
Packet-filter	Visualiza la información de control de acceso definida para el filtro de paquetes especificado o todos los filtros.
Parameters	Enumera los valores de varios parámetros.
Ping	Envía peticiones eco ICMP a otro sistema principal y está atento a una respuesta. Este mandato puede usarse para aislar un problema en un entorno de interred.
Redundant Default Gateway	Especifica si existe una pasarela redundante por omisión y si está activa o inactiva.
Reset	Permite restablecer dinámicamente la configuración IP/RIP.
RIP	Visualiza el estado del protocolo RIP.
RIP-Policy	Visualiza la política de filtros de rutas que se aplica en la interfaz que se especifica.

Tabla 20 (Página 2 de 2). Resumen de los mandatos de supervisión de IP

Mandato	Función
Route	Especifica si existe una ruta para un destino IP concreto y, si es así, qué entrada de tabla de direccionamiento corresponde a la ruta.
Route-table-filtering	Enumera los filtros de cualquier ruta definida e indica si el filtrado de rutas está habilitado o inhabilitado.
Sizes	Visualiza el tamaño de parámetros IP específicos.
Static routes	Visualiza las rutas estáticas que se han configurado. Ello incluye la pasarela por omisión.
Traceroute	Visualiza la vía completa (salto-por-salto) a un destino concreto.
UDP-Forwarding	Visualiza los números de puerto UDP y las direcciones de destino IP que se añadieron con el mandato **add** o el mandato **enable**.
VRID	Visualiza información detallada para un VRID específico
VRRP	Visualiza en forma resumida el estado del protocolo VRRP.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Access Controls

Utilice el mandato **access controls** para presentar el modo global de control de acceso junto con una lista de las reglas globales de control de acceso configuradas.

El control de acceso está o bien inhabilitado (esto es, que no se hace ningún control control de acceso y las reglas de control de acceso se ignoran) o bien habilitado (esto es, que se hace un control de acceso y las reglas de control de acceso son reconocidas. El mandato de talk 6**set access on** habilita 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=0.0.0.0    Dest   =0.0.0.0     Prot=17
                SMask =0.0.0.0    DMAask =0.0.0.0
                SPorts=5004-5511  DPorts=5004-5511
                       T/C=**/**  Log=N
                BypassComp BypassEnc

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
```

Exclusivo (E) significa que los paquetes que coincidan con la regla de control de acceso son eliminados. Inclusivo (I) significa que los paquetes que coincidan con la regla de control de acceso son reenviados. Cuando está habilitado el control de acceso, se eliminan los paquetes que no coincidan con ningún registro de control de acceso. *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 el filtrado del establecimiento de conexión TCP. *T/C* representa el tipo y código ICMP; *SLOG* representa SysLog.

El campo Use especifica el número de veces que el sistema de control de acceso hace coincidir un registro determinado con un paquete de entrada, como por ejemplo el número de veces que un registro concreto del sistema de controles de acceso IP ha sido invocado debido a 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 de TOS. Se muestran los parámetros de TOS. Véase el mandato **add access-control** en talk 6 para una descripción de estos parámetros.

Aggregate

Utilice el mandato **aggregate** para visualizar las rutas agregadas y la indicación de si están activas.

Sintaxis:

aggregate

Ejemplo: `aggregate`

```
IP>aggregate

                      Aggregate Routes

Address         Mask             Policy            Status      Metric
-------------------------------------------------------------------------
10.1.0.0        255.255.0.0      UNCONDITIONAL     ACTIVE          12
10.2.0.0        255.255.0.0      EAST-REGION       ACTIVE          20

Status for last dynamic reconfig: 0x04
```

Aggr-policy

Utilice el mandato **aggr-policy** para visualizar el estado y la política de filtros de rutas de la ruta agregada especificada.

Sintaxis:

aggr-policy

Ejemplo:

```
IP>aggr-policy
IP Address []? 10.2.0.0
IP Mask []? 255.255.0.0

         Aggregate route 10.2.0.0/255.255.0.0 Policy

Status: ACTIVE      Metric:      20
Sufficient Route: 10.2.1.0/255.255.255.0

Checksum 0x4859  Longest-Match Application

IP Address      IP Mask           Match  Index  Type
-----------------------------------------------------
10.2.0.0        255.255.0.0       Range  1      Include
    Match Conditions:  Protocol: Static
    Policy Actions:    Set Metric: 20
```

Cache

Utilice el mandato **cache** para visualizar la antememoria de direccionamiento IP, que contiene los destinos que se han direccionado recientemente. Si un destino no se encuentra en la antememoria, el direccionador lo busca en la tabla de información de direccionamiento para tomar una decisión de reenvío.

Sintaxis:

cache (antememoria - poner en antememoria);

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 enviados recientemente al sistema principal de destino.

Next hop Dirección IP del siguiente direccionador en la vía hacia el sistema principal de destino. También se visualiza el nombre de red de la interfaz que utiliza el direccionador de envío para reenviar el paquete.

Counters

Utilice el mandato **counters** para visualizar las estadísticas relacionadas con el proceso de reenvío de IP. Esto incluye una cuenta de errores de direccionamiento, junto con el número de paquetes que se han descartado 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
   Eth/0  0
    FR/0  0
```

Routing table overflow
Enumera el número de rutas que se han descartado debido a que la tabla de direccionamiento estaba llena.

Net unreachable
Indica el número de paquetes que no pudieron reenviarse debido a destinos desconocidos. Esto no cuenta el número de paquetes que se han enviado al direccionador autorizada (pasarela por omisión).

Bad subnet number
Cuenta el número de paquetes o rutas que se han recibido para subredes ilegales (todo unos o todo ceros).

Bad net number
Cuenta el número de paquetes o rutas que se han recibido para destinos IP ilegales (por ejemplo, direcciones de clase E).

Unhandled broadcasts
Cuenta el número de difusiones IP (no locales) recibidas (éstas no se reenvían).

Unhandled multicasts
Cuenta el número de multidifusiones IP que se han recibido, pero cuyas direcciones no fueron reconocidas por el direccionador (éstas son descartadas).

Unhandled directed broadcasts
Cuenta el número de difusiones IP dirigidas (no locales) recibidas cuando el reenvío de estos paquetes está inhabilitado.

Attempted forward of LL broadcast
Cuenta el número de paquetes que se reciben con una dirección no local IP pero que se enviaron a una dirección de difusión de nivel de enlace (link–level). Éstas son descartadas.

Packets discarded through filter
Cuenta el número de paquetes recibidos que han sido dirigidos a redes/subredes filtradas. Éstas se descartan silenciosamente.

IP multicasts accepted
Cuenta el número de multidifusiones IP que el router ha recibido y procesado satisfactoriamente.

IP packet overflows
Cuenta el número de paquetes que se han descartado debido a la congestión en la cola de entrada del reenviador. Estas cuentas se ordenan según la interfaz de recepción.

Dscache

Utilice el mandato **dscache** para enumerar las acciones, estadísticas y el orden de la antememoria de flujo de 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
```

Dump Routing Table

Utilice el mandato **dump** para visualizar la tabla de direccionamiento IP. Se presenta una entrada separada para cada red/subred IP alcanzable. La pasarela IP por omisión en uso (si hay alguna) aparece al final de la visualización.

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 cómo se ha derivado la ruta.

Sbnt - Indica que la red está dividida en subredes; este tipo de entrada es solamente un sustituto

Dir - Indica una red o subred conectada directamente.

RIP - Indica que la ruta se ha averiguado a través del protocolo RIP.

Del - Indica que la ruta se ha suprimido.

Stat - Indica una ruta configurada estáticamente.

BGP - Indica rutas averiguadas a través del protocolo BGP.

BGPR - Indica rutas averiguadas a través del protocolo BGP que son reanunciadas por OSPF y RIP.

Fltr - Indica un filtro de direccionamiento.

SPF - Indica que la ruta es una ruta OSPF intra-área.

SPIA - Indica que es una ruta OSPF inter-área.

SPE1, SPE2 - Indica rutas OSPF externas (de tipo 1 y tipo 2 respectivamente)

Rnge - Indica un tipo de ruta que es un rango de direcciones de área OSPF activo y no se utiliza en paquetes de reenvío.

Dest net Red/subred IP de destino.

Mask máscara de dirección IP.

Cost Route Cost (coste de ruta)

Age Para las rutas RIP y GBP es el tiempo que ha transcurrido desde que se renovó por última vez la entrada de la tabla.

Next Hop Dirección IP del siguiente direccionador en la vía hacia el sistema principal de destino. También se visualiza el tipo de interfaz que utiliza el direccionador de envío para reenviar el paquete.

Un asterisco (*) después del tipo de ruta indica que la ruta tiene una reserva estático o conectado directamente. El signo de porcentaje (%) después del tipo de ruta indica que esta red/subred siempre aceptará las actualizaciones RIP.

Un número entre paréntesis al final de la comuna indica el número de rutas de igual coste al destino. Los primeros saltos pertenecientes a estas rutas pueden visualizarse con el mandato IP **route**.

IGMP

Utilice el mandato **igmp** para visualizar contadores y parámetros operativos de IGMP.

Sintaxis:

igmp counters
parameters

counters Visualiza las cuentas 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 que establece la consulta en 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
Visualiza los parámetros operativos IGMP de la interfaz del dispositivo conectada.

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 robustez de la interfaz especificada.

Query interval
El número de segundos entre consultas generales IGMP en esa red si este dispositivo es el consultador IGMP designado.

Response interval
El tiempo máximo de respuesta insertado en consultas generales IGMP en esa red si este dispositivo es el consultador IGMP designado.

Leave query interval
El tiempo máximo de respuesta insertado en consultas específicas IGMP en esa red si este dispositivo es el consultador IGMP designado.

Interface Addresses

Utilice el mandato **interface addresses** para visualizar las direcciones de interfaz IP del direccionador. Cada dirección aparece relacionada junto con su correspondiente interfaz de hardware y máscara de dirección IP. Si se ha asignado una dirección IP a la interfaz de puente utilizada para puenteo y direccionamiento en la misma interfaz, también aparecerá en el listado. La interfaz de puente se identifica por*BDG/0*.

Las interfaces de hardware sin direcciones de interfaz IP configuradas no serán utilizadas por el proceso de reenvío IP; aparecen como "Not an IN net". Hay una excepción a esto. No hace falta asignar direcciones de interfaz IP a líneas serie para reenviar el tráfico IP. Estas líneas se denominan no numeradas. Aparecen con la dirección 0.0.0.0.

Sintaxis:

interface

Ejemplo: `interface`

```
Interface  IP Address(es)   Mask(s)           Address- MTU
   TKR/0   133.1.169.2      255.255.252.0   Unspecified
    FR/0     133.1.167.2      255.255.254.0   Unspecified
```

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 la información definida para un filtro de paquetes concreto o para todos los filtros. Los filtros de paquetes son listas de registros de control de acceso específicos de interfaz. Las interfaces se identifican mediante números de interfaz, excepto en el caso de la interfaz de puente que se utiliza para el direccionamiento y el puenteo en la misma interfaz, que está identificada por *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 obtener una relación de 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 eco ICMP a un destino determinado (esto es, lo que se denomina “pinging”) y estar atento a una respuesta. Este mandato puede utilizarse para aislar los problemas del trabajo en red (interred).

Sintaxis:

p**ing**	*dir-dest [dir-orig tamaño-datos ttl velocidad tos valor-datos]*

El proceso ping se realiza de forma continuada, incrementando el número de secuencia ICMP con cada paquete adicional. Cada una de las respuestas eco de ICMP coincidentes recibidas se reporta con su número de secuencia y el tiempo de ida y vuelta. La granularidad (resolución) del cálculo del tiempo de ida y vuelta suele ser de unos 20 milisegundos, según la plataforma.

Para detener el proceso ping, escriba cualquier carácter en la consola. En ese momento se visualizará un resumen de la pérdida de paquetes, el tiempo de ida y vuelta y el número de destinos ICMP a los que no se puede acceder.

Cuando se proporciona una dirección de difusión o difusión múltiple como destino, puede obtenerse información de varias respuestas para cada paquete enviado, una para cada miembro del grupo. Cada una de las respuestas devueltas aparece con la dirección de origen de la que se recibe la respuesta.

Puede especificar el tamaño del proceso ping (número de bytes de datos del mensaje ICMP, excluyendo la cabecera ICMP), el valor de los datos, el valor de tiempo de vida (ttl), la cadencia y los bits TOS que establecer. También puede especificar la dirección IP de origen. Si no se especifica la dirección IP de origen, el direccionador utiliza su dirección local en la interfaz de salida a los destinos especificados. Si se está validando la conectividad de cualquiera de las otras interfaces del direccionador hacia el destino, éntrese la dirección IP para ese interfaz como la dirección de origen.

Sólo es obligatorio el parámetro de destino; todos los demás parámetros son opcionales. Por omisión, el tamaño es de 56 bytes, el valor de ttl es 64, la cadencia es de 1 proceso ping por segundo y el valor TOS es 0. Los cuatro primeros bytes de los datos ICMP se utilizan para una indicación de la hora. Por omisión, los datos restantes son una serie de bytes con valores que se incrementan en unidades de 1, empezando 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 primeros 4 bytes) se establecen en ese valor y ese valor no se incrementa. Por ejemplo, si establece el valor de bytes de datos en 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 redundantes IP por omisión 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 (primario)” o “Backup (de reserva)”. El estado puede ser “Active (activo)” o “Standby (en espera)”.

Reset IP

Utilice el mandato **reset IP** para efectuar ciertos cambios de configuración IP y RIP.

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
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
 IP>
```

RIP

Utilice el mandato **rip** command para visualizar con detalle 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 una) hacia un determinado destino IP. Si existe una ruta, se visualizan las direcciones IP de los saltos siguientes junto con información detallada acerca de la entrada de la tabla de direccionamiento coincidente. (Véase el mandato 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 el filtrado de tabla de direccionamiento está habilitado y enumerar cualquier filtro de tablas de rutas definido.

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 el tamaño configurado de determinados parámetros 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 que se utiliza de la tabla de direccionamiento. Este número incluye tanto las entradas activas como las inactivas. El valor que se visualiza 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 lo suficientemente grande para mantener las entradas actuales activas además de las entradas de direccimonamiento que se prevean.

Reassembly buffer size El tamaño configurado del almacenamiento de reserva de reensamblaje que se utiliza para reensamblar paquetes IP fragmentados.

Largest reassembled pkt El mayor paquete IP que este direccionador ha tenido que reensamblar.

Size of routing cache La medida configurada de la antememoria de direccionamiento .

# of cache entries in use El número de entradas que la antememoria utiliza actualmente.

Static Routes

Utilice el mandato **static routes** para visualizar la lista de rutas estáticas configuradas. También aparecen en la lista las pasarelas por omisión y las pasarelas de subred por omisión configuradas.

Cada destino de una ruta estática se especifica mediante un par dirección-máscara. Las pasarelas por omisión aparecen como rutas estáticas con el destino 0.0.0.0 y la máscara 0.0.0.0. Las pasarelas de subred por omisión también aparecen como rutas estáticas hacia todo el conjunto de red IP y sus subredes. IP subnetted network.

El ejemplo siguiente muestra una pasarela por omisión configurada, una pasarela de subred por omisión configurada (suponiendo que 128.185.0.0 tenga 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 utilización de esta ruta.

Next Hop El siguiente direccionador por el que pasará un paquete si utiliza esta ruta.

Traceroute

Utilice el mandato **traceroute** para visualizar toda la vía hacia un destino concreto, salto por salto. Para cada salto sucesivo, **traceroute** envía por omisión tres sondas e presenta la dirección IP del que establece la respuesta, junto con el tiempo de ida y vuelta que conlleva la respuesta. Si una determinada sonda no recibe ninguna respuesta se visualiza un asterisco. Cada línea que se visualiza hace referencia a este conjunto de tres sondas, con el número situado más a la izquierda indicando la distancia desde el direccionador que ejecuta el mandato (en términos de saltos de direccionador).

El rastreo de rutas se hace cuando se alcanza el destino, cuando se recibe un mensaje de destino de ICMP inaccesible (ICMP Destination Unreachable) o la longitud de la vía alcanza un máximo de 32 saltos de direccionador (por omisión).

Cuando una sonda recibe un resultado inesperado, existen varios indicadores que pueden visualizarse. “!N” ndica que se ha recibido un mensaje de ICMP de destino no accesible (red no accesible). “!H” indica que se ha recibido un mensaje de ICMP de destino no accesible (sistema principal no accesible). “!P” indica que se ha recibido un mensaje de ICMP de destino no accesible (protocolo no accesible); dado que la sonda es un paquete UDP que se envía a un puerto desconocido, se

espera un mensaje de puerto no accesible. “!” indica que se ha alcanzado el destino, pero que la respuesta enviada por el destino se ha recibido con un TTL de 1. Ello habitualmente indica un error en el destino, habitual en algunas versiones de UNIX, por el cual un destino inserta el TTL de la sonda en sus respuestas. Desafortunadamente, ello conduce a la existencia de un número de líneas que consisten únicamente en asteriscos antes de alcanzar finalmente el destino.

Sintaxis:

tr**aceroute** *dir-dest [dire-orig tamaño-datos sondas espera tos ttl-máx]*

dir-dest La dirección que se encuentra en el extremo más lejano de la ruta.

dir-orig La dirección de origen desde la que se origina el rastreo.

tamaño-datos
El tamaño en bytes del campo de datos del mensaje de rastreo de rutas. El campo de datos no incluye la cabecera UDP.

sondas Número de mansajes UDP de rastreo de rutas enviados desde cada salto.

espera Tiempo en segundos entre cada reintento.

tos El establecimiento de bits de TOS en los mensajes UDP. Por ejemplo, un valor de X'10' (B'00010000') establece los bits de TOS en B'1000'. El valor por omisión es 0, que establece los bits de TOS en 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
Visualiza la dirección del área de destino y el tamaño del paquete que se envía a esa dirección.

1 El primer rastreo que muestra el NSAP del destino y el intervalo de tiempo que ha utilizado el paquete para llegar a destino. El paquete se rastrea tres veces.

Destination unreachable
Indica que no hay ninguna ruta disponible hacia el destino.

3 * * * Indica que el direccionador espera algún tipo de respuesta del destino, pero que el destino no responde.

UDP-Forwarding

Utilice el mandato **UDP-forwarding** para visualizar el puerto y direcciones UDP que se añadieron con los mandatos **add udp-destination** o **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 de un determinado direccionador virtual, que se identifica mediante una dirección de interfaz y VRID. Tenga presente que, cuando el direccionador maestro notifica a los sistemas principales que utiliza la dirección MAC de hardware estampada como dirección MAC virtual del VRID, se envían tres ARP gratuitos.

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:    10:00:5A:63:3B:88
            Source MAC Address:     10:00:5A:63:3B:88
            Ethernet V2 Interface:  UP
            Preempt mode active

  Priority:             255       Advertise interval:   1
  Advertise Timer:      1         Skew (in ticks):      0
  Authentication Type:  NONE      Authentication Key:
  State transitions:    2         Advertisements out:   9
  Advertisements in:    0         Advertisements error: 0
  ARPs Modified:        0         Gratuitous ARPs:      3
  VRID Address:         153.2.2.25
```

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
```

Soporte de reconfiguración dinámica de IP

En este apartado se describe el modo en que la reconfiguración dinámica (DR) afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

IP da soporte al mandato **delete interface** de CONFIG (Talk 6) sin restricciones.

Mandato activate interface de GWCON (Talk 5)

IP da soporte al mandato **activate interface** de GWCON (Talk 5) con las matizaciones siguientes:

- IP se activará en una interfaz recién activada sólo si ya está instalado (es decir, si se ha configurado IP en una interfaz de red en tiempo de carga).
- La configuración de VRRP (**add vrid** y **add vr-address**) se instala sólo si VRRP ya está habilitado (**enable vrrp**).
- Los filtros de paquetes (**add packet-filter**) y las reglas de control de acceso asociadas (**update packet-filter**, **add access-control**) se instalan sólo si ya está habilitado el control de acceso (**set access-control on**).

Todos los mandatos específicos de interfaz IP están soportados por el mandato **activate interface** de GWCON (Talk 5).

Mandato reset interface de GWCON (Talk 5)

IP da soporte al mandato **reset interface** de GWCON (Talk 5) con las matizaciones siguientes:

- IP se activará en una interfaz recién activada sólo si ya está instalado (es decir, si se ha configurado IP en una interfaz de red en tiempo de carga).
- La configuración de VRRP (**add vrid** y **add vr-address**) se instala sólo si VRRP ya está habilitado (**enable vrrp**).
- Los filtros de paquetes (**add packet-filter**) y las reglas de control de acceso asociadas (**update packet-filter**, **add access-control**) se instalan sólo si ya está habilitado el control de acceso (**set access-control on**).

Todos los mandatos específicos de interfaz IP están soportados por el mandato **reset interface** de GWCON (Talk 5).

Mandatos de restablecimiento de componente de GWCON (Talk 5)

IP da soporte a los mandatos **reset** de GWCON (Talk 5) específicos de IP siguientes:

Mandato GWCON, protocol ip, reset ip

Descripción: Instala todos los cambios de configuración IP soportados.

Efecto en la red: Ninguno.

Limitaciones: Ninguna.

Todos los cambios de configuración IP se activan de forma automática excepto los siguientes:

Mandatos cuyos cambios no los activa el mandato GWCON, protocol ip, reset ip
CONFIG, protocol ip, add filter
CONFIG, protocol ip, add route
CONFIG, protocol ip, change route
CONFIG, protocol ip, delete filter
CONFIG, protocol ip, delete route

Mandatos de cambio inmediato de CONFIG (Talk 6)

IP da soporte a los mandatos de CONFIG que cambian de forma inmediata el estado operativo del dispositivo indicados más abajo. Los cambios se guardan y se conservan si se vuelve a cargar o iniciar el dispositivo o bien si se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
CONFIG, protocol ip, add filter
CONFIG, protocol ip, add route
CONFIG, protocol ip, change route
CONFIG, protocol ip, delete filter
CONFIG, protocol ip, delete route
CONFIG, protocol ip, disable icmp-redirect
CONFIG, protocol ip, enable icmp-redirect
CONFIG, protocol ip, set ttl

Mandatos no reconfigurables dinámicamente

En la tabla siguiente figuran los mandatos de configuración de IP que no pueden cambiarse dinámicamente. Para activar estos mandatos, es necesario volver a cargar o a arrancar el dispositivo.

Mandatos
CONFIG, protocol ip, add distributed default gateway
CONFIG, protocol ip, add redundant default gateway
CONFIG, protocol ip, add route-table-filter
CONFIG, protocol ip, delete default network-gateway
CONFIG, protocol ip, delete default subnet-gateway
CONFIG, protocol ip, delete distributed default gateway
CONFIG, protocol ip, delete redundant default gateway
CONFIG, protocol ip, delete route-table-filter
CONFIG, protocol ip, disable arp-net-routing
CONFIG, protocol ip, disable arp-subnet-routing
CONFIG, protocol ip, disable classless
CONFIG, protocol ip, disable per-packet-multipath
CONFIG, protocol ip, disable route-table-filtering
CONFIG, protocol ip, disable simple-internet-access
CONFIG, protocol ip, enable arp-net-routing
CONFIG, protocol ip, enable arp-subnet-routing
CONFIG, protocol ip, enable classless
CONFIG, protocol ip, enable per-packet-multipath
CONFIG, protocol ip, enable route-table-filtering
CONFIG, protocol ip, enable simple-internet-access
CONFIG, protocol ip, set cache-size
CONFIG, protocol ip, set default network-gateway
CONFIG, protocol ip, set default subnet-gateway
CONFIG, protocol ip, set dscache-size
CONFIG, protocol ip, set internal-ip-address
CONFIG, protocol ip, set reassembly-size
CONFIG, protocol ip, set router-id
CONFIG, protocol ip, set routing table-size

Soporte de reconfiguración dinámica de RIP

En este apartado se describe el modo en que la reconfiguración dinámica (DR) afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

RIP da soporte al mandato **delete interface** de CONFIG (Talk 6) con la matización siguiente:

Los registros de política de ruta asociados con una interfaz no se suprimen de forma automática cuando se suprime la interfaz.

Mandato activate interface de GWCON (Talk 5)

RIP da soporte al mandato **activate interface** de GWCON (Talk 5) con la matización siguiente:

> Para poder activar RIP en una interfaz de red, debe estar habilitado globalmente.

Todos los mandatos específicos de interfaz RIP están soportados por el mandato **activate interface** de GWCON (Talk 5).

Mandato reset interface de GWCON (Talk 5)

RIP da soporte al mandato **reset interface** de GWCON (Talk 5) con la matización siguiente:

> Para poder activar RIP en una interfaz de red, debe estar habilitado globalmente.

Todos los mandatos específicos de interfaz RIP están soportados por el mandato **reset interface** de GWCON (Talk 5).

Mandatos de restablecimiento de componente de GWCON (Talk 5)

RIP da soporte a los mandatos **reset** de GWCON (Talk 5) específicos de RIP siguientes:

Mandato GWCON, protocol ip, reset ip

Descripción: Se restablece toda la configuración RIP, incluidas todas las políticas de envío y recepción de interfaz.

Efecto en la red: No causa trastornos en la red.

Limitaciones: Ninguna.

Todos los mandatos RIP están soportados por el mandato **GWCON, protocol ip, reset ip**.

Utilización de OSPF

En este capítulo se describe la forma de utilizar el protocolo OSPF (Open Shortest Path First), que es un protocolo IGP (Interior Gateway Protocol). El direccionador admite los siguientes IGP para crear la tabla de direccionamiento IP: OSPF y RIP. El protocolo OSPF se basa en la tecnología de estado del enlace o en el algoritmo de "primero la vía más corta" (SPF). RIP se basa en el algoritmo vector-distancia o Bellman-Ford.

Este capítulo consta de los siguientes apartados:

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 la accesibilidad a la red y la información de direccionamiento existente en un AS y utilizan esta información para crear la tabla de direccionamiento IP. Los IGP también pueden importar información de direccionamiento externa al AS. El direccionador puede simultáneamente ejecutar OSPF y RIP. Cuando lo hace, se prefieren las rutas OSPF. En general, se recomienda el uso del protocolo OSPF debido a su eficacia, su solidez y a que necesita menos ancho de banda.

El protocolo de direccionamiento OSPF

El direccionador admite una implementación completa del protocolo de direccionamiento OSPF, tal y como se especifica en el documento RFC 1583 (versión 2). OSPF es un protocolo de direccionamiento de estado del enlace que detecta y se informa de las mejores rutas para los destinos accesibles. OSPF puede percibir rápidamente cambios en la topología de un AS y, después de un corto periodo de convergencia, calcular nuevas rutas. El protocolo OSPF no encapsula paquetes IP pero los reenvía basándose sólo en su dirección de destino.

Resumen del direccionamiento OSPF

Cuando se inicializa un direccionador, éste utiliza el protocolo Hello para enviar paquetes Hello a sus vecinos y éstos, a su vez, envían sus paquetes al direccionador. En redes de difusión y de punto a punto, el direccionador detecta de forma dinámica a sus direccionadores vecinos mediante el envío de paquetes Hello a las direcciones multidifusión *ALLSPFRouters (224.0.0.5);* en las redes de no difusión debe configurar la información de manera que el direccionador pueda descubrir a sus *vecinos*. En todas las redes multiacceso (de difusión o no), el protocolo Hello también selecciona un *direccionador designado* para la red.

El direccionador intentará entonces formar adyacencias con sus vecinos para sincronizar sus bases de datos topológicas. Las adyacencias controlan la distribución (envío y recepción) de los paquetes del protocolo de direccionamiento y la distribución de las actualizaciones de la base de datos topológica. En redes multiacceso,

el direccionador designado determina los direccionadores que se convertirán en adyacentes.

Un direccionador anuncia de manera periódica su estado o el estado del enlace a sus adyacencias. Los *anuncios de estado de enlace* (LSA) inundan totalmente un área y garantizan que todos los direccionados tienen exactamente la misma base de datos topológica. Esta base de datos es una colección de los anuncios de estado del enlace recibidos de cada direccionador perteneciente a un área. De la información contenida en la base de datos, cada direccionador puede calcular un árbol de vía de acceso más corta con él mismo designado como raíz. El árbol de vía de acceso más corta genera la tabla de direccionamiento.

OSPF está diseñado para ofrecer servicios de los que no se dispone con RIP. Entre otras, sus características son las siguientes:

- *Direccionamiento de menor coste.* Le permite configurar los costes de la vía de acceso en cualquier combinación de parámetros de red. Por ejemplo, ancho de banda, retardo y coste en dólares.
- *Ausencia de limitaciones para la métrica de direccionamiento.* Mientras RIP restringe la métrica de direccionamiento a 16 saltos, OSPF no tiene restricción.
- *Direccionamiento multivía.* Le permite utilizar varias vías de acceso de igual coste para conectar los mismos puntos. Puede utilizar estas vías de acceso para una distribución de la carga que ocasione un uso más eficaz del ancho de banda de la red.
- *Direccionamiento de área.* Reduce los recursos (memoria y ancho de banda de la red) consumidos por el protocolo y proporciona un nivel adicional de protección del direccionamiento.
- *Máscara de subred de longitud variable.* Le permite dividir una dirección IP en subredes de tamaño variable, conservando el espacio de la dirección IP.
- *Autenticación de direccionamiento* Proporciona más seguridad de direccionamiento.

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 únicos. Una línea serie de 56 kbps que conecte dos direccionadores es un ejemplo de red punto a punto.
- *Difusión.* Redes que dan soporte a más de dos direccionadores conectados y capaces de dirigir un mensaje físico a todos los direccionadores conectados. Una red en anillo es un ejemplo de red de difusión.
- *Multiaccesode no difusión (NBMA).* Redes que dan soporte a más de dos direccionadores conectados pero no pueden difundir. Una red de datos públicas X.25 es un ejemplo de red de no difusión. Para que OSPF funcione correctamente, esta red necesita información extra de configuración sobre otros direccionadores OSPF conectados a la red de no difusión.
- *Punto a multipunto.* Redes que dan soporte a más de dos direccionadores conectados, no pueden difundir y no están totalmente conectados en malla. Una red Frame Relay sin PVC entre todos los direccionadores conectados es un ejemplo de red de punto a multipunto. Al igual que las redes de no difusión, es necesaria información de configuración sobre otros direccionadores OSPF conectados a la red.

Direccionador designado

Cada red de acceso múltiple de no difusión o de difusión tiene un direccionador designado que realiza dos funciones primordiales para el protocolo de direccionamiento: produce anuncios del enlace de red y se convierte en adyacente de todos los otros direccionadores de la red.

Cuando un direccionador designado produce anuncios del enlace de red, lista todos los direccionadores, incluido él mismo, conectados actualmente a la red. El ID de enlace para este anuncio es la dirección de la interfaz IP del direccionador designado. Al utilizar la máscara de subred/red, el direccionador designado obtiene el número de red IP.

El direccionador designado se convierte en adyacente de todos los otros direccionadores y se encarga de sincronizar las bases de datos de estado de enlace de las redes de difusión.

El protocolo Hello OSPF selecciona el direccionador designado una vez determinada la prioridad del direccionador del campo *Rtr Pri* del paquete Hello. Cuando el direccionador de una interfaz se vuelve primero funcional, comprueba si puede ver que la red tiene actualmente un direccionador designado. Si lo tiene, acepta el direccionador designado sin tener en cuenta la prioridad del direccionador. Si no lo tiene, se declara a sí mismo como el direccionador designado. Si el direccionador se declara a sí mismo como direccionador designado a la vez que otro direccionador lo hace, el direccionador designado será aquel con la prioridad de direccionador más alta (*Rtr Pri*). Si ambas *Rtr Pris* son iguales, aquel que tenga el ID más alto será el elegido.

Una vez seleccionado el direccionador designado, éste se convierte en el extremo final de muchas adyacencias. En una red de difusión, el direccionador optimiza el procedimiento de inundación al permitir que la ruta designada multidifunda sus paquetes de actualización de estado de enlace a la dirección ALLSPFRouters (224.0.0.5) en lugar de enviar paquetes distintos a través de cada adyacencia.

OSPF multidifusión

La multidifusión es una técnica de la LAN que permite hacer copias de un paquete único para pasar a una subred de todos los destinos posibles seleccionada. Algunos hardware (Ethernet, por ejemplo) dan soporte a la multidifusión permitiendo que la interfaz de una red pertenezca a uno o más grupos multidifusión. Consulte “Soporte multidifusión IP” en la página 263 para obtener más detalles sobre la multidifusión IP admitida por el direccionador.

El protocolo OSPF admite direccionamiento multidifusión IP a través de extensiones multidifusión de OSPF (MOSPF).

Un direccionador MOSPF distribuye la información de ubicación de grupo por todo el dominio de direccionamiento inundándolo con un tipo de anuncio de estado de enlace denominado LSA de pertenencia a grupo (group-membership-LSA) (tipo 6). Esto permite que los direccionadores MOSPF reenvíen eficazmente un datagrama multidifusión a sus diferentes destinos. Para ello, cada direccionador calcula la vía de acceso del datagrama multidifusión como si se tratara de un árbol cuya raíz sea el origen del datagrama y cuyas ramas terminales sean LAN que contienen miembros de grupo.

Mientras se ejecuta el MOSPF, el reenvío de datagramas multidifusión funciona de la siguiente forma:

- Aunque el reenvío de multidifusiones IP no es fiable, los datagramas multidifusión IP se entregan con la misma optimización que la entrega de unidifusiones IP.
- Los datagramas multidifusión recorren la vía de acceso más corta entre el origen del datagrama y cualquier destino (coste de estado de enlace OSPF). Esto es así debido a que se crea un árbol distinto para cada par de grupo de destino y cada origen de datagrama.
- En cada salto, se reenvía un datagrama multidifusión como multidifusión del enlace de datos. No se utiliza el protocolo ARP. En algunas tecnologías de red, se produce la correlación entre direcciones IP de clase D y la multidifusión del enlace de datos, mientras que otras direcciones IP de clase D están correlacionadas con la dirección de difusión del enlace de datos.
- Cuando las vías de acceso que vayan del origen de datagrama a dos miembros de grupo distintos comparten un segmento común inicial, sólo se reenvía un datagrama único hasta que las vías de acceso vayan en direcciones distintas. La vía de acceso se puede dividir en un direccionador o una red. Si la vía de acceso se parte en un direccionador, el direccionador replica el paquete antes de que se envíe. Si la vía de acceso se parte en una red, se replica a través de una multidifusión del enlace de datos.
- La configuración de una red puede constar de direccionadores MOSPF y direccionadores sin extensiones multidifusión. En esta configuración, todos los direccionadores interoperan en el direccionamiento de unidifusiones. Esto le permite introducir lentamente una posibilidad multidifusión en una interred.

  Algunas configuraciones de direccionadores que no sean MOSPF o MOSPF pueden producir errores inesperados en el direccionamiento multidifusión.
- El direccionador se puede configurar para enviar capturas SNMP a una dirección de grupo multidifusión mediante la adición de una dirección de grupo a un determinado nombre de comunidad SNMP.

Configuración de OSPF

En los siguientes apartados se presenta la información para configurar inicialmente el protocolo OSPF. Esta información perfila las tareas requeridas para activar el protocolo OSPF y ejecutarlo. La información sobre cómo realizar posteriores cambios en la configuración se explica en “Mandatos de configuración de OSPF” en la página 383.

Los siguientes pasos se refieren a las tareas necesarias para activar y ejecutar OSPF. En los siguientes apartados se explica cada paso con detalle y se incluyen ejemplos de los mismos.

Antes de que el direccionador ejecute el protocolo OSPF, debe:

1. Activar el protocolo OSPF. Al hacerlo, debe calcular el tamaño final del dominio de direccionamiento OSPF. (Consulte “Habilitación del protocolo OSPF” en la página 367.)
2. Establecer el ID del direccionador OSPF. En tecnologías que no admitan difusión o multidifusión del enlace de datos (cso de Frame Relay), el direccionador

debe replicar el datagrama multidifusión y reenviarlo como unidifusión del enlace de datos. (Consulte “Establecimiento de los ID de direccionador OSPF” en la página 368.)

3. Defina las áreas OSPF conectadas al direccionador. Si no se define ninguna área OSPF, se adoptará una única área de red troncal. (Consulte “Definición de áreas OSPF conectadas y troncales” en la página 368.)
4. Defina las interfaces de red OSPF del direccionador. Establezca el coste del envío de paquete de cada interfaz, junto con el conjunto de los parámetros operativos OSPF. (Consulte “Establecimiento de las interfaces OSPF” en la página 372.)
5. Si desea reenviar multidifusiones IP (direcciones IP de clase D), habilite la posibilidad de direccionamiento multidifusión IP. (Consulte “Reenvío multidifusión” en la página 374.)
6. Si el direccionador intercambia información con redes de no difusión, como por ejemplo X.25 o Frame-Relay, establezca parámetros de interfaz adicionales. (Consulte “Establecimiento de parámetros de interfaz de red de no difusión” en la página 375 y “Configuración de subredes de área amplia” en la página 375.)
7. Si desea que el direccionador importe rutas de otros protocolos de direccionamiento que se ejecuten en este direccionador (BGP, RIP o rutas configuradas estáticamente), habilite el direccionamiento limítrofe de AS. Además, debe definir si las rutas se importan como externas de tipo 2 o de tipo 1. (Consulte “Habilitación del direccionamiento limítrofe AS” en la página 377.)
8. Si desea arrancar mediante un direccionador vecino de una interfaz punto a multipunto o punto a punto, debe configurar la dirección IP del vecino. Para hacerlo, añada un vecino OSPF al destino de la interfaz punto a punto.

Habilitación del protocolo OSPF

Al habilitar el protocolo de direccionamiento OSPF, debe proporcionar los siguientes dos valores para calcular el tamaño final del dominio de direccionamiento OSPF:

- El número total de rutas externas de AS que se importarán al dominio de direccionamiento OSPF. Se puede dirigir un único destino a diversas rutas externas cuando lo importan distintos direccionadores limítrofes AS. Por ejemplo, si el dominio de direccionamiento OSPF tiene dos direccionadores limítrofes de AS y ambos importan rutas a los mismos 100 destinos, establezca el número de rutas externas de AS en 200.
- El número total de rutas OSPF del dominio de direccionamiento.

Configure de forma idéntica estos dos valores en todos los direccionadores OSPF. Cada direccionador que ejecute el protocolo OSPF tiene una base de datos en la que se describe un mapa del dominio de direccionamiento. Esta base de datos es idéntica en todos los direccionadores que la forman. Desde esta base de datos se crea la tabla de direccionamiento IP mediante la construcción de un árbol de la vía más corta, con el propio direccionador como raíz. El dominio de direccionamiento remite a un AS que ejecuta el protocolo OSPF.

Para habilitar el protocolo de direccionamiento OSPF, utilice el mandato **enable** tal y como 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 del enlace (LSA) generado por el direccionador. No obstante, los direccionadores con muchos enlaces de marcación OSPF (por ejemplo, los enlaces de marcación RDSI) pueden necesitar un LSA mayor. Además, en estas situaciones, puede que sea necesario incrementar el **tamaño de paquete (packet-size)** en la configuración general.

Establecimiento de los ID de direccionador OSPF

A todos los direccionadores del dominio de direccionamiento OSPF se les debe asignar un único ID de direccionador de 32 bits. Seleccione el valor utilizado para el ID del direccionador OSPF de la siguiente forma:

- Si utiliza el mandato de configuración de IP **set router ID**, el valor configurado se utiliza como ID del direccionador OSPF. El direccionador OSPF configurado debe ser la dirección interna o una de las direcciones IP del direccionador.
- Si utiliza el mandato de configuración de IP **set internal address**, la dirección configurada se utiliza como ID del direccionador OSPF. Se recomienda utilizar el mismo valor para el ID del direccionador y para la dirección interna, en caso de definirse.

  También se puede determinar si se anuncia la dirección interna y establecer la métrica anunciada. El valor por omisión es anunciar cualquier dirección IP interna configurada cuya métrica sea 0.
- Si no se configuran ni el ID del direccionador ni la dirección interna durante la configuración IP, la primera dirección de la interfaz OSPF se utilizará como ID del direccionador OSPF.

Definición de áreas OSPF conectadas y troncales

En la Figura 32 en la página 369 se muestra un ejemplo del datagrama de la estructura de un dominio de direccionamiento OSPF. Una división se encuentra entre las subredes IP del dominio OSPF y las subredes IP externas a dicho dominio. Las subredes incluidas dentro del dominio OSPF se subdividen en regiones denominadas *áreas*. Las áreas OSPF son conjuntos de subredes IP contiguas. La función de las áreas es reducir la actividad general de OSPF la hora de encontrar rutas a los destinos de un área diferente. La actividad general se reduce cuando existe menos información intercambiada entre los direccionadores o cuando se necesitan menos ciclos CPU para que el cálculo de la tabla de direccionamiento sea menos complejo.

Todos los dominios de direccionamiento OSPF deben tener al menos un *área troncal*. La red troncal se identifica siempre con el número de área 0.0.0.0. En redes OSPF pequeñas, la red troncal es la única área requerida. En redes mayores con varias áreas, la red troncal proporciona un "centro neurálgico" que conecta las áreas. A diferencia de otras áreas, las subredes de red troncal pueden estar físicamente separadas. En este caso, la conectividad lógica de la red troncal se mantiene al configurar *enlaces virtuales* entre los direccionadores troncales a través de áreas de tránsito no troncales interpuestas.

Los direccionadores que conecten a más de un área funcionan como *direccionadores limítrofes* del área. Todos los direccionadores limítrofes de área

forman parte de la red troncal, de manera que un direccionador limítrofe se debe conectar directamente a una subred IP troncal o a otro direccionador troncal de un enlace virtual. Además, debe existir un conjunto de subredes troncales y de enlaces virtuales que conecte a todos los direccionadores troncales.

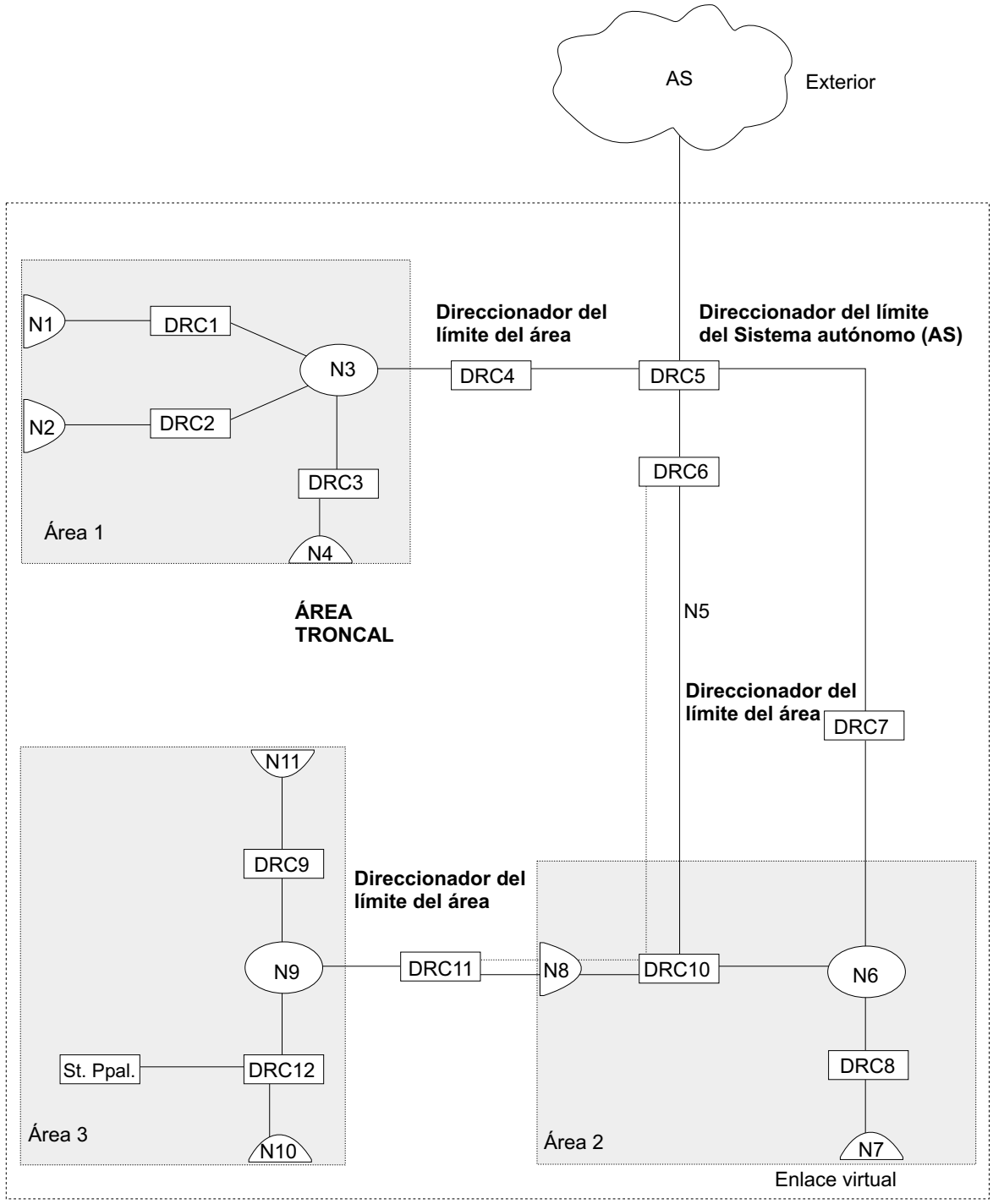


Figura 32. Áreas OSPF

La información y algoritmos que utiliza OSPF para calcular las rutas varía dependiendo de si la subred IP de destino está dentro de la misma área, en un área distinta del mismo dominio o fuera del dominio OSPF. Todos los direccionadores

mantienen una correlación completa de todos los enlaces que se encuentran en su área. Todos los enlaces de direccionador a red multiacceso, de red a direccionador multiacceso y de direccionador a direccionador forman parte de la correlación. Se utiliza un algoritmo de "primero la vía de acceso más corta" para calcular las mejores rutas a los destinos de área de esta correlación. Las rutas entre las áreas se calculan a partir de los anuncios de resumen producidos por los direccionadores limítrofes del área en el caso de las subredes IP, los rangos de las subredes OP y los direccionadores limítrofes externos al sistema anónimo (ASE) localizados en otras áreas del dominio OSPF. Las rutas externas se calculan a partir de los anuncios ASE generados por los direccionadores limítrofes ASE y con los que se ha inundado el dominio de direccionamiento OSPF.

La red troncal se encarga de distribuir la información de direccionamiento entre las áreas. El área troncal está formado por cualquiera de los siguientes elementos:

- Redes pertenecientes al área 0.0.0.0
- Direccionadores conectados a esas redes
- Direccionadores pertenecientes a varias áreas
- Enlaces virtuales configurados

Definición de áreas conectadas

Las áreas troncales, son el tipo por omisión, se inundan con todos los tipos de LSA. Para definir áreas apéndice y áreas NSSA que no deben inundarse con todos los tipos de LSA, puede utilizar el mandato **set area**. Si no lo utiliza, el valor por omisión es que todas las interfaces del direccionador están conectadas al área troncal.

Las áreas apéndice son áreas que no permiten que ningún LSA de tipo 5 se propague por el área y, en lugar de ello, dependen del direccionamiento por omisión a los destinos externos. El tipo habitual de área apéndice tiene un único direccionador, a través del cual el tráfico procedente de ella pasa a los demás dispositivos de la red.

Los anuncios OSPF ASE no inundan nunca las áreas apéndice. Además, el mandato **set area** tiene una opción para suprimir todo tipo de producción en el apéndice de los anuncios de resumen para rutas entre áreas. Los anuncios de resumen son LSA de tipo 3 y los utilizan los direccionadores limítrofes de área para anunciar rutas entre áreas. Si opta por inhibir el anuncio de los LSA de resumen, el direccionador limítrofe de área anunciará una ruta por omisión de tipo 3 al apéndice. Como resultado, el tráfico del apéndice destinado a subredes IP desconocidas se reenvía al direccionador limítrofe de área por la ruta por omisión. El direccionador limítrofe utiliza su información de direccionamiento más completa para reenviar el tráfico de una vía de acceso correcta hacia su destino.

Un área puede definirse como apéndice cuando:

1. No haya necesidad de que el área maneje tráfico troncal de tránsito.
2. Los direccionadores del área puedan utilizar un valor por omisión generado por el direccionador limítrofe del área para el tráfico enviado fuera del sistema autónomo.
3. No haya necesidad de que los direccionadores del área sean direccionadores limítrofes de AS (direccionadores OSPF que anuncien rutas de orígenes externos en forma de anuncios externos AS). Un origen externo es una red en la que se ejecuta un protocolo que no es OSPF.

En este caso, sólo los direccionadores limítrofes del área y los direccionadores de la red troncal tendrán que calcular y mantener las rutas externas AS.

Un área no se puede configurar como apéndice cuando se utiliza como área de tránsito para enlaces virtuales.

Para establecer los parámetros de un área apéndice OSPF, utilice el mandato **set area** y responda a las siguientes preguntas:

```
Area number [0.0.0.0]? 0.0.0.1
Is this a stub area? [No]:  yes
Stub default cost? [0]:
Import summaries? [Yes]:
```

El mandato **set area** sirve también para definir las áreas como NSSA. Las áreas NSSA están descritas en el documento RFC 1587. Físicamente, son áreas apéndice desde el punto de vista de un direccionador limítrofe de área, y áreas troncales desde el punto de vista de los direccionadores que están dentro de ellas. Al igual que ocurre con las áreas apéndice, no se puede inundar las áreas NSSA con anuncios externos de otras áreas. No obstante, a diferencia de las áreas apéndice, las áreas NSSA no dependen por completo de las rutas por omisión para llegar hasta los destinos externos. En lugar de ello, los direccionadores limítrofes del área NSSA permiten que, en algunos casos, los anuncios externos procedentes del interior del área se anuncien fuera de ella según convenga. Asimismo y también a diferencia de las áreas apéndice, las áreas NSSA permiten que los anuncios externos procedentes del interior del área se anuncien dentro de ella.

Los anuncios externos que son locales para el área NSSA se anuncian como LSA de tipo 7, que es el tipo de LSA que se utiliza únicamente en áreas NSSA y que no se anuncia nunca fuera de ellas. Sin embargo, si es preciso, los direccionadores limítrofes del área NSSA pueden resumir los LSA de tipo 7 y reanunciarlos como LSA de tipo 5.

Las aplicaciones del tipo de área NSSA son las siguientes:

Agregación de rutas externas para limitar el tamaño de la tabla de rutas:
Si no se utilizan áreas NSSA, no existe mecanismo alguno para agregar los anuncios externos procedentes de la mayoría de direccionadores OSPF. Ni tampoco existe modo alguno de evitar que se anuncies las rutas externas en todo el dominio de direccionamiento OSPF.

Separar la ruta por omisión al cortafuegos por área:
En muchas redes de empresas, conviene tener un cortafuegos Internet separado en cada ubicación. Esto puede conseguirse utilizando áreas NSSA sin tener que anunciar el área por omisión específica de área en todo el dominio de direccionamiento.

Implementación de extranets:
Muchas empresas pueden utilizar un área troncal OSPF con áreas NSSA conectadas (una por empresa) para implementar una extranet (red administrada por varias partes cooperantes) y contar igualmente con un direccionamiento flexible dentro del área NSSA.

Definición de rangos de direcciones de subred para un área conectada

La propagación de los LSA disminuye también definiendo rangos de direcciones de subred para un área conectada a un direccionador limítrofe de área. El rango se define mediante una dirección IP y una máscara de dirección. Se considera que las subredes están dentro del rango si la dirección IP de subred y la dirección IP de rango coinciden después de aplicar la máscara de rango a ambas direcciones.

Cuando se añade un rango, el direccionador limítrofe suprime los anuncios de resumen para las subredes de las áreas incluidas en el rango. Los anuncios suprimidos se habrían originado en las demás áreas a las que el direccionador limítrofe está conectado. En cambio, el direccionador limítrofe de área puede producir un único anuncio de resumen para el rango o bien ningún anuncio, dependiendo de la opción seleccionada con el mandato **add range**.

Observe que, si no se anuncia el rango, no existirán rutas entre áreas para ningún destino que se desactive dentro del rango. Igualmente, observe que los rangos no se pueden utilizar para áreas que los enlaces virtuales utilicen como áreas de tránsito.

Establecimiento de las interfaces OSPF

Las interfaces OSPF son una subred de las interfaces IP definidas durante la configuración IP. Los parámetros configurados para las interfaces OSPF determinan la topología del dominio OSPF, las rutas seleccionadas mediante el dominio y las características de la interacción entre los direccionadores OSPF directamente conectados. El mandato **set interface** se utiliza para definir una interfaz OSPF y para especificar algunas de sus características. Otras características de la interfaz se han especificado en respuesta a la pregunta **add address** durante la configuración IP.

Topología de dominio OSPF

La definición de la topología de un dominio OSPF se basa en una definición de los direccionadores directamente que están directamente conectados a través de un medio físico o de tecnología de red y el área de las que forman parte estas conexiones. El caso básico es que todos los direccionadores conectados a una subred física estén directamente conectados pero es posible definir varias subredes IP en una subred física única. En este caso, OSPF tendrá en cuenta los direccionadores que se vayan a conectar directamente sólo cuando tengan interfaces OSPF conectadas a la misma subred IP. También es posible encontrarse con casos en los que los direccionadores conectados a la misma red no tengan conexión de la capa de enlace directo.

En medios LAN, los direccionadores OSPF directamente conectados están determinados por la subred IP y el medio físico relacionado con una interfaz OSPF. La dirección IP de la interfaz OSPF se especifica al responder a la pregunta **Interface IP address**. Esta dirección debe coincidir con la dirección de una interfaz IP definida con el mandato **add address** durante la configuración IP. La dirección IP, junto con la máscara de subred definida con el mandato **add address** determina la subred IP con la que la interfaz OSPF está conectada. El *índice de red* asociado a la interfaz IP mediante el mandato add address determina la subred física a la que la interfaz OSPF está conectada. La posibilidad de difusión que poseen las LAN permite que OSPF utilice mensajes Hello multidifusión para descubrir otros direccionadores que tienen interfaces conectadas a la misma subred IP. Por lo

tanto, los parámetros de la interfaz son todos los necesarios para que OSPF determine los direccionadores que están directamente conectados a través de una LAN.

Las LAN se pueden utilizar par conectar un direccionador OSPF con sistemas principales IP. En este caso, es necesario definir una interfaz OSPF para toda aquella subred IP definida para la LAN. De lo contrario, OSPF no generará rutas con esas subredes IP como destinos. Para evitar tráfico Hello OSPF en estas redes LAN sin otros direccionadores conectados, la red se puede definir como una red multiacceso de no difusión. La prioridad del direccionador debe establecerse también en cero porque no es necesario ningún direccionador designado.

Las necesidades a la hora de configurar interfaces OSPF que conecten líneas serie varían según la tecnología de la capa más baja.

En líneas punto a punto, sólo es accesible, a través de la interfaz, otro direccionador. Por lo tanto el direccionador directamente conectado se puede determinar sin otra configuración. De hecho, al no haber en absoluto necesidad de configurar una subred IP, las interfaces OSPF no numeradas se pueden utilizar para líneas punto a punto. En este caso, el mismo índice de red utilizado como dirección IP para el mandato IP add address se utiliza como dirección Ip para el mandato OSPF set interface.

En tecnologías de subred como Frame Relay y X.25 que admiten conexiones con varios direccionadores a través de una única línea serie, la configuración de las interfaces OSPF es parecida a la utilizada para una LAN, pero debido a que en estas tecnologías de red los direccionadores directamente conectados no se descubren de forma dinámica, es necesaria otra configuración en la que se especifiquen los vecinos directamente conectados. Para obtener más información sobre la configuración necesaria, consulte “Configuración de subredes de área amplia” en la página 375.

Costes de los enlaces OSPF

OSPF calcula los direcciones buscando la vía de acceso de menor coste a un destino. El coste de cada vía de acceso es la suma de los costes de los distintos enlaces de una vía de acceso. El coste de un enlace con un direccionador directamente conectado se especifica en el mandato **set interface** de **Type of Service 0 cost**.

La configuración correcta de los costes basándose en la conveniencia o no de utilizar interfaces para el tráfico de datos es crítico cuando se trata de obtener las rutas deseadas a través de un dominio OSPF. Los factores que hacen que los enlaces individuales resulten más o menos convenientes puede variar según el tipo de red, pero el objetivo más común es seleccionar rutas con el menor retardo y la mayor capacidad. En general, esta política se puede realizar ejecutando el coste de un enlace inversamente proporcional al ancho de banda del medio utilizado para la subred física.

Un enfoque recomendable consiste en utilizar un coste de uno para la tecnología de ancho de banda más alta.

Tabla 21. Ejemplo de costes para enlaces OSPF	
Ancho de banda de la interfaz	Coste
Ethernet a 100 Mbps	1
Ethernet	10
Red en anillo a 16 Mbps	6
Red en anillo a 4 Mbps	25
línea serie	Coste según el ancho de banda
Red en anillo emulada (véase la nota).	1
Ethernet emulada (Véase la nota).	1

Nota: Ethernet emulada se ejecutará en la velocidad de la interfaz (por ejemplo, 155 Mbps) y se deberá configurar con un coste de 1.

El coste de una interfaz OSPF se puede cambiar dinámicamente desde el entorno de supervisión del direccionador. El nuevo coste inunda rápidamente el dominio de direccionamiento OSPF y modifica al direccionador inmediatamente.

Cuando el direccionador se reinicia/recarga, el coste de la interfaz vuelve al valor configurado en SRAM.

Interacciones entre direccionadores vecinos

Un número de los valores configurados con el mandato **set interface** se utiliza para especificar parámetros que controlen la interacción de direccionadores directamente conectados. Éstos incluyen:

- El intervalo de retransmisión
- El retardo de transmisión
- La prioridad del direccionador
- El intervalo de paquetes Hello
- El intervalo de direccionador muerto
- El circuito de petición
- La supresión de paquetes Hello
- El intervalo de sondeo
- La clave de autenticación

En la mayoría de los casos se utilizan los valores por omisión.

Nota: El intervalo de paquetes Hello, el intervalo de direccionador muerto y la clave de autenticación deben tener el mismo valor en todos los direccionadores OSPF conectados a la misma subred IP. Si estos valores no son los mismos, los direccionadores fallarán al formar conexiones directas (adyacencias).

Reenvío multidifusión

Para habilitar el direccionamiento de los datagramas multidifusión IP (clase D), utilice el mandato **enable multicast-routing**. Al habilitar el direccionamiento multidifusión, se le solicitará la forma en que desea que el direccionador reenvíe la multidifusión entre áreas OSPF.

```
OSPF Config>enable multicast forwarding
Inter-area multicasting enabled?  [No]: yes
```

Cuando el mandato **enable multicast forwarding** se invoca primero, la multidifusión se habilita en todas las interfaces OSPF con los parámetros por omisión.

Si desea cambiar los parámetros MOSPF, utilice el mandato **set interface**. Los parámetros multidifusión sólo se le consultarán en caso de haber habilitado primero el reenvío multidifusión.

En redes situadas en el borde de un sistema autónomo, en el que existan varios protocolos de direccionamiento multidifusión (o varias instancias de un único protocolo de direccionamiento multidifusión), puede que sea necesario configurar el reenvío como unidifusiones para evitar la replicación de datagramas. En cualquier caso, para todos los direccionadores conectados a una red común, los parámetros de la interfaz reenvían datagramas multidifusión y el reenvío como unidifusiones del enlace de datos se debe configurar de forma idéntica.

Establecimiento de parámetros de interfaz de red de no difusión

Si el direccionador está conectado a una red multiacceso de no difusión, como por ejemplo una PDN X.25, debe configurar los siguientes parámetros para ayudar al direccionador a descubrir a sus vecinos OSPF. Esta configuración es necesaria sólo si el direccionador reúne los requisitos necesarios para convertirse en direccionador designado de la red de no difusión.

Configure en primer lugar el intervalo de sondeo OSPF con el siguiente mandato:

```
OSPF Config> set non-broadcast
Interface IP address [0.0.0.0]? 128.185.138.19
Poll Interval [120]?
```

A continuación, configura las direcciones IP de todos los otros direccionadores OSPF que se conectarán a la red de no difusión. Para cada direccionador configurado, debe especificar los requisitos que necesita para convertirse en el 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]?
```

El establecimiento de la no difusión se puede también utilizar para forzar una red sin que se anuncien otros direccionadores OSPF. La prioridad del direccionador para la interfaz se debe establecer en cero y no se debe definir ningún vecino.

Configuración de subredes de área amplia

Frame Relay y X.25 permiten establecer conexiones directas entre varios direccionadores por medio de una única línea serie. Es necesaria una configuración adicional realizada con el mandato **set interface** para las interfaces OSPF que estén conectadas a este tipo de red. Debido a que los mensajes del protocolo OSPF se envían directamente a vecinos específicos de estas redes, la configuración (en lugar del descubrimiento dinámico) se utiliza para determinar las relaciones de vecino y los cometidos del direccionador.

Nota: Las configuraciones que se describen en este apartado no se pueden aplicar a redes punto a punto.

OSPF puede asumir dos patrones para las conexiones directas entre direccionadores de estas subredes:

- Punto a multipunto
- Multiacceso de no difusión (NBMA)

El factor clave que distingue estos dos patrones es si existe o no una conexión directa entre todos los pares de direccionadores que están conectados a la subred (*conectividad de la malla completa*) o si alguno de los direccionadores está conectado mediante vías de acceso de varios saltos a otros direccionadores como intermediarias (*conectividad de la malla parcial*).

El multiacceso de no difusión (NBMA) necesita *conectividad de la malla completa* mientras que el punto a multipunto necesita sólo *conectividad de la malla parcial*.

El punto a punto es la opción por omisión ya que funciona tanto en conectividades de la malla completa como en conectividades de la malla parcial. Sin embargo, cuando la conectividad de la malla completa se encuentra disponible, el NBMA es una solución más eficaz.

Configuración de subredes de punto a multipunto

El punto a multipunto se puede configurar más fácilmente que el NBMA al no haber DR, pero las relaciones entre los vecinos se deben configurar para todos los pares de direccionadores que intercambien tráfico de datos directamente a través de la red de punto a multipunto. Cada par de direccionadores directamente conectados intercambiarán mensajes Hello, por lo tanto un extremo podrá descubrir al otro a través de estos mensajes. El direccionador configurado par enviar el primer mensaje Hello debe, sin embargo, tener la dirección IP de su vecino configurada con el mandato **add neighbor**.

Es importante recordar que OSPF no calculará las rutas correctas si alguno de los direccionadores conectados a una subred lo representa como NBMA y otro lo representa como punto a multipunto. De todas formas, no utilice nunca el mandato **set non-broadcast** para una interfaz de una red punto a multipunto.

Punto a multipunto también puede configurarse para una interfaz que dé soporte a la posibilidad de difusión, como por ejemplo una LAN o una ELAN ATM. Esta configuración resulta útil en las siguientes situaciones:

- Soporte de redireccionamiento cuando el medio de difusión no es fiable.
- Realización de pruebas de las posibilidades punto a multipunto OSPF sin tener utilizar una conmutación X.25, ATM o Frame Relay cara.
- Priorización de ruta simple mediante la configuración de coste por vecino disponible sólo en topologías punto a multipunto.

Configuración de subredes NBMA

En subredes IP NBMA, algunas subredes de los direccionadores OSPF conectados están configuradas para convertirse en el direccionador designado (DR). Todos los direccionadores que poseen los requisitos para convertirse en DR envían periódicamente mensajes Hello a todos los otros direccionadores que poseen los requisitos para convertirse en DR. Estos mensajes se utilizan en el protocolo para seleccionar un DR y un DR de reserva. Tanto el DR como el DR de reserva intercambian periódicamente mensajes Hello con los otros direccionadores OSPF que están conectados a la subred IP NBMA. También, el flujo de la información de ruta OSPF de la subred IP NBMA está sólo entre cada uno de los direccionadores conectados y el DR o DR de reserva.

Seleccione NBMA con el mandato **set non-broadcast** para interfaces conectadas a una subred NBMA. Este mandato debe utilizarse en todas las interfaces conectadas a la red NBMA.

La configuración necesaria para un direccionador OSPF conectado a una subred NBMA depende de si el direccionador cumple o no con los requisitos para convertirse en el DR.

- En el caso de un direccionador que no cumpla con los requisitos para convertirse en DR, se debe utilizar el mandato **set interface** para establecer la prioridad del direccionador en 0.
- En el caso de un direccionador susceptible de convertirse en DR, se debe utiliza el mandato **set interface** para establecer la prioridad del direccionador en un valor distinto de cero y el mandato **add neighbor** para identificar a todos los direccionadores OSPF con interfaces conectadas a la subred NBMA y para indicar cual de ellos es convertible en DR.

Nota: En configuraciones en estrella, utilice el mandato **add neighbor** en el eje (los vecinos del sitio remoto no necesitan configuración). El mandato **add neighbor** surtirá efecto inmediatamente sin necesidad de reiniciar el direccionador.

Habilitación del direccionamiento limítrofe AS

Para importar rutas averiguadas de otros protocolos (la información configurada estáticamente y RIP) al dominio OSPF, habilite el direccionamiento limítrofe AS. Debe hacer esto aunque la única ruta que desee importar sea el valor por omisión (destino 0.0.0.0).

Al habilitar el direccionamiento limítrofe AS, se le solicitará las rutas externas que desea importar. Puede elegir importar o no rutas pertenecientes a las siguientes categorías.

- Rutas BGP
- Rutas RIP
- Rutas estáticas
- Rutas directas

Por ejemplo, puede importar rutas directas y BGP pero no rutas estáticas o RIP.

Además de las categorías externas enumeradas anteriormente, puede configurar si desea importar o no rutas de subred al dominio OSPF. El elemento de esta configuración toma por omisión el valor ENABLED (las subredes se importan).

Si no se importan las rutas de subred, OSPF importará solamente las rutas externas que sean de red. Consulte “Rutas por omisión, de red, de subred y de sistema principal” en la página 241.

También puede optar por importar o no en el dominio OSPF rutas agregadas. En el apartado “Agregación de ruta” en la página 254 hallará más información.

El tipo de métrica utilizada en rutas de importación determina la forma en que el coste importado es visto por el dominio OSPF. Al comparar dos métricas del tipo 2, sólo se considerará el coste externo al discriminar la mejor ruta. Al comparar dos métricas del tipo 1, los costes externo e interno de la ruta se combinan antes de hacer la comparación. Por ejemplo, puede establecer el direccionador de manera

que su valor por omisión se origine sólo si se recibe un direccionador 10.0.0.0 desde el número de AS 12. El establecimiento del número de AS en 0 significa “desde cualquier AS.” El establecimiento del número de red en 0.0.0.0 significa “cualquier ruta recibida.”

La sintaxis del mandato **enable** es la siguiente:

La sintaxis del mandato **enable as boundary routing** 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]
Import aggregate routes? [No]:
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** de la página 390 para obtener información sobre cómo utilizar una política de filtro de la ruta para definir los parámetros de direccionamiento limítrofe AS.

Otras tareas de configuración

Establecimiento de enlaces virtuales

Para mantener la conectividad de la red troncal, debe tener todos los direccionadores troncales interconectados mediante enlaces permanentes o virtuales. Puede configurar enlaces virtuales entre dos direccionadores limítrofes de área cualquiera que compartan un área común que no sea apéndice ni troncal. Los enlaces virtuales se consideran interfaces de direccionador distintas conectadas al área troncal. Por lo tanto, se le solicitará también especificar muchos de los parámetros de la interfaz al configurar un enlace virtual.

En el siguiente ejemplo se ilustra la configuración de un enlace virtual. Los enlaces virtuales se deben configurar en cada uno de los dos extremos del enlace. Observe que debe especificar los ID del direccionador OSPF de la misma forma 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 ha configurado ningún coste para el enlace virtual porque el coste es el coste intra área OSPF entre los extremos del enlace virtual a través del área de tránsito.

Configuración para comparaciones del protocolo de direccionamiento

Si además de OSPF utiliza un protocolo de direccionamiento, o cuando cambia el protocolo de direccionamiento a OSPF, debe establecer la comparación de protocolo de direccionamiento.

El direccionamiento OSPF de un sistema autónomo se produce en estos tres niveles: intra-área, entre áreas y exterior.

El direccionamiento intra-área se produce cuando la dirección de destino y origen de un paquete reside en la misma área. La información relativa a otras áreas no afecta a este tipo de direccionamiento.

El direccionamiento entre áreas se produce cuando las direcciones de origen y destino del paquete residen en diferentes áreas del mismo AS. OSPF hace direccionamiento entre áreas dividiendo la vía de acceso en tres piezas contiguas: una vía de acceso intra-área desde el origen al direccionador limítrofe de un área; una vía de acceso troncal entre las áreas de destino y origen y otra vía de acceso intra-área hasta el destino. Puede visualizar este nivel superior del direccionamiento como topología en estrella con la red troncal como eje y cada una de las áreas como emisor.

Las rutas exteriores son vías de acceso a redes que permanecen fuera del AS. Estas rutas se originan desde los protocolos de direccionamiento, como BGP, o desde las rutas estáticas especificadas por el administrador de la red. La información sobre direccionamiento exterior proporcionada por BGP no interfiere con la información de direccionamiento interna proporcionada por el protocolo OSPF.

Los direccionadores limítrofes de AS pueden importar rutas externas al dominio de direccionamiento OSPF. OSPF representa a estas rutas como anuncios del enlace externo AS.

OSPF importa rutas externas en distintos niveles. El primer nivel, denominado rutas del tipo 1, se utiliza cuando la métrica externa es comparable a la métrica OSPF (por ejemplo, ambos deben utilizar el retardo en milisegundos). El segundo nivel, denominado rutas del tipo 2, supone que el coste externo es mayor que el coste de cualquier vía de acceso OSPF (estado del enlace).

Las rutas externas importadas se identifican con 32 bits de información. En un direccionador, este campo de 32 bits, indica que el número de AS desde el que se ha recibido la ruta. Esto permite un comportamiento más inteligente a la hora de determinar si se reanuncia la información externa a otros sistemas autónomos.

OSPF una jerarquía de direccionamiento de 4 niveles (observe la Figura 33 en la página 380). El mandato **set comparison** dice al direccionador dónde se sitúan las rutas estáticas/RIP/BGP en la jerarquía OSPF. Los dos niveles inferiores se componen de las rutas internas OSPF. Las rutas OSPF intra-área y entre áreas tienen preferencia sobre la información obtenida de cualquier otra fuente, estando todas éstas ubicadas en un único nivel.

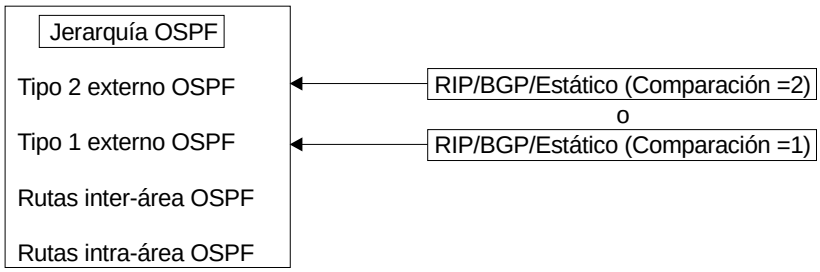


Figura 33. Jerarquía del direccionamiento OSPF

Para situar las rutas estática/RIP/BGP en el mismo nivel como rutas externas del tipo 1 OSPF, establezca la comparación en 1. Para situar las rutas estática/RIP/BGP en el mismo nivel como rutas externas del tipo 2 OSPF, establezca la comparación en 2. El valor por omisión es 2.

Por ejemplo, suponga que la comparación está establecida en 2. En tal caso, cuando las rutas RIP se importan al dominio OSPF, se importarán como externas del tipo 2. Todas las rutas externas OSPF del tipo 1 prevalecen sobre las rutas RIP recibidas, sin tener en cuenta la métrica. No obstante, si las rutas RIP tienen un coste menor, las rutas RIP alterarán temporalmente las rutas externas OSPF del tipo 2. Los valores de comparación para todos los direccionadores OSPF deben coincidir. Si los valores de comparación establecidos para los direccionadores son incoherentes, el direccionamiento no funcionará de manera correcta.

La sintaxis del mandato **set comparison** es la siguiente:

```
OSPF Config> set comparison
Compare to type 1 or 2 externals [2]?
```

Circuito de petición

En cada interfaz se puede configurar un circuito de petición. No existe dependencia en el medio físico o el modelo utilizados por OSPF para el cálculo de la ruta. Cuando se configura un circuito de petición y no existen problemas de compatibilidad:

- Sólo se anunciarán en la interfaz los anuncios de estado de enlace (LSA) con cambios reales. Normalmente, el algoritmo de inundación fiable de OSPF hará que los LSA se renueven con una nueva instancia cada 30 minutos, incluso en caso de producirse cambios en la topología.
- El bit DoNotAge se establecerá para los LSA con los que se inunda la interfaz. Esto es necesario porque no se renovarán en la interfaz.

Supresión de paquetes Hello de petición

Se trata de un parámetro adicional que puede utilizar para configurar una interfaz que solicite la supresión de paquetes Hello. Este parámetro será válido para interfaces punto a punto y punto a multipunto. Además, la subred a la que se conecta la interfaz debe poder notificar al OSPF que los datos no se pueden entregar a través de una conexión. Actualmente, las interfaces petición de marcación ISDN son los únicos tipos de interfaz que dan soporte a la supresión de paquetes Hello.

Intervalo de sondeo

Cuando la supresión de paquetes Hello no está activa, el intervalo de sondeo se utiliza sólo con redes multiacceso de no difusión y se establece con el mandato **set non-broadcast**. Puede configurar este parámetro después de configurar una interfaz como circuito de petición y después de que la supresión de paquetes Hello se haya solicitado. OSPF utilizará este parámetro para tratar de restablecer una conexión cuando una línea punto a punto esté desactivada debido a que ha habido un error a la hora de transmitir datos y la red todavía parezca funcionar.

Conversión de RIP a OSPF

Para convertir el sistema autónomo de RIP a OSPF, instale el direccionador uno OSPF de una vez, dejando RIP ejecutándose. De manera gradual, todos los direccionadores internos se desplazarán de ser informados a través de RIP a ser informados por OSPF (las rutas OSPF tienen preferencia sobre las rutas RIP). Si desea que los direccionadores sean exactamente los mismos que en RIP (para comprobar que la conversión está funcionando correctamente), utilice la cuenta de saltos como métrica OSPF. Para ello, establezca el coste de cada interfaz OSPF en 1.

Recuerde que el tamaño de el sistema OSPF se debe calcular una vez el protocolo habilitado. El cálculo del tamaño debe reflejar el tamaño final del dominio de direccionamiento OSPF.

Después de instalar OSPF en los direccionadores, active el direccionamiento limítrofe de AS en todos aquellos direccionadores que necesiten todavía captar rutas a través de otros protocolos (BGP, RIP y rutas configuradas estáticamente). El número de estos direccionadores limítrofes de AS se debe mantener en el mínimo.

Por último, debe inhabilitar la recepción de información RIP en todos aquellos direccionadores que no sean direccionadores limítrofes AS.

Cambio dinámico de los parámetros de configuración de OSPF

Los parámetros de configuración de OSPF se pueden cambiar dinámicamente mediante la actualización de la configuración a través de la facilidad de configuración OSPF y el posterior restablecimiento del protocolo OSPF a través de la consola OSPF. La política de direccionamiento limítrofe AS, áreas, interfaces y vecinos OSPF se pueden añadir, eliminar o cambiar mediante esta técnica. En la mayoría de los casos, estos cambios son completamente inocuos. Por ejemplo, la adición de una interfaz OSPF no afectará a otras interfaces OSPF (salvo el origen de nuevos anuncios de estado de enlace OSPF).

Los cambios que requieren todos los anuncios OSPF de un direccionador para que se vuelvan a crear hacen que OSPF se reinicie. Estos cambios son:

- Habilitación/inhabilitación del reenvío multidifusión OSPF (MOSPF)
- Habilitación/inhabilitación de los circuitos de petición (RFC 1793)
- Cambio del valor del ID del direccionador

En la mayoría de los casos, esto será claro para los usuarios ya que la única desconexión será el tiempo que tardarán en restablecerse las adyacencias de vecino OSPF.

Desde el momento en que la memoria del direccionador se reserva preferentemente para ubicar almacenamientos intermedios de entrada/de salida, OSPF no se podrá habilitar dinámicamente a menos que estuviese habilitado la última vez que se reinició el direccionador. Además, la cantidad de memoria reservada para OSPF no se puede incrementar sin reiniciar previamente el sistema. La cantidad de memoria reservada viene determinada por la estimación para los direccionadores y rutas externas de AS especificada 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 el programa de red multiprotocolo y el procesador de red IBM 6611 Nways

Las mejoras indicadas a continuación permiten realizar una migración desde los procesadores de red IBM 6611 Nways® existentes a los 2212:

- **Rangos de área de menor coste**

  En rangos de resumen OSPF, el 6611 calcula el coste según el coste menor de las redes que lo componen, mientras el 2212 lo calcula según el coste mayor de las redes que lo componen. **Los rangos de área de menor coste** dan la opción de calcular rangos de menor coste.

- **Coste vecino punto a multipunto**

  El 6611 da soporte al concepto de enlaces Frame Relay de punto a punto lógico pero no da soporte al punto a multipunto OSPF a través de Frame Relay. El punto a multipunto es más eficaz pero no permite especificar un coste diferente para cada vecino. **El coste vecino punto a multipunto** se ha añadido para permitir especificar un coste TOS 0 distinto para cada vecino.

Configuración y supervisión de OSPF

En este capítulo se describe la forma de utilizar el protocolo OSPF (Open Shortest Path First). OSPF es un IGP (Interior Gateway Protocol). El direccionador admite los siguientes IGP para crear la tabla de direccionamiento IP: OSPF y RIP. El protocolo OSPF se basa en la tecnología de estado de enlace o en el algoritmo de "primero la vía más corta" (SPF). RIP se basa en el algoritmo vector-distancia o Bellman-Ford. Este capítulo consta de los siguientes apartados:

Acceso al entorno de configuración de OSPF

Para acceder al entorno de configuración de OSPF, escriba 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 utilizar OSPF, debe configurarlo con los mandatos de configuración de OSPF. En el siguiente apartado se resumen y explican los mandatos OSPF.

Nota: Salvo los mandatos que aparecen en "Cambio dinámico de los parámetros de configuración de OSPF" en la página 381, que hacen que OSPF se reinicie inmediatamente con los parámetros cambiados, los mandatos de configuración de OSPF no se hacen efectivos de forma inmediata. Permanecen inactivos hasta que se emita el mandato Talk 5 **reset ospf**.

Escriba estos mandatos en el indicador `OSPF config>`. En la Tabla 22 en la página 384 se muestran estos mandatos.

Tabla 22. Resumen de los mandatos de configuración de OSPF

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Add	Añade información a la información OSPF existente. Puede añadir rangos a áreas y vecinos a redes de no difusión.
Delete	Elimina información OSPF de SRAM.
Disable	Inhabilita todo el protocolo OSPF, la posibilidad de direccionamiento limítrofe de AS, la posibilidad de circuito de petición o el direccionamiento multidifusión IP.
Enable	Habilita todo el protocolo OSPF, la posibilidad de direccionamiento limítrofe de AS, la posibilidad de circuito de petición o el direccionamiento multidifusión IP.
Join	Configura el direccionador para que pertenezca a uno o más grupos multidifusión.
Leave	Quita al direccionador de entre los miembros de un grupo multidifusión.
List	Muestra la configuración OSPF.
Set	Establece o cambia la información de la configuración relativa a los enlaces virtuales, las redes de no difusión, las interfaces o las áreas OSPF. Este mandato también permite establecer la forma en que las rutas OSPF se comparan con la 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 xxxi.

Respuesta a los mandatos de configuración de OSPF

Salvo los mandatos que aparecen en “Cambio dinámico de los parámetros de configuración de OSPF” en la página 381, que hacen que OSPF se reinicie inmediatamente con los parámetros cambiados, los mandatos de configuración de OSPF no se hacen efectivos de forma inmediata. Permanecen inactivos hasta que se emita el mandato Talk 5 **reset ospf**.

Add

Utilice el mandato **add** para añadir más información a la información OSPF existente. Con este mandato puede añadir rangos a áreas y vecinos a redes de no difusión.

Sintaxis:

add nssa range . . .
range . . .
neighbor . .

nssa-range *núm-área dirección-IP máscara-dirección-IP inihibir-anuncio identificador-LSA-externo*
Añade un rango para el resumen de direcciones externas al área NSSA. Los rangos de NSSA están definidos por un par de dirección-máscara IP y definen el conjunto de rutas externas que se han de agregar o confinar en el área NSSA. Si el direccionador es un direccionador limítrofe de área y es elegido conversor de NSSA para el área NSSA, los rangos

se utilizarán para producir LSA de tipo 5 (esto se denomina agregación).

1. *Núm-área* indica el área NSSA a la que se añadirá el rango:

   Valores válidos: el número de área de cualquier área OSPF configurada. Para configurar el área NSSA, se utiliza el mandatp **set area**.

   Valor por omisión: ninguno

2. *Dirección-IP* es la dirección IP del rango de NSSA. Éste abarcará las rutas externas de NSSA si son iguales a esta dirección cuando se unen a la máscara de dirección IP por medio de un operador AND lógico.

   Valores válidos: cualquier dirección IP válida

   Valor por omisión: ninguno

3. *Máscara-dirección-IP* es la máscara de dirección que identifica las rutas que abarca el rango.

   Valores válidos: cualquier máscara de dirección IP válida. No obstante, cuando la máscara se une con la dirección IP de rango por medio de un operador AND lógico, el valor resultante debe ser igual a dicha dirección.

   Valor por omisión: ninguno

4. El parámetro *inhibir-anuncio* indica si se produce o no un anuncio de tipo 5 OSPF cuando hay rutas externas de NSSA que están comprendidas en el rango especificado. El valor por omisión, **No**, indica que deben producirse.

   Valores válidos: Yes o no

   Valor por omisión: No

5. El parámetro *identificador-LSA-externo* es un valor hexadecimal de 4 bytes. Permite que la configuración manual de un identificador se anuncie con las rutas externas OSPF de LSA de tipo 5. Los direccionadores OSPF que reciban el anuncio podrán reconocer el identificador y manejar las rutas de forma exclusiva. Este parámetro no es aplicable si se especifica **yes** para *inhibir-anuncio*.

   Valores válidos: X'0-9', X'A-F' y X'a-f'.

   Valor por omisión: ninguno. El identificador anunciado se generará como si el direccionador produjese el LSA de tipo 5.

Ejemplo: add nssa-range

```
NSSA Area ID [0.0.0.1]?
IP Address [0.0.0.0]? 10.1.0.0
IP Address Mask [0.0.0.0]? 255.255.0.0
Inhibit advertisement? [No]:
External LSA Tag Value [0]? 1CD2
NSSA 0.0.0.1 Range 10.1.0.0/255.255.0.0 added or modified.
```

range *núm-área dirección-IP máscara-dirección-IP*

Añade rangos a áreas OSPF. Las áreas OSPF se pueden definir como rangos de dirección. Fuera del área, se anuncia una única ruta para cada rango de dirección. Por ejemplo, si un área OSPF estuviese formada por todas las subredes de la red de clase B 128.185.0.0, se definiría como formada por un único rango de dirección. El rango de

dirección se especificaría como dirección de 128.185.0.0 con máscara de 255.255.0.0. Fuera del área, toda la subred se anunciaría como ruta única a la red 128.185.0.0.

Los rangos se pueden definir para controlar las rutas que se anuncian fuera de un área. Existen dos opciones:

- Cuando OSPF se configura para anunciar el rango, se anuncia una única ruta entre áreas si al menos una de las rutas componentes del rango está activa dentro del área.
- Cuando OSPF se configura para no anunciar el rango, no se anuncian rutas entre áreas para rutas desactivadas dentro del rango.

Los rangos no se pueden utilizar para áreas que los enlaces virtuales utilicen como áreas de tránsito. Igualmente, si, al definir rangos para un área, el área está particionada pero está conectada mediante una red troncal, OSPF no funcionará de forma correcta.

Ejemplo:

```
add range 0.0.0.2 128.185.0.0 255.255.0.0

inhibit advertisement ? [No]
```

1. *núm-área* tiene:

   Valores válidos: cualquier número de área válido

   Valor por omisión: ninguno

2. *dirección-IP* tiene:

   Valores válidos: cualquier dirección IP válida

   Valor por omisión: ninguno

3. *máscara-dirección-IP* tiene:

   Valores válidos: cualquier máscara de dirección IP válida

   Valor por omisión: ninguno

neighbor Configura vecinos adyacentes al direccionador de esta interfaz. En redes multiacceso de no difusión, los vecinos necesitan configurarse sólo en los direccionadores que se puedan convertir en el direccionador designado. En redes de punto a multipunto, al menos uno de los extremos de cada conexión lógica debe tener un vecino configurado. En redes de punto a multipunto, se puede configurar un coste alternativo TOS 0. 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. *IP Address of Neighbor* tiene:

   Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

3. Responda a la pregunta, `Can that router become designated router on this net`? En interfaces de punto a multipunto, este parámetro no se puede aplicar y se debe establecer en “No”.

   Valores válidos: Yes o No

   Valor por omisión: Yes

4. `Alternate TOS 0 cost` le 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 eliminar información OSPF de SRAM.

Sintaxis:

delete
- area . . .
- interface . . .
- nssa-range . . .
- neighbor . . .
- non-broadcast . . .
- range . . .
- virtual-link

area *núm-área*

Elimina áreas OSPF de la configuración OSPF actual.

Ejemplo: **`delete area 0.0.0.1`**

núm-área tiene:

Valores válidos: cualquier número de área válido

Valor por omisión: ninguno

interface *dirección-IP-interfaz*

Elimina una interfaz de la configuración OSPF actual.

Ejemplo: **`delete interface 128.185.138.19`**

dirección-IP-interfaz tiene:

Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

nssa range *núm-área dirección-IP máscara-dirección-IP*

Suprime del área NSSA especificada un rango para el resumen de direcciones externas.

1. *núm-área* indica el área NSSA de la que se suprimirá el rango:

   Valores válidos: cualquier área NSSA OSPF configurada

   Valor por omisión: ninguno

2. *dirección-IP* es la dirección IP del rango de NSSA que se ha de suprimir.

   Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

3. *máscara-dirección-IP* es la máscara de dirección que identifica el rango que se ha de suprimir.

   Valores válidos: cualquier máscara de dirección IP válida

   Valor por omisión: ninguno

Ejemplo: delete nssa-range

```
NSSA Area ID [0.0.0.1]?
IP Address [0.0.0.0]? 10.1.0.0
IP Address Mask [0.0.0.0]? 255.255.0.0
NSSA 0.0.0.1 Range 10.1.0.0/255.255.0.0 0 deleted.
```

neighbor *dirección-IP-interfaz dirección-IP-vecino*

Elimina vecinos configurados de la configuración 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. *dirección-IP-interfaz* tiene:

   Valores válidos: cualquier dirección IP válida

   Valor por omisión: ninguno

2. *dirección-IP-vecino* tiene:

   Valores válidos: cualquier dirección IP válida

   Valor por omisión: ninguno

non-broadcast *dirección-IP-interfaz*

Elimina información sobre la red de no difusión de la configuración OSPF actual.

Ejemplo: `delete non-broadcast 128.185.133.21`

1. *dirección-IP-interfaz* tiene:

   Valores válidos: cualquier dirección IP válida

   Valor por omisión: ninguno

range *núm-área dirección-IP*

Elimina rangos de áreas OSPF.

Ejemplo: `delete range 0.0.0.2 128.185.0.0 255.255.0.0`

1. *núm-área* del rango tiene:

   Valores válidos: cualquier dirección de area válida

   Valor por omisión: ninguno

2. *dirección-IP* tiene:

   Valores válidos: cualquier dirección IP válida

   Valor por omisión: ninguno

3. *máscara-IP* tiene:

   Valores válidos: cualquier máscara de dirección IP válida

   Valor por omisión: ninguno

virtual-link

Elimina un enlace virtual configurado con 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 vecino 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 inhabilitar todo el protocolo OSPF, la topología punto a multipunto de una interfaz, la posibilidad de circuito de petición o la posibilidad de direccionamiento limítrofe de AS.

Sintaxis:

disable as boundary routing
demand-circuits
least-cost-ranges
multicast forwarding
ospf routing protocol
p2mp
rfc1583compatibility
subnet

as boundary routing

Inhabilita la posibilidad de direccionamiento limítrofe de AS. Cuando está inhabilitado, el direccionador no importa información externa al dominio OSPF.

Ejemplo: **`disable as boundary routing`**

demand-circuits

Inhabilita la posibilidad del circuito de petición. Una vez inhabilitado, el direccionador no indicará que admite el proceso de circuito de petición en el LSA de su enlace de direccionador y no producirá ningún LSA con el bit DoNotAge establecido. Si un direccionador del dominio de direccionamiento o del área apéndice OSPF no admite circuitos de petición, ninguno de los direccionadores del dominio de direccionamiento o del área apéndice OSPF producirá LSA DoNotAge.

Ejemplo: **`disable demand-circuits`**

least-cost-ranges

Inhabilita el cálculo de los rangos de área OSPF basados en el coste de la red componente más cercana (coste más bajo). Esta opción está inhabilitada por omisión.

multicast forwarding
Inhabilita el direccionamiento multidifusión IP de todas las interfaces. Cuando está inhabilitado, el direccionador no reenvía datagramas multidifusión IP (clase D).

Ejemplo: `disable multicast forwarding`

OSPF routing protocol
Inhabilita todo el protocolo OSPF.

Ejemplo: `disable OSPF routing protocol`

P2MP *interfaz-IP*
Altera temporalmente el funcionamiento punto a multipunto (P2MP) de una red de difusión.

Interfaz-IP es la dirección de una interfaz con una red de difusión configurada como red de punto a multipunto mediante el mandato **enable p2mp**.

Valores válidos: la dirección IP válida de una interfaz OSPF configurada.

Valor por omisión: ninguno

RFC1583 Compatibility
Inhabilita la selección de la ruta externa del AS compatible con las especificaciones del documento RFC 1583. Se recomienda no inhabilitar la compatibilidad RFC1583 a menos que tenga la misma ruta externa accesible a través de más de un área OSPF y sufra problemas con el bucle de direccionamiento parecidos a los descritos en el documento RFC2178. El valor por omisión es habilitado.

Ejemplo: `disable rfc1583Compatibility`

subnet En interfaces conectadas a una línea serie punto a punto, esta opción inhabilita el anuncio de una ruta apéndice a la subred que representa a la línea serie en lugar de a la ruta del sistema principal para la dirección del otro direccionador. Debe proporcionar la dirección del direccionador para que la interfaz la identifique.

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 habilitar todo el protocolo OSPF, el anuncio de un apéndice para direccionar a una subred, la topología punto a multipunto de una interfaz de difusión, la posibilidad de circuito de petición o la posibilidad de direccionamiento limítrofe de AS.

Sintaxis:

en**able**	as boundary routing demand-circuits least-cost-ranges

multicast forwarding
ospf routing protocol
p2mp
rfc1583compatibility
send outage-only
subnet

as boundary routing

Habilita la posibilidad de direccionamiento limítrofe de AS que le permite importar rutas averiguadas de otros protocolos (por ejemplo, BGP, RIP e información configurada estáticamente) al dominio OSPF. Para obtener más información acerca del uso del mandato **enable**, consulte “Configuración de OSPF” en la página 366.

Si no se importan las rutas de subred, OSPF importará solamente las rutas externas que sean de red. Consulte “Rutas por omisión, de red, de subred y de sistema principal” en la página 241.

También puede especificar si se han de importar o no en el dominio OSPF rutas agregadas. En el apartado “Agregación de ruta” en la página 254 hallará más información.

Una de las opciones del mandato permite utilizar una política de filtros de rutas para determinar las rutas importadas y los detalles específicos de su anuncio, como son el tipo de externo OSPF, la métrica, el valor de identificador (que es normalmente el número del AS) y el protocolo. Consulte “Configuración de políticas de filtros de rutas” en la página 331 para obtener más información sobre la configuración de una política de filtro de rutas. En el ejemplo 1 se muestra la configuración del direccionamiento limítrofe de AS cuando no se utiliza una política de filtros de rutas y en el ejemplo 2 se muestra la misma configuración pero cuando se utiliza una política de filtros 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]
Import aggregate routes? [No]:
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* le indica si se utiliza una política de ruta configurada para determinar las rutas que no sean OSPF importadas al OSPF como rutas externas OSPF. Si se responde a esta pregunta con **yes**, muchas de las demás preguntas desaparecerán al no ser aplicables en caso de que la política de direccionamiento está configurada. La política de direccionamiento proporciona más granularidad cuando se especifican las rutas importadas.

   Valores válidos: yes o no

Valor por omisión: no

2. La pregunta *Router Policy Identifier* solicita la serie que sirve para identificar una política de filtro de rutas configurada.

   Valores válidos: serie de 1 a 15 caracteres ASCII

   Valor por omisión: ninguno

3. La pregunta *Import BGP* indica si las rutas BGP se importarán al 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 al OSPF como rutas externas OSPF.

   Valores válidos: Yes o No

   Valor por omisión: No

5. La pregunta *Import static* indica si las rutas estáticas se importarán al 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 al 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 al OSPF como rutas externas OSPF.

   Valores válidos: Yes o No

   Valor por omisión: Yes

8. La pregunta *Always originate default route* indica si se produce incondicionalmente una ruta por omisión como 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 creado por OSPF será del tipo 1 ó 2 de externa AS. Las métricas de tipo 1 se considera que están en el mismo contexto de los costes OSPF mientras las métricas de tipo 2 se consideran superiores a cualquier métrica OSPF.

   Valores válidos: 1 ó 2

   Valor por omisión: 2

10. *Default route cost* es el parámetro que especifica el coste que OSPF relaciona con la ruta por omisión de su direccionador limítrofe del área. El coste se utiliza para determinar la vía de acceso más corta para la ruta por omisión al direccionador limítrofe del área.

    Valores válidos: de 0 a 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: cualquier dirección IP válida

    Valor por omisión: ninguno

multicast forwarding

Habilita el reenvío de datagramas multidifusión IP (clase D). Al habilitar el direccionamiento multidifusión, se le solicitará si desea reenviar datagramas multidifusión IP entre áreas OSPF. Para ejecutar el MOSPF (OSPF con extensiones multidifusión), el direccionador que está ejecutando OSPF necesita únicamente utilizar este mandato. No es necesario volver a especificar la información de su configuración.

Ejemplo: `enable multicast forwarding`

```
Inter-area multicasting enabled (Yes or No): yes
```

demand-circuits

Habilita el proceso de circuito de petición para el direccionador. El direccionador indicará que admite el proceso de circuito de petición en el LSA de su enlace de direccionador. El valor por omisión se habilita para que los circuitos de petición se puedan utilizar sin volver a configurar cada direccionador del dominio de direccionamiento OSPF.

```
OSPF Config> enable demand-circuits
```

least-cost-ranges

Habilita el cálculo de los rangos de área OSPF basados en el coste de la red componente más cercana (coste más bajo). La habilitación de este parámetro se hará necesaria para que la compatibilidad con IBM 6611s actúe como direccionadores limítrofes de área (ABR) del mismo área. También se puede utilizar en situaciones en las que la red componente de coste más bajo reduzca significativamente el número de recreaciones OSPF LSA motivadas por cambios de coste. Esta opción está inhabilitada por omisión.

OSPF routing protocol

Habilita todo el protocolo OSPF. Al habilitar el protocolo de direccionamiento OSPF, debe proporcionar los siguientes dos valores para calcular el tamaño de la base de datos de estado de enlace OSPF:

- El número total de rutas externas de AS que se importarán al dominio de direccionamiento OSPF. Se puede dirigir un único destino a diversas rutas externas cuando lo importan distintos direccionadores limítrofes del AS. Por ejemplo, si el dominio de direccionamiento OSPF tiene dos direccionadores limítrofes de AS y ambos importan rutas a los mismos 100 destinos, establezca el número de rutas externas de AS en 200.

  Valores válidos: de 0 a 65535

  Valor por omisión: 100

- El número total de rutas OSPF del dominio de direccionamiento.

  Valores válidos: de 0 a 65535

  Valor por omisión: 50

- Además, puede especificar el tamaño máximo de LSA. Puede que este valor necesite incrementarse si tiene un direccionador grande con muchos enlaces de marcación OSPF (por ejemplo, RDSI primario) en la misma área OSPF. Normalmente, 2048 es ya suficiente para cualquier LSA.

  Valores válidos: de 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]?
```

P2MP *interfaz-IP*

Altera temporalmente el tipo de red por omisión de una red de difusión con el fin de el funcionamiento sea forzosamente punto a multipunto. Todos los direccionadores de la subred deben tener la misma especificación, y será necesario que la definición de vecino sea la correspondiente a un tipo de red que sea punto a multipunto de forma inherente, como por ejemplo Frame Relay. Esta opción es aplicable únicamente para redes que admitan de manera inherente la difusión, como por ejemplo redes LAN y ELAN ATM.

Interfaz-IP indica la interfaz OSPF que ha de ser una red P2MP.

Valores válidos: cualquier interfaz OSPF configurada

Valor por omisión: ninguno

RFC1583Compatibility

Habilita la selección de la ruta externa de AS compatible con las especificaciones del documento RFC 1583. El valor por omisión es habilitado.

Ejemplo: `enable rfc1583Compatibility`

subnet En interfaces a una línea serie punto a punto, esta opción habilita el anuncio de una ruta apéndice a la subred que representa a la línea serie en lugar de a la ruta del sistema principal para la dirección del otro direccionador. Debe proporcionar la dirección del direccionador para que la interfaz la identifique.

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 multidifusión. Cuando el direccionador es miembro de un grupo multidifusión, responde a las consultas PING y SNMP enviadas a la dirección del grupo.

Para solicitar ser miembro de un grupo de manera más inmediata (no es necesario reiniciar/recargar), emita el mandato **join** del proceso de supervisión de OSPF. Desde el proceso de supervisión de OSPF el mandato join realiza igualmente un seguimiento del número de veces que se une un determinado grupo. Los grupos

multidifusión IP unidos mediante la supervisión OSPF no se conservan a lo largo de las recargas y reinicios del direccionador.

Sintaxis:

j**oin** *dirección-grupo-multidifusión*

Ejemplo: `join 224.185.0.0`

El parámetro *dirección-grupo-multidifusión* especifica la dirección IP multidifusión/grupo de clase D.

Valores válidos: dirección IP de clase D desde el valor 224.0.0.1 al 239.255.255.255

Valor por omisión: ninguno

Leave

Utilice el mandato **leave** para eliminar un miembro del direccionador que se encuentre en un grupo multidifusión. Se evitará de esta forma que el direccionador responda a las consultas PING y SNMP enviadas a la dirección del grupo.

Para eliminar a un miembro de un grupo de manera más inmediata (no es necesario reiniciar/recargar), emita el mandato **leave** del proceso de supervisión de OSPF. El mandato no eliminará el miembro de un grupo hasta que el número de "leaves" ejecutados iguale al número de "joins" previamente ejecutados.

Sintaxis:

le**ave** *dirección-grupo-multidifusión*

Ejemplo: `leave 224.185.0.0`

El parámetro *dirección-grupo-multidifusión* especifica la dirección IP multidifusión/grupo de clase D.

Valores válidos: dirección IP de clase D desde el valor 224.0.0.1 al 239.255.255.255

Valor por omisión: ninguno

List

Utilice el mandato **list** para mostrar la información sobre la configuración OSPF.

Sintaxis:

li**st** all
areas
interfaces
neighbors
non-broadcast
virtual-links

all Lista toda la información sobre la 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 habilitado o inhabilitado.
# AS ext. routes	Muestra el número calculado de rutas externas del sistema autónomo. El direccionador no puede aceptar más de este número de rutas externas del AS.
Estimated # routers	Muestra el número estimado de direccionadores encontrados en la configuración OSPF.
Maximum LSA size	Muestra el LSA de máximo tamaño que creará el direccionador.
External comparison	Muestra el tipo de ruta externa utilizada por OSPF al importar información externa al dominio OSPF y al comparar rutas externas OSPF con rutas RIP/BGP.
RFC 1583 compatibility	Indica si la ruta externa de AS OSPF es compatible con las especificaciones del documento RFC 1583.
AS boundary capability	Muestra si el direccionador importará rutas externas al dominio OSPF.
Import external	Muestra las rutas que se importarán.
Orig default route	Muestra si el direccionador importará un valor por omisión al dominio OSPF. Si el valor es “YES”, y aparece entre paréntesis un número de red distinto de cero, se indica que la ruta por omisión se creará sólo si se encuentra disponible una ruta para esa 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 creada.
Multicast forwarding	Muestra si se reenviarán datagramas multidifusión IP.
Demand circuits	Muestra si se da soporte al proceso de circuitos de petición.
Least Cost Area Ranges	Muestra si se calcularán los rangos de área de coste más bajo.
LSA Max Random Initial Age	Muestra la antigüedad máxima inicial para los LSA autocreados. Si el valor es cero (el valor por omisión), todos los LSA se crearán con una antigüedad de 0.

External comparison	Muestra el tipo de ruta externa utilizada por OSPF al importar información externa al dominio OSPF y al comparar rutas externas OSPF con rutas RIP/BGP.
Inter-area multicast	Muestra si los datagramas multidifusión IP se reenviarán entre las áreas.
Area-ID	Muestra el ID del área conectada (información del resumen del área)
AuType	Muestra el método utilizado para la autenticación del área.“Simple-pass” significa que se ha utilizado un esquema de contraseña simple para autenticar el área.
Stub area	Muestra si el área resumida es un área apéndice. Las áreas apéndice no llevan rutas externas, creando una base de datos de direccionamiento más pequeña. No obstante, las áreas apéndice no pueden contener direccionadores limítrofes de AS ni admiten enlaces virtuales configurados.
OSPF interfaces	En cada interfaz se imprime la dirección IP junto con los parámetros configurados. “Area” es el área OSPF a la que está conectada la interfaz. “Cost” indica el coste TOS 0 (o métrica) relacionado con la interfaz. “Rtrns” es el intervalo de retransmisión, que es el número de segundos entre retransmisiones de información de direccionamiento no reconocidas. “TrnsDly” es el retardo de transmisión, es decir, el cálculo del número de segundos que tarda la transmisión de información de direccionamiento por la interfaz (debe ser mayor que 0). “Pri” es la prioridad de direccionador de la interfaz, que se utiliza cuando se selecciona el direccionador designado. “Hello” es el número de segundos transcurridos entre paquetes Hello enviados fuera de la interfaz. “Dead” es el número de segundos transcurridos después del cese de los mensajes Hello para anunciar que el direccionador se considera inactivo.
Virtual links	Enumera los enlaces virtuales que se han configurado con el direccionador como extremos. “Virtual endpoint” indica el ID del direccionador OSPF del otro extremo. “Transit area” indica el área no troncal en la que se configura el enlace virtual. Se considera que los enlaces virtuales están tratados por el protocolo OSPF de forma similar a las redes de punto a punto. Los otros parámetros que muestra el mandato (“Rtrns”, “TrnsDly”, “Hello,” y “Dead”) se mantienen para todas las interfaces. Consulte el mandato OSFP "list interfaces" para obtener más información.

areas Muestra toda la información relativa a las áreas OSPF configuradas.

Ejemplo: `list areas`

```
                  --Area configuration--
Area ID           Stub/NSSA Default-Cost(Type)  Inhibit-Sum/External  NSSA-Trans
0.0.0.0           Transit        N/A            N/A                    N/A
0.0.0.1           NSSA           0(2)           No /No                 Elected
0.0.0.5           NSSA           5(2)           No /No                 Elected

                       --NSSA Area ranges--
Area ID          Address         Mask            Advertise             Tag
0.0.0.1          193.1.1.0       255.255.255.0   No                    N/A
0.0.0.5          192.168.0.0     255.255.0.0     Yes                   0xACEEACEE
```

Area-ID	La dirección del área.
Stub/NSSA	Indica si el área es de tránsito, apéndice o NSSA.
Default-cost (Type)	El coste de una ruta producida por direccionador limítrofe de área (ABR) y, para las áreas NSSA, el tipo configurado.

Inhibit-Sum/ External	Si el anuncio de rutas externas y de resumen está inhibido o no. Cuando la importación de rutas externas está inhibida, un ABR que actúe de direccionador limítrofe de AS no anunciará LSA de tipo 7 en el área.
NSSA-Trans	Indica si un ABR del área NSSA tendrá participación en el proceso de elección de conversión de LSA de tipo 7 de NSSA o bien los LSA de tipo 7 se convertirán incondicionadamente en LSA de tipo 5.
NSSA Area ranges-Area ID	La dirección de área OSPF que indica el área NSSA a la que pertenece el rango.
Address/Mask	La dirección y la máscara IP que identifican el área NSSA.
Advertise	Indica si se produce o no un anuncio de tipo 5 OSPF cuando hay rutas externas de NSSA que están comprendidas en el rango de NSSA.
Tag	Es el identificador, si se ha configurado uno, del rango de NSSA. Se trata de un valor hexadecimal de 4 bytes configurado manualmente que se anuncia con las rutas externas OSPF de LSA de tipo 5. Existe sólo si el valor de *Advertise* es *Yes*.

interfaces

En cada interfaz se imprime la dirección IP junto con los parámetros configurados. “Area” es el área OSPF a la que está conectada la interfaz. “Cost” indica el coste TOS 0 (o métrica) relacionado con la interfaz. “Rtrns” es el intervalo de retransmisión, que es el número de segundos transcurridos entre retransmisiones de información de direccionamiento no reconocidas. “TrnsDly” es el retardo de transmisión, es decir, el cálculo del número de segundos que tarda la transmisión de información de direccionamiento por la interfaz (debe ser mayor que 0). “Pri” es la prioridad de direccionador de la interfaz, que se utiliza cuando se selecciona el direccionador designado. “Hello” e el número de segundos transcurridos entre paquetes Hello enviados fuera de la interfaz. “Dead” es el número de segundos transcurridos después de que cesen los mensajes Hello para anunciar que el direccionador se considera 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 multidifusión no aparecen si la multidifusión esta inhabilitada. Los parámetros del circuito de petición no aparecen si ninguna de las interfaces está configurada como circuito de petición.

neighbors

Muestra los vecinos de las redes de no difusión. Aparece la dirección IP del vecino y la dirección IP de la interfaz del vecino. Indica también si el vecino se puede convertir o no en “direccionador designado” de la red y en coste TOS 0 alternativo para redes de 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

Muestra toda la información relacionada con interfaces conectadas a redes multiacceso de no difusión. En todas las interfaces de no difusión, siempre que el direccionador se pueda convertir en direccionador designado de la red conectada, el intervalo de sondeo aparece junto con una lista de los vecinos del direccionador en la red de no difusión.

Ejempl0: `list non-broadcast`

```
        --NBMA configuration--
Interface Addr      Poll Interval
128.185.235.34      120
```

virtual-links

Lista todos los enlaces virtuales configurados con el direccionador como extremos. “Virtual endpoint” indica el ID del direccionador OSPF del otro extremo. “Transit area” indica el área no troncal en la que se configura el enlace virtual. Se considera que los enlaces virtuales están tratados por el protocolo OSPF de forma similar a las redes de punto a punto. Los otros parámetros que muestra el mandato (“Rtrns”, “TrnsDly”, “Hello,” y “Dead”) se mantienen para todas las interfaces. Consulte el mandato 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 mostrar o cambiar la información de la configuración relativa a áreas OSPF, interfaces, redes de no difusión o enlaces virtuales. Este mandato también permite establecer la forma en que las rutas OSPF se comparan con la información obtenida de otros protocolos de direccionamiento.

Sintaxis:

set
- area
- comparison
- cost-internal-address
- interface
- non-broadcast
- virtual-link
- max-random-initial-lsa-age

area Establece los parámetros de un área OSPF. Si no se ha definido ninguna área, el software del direccionador supone que todas las redes conectadas directamente al direccionador pertenecen al área troncal

(área ID 0.0.0.0). Las áreas se pueden establecer como apéndice o como NSSA.

Ejemplo: `set area`

```
Area number [0.0.0.0]? 0.0.0.1
Is this a stub area? [No]:
Is this an NSSA Area? [No]: yes
Always perform NSSA Translation? [No]:
Import Local Externals? [Yes]:
Stub/NSSA default cost [0]?
Import summaries? [Yes]:
NSSA Type (1 or 2) for Default [2]?
```

- *Area number* - es la dirección del área OSPF. En el caso de las áreas NSSA, este número indica el área NSSA a la que se añadirá el rango.
- *Is this a stub area?* Si contesta *yes*:
  - El área no recibe ningún anuncio de enlace externo al AS, reduciendo el tamaño de la base de datos y disminuyendo el uso de la memoria en los direccionadores del área apéndice.
  - No se pueden configurar enlaces virtuales a través de un área apéndice.
  - No se pueden configurar direccionadores de un área apéndice como direccionador limítrofe de AS.

  Valores válidos: yes o no

  Valor por omisión: no

  External Routing in Stub Areas. No se pueden configurar redes troncales como áreas apéndice. El direccionamiento externo de las áreas apéndice se basa en la ruta por omisión. Todos los direccionadores de áreas limítrofes conectados a un área apéndice crean una ruta por omisión con este objetivo. El coste de esta área por omisión se puede configurar también con el mandato **set area**.
- *Is this an NSSA Area?* indica si el área es o no un área NSSA OSPF. Esta pregunta es aplicable sólo si se responde *no* a la pregunta *Is this a stub area?*

  Valores válidos: yes o no

  Valor por omisión: no
- *Always perform NSSA translation?* indica si el direccionador, cuando actúa de direccionador limítrofe de área, convertirá incondicionadamente las rutas externas de NSSA instaladas en anuncios de estado de enlace de tipo 5. Si se responde *no* y el direccionador es un direccionador limítrofe de área, participará en la elección del conversor de NSSA según lo establecido en las especificaciones IETF actuales sobre NSSA de OSPF. Esta pregunta es aplicable sólo si se responde *yes* a la pregunta *Is this an NSSA?*

  Valores válidos: yes o no

  Valor por omisión: no
- *Import Local Externals?* indica si las rutas que se anuncian por medio de la política de importación de límites de AS también inundarán esta área NSSA como anuncios de tipo 7. Esta pregunta es

aplicable sólo si se responde *yes* a la pregunta *Is this an NSSA?* y está habilitada la importación de límites de AS.

Valores válidos: yes o no

Valor por omisión: no

- *Stub/NSSA Default Cost?* especifica el coste de un anuncio por omisión con el que se inunda el área apéndice o NSSA cuando el direccionador actúa de direccionador limítrofe de área. Esta pregunta es aplicable sólo si se responde *yes* a la pregunta *Is this a stub area?* o *Is this an NSSA?*

  Valores válidos: de 0 a 16 777 215

  Valor por omisión : 0

- *Import summaries?* indica si el direccionador (cuando actúa de direccionador limítrofe de área) inhibirá el anuncio de los LSA de tipo 3. En el caso de las áreas apéndice, el direccionador limítrofe de área producirá siempre un anuncio por omisión de tipo 3, independientemente de cuál sea la respuesta a esta pregunta. En el caso de las áreas NSSA, si responde *no*, los direccionadores limítrofes de área producirán un anuncio por omisión de tipo 3. Si responde *yes* o por omisión se toma este valor, las áreas NSSA se inundarán con un anuncio por omisión de tipo 7. Esta pregunta aparece sólo si se responde *yes* a la pregunta *Is this a stub area?* o *Is this an NSSA?*

  Valores válidos: yes o no

  Valor por omisión: yes

- *NSSA Type (1 or 2) for Default* especifica el tipo externo OSPF (1 ó 2) correspondiente a un anuncio por omisión en el área NSSA cuando el direccionador actúa de direccionador limítrofe de área. Esta pregunta es aplicable sólo si se responde *yes* a *Is this an NSSA?* y *no* a *Import summaries?*. Si no se anuncian resúmenes en el área NSSA, se anuncia un anuncio por omisión de tipo 3, tal y como sucede con las áreas apéndice.

  Valores válidos: 1 ó 2

  Valor por omisión: 2

comparison

Dice al direccionador dónde se sitúan las rutas estáticas/RIF/BGP dentro de la jerarquía de OSPF. Los dos niveles inferiores se componen de las rutas internas OSPF. Las rutas internas de OSPF tienen preferencia sobre la información obtenida de otras fuentes, estando todas éstas ubicadas en un único nivel.

Ejempl0: `set comparison`

```
OSPF Config> set comparison
Compare to type 1 or 2 externals [2]?
```

cost internal address

Establece el coste del anuncio de dirección interna dentro de la red de direcciones internas en el LSA de tipo 1 del direccionador. Si se especifica *-1*, no se anuncia la dirección interna.

Ejemplo:

```
OSPF Config>set cost-internal-address
Internal Address Cost? [10]? 8
```

- *Internal Address Cost?* especifica el coste del anuncio de la dirección interna. Si se especifica *-1*, no se incluirá la dirección interna en los anuncios de tipo 1 del direccionador.

  Valores válidos: de -1 a 65 535

  Valor por omisión : 0

interface Establece los parámetros OSPF en las interfaces de la red del direccionador.

1. *Interface IP address* es para todas las interfaces del direccionador.
2. *Attaches to area* es el área OSPF a la que está conectada la interfaz.
3. Los valores del temporizador son los mismos valores para todos los direccionadores conectados a un segmento de red común.
   a. *Retransmission interval* es el intervalo después del que se reenviará una petición de enlace para uno o más anuncios de estado de enlace.

      Valores válidos : de 1 a 65 535 segundos

      Valor por omisión: 5

   b. *Transmission delay* es el cálculo del número de segundos que tarda en transmitirse la información de estado de enlace a través de la interfaz.

      Todos los anuncios de estado de enlace tienen un tiempo de vida finito igual a la máxima antigüedad (MaxAge) constante (1 hora). Como cada anuncio de estado de enlace se envía a una determinada interfaz, su antigüedad está determinada por el retardo de transmisión configurado. El retardo mínimo es de 1 segundo.

      Valores válidos: de 1 a 65 535 segundos

      Valor por omisión: 1

   c. *Hello Interval* es el intervalo transcurrido entre los paquetes Hello enviados por la interfaz.

      Valores válidos: de 1 a 65 535 segundos

      Valor por omisión: 10

   d. *Dead Router Interval*

      "Dead Router Interval" es el intervalo después del cual un direccionador que no ha enviado ningún mensaje Hello se considerará muerto. Este intervalo toma por omisión un valor cuatro veces mayor que el configurado para el intervalo de paquetes Hello. El valor para este parámetro debe ser mayor que el del intervalo de paquetes Hello.

      Valores válidos: de 2 a ≥ 65 535 segundos

      Valor por omisión: 40 (o cuatro veces el intervalo de paquetes Hello configurado)

4. El valor de *Router Priority* se utiliza para que las redes multiacceso de difusión y de no difusión seleccionen el direccionador designado. En enlaces de punto a punto, este valor debe ser **0**, lo que significa que el direccionador no debe seleccionarse como designado para la red.

   Valores válidos: de 0 a 255

   Valor por omisión: 1

5. *Type of service 0 cost* es el coste utilizado para la interfaz cuando se calculan las rutas de la vía de acceso más corta para el área.

   Valores válidos: de 1 a 65534

   Valor por omisión: 1

6. *Demand Circuit* indica si la interfaz será tratada como circuito de petición o no. En los circuitos de petición, la inundación de LSA se efectuará en la interfaz con el bit DoNotAge establecido, pero únicamente cuando exista un cambio real en el LSA. Consulte el documento RFC 1793 para obtener más información.

   Valores válidos: yes o no

   Valor por omisión: no

7. *Hello Suppression* indica si los paquetes Hello serán eliminados de la interfaz después de que los vecinos alcancen el estado completo. Los circuitos de petición se deben habilitar en la interfaz para que la supresión de paquetes Hello se solicite o se permita. Actualmente, sólo se da soporte a la supresión de paquetes Hello en enlaces RDSI de marcación a petición. Consulte el documento RFC 1793 para obtener más información.

   Valores válidos: allow, request o disable

   Valor por omisión: allow

   Allow Permite que un vecino solicite la supresión de paquetes Hello

   Request Solicita la supresión de paquetes Hello de un vecino.

   Disable Inhabilita la supresión de paquetes Hello y continúa mandando mensajes Hello.

8. *Demand Circuit Down Poll Interval* indica la duración entre los sondeos Hello enviados cuando existe un error al enviar datos en circuitos de petición con la supresión de paquetes Hello activada. Actualmente, sólo se da soporte a la supresión de paquetes Hello en enlaces RDSI de marcación a petición. Consulte el documento RCF 1793 para obtener más información.

   Valores válidos: de 1 a 65535

   Valor por omisión: 60

9. *Authentication type* define el procedimiento de autenticación utilizado para paquetes OSPF de la interfaz. Las opciones son 1, que indica una contraseña sencilla, o 0, que indica que no es necesario ningún tipo de autenticación para intercambiar paquetes OSPF en la

interfaz. Cuando se especifica 1, la clave de autenticación se debe también especificar.

Valores válidos: 0, 1

Valor por omisión : 0

10. *Authentication key* es el parámetro que define la contraseña utilizada para esta área OSPF. Cuando se utiliza autenticación de contraseña, sólo se aceptarán los paquetes con la clave de autenticación correcta.

    Valores válidos: cualquier serie de 1 a 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 preguntas, proporcione la dirección IP de todas las interfaces del direccionador y responda a las preguntas a continuación. Para los siguientes parámetros, debe especificar el mismo valor en todos los direccionadores conectados a una red común:

- Hello interval
- Dead router interval
- Authentication key (si se utiliza una autenticación de 1)

El indicador "first" solicita el área OSPF a la que la interfaz está conectada. Por ejemplo, supongamos que la máscara de la dirección de la interfaz es 255.255.255.0, indicando que la interfaz conectada a una subred (128.185.138.0) de la red 128.185.0.0. Todos los otros direccionadores OSPF conectados a la subred 128.185.138.0 deben tener también el parámetro *Hello interval* establecido en 10, *dead router interval* establecido en 40 y *authentication key* establecido en xyz_q.

Observe que las interfaces IP conectadas a líneas punto a punto puede que no estén numeradas. En tal caso, se configura un índice de red en lugar de una dirección IP. Esta implementación de OSPF funcionará con 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 multidifusión (la multidifusión se ha habilitado), los parámetros MOSPF de cada interfaz OSPF se establecen en los valores por omisión. Esto acarrea lo siguiente:

- Que está habilitado el reenvío multidifusión.
- Que los datagramas multidifusión se reenvían como multidifusiones del enlace de datos.
- Que los miembros del sistema principal IGMP salen de la interfaz cada 60 segundos.

- Que las entradas de la base de datos local se eliminan 180 segundos después de que la interfaz deje de recibir los informes sobre miembros del sistema principal IGMP para el grupo.

Si desea cambiar los parámetros MOSPF, utilice el mandato **set interface**. Sólo se le consultarán los parámetros multidifusión (los último cinco parámetros mostrados en la parte superior de la pantalla) si antes ha habilitado el reenvío multidifusión.

En redes situadas en el borde de un sistema autónomo, en el que existan varios protocolos de direccionamiento multidifusión (o varias instancias de un único protocolo de direccionamiento multidifusión), puede que sea necesario configurar el reenvío como unidifusiones del enlace de datos para evitar la replicación de datagramas. En cualquier caso, para todos los direccionadores conectados a una red común, los parámetros de la interfaz “reenvían datagramas multidifusión” y “el reenvío como unidifusiones del enlace de datos” se debe configurar de forma idéntica.

non-broadcast

Altera temporalmente el valor por omisión de punto a multipunto para seleccionar el NBMA para redes X.25, Frame Relay . Este parámetro especifica el intervalo que determina la frecuencia de mensajes Hello enviados a los vecinos inactivos. Debe establecer la no difusión de forma coherente a lo largo de todas las interfaces conectadas a la misma subred para que el protocolo OSPF funcione correctamente.

En redes Frame Relay, sin embargo, el mandato **set non-broadcast** se utiliza para configurar una interfaz OSPF conectada a una red multiacceso de no difusión. Si no se utiliza el mandato **set non-broadcast**, se supone que la interfaz está conectada a una red de punto a multipunto. En redes Frame Relay, todas las interfaces OSPF se deben configurar como interfaces conectadas al mismo tipo de red (multiacceso de no difusión o de punto a multipunto), por lo tanto, si el mandato **set non-broadcast** se utiliza para una interfaz del direccionador, se debe configurara en las interfaces de todos los direccionadores conectados 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
El intervalo de sondeo NBMA se utiliza para enviar paquetes Hello para desactivar vecinos. (Los vecinos inactivos son los vecinos de los que el direccionador no ha recibido nada durante un periodo mayor al del parámetro Dead Router Interval). El direccionador continúa sondeando a estos vecinos a una velocidad reducida. Establezca el intervalo de sondeo NBMA en un valor más alto que el configurado para el intervalo de paquetes Hello del direccionador.

Valores válidos: de 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 direcciones limítrofes de área cualesquiera. Para mantener la conectividad troncal, debe tener todos los direccionadores troncales interconectados mediante enlaces permanentes o virtuales. Los enlaces virtuales se consideran interfaces de direccionador distintas conectadas al área troncal. Por lo tanto, se le solicitará también especificar muchos de los parámetros de la interfaz al configurar un enlace virtual.

Los enlaces virtuales se pueden configurar entre dos direcciones troncales cualesquiera que tengan una interfaz conectada a un área no troncal común. Los enlaces virtuales se utilizan para mantener la conectividad troncal y se deben configurar en ambos extremos.

Nota: Esta implementación OSPF admite el uso de enlaces virtuales en caso de que uno de los enlaces del extremo sea una línea punto a punto no numerada. Para que esta configuración funcione, el ID del direccionador se debe utilizar como dirección de origen en los mensajes de protocolo OSPF enviados a través del enlace virtual. El uso del ID del direccionador se puede asegurar configurando la dirección IP interna con la dirección utilizada como ID del direccionador. Otro de los requisitos necesarios para que esta configuración funcione correctamente es que, en cada uno de los extremos del enlace virtual, las implementaciones OSPF le den soporte.

1. *Virtual endpoint (router ID)* define el ID del vecino virtual.

   Valores válidos: cualquier dirección IP válida

   Valor por omisión: ninguno

2. *Link's transit area* es el área no troncal y no apéndice a través de la cual se configura el enlace virtual. Los enlaces virtuales pueden configurar entre dos direccionadores limítrofes de área que tengan una interfaz conectada a un área común que no sea troncal ni apéndice. Los enlaces virtuales se deben configurar en cada uno de los dos extremos del enlace.

   Valores válidos: de 0.0.0.1 a 255.255.255.255

   Valor por omisión: 0.0.0.1

3. Los valores del temporizador son los mismos valores para todos los direccionadores conectados a un segmento de red común.

   a. *retransmission interval* es el intervalo después del que se reenviará una petición de enlace para uno o más anuncios de estado de enlace.

      Valores válidos: de 1 a 65 535 segundos

      Valor por omisión: 10

b. *Transmission delay* es el cálculo del número de segundos que tarda en transmitirse la información de estado de enlace a través de la interfaz.

   Todos los anuncios de estado de enlace tienen un tiempo de vida finito igual a la máxima antigüedad (MaxAge) constante (1 hora). Como cada anuncio de estado de enlace se envía a una determinada interfaz, su antigüedad está determinada por el retardo de transmisión configurado. El retardo mínimo es de 1 segundo.

   Valores válidos: de 1 a 65535 segundos

   Valor por omisión: 5

c. *Hello Interval* es el intervalo transcurrido entre los paquetes Hello enviados por la interfaz.

   Valores válidos: de 1 a 255 segundos

   Valor por omisión: 30

d. *Dead Router Interval* es el intervalo después del cual un direccionador que no ha enviado ningún mensaje Hello se considerará muerto. Este parámetro toma por omisión un valor seis veces mayor que el configurado para "Hello Interval" y se debe establecer en un valor mayor que aquel.

   Valores válidos: de 2 a 65535 seconds

   Valor por omisión: 180

4. *Authentication type* define el procedimiento de autenticación utilizado para paquetes OSPF del enlace virtual. Las opciones son 1, que indica una contraseña sencilla, o 0, que indica que no es necesario ningún tipo de autenticación para intercambiar paquetes OSPF en la interfaz. Cuando se especifica 1, la clave de autenticación se debe también especificar.

   Valores válidos: 0, 1

   Valor por omisión : 0

5. *Authentication key*. Define la contraseña utilizada para esta área OSPF. Cuando se utiliza autenticación de contraseña, sólo se aceptarán los paquetes con la clave de autenticación correcta.

Valores válidos: cualquier serie de 1 a 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 máxima inicial de los LSA autocreados. El valor por omisión es 0 y normalmente se debería modificar sólo si experimenta problemas con la sincronización a la hora de crear LSA.

Valores válidos: 0 - 1770

Valor por omisión : 0

Ejemplo:

```
OSPF Config>  set max-random-initial-lsa-age
Maximum initial LSA age [0]?
```

Acceso al entorno de supervisión de OSPF

Utilice el siguiente procedimiento para acceder a los mandatos de supervisión de OSPF. Este proceso le proporciona acceso al proceso de *supervisión* de OSPF.

1. En el indicador OPCON, especifique **talk 5**. (Para obtener más información sobre este mandato, consulte “Proceso OPCON y mandatos de OPCON” en *Access Integration Services Guía del usuario de software*.) Por ejemplo:

   ```
   * talk 5
   +
   ```

   Después de especificar el mandato **talk 5**, el indicador GWCON (+) aparecerá en el terminal. Si el indicador no aparece al especificar primero la configuración, pulse de nuevo **Intro**.

2. En el indicador +, escriba el mandato **protocol ospf** para que aparezca el indicador OSPF>.

   Ejemplo:

   ```
   + prot ospf
   OSPF>
   ```

Mandatos de supervisión de OSPF

En este apartado se resumen y explican todos los mandatos de supervisión de OSPF. Dichos mandatos permiten supervisar el protocolo de direccionamiento OSPF.En la Tabla 23 aparecen los mandatos de supervisión de OSPF.

Escriba los mandatos de supervisión de OSPF en el indicador OSPF>.

Tabla 23 (Página 1 de 2). Resumen de los mandatos de supervisión de OSPF

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Advertisement	Muestra un anuncio de estado de enlace perteneciente a la base de datos OSPF.
Area summary	Muestra los parámetros y estadísticas del área OSPF.
AS external	Lista los anuncios externos de AS pertenecientes a la base de datos de estado de enlace OSPF.

Tabla 23 (Página 2 de 2). Resumen de los mandatos de supervisión de OSPF

Mandato	Función
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 los parámetros y estadísticas de la interfaz OSPF.
Join	Configura el direccionador para que pertenezca a uno o más grupos multidifusión.
Leave	Quita al direccionador de entre los miembros de un grupo multidifusión.
Mcache	Muestra una lista de las entradas de antememoria de reenvío multidifusión actualmente activas.
Mgroups	Muestra los miembros de grupos de las interfaces conectadas del direccionador.
Mstats	Muestra diferentes estadísticas del direccionamiento multidifusión.
Neighbor summary	Muestra los parámetros y estadísticas de los vecinos OSPF.
Ping	Envía continuamente peticiones ICMP de eco (o pings) a un destino determinado, imprimiendo una línea por cada respuesta recibida.
Policy	Muestra cualquier política de importación del direccionador limítrofe de AS.
Reset	Restablece la configuración OSPF dinámicamente.
Routers	Muestra los direcciones OSPF limítrofes de área que son accesibles y los direccionadores limítrofes del AS.
Size	Muestra el número de LSA que se encuentran actualmente en la base de datos de estado de enlace, categorizados según el tipo.
Statistics	Muestra estadísticas OSPF en las que se detalla el uso de la red y la memoria.
Traceroute	Muestra la vía de acceso completa (salto por salto) de un determinado destino.
Weight	Cambia dinámicamente 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 xxxi.

Advertisement Expansion

Utilice el mandato **advertisement expansion** para imprimir el contenido de un anuncio de estado de enlace dentro de la base de datos OSPF. Para obtener un resumen de los anuncios del direccionador, utilice el mandato **database**.

Un anuncio de estado de enlace se define a través del tipo de estado de enlace, del ID de estado de enlace y del direccionador que lo anuncia. Existe una base de datos de estado de enlace distinta para cada área OSPF. Proporcionar un ID de área a la línea de mandatos sirve para decirle al software la base de datos que desea buscar. Los distintos tipos de anuncios, que dependen del valor dado al tipo de estado de enlace, son:

- Enlaces del direccionador - Contienen descripciones de una única interfaz del direccionador.
- Enlaces de la red - Contienen la lista de los direccionadores conectados a una determinada interfaz.
- Redes de resumen - Contienen descripciones de una única ruta entre áreas.
- Direccionadores limítrofes de AS de resumen - Contienen descripciones de la ruta hacia un direccionador limítrofe de AS situado en otra área.
- Redes externas de AS - Contienen descripciones de una única ruta.
- Miembros de grupos multidifusión - Contienen descripciones de miembros de un determinado grupo situado en la vecindad del direccionador que anuncia.

  Nota: Los ID de estado de enlace, los direccionadores de anuncio (especificados por sus ID de direccionador) y los ID de áreas tienen el mismo formato que las direcciones IP. Por ejemplo, el área troncal se puede establecer en 0.0.0.0.

En el **ejemplo 1** se muestra la expansión del anuncio de los enlaces del direccionador. El ID del direccionador es 128.185.184.11. Se trata de un direccionador limítrofe de AS que tiene tres interfaces conectadas al área troncal (todas de coste 1). Se ha habilitado el direccionamiento multidifusión. Las descripciones detalladas de los campos se proporcionan en el ejemplo.

Este mandato también se ha mejorado en dos sentidos. Para empezar, al mostrar los LSA de la red y del direccionador, aparece el coste inverso de cada enlace de direccionador a direccionador y de cada enlace de direccionador a red de tránsito, así como el coste directo mostrado anteriormente. Esto se debe a que el direccionamiento de los datagramas multidifusión cuyo origen se sitúa en distintos sistemas autónomos/áreas se basa en el coste inverso en lugar de en el coste directo. En aquellos casos en los que no exista enlace inverso (lo que significa que el enlace no será nunca utilizado por el Dijkstra), el coste inverso aparecerá como “1-way”.

Por otro lado, las opciones OSPF de los LSA aparecen de la misma forma que aparecían en el mandato OSPF detallado **neighbor**.

Aparecen también los nuevos LSA de miembros de grupo. La “LS destination” de cada LSA de miembro de grupo es una dirección de grupo. Un direccionador crea LSA de miembros de grupo para cada grupo que tenga miembros en una o más de las redes conectadas al direccionador. Los LSA de miembros de grupo del grupo listan aquellas redes de tránsito conectadas que tienen miembros de grupo (los vértices tipo “2”), y cuando son miembros que pertenecen a una o más redes apéndice conectadas, o cuando el direccionador es miembro del grupo multidifusión, se incluye un vértice tipo “1” cuyo ID sea el ID de direccionador OSPF del direccionador.

Sintaxis:

ad**vertisement** *tipo-ls id-estado-enlace direccionador-anunciante id-área*

Example 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 posibilidades OSPF opcionales admitidas por el objeto OSPF correspondiente al anuncio. Estas posibilidades son las siguientes:

- **E** — Indica que el tipo 5 (anuncios externos) es admitido en el área correspondiente al anuncio. Siempre está establecido para el tipo 5 (anuncios externos).
- **T** — Se da soporte al direccionamiento basado en IP TOS (tipo de servicio).
- **MC** — Se da soporte al reenvío multidifusión. Sólo se establecerá en anuncios creados por direcciones con el MOSPF habilitado.
- **DC** — Se admiten circuitos de petición, tal y como se describe en el documento RFC 1793.

LS type — Clasifica el anuncio y dicta su contenido: 1 (anuncio de enlaces del direccionador), 2 (anuncio del enlace de red), 3 (anuncio del enlace de resumen), 4 (anuncio del ASBR de resumen), 5 (enlace externo de AS) y 6 (anuncio de miembro de grupo).

LS destination — Identifica lo que se describe mediante el anuncio. Depende del tipo de anuncio. En resúmenes ASBR y enlaces, se trata del ID del direccionador OSPF. En enlaces de red, es la dirección IP del direccionador designado de la red. En enlaces de resumen y enlaces externos de AS, es un número de subred/red. En anuncios de miembros de grupo, se trata de un grupo multidifusión determinado.

LS originator — ID del direccionador OSPF del direccionador creador.

LS sequence number — Se utiliza para distinguir distintas instancias de un mismo anuncio. Debe ser un entero de 32 bits con signo. Empieza en 0x80000001 y se incrementa en uno cada vez que el anuncio se actualiza.

LS checksum — Suma de comprobación del contenido del anuncio utilizada para detectar la corrupción de los datos.

LS length — Tamaño del anuncio en bytes.

Router type	Indica el nivel de funcionamiento del direccionador. ASBR indica que el direccionador es un direccionador limítrofe de AS, ABR que el direccionador es un direccionador limítrofe de área y W que el direccionador es un receptor multidifusión comodín.
# Router ifcs	Número de las interfaces del direccionador descritas en el anuncio.
Link ID	Indica a lo que se conecta la interfaz. Depende del tipo de interfaz. En interfaces conectadas a direccionadores (caso de los enlaces punto a punto), el ID del enlace es el ID del direccionador del vecino. En interfaces conectadas a redes de tránsito, es la dirección IP del direccionador designado de la red. En interfaces conectadas a redes apéndice, es el número de la subred/red de la red.
Link Data	4 bytes de información suplementaria relativa al enlace, puede ser la dirección IP de la interfaz (en interfaces conectadas a redes punto a punto y redes de tránsito) o la máscara de la subred (en interfaces conectadas a redes apéndice).
Interface type	Una de las siguientes: 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	Número de valores TOS distintos de cero para los que se proporcionan las métricas de la interfaz.
TOS 0 metric	Coste de la interfaz. El coste inverso del enlace se proporciona entre paréntesis (obtenido de otro anuncio). Si no existe enlace inverso, aparece “1-way”.

Los campos: LS age, LS options, LS type, LS destination, LS originator, LS sequence no, LS checksum y LS length son campos comunes a todos los anuncios. "Router type" y "# router ifcs" sólo aparecen en anuncios de enlaces del direccionador. Todos los enlaces del anuncio de direccionador se describen en los campos "Interface type", "Link Data" y "Link ID" (tipo de interfaz, datos del enlace e ID del enlace). A cada enlace se le puede asignar un coste distinto para cada tipo de servicio IP (TOS); esto se describe en los campos "TOS 0 metric" y "No. of metrics" (métrica TOS 0 y número de métricas).

En el **ejemplo 2** se muestra la expansión de un anuncio de miembro de grupo. Un anuncio de miembro de grupo para una determinada combinación de direccionador de anuncio/grupo muestra las redes directamente conectadas al direccionador de anuncio que posee miembros de grupo. También muestra si el propio direccionador es miembro del grupo especificado. El siguiente ejemplo muestra que la red 128.185.184.0 posee 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 posee miembros de grupo, uno del: 1 (el propio direccionador, o redes apéndice conectadas al direccionador) o2 (una red de tránsito).

Vertex ID — Cuando el tipo de vértice es 1, se trata siempre del ID del direccionador que anuncia. Cuando el tipo de vértice es 2, se trata de la dirección IP del direccionador designado de la red de tránsito.

Area Summary

Utilice el mandato **area summary** para ver una presentación resumida de la información de área OSPF o una presentación detallada de la información correspondiente al área especificada. Si no especifica ninguna área o bien no se encuentra el área, se visualizará un resumen de las áreas configuradas. Si se especifica un área configurada, se visualizará información detallada sobre ella.

Sintaxis:

ar**ea** *número-área*

número-área

Número que indica el área cuya información detallada se ha de visualizar.

Valores válidos: una dirección IP OSPF que identifique un áreas NSSA OSPF configurada

Valor por omisión: ninguno

Ejemplo 1:

```
          OSPF>area

    Area ID           Type    #ifcs  #nets  #rtrs  #brdrs  DC-Status
    0.0.0.1           NSSA        2      0      2       1      On
```

ifcs — Indica el número de interfaces del direccionador conectadas a un área determinada. Estas interfaces no tienen por que ser necesariamente funcionales.

nets — Indica el número de redes de tránsito que se han encontrado al hacer el cálculo de árbol SPF para el área.

rtrs — Indica el número de direccionadores encontrados al hacer el cálculo de árbol SPF para el área.

brdrs — Indica el número de direccionadores limítrofes de área encontrados al hacer el cálculo de árbol SPF para el área.

DC-Status — Indica si el proceso de circuito de petición está activo para el área.

Ejemplo 2:

```
OSPF>area 0.0.0.1

                          Area 0.0.0.1
      Area Index:                       0 Configured Interfaces:           2
      Type:                          NSSA Inhibit Summaries:             Yes
      Stub Default Cost:                0 NSSA Default Type:               1
      NSSA Translation:                No NSSA Always Translate:          No
      NSSA Type 7 ABR Default Type:     1 NSSA Type 7 Default Originated: No
      Active Interfaces:                2 Demand Circuit Capability:     Yes
      Area Networks:                    0 Area Routers:                    2
      Reachable ASBRs:                  2 Reachable ABRs:                  1
      Number of LSAs:                   7 Noage LSAs:                      0
      Area Checksum:           0x0003D1CF Dynamic Config Change Flag: 0x0000

                        --Area ranges--
     Address          Mask             Active Advertise Cost
     153.2.0.0        255.255.0.0          No       Yes
```

Area Index Posición del área OSPF con relación a las demás áreas. Lo utiliza internamente la implementación OSPF de IBM.

Stub Default Cost Coste de una ruta por omisión con la que se inunda el área NSSA cuando el direccionador actúa de direccionador limítrofe de área (ABR).

NSSA Translation Indica si el direccionador limítrofe de un área NSSA convierte los anuncios de NSSA de tipo 7 en anuncios externos de tipo 5.

NSSA Type 7 ABR Default Type Cuando un direccionador limítrofe de área produce un anuncio por omisión de tipo 7, esto indica el tipo de métrica externa (1 ó 2).

Active Interfaces Número de interfaces activas dentro del área.

Area Networks Número de redes dentro del área.

Reachable ASBRs Número de direccionadores limítrofes de sistema autónomo (ASBR) a los que se puede llegar desde el área NSSA.

Number of LSAs Número de LSA que hay en la base de datos de estado de enlace de área.

Area Checksum Suma de comprobación de todos los LSA que hay en la base de datos de estado de enlace de área.

Configured Interfaces Número de interfaces configuradas dentro del área. Este número incluye tanto las interfaces activas como las inactivas.

Inhibit Summaries Indica si el direccionador (cuando actúa de direccionador limítrofe de área) inhibirá el anuncio de los LSA de tipo 3.

NSSA Default Type Tipo de métrica de un anuncio por omisión de NSSA de tipo 7.

NSSA Always Translate Indica si se ha configurado la conversión de NSSA incondicionada para el área NSSA. No obstante, un direccionador sólo realizará una conversión incondicionada cuando actúe de direccionador limítrofe de área.

NSSA Type 7 Default Originated Indica si el direccionador limítrofe de área ha producido actualmente un anuncio por omisión de tipo 7.

Demand Circuit Capability Indicates indica si la interfaz será tratada como circuito de petición o no a efectos de inundación de LSA. En los circuitos de petición, la inundación de LSA se efectuará en la interfaz con el bit DoNotAge

establecido, pero únicamente cuando exista un cambio real en el LSA. Consulte el documento RFC 1793 para obtener más información.

Area Routers Número de direccionadores dentro del área.

Reachable ABRs Número de direccionadores limítrofes de área (ABR) a los que se puede llegar desde el interior del área.

Noage LSAs Número de LSA Noage que hay en el área (según la definición dada en el documento RFC 1795).

Dynamic Config Change Flag Identificador que representa lo que ha cambiado durante la última reconfiguración dinámica (utilizado por el equipo de desarrollo).

Address Dirección IP del rango de NSSA.

Mask Máscara IP de la dirección.

Active Indica si el direccionador limítrofe de área ha descubierto o no anuncios de tipo 7 en el rango de NSSA.

Advertise Cost Métrica anunciada en el LSA de tipo 5 convertido.

AS-external advertisements

Utilice el mandato **AS-external advertisements** para listar los anuncios externos de AS que pertenecen al dominio de direccionamiento OSPF. Se imprime una línea para cada anuncio. Cada anuncio se define mediante los siguientes tres parámetros: su tipo de estado de enlace (siempre 5 para anuncios externos de AS), su ID de estado de enlace (denominado destino LS) y el direccionador de 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 es 5 para anuncios externos de AS.

LS destination Indica un número de subred/red IP. Estos números de red pertenecen a otros sistemas autónomos.

LS originator Direccionador anunciante.

Unreach Indica el tiempo que el destino asociado con un LSA que sea DoNotAge ha resultado inaccesible. Si el LSA es DoNotAge, *DA* aparecerá después de la columna Age y antes de la columna Unreach. Si el LSA **no** es DoNotAge, estará vacío.

Seqno, Age, Xsum Puede que existan varias instancias de un anuncio en el dominio de direccionamiento OSPF en cualquier momento. No obstante, sólo la instancia más reciente se guardará en la base de datos OSPF de estado de enlace (y será impresa por este mandato). Los campos número de secuencia LS, (Seqno), antigüedad LS (Age) y suma de comprobación LS (Xsum) se compararán para ver la instancia más reciente. El campo

antigüedad LS se indica en segundos. Su valor máximo es de 3600 segundos.

Options Se trata de las opciones de estado de enlace, que son las posibilidades OSPF opcionales que admite el objeto OSPF correspondiente al anuncio. Estas posibilidades son las siguientes:

E Indica que el tipo 5 (anuncios externos) está soportado en el área correspondiente al anuncio. Siempre está establecido para el tipo 5 (anuncios externos).

T Se da soporte al direccionamiento basado en IP TOS (tipo de servicio).

MC Se da soporte al reenvío multidifusión. Sólo se establecerá en anuncios creados por direcciones con el MOSPF habilitado.

DC Se admiten circuitos de petición, tal y como se describe en el documento RFC 1793.

Al final de la pantalla, se imprime el número total de anuncios externos de AS, junto con el total de la suma de comprobación de todo su contenido. El total de la suma de comprobación es simplemente la suma de 32 bits (sin tener en cuenta las que se llevan) de los campos de la suma de comprobación LS del anuncio individual. Esta información se puede utilizar para determinar rápidamente si dos direccionadores OSPF tienen sus bases de datos sincronizadas.

Database Summary

Utilice el mandato **database summary** para mostrar la descripción del contenido de la base de datos de estado de enlace de un área OSPF determinada. Los anuncios externos de AS no aparecen en la pantalla. Se imprime una línea para cada anuncio. Cada anuncio se define mediante los siguientes tres parámetros: su tipo de estado de enlace (denominado tipo), su ID de estado de enlace (denominado destino LS) y el direccionador de anuncio (denominado originador LS).

Sintaxis:

da**tabase** *id-área*

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 Los distintos tipos de LS aparecen con distinta numeración: tipo 1 (anuncios de enlaces del direccionador), tipo 2 (anuncios de enlaces de red), tipo 3 (resúmenes de la red), tipo 4 (resúmenes de direccionadores limítrofes de AS) y 6 (LSA de miembros de grupo).

LS destination Indica lo descrito mediante el anuncio.

LS originator Direccionador anunciante.

Unreach Indica el tiempo que el destino asociado con un LSA que sea DoNotAge ha resultado inaccesible. Si el LSA es DoNotAge, *DA* aparecerá después de la columna Age y antes de la columna Unreach. Si el LSA **no** es DoNotAge, estará vacío.

Seqno, Age, Xsum Puede que existan varias instancias de un anuncio en el dominio de direccionamiento OSPF en cualquier momento. No obstante, sólo la instancia más reciente se guardará en la base de datos OSPF de estado de enlace (y será impresa por este mandato). Los campos número de secuencia LS, (Seqno), antigüedad LS (Age) y suma de comprobación LS (Xsum) se compararán para ver la instancia más reciente. El campo antigüedad LS se indica en segundos. Su valor máximo es de 3600 segundos.

Options Se trata de las opciones de estado de enlace, que son las posibilidades OSPF opcionales que admite el objeto OSPF correspondiente al anuncio. Estas posibilidades son las siguientes:

E Indica que el tipo 5 (anuncios externos) está soportado en el área correspondiente al anuncio. Siempre está establecido para el tipo 5 (anuncios externos).

T Se da soporte al direccionamiento basado en IP TOS (tipo de servicio).

MC Se da soporte al reenvío multidifusión. Sólo se establecerá en anuncios creados por direcciones con el MOSPF habilitado.

DC Se admiten circuitos de petición, tal y como se describe en el documento RFC 1793.

Al final de la pantalla, se imprime el número total de anuncios externos de AS, junto con el total de la suma de comprobación de todo su contenido. El total de la suma de comprobación es simplemente la suma de 32 bits (sin tener en cuenta las que se llevan) de los campos de la suma de comprobación LS del anuncio individual. Esta información se puede utilizar para determinar rápidamente si dos direccionadores OSPF tienen sus bases de datos sincronizadas.

Nota: Cuando se comparan direccionadores de no difusión con los de difusión, la suma de comprobación de la base de datos anterior (y también el número de anuncios) no tienen por qué coincidir necesariamente, ya que los direccionadores de no difusión no manejan o almacenan LSA de miembros de grupo. Además, si el proceso de circuito de petición está activado en el dominio de direccionamiento OSPF o en el área apéndice OSPF, la suma de comprobación de la base de datos será más bien diferente a los direccionadores con circuitos de petición. Consulte el documento RFC 1793 para obtener más información.

Dump Routing Tables

Utilice el mandato **dump routing tables** para mostrar todas las rutas que OSPF ha calculado y que ahora se encuentran en la tabla de direccionamiento. Su salida en pantalla tiene un formato parecido al del mandato de supervisión de IP "dump routing tables".

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 cómo se ha derivado la ruta.

Sbnt - Indica que la red está conectada a otra red; tal entrada es tan sólo un espacio reservado.

Dir - Señala una red o subred conectada directamente.

RIP - Señala que la ruta se encontró a través del protocolo RIP.

Del - Indica que la ruta se ha eliminado.

Stat - Señala una ruta configurada estáticamente.

BGP - Señala rutas encontradas mediante el protocolo BGP.

BGPR - Señala rutas encontradas mediante el protocolo BGP que se han vuelto a anunciar mediante OSPF y RIP.

Fltr - Señala un filtro de direccionamiento.

SPF - Indica que la ruta es una ruta entre áreas OSPF.

SPIA - Indica que es una ruta entre áreas OSPF.

SPE1, SPE2 - Señala rutas externas OSPF (tipo 1 y 2 respectivamente).

Rnge - Señala un tipo de ruta que es un rango de dirección de área OSPF activa y no se utiliza en paquetes de reenvío.

Dest net Red/subred IP de destino.

Mask Máscara de dirección IP.

Cost Coste de ruta.

Age Para las rutas RIP y GBP es el tiempo que ha transcurrido desde que se renovó por última vez la entrada de la tabla.

Next Hop Dirección IP del siguiente direccionador en la vía hacia el sistema principal de destino. También se visualiza el tipo de interfaz que utiliza el direccionador de envío para reenviar el paquete.

Un asterisco (*) después del tipo de ruta indica que la ruta tiene otra de reserva conectada directamente o estáticamente. Un signo de tanto por ciento (%) después del tipo de ruta indica que esta red/subred aceptará siempre las actualizaciones de RIP.

Un número entre paréntesis al final de la columna indica el número de rutas de igual coste conectadas al destino. Los primeros saltos de estas rutas se pueden mostrar con el mandato de supervisión de IP **route**.

Interface Summary

Utilice el mandato **interface summary** para mostrar las estadísticas y parámetros relacionados con las interfaces OSPF. Si no se dan argumentos (véase ejemplo 1), se imprime una sola línea que resume cada interfaz. Si se proporciona una dirección IP (véase ejemplo 2), aparecerán las estadísticas detalladas de la 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 interfaz.

Phys Muestra la interfaz física.

Assoc Area ID del área conectada.

Type Puede ser Brdcst (difusión; por ejemplo, una interfaz Ethernet), P-P (red punto a punto; por ejemplo, una línea serie síncrona), P-2-MP (punto a multipunto; por ejemplo, una red Frame Relay), Multi (de no difusión, multiacceso; por ejemplo, una conexión X.25) o VLink (un enlace virtual OSPF).

State Puede ser uno de los siguientes: 1 (down), 2 (looped back), 4 (waiting), 8 (point-to-point), 16 (DR other), 32 (backup DR) o 64 (designated router).

#nbrs Número de vecinos. Se trata del número de direccionadores cuyos mensajes Hello se han recibido, más aquellos que se han configurado.

#adjs Número de adyacencias. Se trata del número de vecinos en estado Exchange o superiores. Se trata de los vecinos con los que el direccionador se ha sincronizado o 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 interfaz.

Attached Area ID del área conectada.

Physical interface Número y tipo de interfaz física.

Interface Mask Máscara de subred de la interfaz.

Interface type Puede ser Brdcst (difusión; por ejemplo, una interfaz Ethernet), P-P (red punto a punto; por ejemplo, una línea serie síncrona), P-2-MP (punto a multipunto; por ejemplo, una red Frame Relay), Multi (de no difusión, multiacceso; por ejemplo, una conexión X.25) y VLink (un enlace virtual OSPF).

State Puede ser uno de los siguientes: 1 (Down), 2 (Looped back), 4 (Waiting), 8 (Point-to-Point), 16 (DR other), 32 (Backup DR), 64 (Designated router) o 128 (Full).

Authentication Type Indica el tipo de autenticación que está activa para la interfaz. Los tipos soportados son None y 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 del intervalo de paquetes Hello actual.

Rxmt interval Muestra el valor del intervalo de retransmisión actual.

Dead interval Muestra el valor del intervalo de estado Dead.

TX delay Muestra el valor del retardo de retransmisión actual.

Poll interval Muestra el valor del intervalo de sondeo actual.

Max pkt size Muestra el tamaño máximo de paquete OSPF enviado fuera de la interfaz.

Demand circuit Indica si el proceso de circuito de petición está o no activo en la interfaz.

TOS 0 cost Muestra el coste de TOS 0 de la interfaz.

Neighbors Número de vecinos. Se trata del número de direccionadores cuyos mensajes Hello se han recibido, más aquellos que se han configurado.

Adjacencies Número de adyacencias. Se trata del número de vecinos en estado Exchange o superiores.

Full adj Número de adyacentes completas. El número de adyacentes completas es el número de vecinos cuyo estado es Full (y con los que, además, el direccionador tiene sincronizadas bases de datos).

Mcast Floods Número de actualizaciones de estado de enlace con las que se han realizado inundaciones fuera de la interfaz (sin contar las retransmisiones).

Mcast acks Número de acuses de recibo de estado de enlace con los que se han realizado inundaciones fuera de la interfaz (sin contar las retransmisiones).

MC forwarding Muestra si el reenvío multidifusión se ha habilitado en la interfaz.

DL unicast Muestra si los datagramas multidifusión se reenviarán como multidifusiones de enlace de datos o como unidifusiones de enlace de datos.

IGMP monitor Muestra si IGMP está habilitado en la interfaz.

MC data in Muestra el número de datagramas multidifusión recibidos en la interfaz y reenviados satisfactoriamente.

MC data acc Muestra el número de datagramas multidifusión reenviados satisfactoriamente.

MC data out Muestra el número de datagramas reenviados fuera de la interfaz (como multidifusiones de enlace de datos y como unidifusiones de enlace de datos).

Network Capabilities Muestra las posibilidades de red de la interfaz.

IGMP polls sent Muestra el número de consultas de miembros de sistema principal IGMP enviadas fuera de la interfaz.

IGMP polls rcv Muestra el número de consultas de miembros de sistema principal IGMP recibidas en la interfaz.

Unexp polls Muestra el número de consultas de miembros de 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 miembros de sistema principal IGMP recibidos en la interfaz.

Nbr node: type and ID Muestra la identidad del nodo ascendente si se supone que el direccionador ha de recibir datagramas en la interfaz. Type es un número entero del 1 al 3: 1 indica que se trata de un direccionador; 2, red de tránsito; y 3, red apéndice.

Join

Utilice el mandato **join** para establecer el direccionador como miembro de un grupo multidifusión.

Este mandato es parecido al mandato **join** utilizado para la supervisión de la configuración OSPF pero con dos excepciones:

- El efecto sobre el grupo es inmediato cuando los mandatos se dan desde el monitor (por ejemplo, no es necesario reiniciar/recargar). Los grupos multidifusión IP unidos mediante la supervisión OSPF no se conservan a lo largo de las recargas y reinicios del direccionador.
- El mandato hace un seguimiento del número de veces que se “une” un determinado grupo.

Cuando el direccionador es miembro de un grupo multidifusión, responde a las consultas PING y SNMP enviadas a la dirección del grupo.

Sintaxis:

jo**in** *dirección-grupo-multidifusión*

Ejemplo: `join 224.185.0.0`

Leave

Utilice el mandato **leave** para eliminar un miembro del direccionador que se encuentre en un grupo multidifusión. Se evitará de esta forma que el direccionador responda a las consultas PING y SNMP enviadas a la dirección del grupo.

Este mandato es parecido al mandato leave de supervisión de la configuración OSPF pero con dos diferencias:

- El efecto sobre el grupo es inmediato cuando los mandatos se dan desde el monitor (por ejemplo, no es necesario reiniciar/recargar).
- El mandato no eliminará el miembro de un grupo hasta que el número de “leaves” ejecutados iguale al número de “joins” previamente ejecutados. Los grupos multidifusión IP unidos mediante la supervisión OSPF no se conservan a lo largo de las recargas y reinicios del direccionador.

Sintaxis:

le**ave** *dirección-grupo-multidifusión*

Ejemplo: `leave 224.185.0.0`

Mcache

Utilice el mandato **mcache** para mostrar una lista de las entradas de antememoria multidifusión activas actualmente. Las entradas de antememoria multidifusión se crean a petición, siempre que se reciba el primer datagrama multidifusión coincidente. No existe una entrada de antememoria distinta (y, por lo tanto, una ruta distinta) para cada combinación de grupo de destino y red de origen de datagramas.

Las entradas de antememoria se borran cuando se producen cambios topológicos (por ejemplo, se activa o se desactiva una línea punto a punto del sistema MOSPF) y cambios de pertenencia a grupo.

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 Subred/red de origen de datagramas coincidentes.

Destination Grupo de destino de los datagramas coincidentes.

Count Muestra el número de datagramas recibidos que han coincidido con la entrada de antememoria.

Upst Muestra el direccionador/red vecino/a desde el/la que los datagramas se deben recibir para ser reenviados. Cuando el valor es “none”, los datagramas no se reenviarán nunca.

Downstream Muestra el número total de vecinos/interfaces descendentes a los que se reenviará el datagrama. Cuando el valor es 0, el datagrama no se reenviará.

Existe más información en una entrada de antememoria de reenvío multidifusión. Una entrada de antememoria se puede visualizar al detalle proporcionando el origen y el destino del datagrama coincidente en la línea de mandatos. Si la entrada de antememoria coincidente no se encuentra, se crea una. En el ejemplo 2 se muestra 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 mostrada en el formato abreviado del mandato mcache, aparecen los siguientes campos:

Upstream Type Indica el tipo de nodo desde el que se debe recibir el datagrama para que sea reenviado. Los valores posibles de este campo son “none” (que indica que el datagrama no se reenviará), “router” (que indica que el datagrama se recibirá a través de una conexión punto a punto), “transit network,” “stub network” y “external” (que indica que se espera que el datagrama proceda de otro sistema autónomo).

Downstream Imprime una línea distinta en cada interfaz o vecino al que se envía el datagrama. Se proporciona también un valor TTL que indica que los datagramas reenviados fuera de la interfaz o a la interfaz deben tener especificado al menos el valor TTL de su cabecera IP. Cuando el propio direccionador es miembro de un grupo multidifusión, aparece una línea en

la que se especifica “internal Application” como uno de los vecinos/interfaces descendentes.

Mgroups

Utilice el mandato **mgroups** para mostrar los miembros de grupos de las interfaces conectadas del direccionador. Sólo aparecen los miembros de grupo de interfaces en las que el direccionador esté designado o 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 de grupo tal y como se ha anunciado (a través de IGMP) en una interfaz.

Interface Muestra la dirección de la interfaz en la que se ha anunciado la dirección de grupo (a través de IGMP).

Los miembros de grupo interno del direccionador se indican mediante el valor “internal.” En estas entradas, el campo tiempo de vida (véase más arriba) indica el número de aplicaciones que han solicitado ser miembro de un determinado grupo.

Lifetime Muestra el número de segundos durante los que la entrada persiste si un grupo determinado deja de oír los informes de miembros en la interfaz.

Mstats

Utilice el mandato **mstats** para mostrar diferentes estadísticas de direccionamiento multidifusión. El mandato indica si el direccionamiento multidifusión se habilita y si el direccionador es un reenviador multidifusión entre reenviadores multidifusión de AS y/o entre áreas.

Sintaxis:

ms**tats**

Ejemplo:

```
mstats

              MOSPF forwarding:       Disabled
              Inter-area forwarding:  Disabled
              DVMRP forwarding:       Enabled
              PIM forwarding:         Disabled

Datagrams received:           10143  Datagrams fwd (multicast):  10219
Datagrams fwd (unicast):          0  Locally delivered:              0
Unreachable source:               0  Unallocated cache entries:      0
Off multicast tree:               0  Unexpected DL multicast:   0
Buffer alloc failure:             0  TTL scoping:               0
Administrative filtering:       235

# DVMRP routing entries:          5  # DVMRP entries freed:          0
# fwd cache alloc:                1  # fwd cache freed:              0
# fwd cache GC:                   0  # local group DB alloc:         0
# local group DB free:            0
```

MOSPF forwarding Muestra si el direccionador reenviará datagramas multidifusión IP.

Inter-area forwarding Muestra si el direccionador reenviará datagramas multidifusión IP entre áreas.

DVMRP forwarding Muestra si el direccionador está configurado para utilizar DVMRP para direccionamiento multidifusión.

Datagrams received Muestra el número de datagramas multidifusión recibidos por el direccionador (en este total no se incluyen los datagramas cuyo grupo de destino está en el rango que va del valor 224.0.0.1 al 224.0.0.255).

Datagrams (ext source) Muestra el número de datagramas recibidos cuyo origen está fuera del sistema autónomo (AS).

Datagrams fwd (multicast) Muestra el número de datagramas que se han reenviado como difusiones múltiples del enlace de datos (esto incluye réplicas de paquetes, llegado el caso, y por lo tanto el recuento puede ser mayor que el número de paquetes recibidos).

Datagrams fwd (unicast) Muestra el número de datagramas reenviados como difusiones únicas del enlace de datos.

Locally delivered Muestra el número de datagramas reenviados a las aplicaciones internas.

No matching rcv interface Muestra el número total de datagramas recibidos por un reenviador multidifusión que no esté entre AS en una interfaz que no sea MOSPF.

Unreachable source Muestra el número total de datagramas a cuya dirección de origen no se ha podido acceder.

Unallocated cache entries Muestra el número total de datagramas cuyas entradas de antememoria no se han podido crear debido a una falta de recursos.

Off multicast tree Muestra el número total de aquellos datagramas que no se han reenviado porque no existía vecino ascendente o vecinos/interfaces descendentes en la entrada de antememoria coincidente.

Unexpected DL multicast Muestra el total de datagramas recibidos como difusiones múltiples del enlace de datos en aquellas interfaces que se han configurado para la unidifusión del enlace de datos.

Buffer alloc failure Muestra el total de datagramas a los que no se pudo dar réplica debido a una falta de almacenamiento intermedio.

TTL scoping Indica los datagramas que no se han reenviado porque su TTL indicaba que nunca alcanzarían un miembro de grupo.

Administrative filtering. Visualiza el número de datagramas descartados a causa del filtrado de salida.

DVMRP routing entries Muestra el número de entradas de direccionamiento DVMRP.

DVMRP entries freed Indica el número de entradas DVMRP liberadas. 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 de la antememoria de reenvío actual es el número de entradas asignadas (“# fwd cache alloc”) menos el número de entradas de antememoria liberadas (“# fwd cache freed”).

 # fwd cache freed Indica el número de entradas de antememoria liberadas. El tamaño de la antememoria de reenvío actual es el número de entradas asignadas (“# fwd cache alloc”) menos el número de entradas de antememoria liberadas (“# fwd cache freed”).

 # fwd cache GC Indica el número de entradas de antememoria borradas debido a que no se han utilizado recientemente y la antememoria se ha desbordado.

 # local group DB alloc Indica el número de entradas de la base de datos del grupo local asignadas. El número asignado (“# local group DB alloc”) menos el número liberado (“ # local group DB free”) da lugar al tamaño actual de la base de datos del grupo local.

 # local group DB free Indica el número de entradas de la base de datos del grupo local liberadas. El número asignado (“# local group DB alloc”) menos el número liberado (“ # local group DB free”) da lugar al tamaño actual de la base de datos del grupo local.

El número de coincidencias de la antememoria se puede calcular de la siguiente forma: número de datagramas recibidos (“Datagrams received”) menos el total de datagramas descartados por razones de “No matching rcv interface,” “Unreachable source” y “Unallocated cache entries” menos “# local group DB alloc.” El número de pérdidas de la antememoria es “# local group DB alloc”+.

Neighbor

Utilice el mandato **neighbor** para mostrar las estadísticas y parámetros relacionados con los vecinos OSPF. Si no se proporcionan argumentos (véase el ejemplo 1), se imprime una sola línea que resume cada interfaz. Si se proporciona una dirección IP del vecino (véase ejemplo 2), aparecerán las estadísticas detalladas del vecino.

Sintaxis:

n**eighbor**

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 de vecino.

Neighbor ID Muestra el ID de direccionador OSPF del vecino.

Neighbor State Puede ser uno de los siguientes: 1 (Down), 2 (Attempt), 4 (Init), 8 (2-Way), 16 (ExStart), 32 (Exchange), 64 (Loading) o 128 (Full).

LSrxl Muestra el tamaño de la lista de retransmisión de estado de enlace actual del vecino.

DBsum Muestra el tamaño de la lista de resumen de base de datos que estáa la espera de ser enviada al vecino.

LSreq Muestra el número de anuncios más recientes solicitados al vecino.

Ifc Muestra la interfaz compartida por el direccionador y el vecino.

Ejemplo 2: `neighbor 128.185.138.39`

El significado de la mayoría de los siguientes campos se proporciona en el apartado 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 de vecino.

OSPF router ID ID de direccionador OSPF del vecino.

Neighbor State Puede ser uno de los siguientes: 1 (Down), 2 (Attempt), 4 (Init), 8 (2-Way), 16 (ExStart), 32 (Exchange), 64 (Loading) o 128 (Full).

Physical interface Muestra el número y el tipo de la interfaz física de la red que comparten el direccionador y el vecino.

DR choice, backup choice, DR priority Indica los valores observables en el último mensaje Hello recibido del vecino.

Nbr options Indica las posibilidades OSPF opcionales soportadas por el vecino. Estas posibilidades están indicadas por E (procesa externos tipo 5; cuando esta opción no está establecida el área a la que pertenece la red común se habrá configurado como apéndice), T (puede direccionar rutas basadas en TOS) y MC (puede reenviar datagramas multidifusión IP). Este campo es sólo válido para aquellos vecinos en el estado Exchng o superiores.

Alternate TOS 0 cost En interfaces punto a multipunto, indica un coste alternativo TOS 0 para el vecino. En el LSA tipo 1 (enlaces de direccionador) del direccionador, se anunciará este coste en lugar del coste TOS 0 de la interfaz.

DBsumm qlen Indica el número de anuncios que esperan resumirse en los paquetes Database Description. Debe ser cero salvo cuando el vecino está en el estado Exchange.

LS rxmt qlen Indica el número de anuncios con los que se ha inundado el vecino, pero de los que todavía no hay acuse de recibo.

LS req qlen Indica el número de anuncios que se solicitan al vecino cuyo estado es Loading.

Last hello Indica el número de segundos transcurridos desde que se recibió un mensaje Hello procedente del vecino.

 # LS rxmits Indica el número de retransmisiones producidas durante la inundación.

 # direct acks Indica las respuestas a anuncios de estado de enlace duplicados.

 # Dup LS rcvd Indica el número de retransmisiones duplicadas que se han producido durante la inundación.

 # Old LS rcvd Indica el número de anuncios antiguos recibidos durante la inundación.

 # Dup acks rcvd Indica el número de acuses de recibo duplicados recibidos.

 # Nbr losses Indica el número de veces que el vecino ha pasado al estado Down.

 # Adj. resets Cuenta las entradas en el estado ExStart.

Ping

Consulte “Ping” en la página 350 para obtener una explicación del mandato **Ping**.

Policy

Utilice el mandato OSPF **policy** para mostrar la política de importación de rutas limítrofes de AS OSPF del direccionador.

Sintaxis:

policy

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 OSPF **reset** para modificar dinámicamente la configuración del direccionamiento OSP sin necesidad de reiniciar el direccionador. Para obtener más información, consulte “Cambio dinámico de los parámetros de configuración de OSPF” en la página 381.

Nota: Durante el reinicio, las rutas OSPF permanecerán retenidas 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 “Traceroute” en la página 355 para obtener una explicación del mandato **Traceroute**.

Routers

Utilice el mandato **routers** para mostrar todas las rutas del direccionador que han sido calculadas por OSPF y que no se encuentran 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 limítrofe de AS
- **ABR** Indica que el destino es un direccionador limítrofe de área
- **Fadd** Indica que se trata de una dirección de reenvío (para rutas externas)

RType Indica el tipo de ruta y la forma en que la misma se ha derivado:

- **SPF** indica que la ruta es una ruta que se encuentra dentro del área (procede del cálculo Dijkstra)
- **SPIA** indica que se trata de una área entre rutas (procede de tener en cuenta los anuncios de enlace de resumen).

Destination ID OSPF del direccionador de destino. Para entradas tipo D, aparece una de las direcciones IP del direccionador (que corresponde a un direccionador de otro sistema autónomo).

Area Muestra el área de AS a la que pertenece.

Cost Muestra el coste de ruta.

Next hop Dirección del siguiente direccionador situado en la vía de acceso que lleva al sistema principal de destino. Un número entre paréntesis al final de la columna indica el número de rutas de igual coste conectadas al destino.

Size

Utilice el mandato **size** para mostrar el número de LSA que se encuentran actualmente en la base de datos de estado de enlace, categorizados según el 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 mostrar las estadísticas generadas por el protocolo de direccionamiento OSPF. Las estadísticas señalan si la implementación se ha realizado de manera correcta, incluidas la utilización de la memoria y de la red. Muchos de los campos mostrados sirven para confirmar la configuración 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 Visualiza el ID OSPF del direccionador.

External comparison Muestra el tipo de ruta externa utilizada por el direccionador al importar rutas externas.

RFC 1583 compatibility Indica si el cálculo de ruta externa AS OSPF es compatible o no con el documento RFC 1583.

Import external routes Muestra las rutas externas que se importarán. Si se ha configurado una política de importación de filtros de rutas para el direccionamiento limítrofe de AS, aparecerá dicha política.

Orig default route Muestra si el direccionador anunciará una ruta por omisión OSPF. Si el valor es “Yes” y aparece un número distinto a cero entre paréntesis, se anunciará una ruta por omisión en caso de que exista una ruta a la red.

Default route cost Muestra el coste y el tipo de la ruta por omisión (en caso de anunciarse).

Default forward addr Muestra la dirección de reenvío especificada en la ruta por omisión (en caso de anunciarse).

Attached areas Indica el número de áreas con las que el direccionador tiene interfaces activas.

Estimated heap usage Indicación aproximada del tamaño de la base de datos de estado de enlace OSPF (en bytes).

Transit nodes Nodos asignados para almacenar anuncios de enlace de red y de enlace de direccionador.

LS adv. Asignados para almacenar anuncios de enlace externo de AS y de enlace de resumen.

Queue headers Forma listas de anuncios de estado de enlace. Estas listas se utilizan en los procesos de intercambio de base de datos y de inundación; si el número de cabeceras de cola asignadas no es igual al número de cabeceras de cola liberadas, significa que la sincronización de base de datos con algunos vecinos está todavía en proceso.

 # Dijkstra runs Indica las veces que se ha calculado desde cero la tabla de direccionamiento OSPF.

Maximum LSA size LSA de mayor tamaño que puede producir el direccionador. Se trata del menor valor configurado mediante la configuración OSPF y del máximo tamaño de paquete calculado o configurado mediante la configuración general.

Incremental summ updates, incremental VL updates Indica que los nuevos anuncios de enlace de resumen han provocado la reconstrucción parcial de la tabla de direccionamiento.

Buffer alloc failures. Indica los errores que hay en la asignación de almacenamiento intermedio. El sistema OSPF se recuperará de la falta temporal de almacenamiento intermedio de paquetes.

Multicast pkts sent Abarca los paquetes Hello OSPF y los paquetes enviados durante el proceso de inundación.

Unicast pkts sent Abarca las retransmisiones de paquete OSPF y el procedimiento de intercambio de base de datos.

LS adv. aged out Cuenta el número de anuncios que alcanzan los 60 minutos. Los anuncios de estado de enlace no vencen hasta pasados 60 minutos. Normalmente se renuevan antes de que pase este tiempo.

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 se han formado de manera incorrecta y que no se pueden interpretar.

Incremental ext. updates. Muestra el número de cambios acontecidos 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 aleatoria inicial máxima para los LSA autoproducidos.

LSA MINARRIVAL Rejects Muestra el número de LSA rechazados por recibir una instancia nueva en menos de un MINARRIVAL (1 segundo).

External LSA database: Proporciona información sobre la base de datos de LSA:

Current state Informa sobre si la base de datos de LSA externos de AS actuales está en estado normal o de sobrecarga.

Number of LSA Número de LSA externos que se encuentran actualmente en la base de datos

Number of overflows Número de veces que la base de datos de LSA externos de AS ha especificado el estado de sobrecarga.

Weight

Utilice el mandato **weight** para cambiar el coste de uno de las interfaces OSPF de los direccionadores. El nuevo coste es inmediatamente invadido fuera del dominio de direccionamiento OSPF, haciendo que las rutas se actualicen de la forma adecuada.

El coste de la interfaz volverá a ser el coste configurado si el direccionador se reinicia o se recarga. Para hacer que el coste cambie continuamente, debe volver a configurar la interfaz OSPF adecuada una vez invocado el mandato weight. Este mandato creará un nuevo anuncio de los enlaces del direccionador a menos que el coste de la interfaz no cambie.

Sintaxis:

w**eight** *ip-interface-address new-cost*

Ejemplo: `weight 128.185.124.22 2`

Soporte de reconfiguración dinámica de OSPF

En este apartado se describe el modo en que la reconfiguración dinámica (DR) afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

OSPF da soporte al mandato **delete interface** de CONFIG (Talk 6) sin restricciones.

Mandato activate interface de GWCON (Talk 5)

OSPF da soporte al mandato **activate interface** de GWCON (Talk 5) con la matización siguiente:

> Si OSPF no estaba en ejecución antes, pero se ha configurado ahora, es necesario rearrancar para habilitarlo y activar la nueva interfaz.

Todos los mandatos específicos de interfaz OSPF están soportados por el mandato **activate interface** de GWCON (Talk 5).

Mandato reset interface de GWCON (Talk 5)

OSPF da soporte al mandato **reset interface** de GWCON (Talk 5) con las matizaciones siguientes:

- Si OSPF no estaba en ejecución antes, pero se ha configurado ahora, es necesario rearrancar para habilitarlo y activar la nueva interfaz.
- Es posible que el 2212 intente asignar memoria.

Todos los mandatos específicos de interfaz OSPF están soportados por el mandato **reset interface** de GWCON (Talk 5).

Mandatos de restablecimiento de componente de GWCON (Talk 5)

OSPF da soporte a los mandatos **reset** de GWCON (Talk 5) específicos de OSPF siguientes:

Mandato GWCON, protocol ospf, reset ospf

Descripción: Relee SRAM y reinicializa OSPF.

Efecto en la red: Si se habilita o inhabilita el soporte de multidifusión o el soporte de circuito de petición, o bien si se cambia el ID de direccionador, de reiniciará OSPF. Se perderán todas las adyacencias.

Limitación:

Si la memoria de almacenamiento dinámico que se precisa es más de la que hay disponible, debido a la existencia de un número elevado de rutas o direccionadores, debe reiniciarse el direccionador.

Todos los mandatos OSPF están soportados por el mandato **GWCON, protocol ospf, reset ospf**.

Mandato GWCON, protocol ip, reset ip

Descripción: Relee SRAM y reinicializa OSPF.

Efecto en la red: Si se habilita o inhabilita el soporte de multidifusión o el soporte de circuito de petición, o bien si se cambia el ID de direccionador, de reiniciará OSPF. Se perderán todas las adyacencias.

Limitación:

Si la memoria de almacenamiento dinámico que se precisa es más de la que hay disponible, debido a la existencia de un número elevado de rutas o direccionadores, debe reiniciarse el direccionador.

Todos los mandatos OSPF están soportados por el mandato **GWCON, protocol ip, reset ip**.

Mandatos de cambio temporal de GWCON (Talk 5)

OSPF da soporte a los mandatos de GWCON que cambian de forma temporal el estado operativo del dispositivo indicados más abajo. Los cambios se pierden cada vez que se vuelve a cargar o iniciar el dispositivo o que se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
GWCON, protocol ospf, weight
GWCON, protocol ospf, join
GWCON, protocol ospf, leave

Utilización de BGP4

En este capítulo se describe cómo utilizar el protocolo BGP (Border Gateway Protocol) con los mandatos de configuración de BGP.

Este capítulo consta de los siguientes apartados:

Visión general del protocolo BGP

BGP es un protocolo de direccionamiento de pasarela exterior utilizado para intercambiar información de accesibilidad a la red entre sistemas autónomos. Un AS es básicamente una colección de direccionadores y nodos finales que operan bajo una única organización administrativa. Dentro de cada AS, los direccionadores y los nodos finales comparten información de direccionamiento a través de un protocolo de pasarela interior. El protocolo de pasarela interior puede ser tanto RIP como OSPF.

BGP se estableció en Internet en el intercambio libre sobre información de direccionamiento entre sistemas autónomos. Basado en CIDR (Classless Inter-Domain Routing), BGP ha evolucionado para dar soporte a la agregación y reducción de información sobre direccionamiento.

Básicamente, CIDR es una estrategia diseñada para solucionar los siguientes problemas:

- El agotamiento del espacio de direcciones de clase B
- El crecimiento de la tabla de direccionamiento

CIDR elimina el concepto de clases de direcciones y proporciona un método para resumir varias rutas *n* en una única ruta. Esto reduce de manera significativa la cantidad de información de direccionamiento que los direccionadores BGP deben almacenar e intercambiar.

Nota: IBM sólo da soporte a la última versión de BGP, esto es, BGP4, definido en el documento RFC 1654. Todas las alusiones a BGP hechas en este capítulo y en la interfaz de los direccionadores de IBM, se refieren a BGP4 y no son aplicables a versiones anteriores de BGP.

Cómo funciona BGP4

BGP es un protocolo de direccionamiento de sistemas interautónomos. Los direccionadores BGP, fundamentalmente, reúnen y anuncian de manera selectiva información de accesibilidad desde y para vecinos BGP de su propio sistema y de otros sistemas autónomos. La información de accesibilidad consta de las secuencias de números AS que forman las vías de acceso a determinados emisores BGP y de la lista de redes IP a las que se puede acceder mediante cada vía de acceso anunciada. Un AS es un grupo administrativo de redes y direccionadores que com-

parten información de accesibilidad a través de uno o más protocolos de pasarela interior (IGP), caso de RIP o OSPF.

Los direccionadores que ejecutan BGP se denominan emisores BGP. Estos direccionadores funcionan como servidores respecto de sus vecinos BGP (clientes). Cada direccionador BGP abre una conexión TCP pasiva en el puerto 179, y está a la escucha de las conexiones procedentes de los vecinos en esta conocida dirección. El dirección también abre conexiones TCP activas para vecinos BGP habilitados. Esta conexión TCP permite que los direccionadores BGP compartan y actualicen la información de accesibilidad con vecinos de los mismos o de otros sistemas autónomos.

Las conexiones entre emisores BGP del mismo AS se denominan conexiones BGP internas (IBGP), mientras que las conexiones entre emisores BGP de diferentes sistemas autónomos se denominan conexiones BGP externas (EBGP).

Un AS único puede tener uno o varias conexiones BGP para sistemas autónomos externos. En la Figura 34 se muestran dos sistemas autónomos. El emisor BGP de AS1 trata de establecer una conexión TCP con su vecino de AS2. Una vez establecida la conexión, los direccionadores podrán compartir la información de accesibilidad.

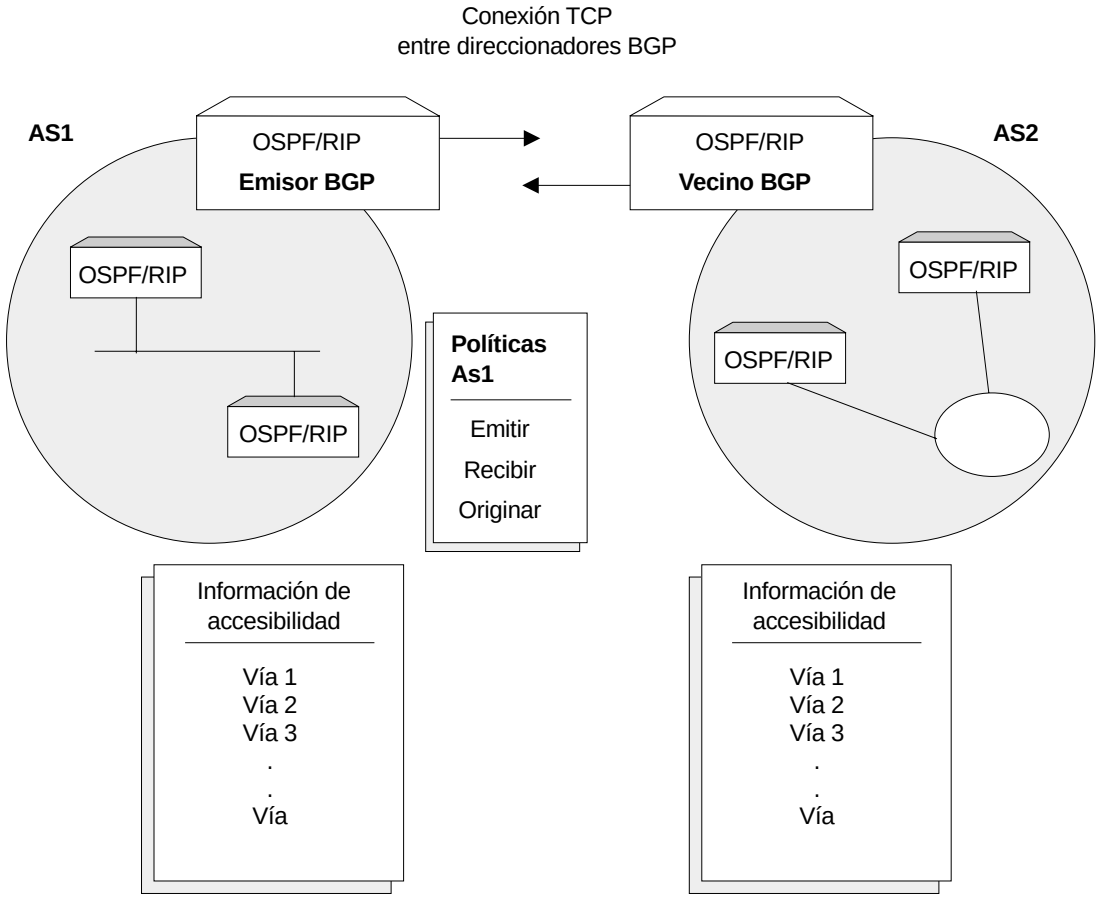


Figura 34. Conexiones BGP entre dos sistemas autónomos. Una vez el emisor BGP de AS1 ha establecido una conexión TCP con su vecino en el AS2, los dos direccionadores podrán, de manera selectiva, intercambiar información de accesibilidad. La información que los direccionadores envían o aceptan está determinada por políticas definidas para cada uno de ellos.

Aunque los sistemas autónomos mostrados en la Figura 34 sólo tienen un direccionador BGP, cada uno podría tener varias conexiones a otros sistemas autónomos. Como ejemplo de esto, en la Figura 35 en la página 437 se muestran tres sistemas autónomos interconectados. El AS1 tiene tres conexiones BGP en sistemas autónomos externos: una en el AS2, otra en el AS3 y otra en el ASx. Igualmente, el AS3 tiene conexiones en el AS1, el AS2 y el ASy.

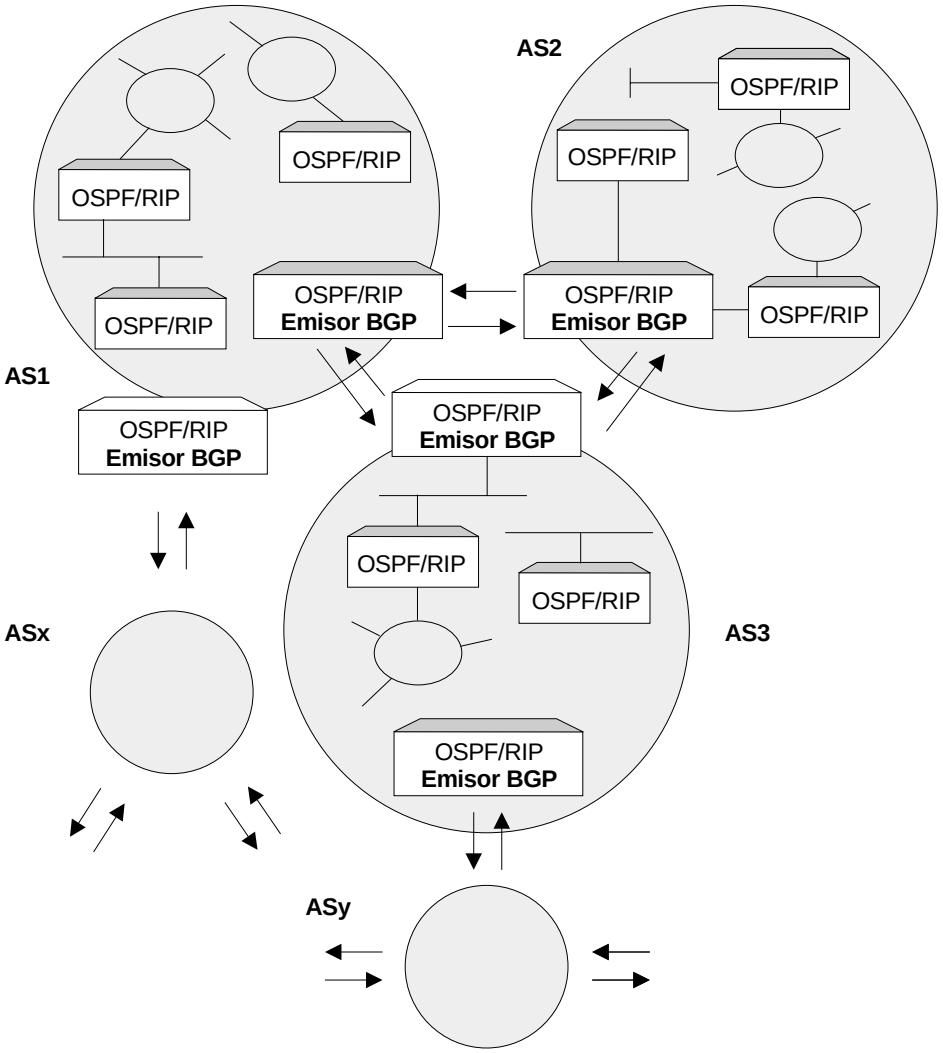


Figura 35. Conexiones BGP entre tres sistemas autónomos. Observe que el AS1 y el AS3 tienen dos emisores BGP.

Una vez establecida una conexión TCP, el emisor BGP mostrado en la Figura 34 en la página 436 podrá enviar su tabla completa de direccionamiento a su vecino BGP en el AS2. No obstante, por razones de seguridad, entre otras, no es aconsejable enviar información de accesibilidad de las reces al AS2. Por lo mismo, no es aconsejable que el AS2 reciba información de accesibilidad de cada red de AS1.

Políticas de origen, envío y recepción

Las decisiones sobre qué información de accesibilidad se anuncia (envía) y qué información de accesibilidad se acepta (recibe) se realizan según las sentencias de la política explícitamente definida para ello. La implementación de BGP de IBM da soporte a tres tipos de sentencias de política:

- Políticas de origen
- Políticas de envío: hay dos tipos de políticas de envío.
  - Las políticas de envío basadas en AS sólo se aplican a un AS determinado o a todos los AS. Si no se configuran políticas de envío, la dirección de destino se desactiva.
  - Las políticas de envío basadas en vecino sólo se aplican a un vecino o vecinos determinados. Si no se han configurado políticas de envío basadas en vecino, se aplicarán las políticas de envío basadas en AS. Si se configura una política de envío basada en el vecino, no se tendrá en cuenta la política de envío basada en el AS.

  Cada sentencia de una política de envío contiene el clasificador de anuncio de la red de destino y un conjunto de acciones asociadas.

  La clasificación de la red de destino se basa en lo siguiente:

  - Red de destino exacta
  - Rango de las redes de destino
  - Número de AS de origen
  - Cualquier número de AS encontrado en el atributo de la vía de acceso al AS

  Las acciones posibles son:

  - Excluir una red de destino de anuncio
  - Incluir una red de destino para anuncio en un AS determinado o en todos los AS (mediante política basada en el AS) o a un vecino determinado (mediante política basada en el vecino)
  - Establecer el valor MED
  - Rellenar la vía de acceso de AS

  Nota: El MED y la vía de acceso de AS sólo sirven en políticas basadas en vecino.

  El valor del atributo MED da indicaciones a los vecinos BGP externos sobre su preferencia de ruta. Se prefieren las rutas con el valor del atributo MED más bajo. Consulte “Proceso de preferencia de ruta” en la página 444 para obtener más información.
- El relleno de la vía de acceso del AS permite añadir números de AS local varias veces (de 1 a 10) a la vía de acceso del AS de la ruta BGP. Se prefiere la ruta con la vía de acceso de AS más baja. Consulte “Proceso de preferencia de ruta” en la página 444 para obtener más información.
- Políticas de recepción: hay dos tipos de políticas de recepción.
  - Las políticas de recepción basadas en AS sólo se aplican a un AS determinado o a todos los AS. Si no se configuran políticas de recepción, la dirección de destino se desactiva.

- Las políticas de recepción basadas en vecino sólo se aplican a un vecino o vecinos determinados. Si no se han configurado políticas de recepción basadas en vecino, se aplicarán las políticas de recepción basadas en AS. Si se han configurado políticas de recepción basadas en vecino, las políticas de recepción basadas en AS no se tendrán en cuenta.

Cada sentencia de una política de recepción contiene el clasificador de anuncio de la red de destino y un conjunto de acciones asociadas.

La clasificación de la red de destino se basa en lo siguiente:

- Red de destino exacta
- Rango de las redes de destino
- Número de AS de origen
- Cualquier número de AS encontrado en el atributo de la vía de acceso al AS

Las acciones posibles son:

- Excluir la red de destino
- Incluir una red de destino de un AS específico o de todos los AS (mediante política basada en el AS) o de un vecino específico (mediante política basada en el vecino)
- Restablecer el valor MED
- Establecer el valor de peso
- Establecer el valor de la métrica IGP
- Establecer el valor de las preferencias locales.

Nota: El MED, el peso y las preferencias locales sólo sirven en políticas basadas en vecino.

El valor de peso sugiere a los direccionadores BGP locales que seleccionen la ruta tomando como base el valor de peso más alto y pasa por alto el algoritmo de preferencia de ruta.

Mensajes BGP

Los direccionadores BGP utilizan cuatro tipos de mensajes para comunicarse con sus vecinos: los mensajes OPEN, KEEP ALIVE, UPDATE y NOTIFICATION.

OPEN

Son los primeros mensajes transmitidos al activarse el enlace con un vecino BGP y establecerse la conexión.

KEEP ALIVE

Los direccionadores BGP los utilizan para informarse unos a otros de que una determinada conexión está activa y funciona.

UPDATE
Contienen la información de la tabla de direccionamiento interior. Los emisores BGP envían mensajes de actualización sólo cuando se produce un cambio en sus tablas de direccionamiento.

NOTIFICATION
Son mensajes que se envían en caso de que un emisor BGP detecte una condición que lo fuerce a terminar una conexión existente. Estos mensajes se anuncian antes de que se transmita la conexión.

Configuración de BGP4
La configuración de BGP comporta tres pasos básicos:

1. "Habilitación de BGP".

   La habilitación de BGP requiere la especificación del número de AS único del direccionador BGP. Los números de AS los asigna el Centro de información de redes del instituto de investigación de Stanford (Stanford Research Institute Network Information Center).

2. "Definición de los vecinos BGP".

   Los vecinos BGP son direccionadores BGP con los que un emisor BGP establece una conexión TCP. Una vez definidos los vecinos, las conexiones con ellos se establecen por omisión.

3. "Adición de políticas" en la página 441.

   Las *políticas* establecidas determinan los direccionadores que el emisor BGP exportará y aquellos que importará. Puede configurar políticas con distintos objetivos. Consulte "Definiciones de política de ejemplo" en la página 441 para obtener más información.

Habilitación de BGP
Para habilitar BGP, utilice el mandato **enable BGP speaker** tal y como se muestra en el ejemplo:

```
BGP Config> enable BGP speaker
AS [0]? 167
TCP segment size [1024]?
```

El *número de AS* debe encontrarse en el rango de 1 a 65535. El tamaño del *segmento TCP* debe estar en el rango de 1 a 65535. El valor por omisión del *segmento TCP* es 1024. Este número representa el máximo tamaño de segmento que utilizará BGP en conexiones TCP pasivas.

Después de emitir el mandato **enable bgp**, debe rearrancar el dispositivo para habilitar BGP.

Definición de los vecinos BGP
Una vez habilitado un emisor BGP, debe definir a sus vecinos. Los vecinos BGP pueden ser internos o externos. Los vecinos internos se encuentran en el mismo AS y no necesitan tener conexión directa uno con otro. Los vecinos externos están en sistemas autónomos diferentes. Deben tener una conexión directa uno con otro.

Para definir vecinos BGP externos o internos, utilice el mandato **add neighbor**. Debe especificar la dirección IP del vecino y asignar un número de AS al vecino tal

y como se muestra a continuación. Los vecinos internos deben tener el mismo número de AS que el emisor 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 al vecino BGP especificado, basado en los parámetros de configuración del vecino de la memoria de configuración.

Adición de políticas

La implementación de BGP de IBM da soporte a tres mandatos de política:

- *Originate Policy*. Permite seleccionar las redes de protocolo de pasarela interior que desea exportar.
- *Receive Policy*. Permite seleccionar la información de la ruta que se desea importar de los iguales BGP.
- *Send Policy*. Permite seleccionar la información de la ruta que se desea exportar a los iguales. Observe que la información de la ruta exportable puede incluir información procedente de sistemas autónomos vecinos, así como las rutas que se originaron en el IGP.

Si añade o modifica una política basada en el vecino, utilice el mandato **reset neighbor** para activar la política del vecino. Si añade o modifica una política basada en el AS, debe rearrancar el dispositivo.

Definiciones de política de ejemplo

En este apartado se proporciona un conjunto de ejemplos de algunas de las políticas específicas que puede configurar en un emisor BGP. Todas las políticas se definen con el mandato BGP **add**. Consulte “Add” en la página 448 para obtener la sintaxis del mandato **add**.

Ejemplos de política de origen

Incluir todas las rutas para anuncio

En este ejemplo se incluyen todas las rutas de la tabla de direccionamiento IGP del emisor BGP destinadas a anuncio. De este modo, puede ver este mandato como la sentencia de política de origen “por omisión” de BGP.

Observe que el mandato especifica un rango de direcciones, en lugar de una dirección única (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

En este ejemplo se especifica también un rango, pero en este caso el objetivo es evitar que el emisor BGP publique direcciones en este rango a sus vecinos.

En este ejemplo se excluyen todas las rutas del rango 194.10.16.0 al 194.10.31.255 de la tabla de direccionamiento IGP, que a su vez evita que aquellas se publiquen.

```
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 es la información RIP recibida. Puede seleccionar redes basadas en un valor de identificador determinado para su anuncio. Consulte la descripción del mandato **Set** en “Configuración y supervisión de IP” en la página 269 para obtener información sobre el establecimiento del valor del identificador.

Por omisión, sólo se seleccionarán para su anuncio las rutas con clase de la tabla de direccionamiento IGP del emisor BGP. Para seleccionar una ruta sin clase para su anuncio utilice el mandato bgp-subnets **patch**. Para obtener información spbre el mandato **patch**, consulte el tema Mandatos CONFIG del capítulo “El proceso y los mandatos CONFIG (CONFIG - Talk 6)” de la publicación *Access Integration Services Guía del usuario de software*.

Ejemplos de política de recepción basada en AS

Importar todas las rutas de todos los vecinos BGP

En este ejemplo se garantiza que el emisor BGP importará todas las rutas de todos sus vecinos a 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 métrico con el que las rutas aceptadas se importan a la tabla de direccionamiento IGP del emisor. Sólo se le solicita teclear un valor de la métrica IGP en caso de configurar una política de inclusión de ruta.

Si el valor *IGP-metric* es -1, las rutas se importarán al IGP; de esta forma, las rutas no se podrán volver a anunciar.

Bloquear rutas específicas de un AS de origen

En este ejemplo se evita que el emisor BGP importe cualquier ruta originada en el AS 168 del AS vecino 165. Debe utilizar este mandato si, por razones de seguridad, no desea que el emisor BGP reciba cualquier ruta del AS 168.

```
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
```

Bloquear vías de acceso AS específicas

En este ejemplo se evita que el emisor BGP importe cualquier ruta que tenga AS 175 en su lista de vías de acceso AS.

```
BGP Config> add no-receive
Enter AS: [0]? 175
```

Ejemplos de política de recepción basada en vecino

Importar todas las rutas de un vecino BGP específico con un peso establecido igual a 100

En este ejemplo se le permite importar todas las rutas del vecino BGP 192.0.190.178. Todas las rutas tendrán un valor de peso de 100 y un valor de métrica IGP de 1.

Defina el nombre de lista de política de la política de recepción.

```
BGP Config> add policy-list
Name[]?S1_100_r
Policy Type(Receive/Send)[Receive]?Receive
```

Adjunte el nombre de lista de la política de recepción definida al vecino específico.

```
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 las políticas de recepción con los mandatos **update** y **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 política de envío basada en vecino

Restringir un anuncio de ruta a un AS específico

En este ejemplo se restringe el emisor BGP. El emisor no puede anunciar rutas en el rango de dirección que va de 143.116.0.0 a 143.116.255.255, que se origina en el AS 165 y llega hasta el 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

En este ejemplo se garantiza que el emisor BGP anunciará todas las rutas originadas en su IGP y todas las rutas averiguadas de sus sistemas autónomos vecinos.

```
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 política de envío basada en vecino

Anunciar todas las rutas conocidas a un vecino específico con un valor del atributo MED igual a 100

En este ejemplo se le permite anunciar todas las rutas dirigidas a un vecino BGP 192.0.190.178. Todas las rutas anunciadas tienen un valor MED de 100.

Defina el nombre de lista de política de la política de envío.

```
BGP Config> add policy-list
Name[]?S1_100_s
Policy Type(Receive/Send)[Receive]?Send
```

Adjunte el nombre o nombres de lista de la política de envío definida al vecino específico.

```
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 del vecino con 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 ruta

Cuando el emisor BGP recibe una vía de acceso de un destino particular de su igual, BGP sigue el siguiente proceso para seleccionar la mejor vía de acceso posible:

- Aplica las políticas de recepción basadas en la configuración.
- Si las políticas de recepción permiten un destino, calcula entonces el grado de preferencia del destino recibido, basado en la la longitud más corta de la vía de acceso AS y el tipo de origen.
- Si hay varias rutas de acceso al mismo destino, ejecuta el proceso de selección de la vía de acceso. Selecciona la mejor vía de acceso posible mediante la comparación de la nueva vía de acceso con la mejor vía de acceso exis-

tente seleccionada.Si la nueva vía de acceso se selecciona como la mejor vía de acceso, instala la nueva vía de acceso en la tabla de reenvío IP.

- BGP anuncia la mejor vía de acceso seleccionada en sus iguales BGP externo e interno sujetos a las políticas de envío.

Proceso de selección de la vía de acceso

La mejor vía de acceso se selecciona según el siguiente orden:

- Prefiera la vía de acceso que ha originado este direccionador.
- Si no es este direccionador el que ha originado la vía de acceso, prefiera la vía de acceso configurada con el valor de peso más alto.
- Si las vías de acceso tienen el mismo valor de peso, prefiera la vía de acceso con el valor de preferencia local mayor.
- Si las vías de acceso tienen el mismo valor de preferencia local, prefiera la vía de acceso con el mayor grado de preferencia.
  - A la vía de acceso con la menor longitud de vía de acceso AS se le da el mayor grado de preferencia.
  - Si las vías de acceso tienen la misma longitud de vía de acceso de AS, el IGP del tipo de origen se prefiere al EGP e Incompleto.
- Si las vías de acceso tienen el mismo grado de preferencia, prefiera la vía de acceso con el valor del atributo MED más bajo.
- Si las vías de acceso tienen el mismo valor para el atributo MED, prefiera la ruta externa (EBGP) a la interna (IBGP).
- Si las vías de acceso todavía son iguales, prefiera la vía de acceso con el ID de BGP menor.

Configuración y supervisión de BGP4

En este capítulo se describen los mandatos de configuración y supervisión de BGP. Consta de los apartados siguientes:

Acceso al entorno de configuración de BGP4

Para acceder al entorno de configuración de BGP, escriba el siguiente mandato en el indicador `Config>`:

```
Config> Protocol BGP
BGP Config>
```

Mandatos de configuración de BGP4

En este apartado se describen los mandatos de configuración de BGP. Estos mandatos le permiten modificar el comportamiento del protocolo BGP ajustándolo a sus necesidades. Es necesario cierta configuración para producir un direccionador BGP completamente operativo. Escriba los mandatos de configuración de BGP en el indicador `BGP config>`.

Tabla 24. Resumen de los mandatos de configuración de BGP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Add	Añade políticas y vecinos BGP
Attach	Conecta la lista de las políticas de envío y recepción a un determinado vecino.
Change	Modifica la información especificada originalmente con el mandato **add**.
Delete	Suprime la información sobre la configuración BGP especificada con el mandato **add**.
Disable	Inhabilita determinadas funciones BGP activadas con el mandato **enable**.
Enable	Habilita los emisores BGP, los vecinos BGP o BGP sin clase.
List	Muestra los elementos de la configuración BGP.
Move	Cambia el orden en que se han definido las políticas y las agrupaciones.
Set	Establece el temporizador de exploración de la tabla de rutas IP.
Update	Manipula una política de un nombre de la lista de políticas configuradas con los mandatos del submenú **add**, **delete**, **change** y **move**.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Add

Utilice el mandato **add** para añadir información 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 emisor BGP agrupe un bloque de direcciones y anuncie una única ruta a sus vecinos BGP. Debe especificar el prefijo de la red común a todos los direccionadores agru-

pados y su máscara. El siguiente ejemplo ilustra la forma de agrupar un bloque de direcciones de 194.10.16.0 a 194.10.31.255.

1. *Prefijo-red* son las direcciones en cuestión. 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. *Máscara-red* es la dirección especificada en el prefijo de la 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
```

Cuando se añade una definición de agrupación, recuerde que debe definir una política para evitar que las rutas en agrupaciones se exporten. Si no hace esto, el direccionador anunciará las rutas individuales y la agrupación que ha definido. No ocurre lo mismo cuando agrupa las rutas, originadas desde su tabla de direccionamiento IGP.

neighbor *dirección-IP-vecino núm-as temp-inicializ temp-conexión temp-retención temp-keepalive tamaño-segmento-tcp*

Utilice el mandato **add neighbor** para definir un vecino BGP. El vecino puede ser interno al emisor BGP de AS o externo. Para activar este vecino dinámicamente, utilice el mandato **reset neighbor** del proceso de supervisión de BGP.

1. Dirección-IP-vecino es la dirección del vecino con el que desea igualarse. Puede estar dentro de su propio sistema autónomo o en otro. Si se trata de un vecino externo, ambos emisores BGP deben compartir la misma red. No existe tal restricción para los vecinos internos. La dirección tiene:

   Valores válidos: cualquier dirección IP válida
   Valor por omisión: ninguno

2. Núm-as es el número de su propio sistema autónomo en el caso de los vecinos internos o el número del sistema autónomo del vecino en el caso de los vecinos externos. El número de AS del vecino tiene:

   Valores válidos: un entero entre 0 - 65535
   Valor por omisión: ninguno

3. *Temp-inicializ* especifica el tiempo que el emisor BGP espera hasta inicializar los recursos y reinicializar la conexión de transporte con el vecino en caso de que el emisor, debido a un error, haya entrado anteriormente en estado IDLE. Si el error continúa, el temporizador se incrementará de forma exponencial.

   Valores válidos: de 0 a 65535 segundos.
   Valor por omisión: 12 segundos

4. *Temp-conexión* especifica el tiempo que el emisor BGP espera hasta reinicializar la conexión de transporte con su vecino, en caso de que la conexión TCP falle mientras está en estado CONNECT o ACTIVE. Entre tanto, el emisor BGP sigue estando a la escucha de cualquier conexión que el vecino pueda iniciar.

   Valores válidos: de 0 a 65535 segundos.
   Valor por omisión: 120 segundos

5. *Temp-retención* sirve para especificar la duración de tiempo que el emisor BGP esperará antes de dar por sentado que el vecino es inaccesible. Ambos vecinos intercambian la información configurada en mensajes OPEN y eligen como temporizador de retención negociado el más pequeño.

   Una vez establecida la conexión BGP entre los vecinos, éstos intercambian mensajes Keepalive en intervalos frecuentes para asegurarse de que la conexión sigue todavía activa y de que los vecinos son accesibles. El intervalo del temporizador de mensajes Keepalive se calcula de forma que sea la tercera parte 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 presente que en líneas conmutadas puede interesar que el valor del temporizador de retención sea 0 para ahorrar ancho de banda (ya que así no se enviarán mensajes Keepalive a intervalos frecuentes).

   Valores válidos: de 0 a 65535 segundos.
   Valor por omisión: 90 segundos

6. *Tamaño-segmento-tcp* especifica el tamaño máximo de los datos que se pueden intercambiar en la conexión TCP con un vecino. Este valor se utiliza para conexiones TCP activas con el vecino.

   Valores válidos: de 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 **add no-receive núm-as** para excluir vías de acceso AS si el número de AS particular aparece en cualquier sitio de la lista de vías de acceso AS.

Núm-as tiene:

Valores válidos: de 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*

MED

Exclusive Las políticas exclusivas evitan que la información de la ruta se incluya en la tabla de direccionamiento del emisor BGP.

Inclusive Las políticas inclusivas garantizan que la ruta especificada se incluirá en la tabla de direccionamiento del emisor BGP.

Prefijo-red Prefijo de la red para la dirección en cuestión.

Valores válidos: cualquier dirección IP válida
Valor por omisión: ninguno

Coincidencia-dirección Dirección, o rango de direcciones, que se verá afectada por la sentencia de política. Entre la *máscara-red* que debe aplicarse al a dirección especificada en Network Prefix para generar una dirección utilizada en una política BGP.

Valores válidos: cualquier dirección IP válida
Valor por omisión: ninguno

Identificador Valor establecido para un AS determinado. Todos los valores de los identificadores deben coincidir con los del AS del que se han averiguado.

Valores válidos: de 0 a 65535
Valor por omisión: ninguno

En este ejemplo se incluyen todas las rutas de la tabla de direccionamiento IGP del emisor BGP destinadas a anuncio.

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 “Ejemplos de política de origen” en la página 441 para obtener ejemplos detallados de este mandato.

policy-list

Utilice el mandato **add policy-list** para configurar un grupo de política que se pueda conectar a un vecino específico con 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 “Ejemplos de política de recepción basada en vecino” en la página 443 y “Ejemplos de política de envío basada en vecino” en la página 444 para obtener ejemplos detallados de este mandato.

receive-policy *(exclusive/ inclusive) prefijo-red máscara-red coincidencia-dirección núm-as-origen núm-as-adyacente métrica-igp (sólo inclusive)*

Utilice el mandato **add receive-policy** las rutas que se van a importar a la tabla de direccionamiento del emisor BGP.

Las políticas exclusivas evitan que la información de la ruta se incluya en la tabla de direccionamiento del emisor BGP.

1. *Prefijo-red* son las direcciones en cuestión.

   Valores válidos: cualquier dirección IP válida
   Valor por omisión: ninguno

2. *Máscara-red* es la dirección especificada en el prefijo de la red para generar una dirección utilizada en una política BGP.

   Valores válidos: cualquier máscara IP válida
   Valor por omisión: ninguno

3. *Coincidencia-dirección* es un rango de direcciones o una dirección exacta.

4. *Núm-as-origen* tiene:

   Valores válidos: de 0 a 65535
   Valor por omisión: ninguno

5. *Núm-as-adyacente* especifica el número del AS vecino.

   Valores válidos: de 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 “Ejemplos de política de recepción basada en AS” en la página 442 para obtener ejemplos detallados de este mandato.

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 las rutas del emisor BGP que se volverán a anunciar. Estas rutas pueden ser externas o internas al emisor BGP de AS.

Las políticas exclusivas evitan que la información de la ruta se incluya en la tabla de direccionamiento del emisor BGP.

1. *Prefijo-red* son las direcciones en cuestión.

   Valores válidos: cualquier dirección IP válida
   Valor por omisión: ninguno

2. *Máscara-red* es la dirección especificada en el prefijo de la red para generar una dirección utilizada en una política BGP.

   Valores válidos: cualquier dirección IP válida
   Valor por omisión: ninguno

3. *Coincidencia-dirección* es un rango de direcciones o una dirección exacta.
4. *Identificador* es el valor establecido para un AS determinado. Todos los valores de los identificadores deben coincidir con los del AS del que se han averiguado.

   Valores válidos: de 0 a 65535
   Valor por omisión: ninguno
5. *Núm-as-adyacente* especifica el número del AS vecino.

   Valores válidos: de 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 “Ejemplos de política de envío basada en vecino” en la página 443 para obtener ejemplos detallados de este mandato.

Attach

Utilice el mandato **attach policy-to-neighbor** para conectar un nombre de la lista de políticas configuradas a un vecino específico. Puede adjuntar hasta tres nombres de lista de políticas de envío y de recepción.

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 “Ejemplos de política de recepción basada en vecino” en la página 443 y “Ejemplos de política de envío basada en vecino” en la página 444 para obtener ejemplos detallados de este mandato.

Change

Utilice el mandato **change** para cambiar un elemento de la configuración BGP instalado anteriormente con el mandato add.

Sintaxis:

ch**ange**	aggregate . . .
	neighbor . . .
	originate-policy . . .
	policy-to-neighbor
	receive-policy . . .
	send-policy. . .

aggregate *núm-índice prefijo-red máscara-red*

En este ejemplo se cambia la agrupación actual (agrupación 1). El cambio hace que la agrupación 1 utilice un prefijo y una máscara de red diferentes para agrupar a todos los direccionadores del rango de dirección que va del valor 128.185.0.0 al 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-vecino núm-as temp-inicializ temp-conexión temp-retención temp-keepalive tamaño-segmento-tcp*

En el siguiente ejemplo se cambia el valor del temporizador de retención por cero para el vecino 192.0.251.165.

La *dirección-IP-vecino* que se va a modificar tiene:

Valores válidos: cualquier dirección IP válida
Valor por omisión: ninguno

Para volver a activar este vecino dinámicamente, utilice el mandato **reset neighbor** del proceso 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 alterar una definición de política de origen existente.

En este ejemplo se modifica la política de origen del emisor BGP. En lugar de excluir de la tabla de direccionamiento IGP a las redes con prefijo 194.10.16.0, la política incluirá ahora a 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 cambiar la conexión de una lista de política a un vecino determinado.

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-origen núm-as-adyacente métrica-igp (sólo inclusive)*

Utilice el mandato **change receive-policy** para alterar una definición de política de recepción existente.

En este ejemplo se añade una restricción a la política de recepción del emisor BGP. En lugar de importar información sobre la ruta desde cualquier igual BGP a su tabla de direccionamiento IGP, ahora se evitará que las rutas del AS 165 se importen.

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 núme-as-adyacente*
Utilice el mandato **change send-policy** para alterar una política de envía a otra que sea más inclusiva o más exclusiva.

En este ejemplo se añade una restricción a la política de envío del emisor BGP. La restricción garantiza que todas las rutas que se encuentran en el rango de dirección que va del valor 194.10.16.0 al 194.10.31.255 sean excluidas al anunciarlas 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 BGP instalado anteriormente con 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 de la agrupación que desea suprimir.

Ejemplo: `delete aggregate 1`

neighbor *dirección-IP-vecino*
Utilice este mandato para suprimir un vecino BGP. Debe especificar la dirección de la red del vecino.

La *dirección de red del vecino que va a suprimirse* tiene:

Valores válidos: cualquier dirección IP válida
Valor por omisión: ninguno

Para desactivar este vecino dinámicamente, utilice el mandato **reset neighbor** del proceso de supervisión de BGP.

Ejemplo: `delete neighbor 192.0.251.165`

no-receive *as*

Utilice este mandato para suprimir la política de no recepción configurada para un AS particular. Debe especificar el número AS.

Núm-as tiene:

Valores válidos: de 0 a 65535
Valor por omisión: ninguno

Ejemplo: `delete no-receive 168`

originate-policy *núm-índice*

Utilice este mandato para suprimir una política de origen determinada. Debe especificar el número de índice relacionado con la política.

Ejemplo: `delete originate-policy 2`

policy-list

Utilice el mandato **delete policy-list** para suprimir una lista de política.

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 política-a-vecino se ajustará en consecuencia.

policy-to-neighbor

Utilice el mandato **delete policy-to-neighbor** para suprimir la conexión de un nombre de la lista de políticas existente con un vecino determinado.

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 política de recepción específica. Debe especificar el número de índice relacionado con 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 política de envío específica. Debe especificar el número de índice relacionado con la política.

Ejemplo: `delete send-policy 4`

Disable

Utilice el mandato **disable** para desactivar un emisor o vecino BGP anteriormente habilitado. Observe que los vecinos están implícitamente habilitados siempre que se añadan 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 inhabilitar el protocolo BGP.

Ejemplo: `disable bgp speaker`

classless-bgp

Utilice este mandato para inhabilitar una ruta sin clase para anuncio.

Ejemplo: `disable classless-bgp`

Nota: Asegúrese de que el mandato **patch bgp-subnets** está inhabilitado.

compare-med-from-diff-AS

Utilice este mandato para inhabilitar una comparación MED entre sistemas autónomos distintos.

Ejemplo: `disable compare-med-from-diff-AS`

neighbor *dirección-IP-vecino*

Dirección-IP-vecino 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 la información, posibilidades y funciones BGP añadidas a la configuración 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 habilitar el protocolo BGP.

Nota: IBM sólo da soporte a la última versión de BGP, BGP4, que definida en el documento RFC 1654.

1. *Núm-AS* está asociado con este conjunto de direccionadores y nodos.

   Valores válidos: de 0 a 65535
   Valor por omisión: ninguno

2. *Tamaño-segemento-tcp* sirve para especificar el tamaño de segmento máximo que BGP debe utilizar en conexiones TCP pasivas.

   Valores válidos: de 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 habilitar una ruta sin clase para anuncio.

Ejemplo: **`enable classless-bgp`**

compare-med-from-diff-AS

Utilice este mandato para habilitar la comparación MED entre sistemas autónomos distintos.

Ejemplo: **`enable compare-med-from-diff-AS`**

neighbor *dirección-IP-vecino*

Utilice este mandato para habilitar un vecino BGP.

Dirección-IP-vecino tiene:

Valores válidos: cualquier dirección IP válida
Valor por omisión: ninguno

Ejemplo: **`enable neighbor 192.0.190.178`**

List

Utilice el mandato **list** para mostrar diferentes piezas de los datos de configuración BGP, según el submandato invocado.

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 todas las rutas agrupadas 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 los registros "no-receive-as", las rutas agrupadas, las políticas y los vecinos BGP de la configuración BGP actual.

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 derivar información sobre el emisor BGP. La información proporcionada es la siguiente:

Ejemplo: `list BGP speaker`

```
BGP Protocol:          Enabled
AS:                    165
TCP-Segment Size:      1024
```

neighbor Utilice el mandato **list neighbor** para derivar información sobre vecinos 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 derivar información sobre definiciones "no-receive-AS" añadidas a la configuración BGP.

Ejemplo: `list no-receive`

```
AS-PATH with following autonomous systems will be discarded:
AS  178
AS  165
```

originate-policy *all índice prefijo*

Utilice el mandato **list originate-policy** para derivar información sobre las políticas de origen añadidas a la configuración 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 mostrar los nombres de las listas de políticas configuradas.

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 las políticas adjuntadas a los vecinos.

Ejemplo: `list policy-to-neighbor`

```
Neighbor addrs  receive          send
192.0.251.165   nbr1-rcv         nbr1-snd
```

receive-policy adj-as-number *all* **o** *índice* **o** *prefijo*

Utilice el mandato **list receive-policy** para derivar información sobre las políticas de recepción añadidas a la configuración BGP. Puede visualizar todas las políticas de recepción definidas para un AS o las políticas según el índice o número 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** *índice* **o** *prefijo*

Utilice el mandato **list send-policy** para mostrar la información sobre las políticas de envío definidas para sistemas autónomos especificados. Puede visualizar todas las políticas de envío definidas para un AS o las políticas según el índice o número 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 cambiar el orden en el que se han definido los agrupamientos y las políticas. De esta forma se cambia el orden en el que el direccionador aplica las políticas existentes a la información de ruta. Antes de utilizar este mandato, es aconsejable utilizar el mandato **list** para ver las políticas que se han definido.

Sintaxis:

move *aggregate* o *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. El valor del temporizador de exploración de la tabla de rutas se utiliza para establecer el intervalo de tiempo que dura la exploración de la tabla de reenvíos IP en actualizaciones BGP.

Sintaxis:

set ip-route-table-scan-timer

Ejemplo:

```
set ip-route-table-scan-timer
```

Update

Utilice el mandato y los submandatos **update** para manipular las 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: Para las políticas de recepción exclusivas, no se le solicitarán los parámetros MED, Local-pref, Weight y IGP-metric. Los valores MED y Local-pref se utilizarán desde el anuncio recibido si están configurados como '0'. El valor '0' para el parámetro weight indica que se ignora el valor weight en el proceso de selección de la ruta.

Change

Utilice el mandato **Change** para cambiar las políticas del mandato **update**.

Ejemplo:

```
Enter index of receive-policy to be modified [1]?
```

Delete

Utilice el mandato **delete** para suprimir las políticas del mandato **update**.

Ejemplo:

```
Enter index of receive-policy to be deleted [1]?
```

Move

Utilice el mandato **move** para mover las políticas del mandato **update**.

Ejemplo:

```
Enter index of receive-policy to move [1]?
Move record after record number [0]?
```

List

Utilice el mandato **list** para listar las 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: Para las políticas de envío exclusivas, no se le solicitarán los parámetros MED y ASpad. El valor 0 para el parámetro MED indica que el atributo MED no está incluido en el anuncio. El valor 0 para el parámetro ASpad indica que no habrá otro número de AS local insertado en la vía de acceso del AS.

Change

Utilice el mandato **Change** para cambiar las políticas del mandato **update**.

Ejemplo:

```
Enter index of send-policy to be modified [1]?
```

Delete

Utilice el mandato **delete** para suprimir las políticas del mandato **update**.

Ejemplo:

```
Enter index of send-policy to be deleted [1]?
```

Move

Utilice el mandato **move** para mover las políticas del mandato **update**.

Ejemplo:

```
Enter index of send-policy to move [1]?
Move record after record number [0]?
```

List

Utilice el mandato **list** para listar las 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
```

Acceso al entorno de supervisión de BGP

Para acceder al entorno de supervisión de BGP, escriba el siguiente mandato en el indicador +:

```
+ Protocol BGP
BGP>
```

Mandatos de supervisión de BGP4

En este apartado se describen los mandatos de supervisión de BGP. Estos mandatos le permiten modificar el comportamiento del protocolo BGP ajustándolo a sus necesidades. Es necesario cierta configuración para producir un direccionador BGP completamente operativo. Escriba los mandatos de supervisión de BGP en el indicador `BGP config>`.

Tabla 25. Resumen de los mandatos de supervisión de BGP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Destinations	Muestra todas las entradas de la tabla de direccionamiento BGP.
Disable neighbor	Inhabilita un vecino determinado o todos ellos.
Dump routing tables	Muestra el contenido de la tabla de direccionamiento IP.
Enable neighbor	Habilita un vecino determinado o todos ellos.
Neighbors	Muestra los vecinos actualmente activos.
Parameter	Muestra los globales BGP instalados en el sistema BGP.
Paths	Muestra todas las vías de acceso disponibles en la base de datos.
Ping	Envía peticiones de eco ICMP a otro sistema principal una vez por segundo y espera una respuesta. Este mandato se puede utilizar para aislar problemas en un entorno interred.
Policy-list	Muestra la política instalada actualmente para un vecino específico y el uso de las estadísticas de cada política.
Reset neighbor	Restablece un vecino determinado.
Traceroute	Muestra la vía de acceso completa (salto por salto) a un destino determinado.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Destinations

Utilice el mandato **destinations** para volcar todas las entradas de la tabla de direccionamiento BGP o para mostrar la información sobre las rutas anunciadas o recibidas a o desde direcciones de vecino BGP especificadas (destinos).

Sintaxis:

destinations *dirección-red/dirección-red máscara-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 red de destino o la ruta especificadas. El mandato muestra la forma en que una ruta específica se ha averiguado, la mejor vía de acceso a un destino específico, la métrica asociada a la ruta, etc.

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 Enumeración de los sistemas anónimos de la vía de acceso.

- -seq: Secuencia de sistemas autónomos de la vía de acceso en orden
- -set: Conjunto de sistemas autónomos de la vía de acceso.

Origin Originador del destino. Este puede ser EGP, IGP, o Incomplete (originado por otros medios no conocidos).

LocalPref Grado de preferencia del direccionador de origen para el destino.

Metric Métrica de la vía de acceso con la que se importa la ruta.

Weight Peso de la vía de acceso.

MED Valor discriminador de varias salidas, utilizado para discriminar entre varios puntos de entrada/salida hacia el mismo AS.

NextHop Dirección del direccionador utilizada como dirección de reenvío en destinos accesibles a través de una determinada vía de acceso.

AtomicAggr Indica si el direccionador que anuncia la vía de acceso incluye la vía de acceso de una agrupación "atómica".

destinations *dirección-red máscara-red*

Muestra información detallada sobre la red de destino o la ruta especificadas. El mandato muestra la forma en que una ruta específica se ha averiguado, la mejor vía de acceso a un destino específico, la métrica asociada a la ruta, etc.

Este mandato es útil en casos donde varias direcciones de red tienen el mismo prefijo y máscaras distintas. En tal caso, la especificación de la máscara de la red restringe el ámbito de la 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*

Muestra todas las rutas anunciadas al vecino 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*

Muestra todas las rutas recibidas desde el vecino 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 inhabilitar un vecino determinado o todos los vecinos habilitados. Este mandato concluye la sesión BGP y elimina las rutas averiguadas del vecino.

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 obtener una explicación completa del mandato **dump routing tables**, consulte “Dump Routing Table” en el capítulo “Supervisión de IP” de *Configuración y supervisión de protocolos - Manual de consulta, volumen 1*

Enable Neighbor

Utilice el mandato **enable neighbor** para habilitar un vecino determinado o todos los vecinos que hayan sido inhabilitados. Este mandato inicia la sesión BGP con vecino.

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 mostrar la información existente en todos los vecinos BGP activos.

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 vecino BGP.

State Especifica el estado de la conexión. Los estados posibles son:

- **Connect** Esperando que la conexión TCP con el vecino se complete.
- **Active** En caso de producirse errores en la conexión TCP, el estado se cambia a activo y el intento de obtención del vecino continúa.
- **OpenSent** En este estado se ha enviado OPEN y BGP espera un mensaje OPEN del vecino.
- **OpenConfirm** En este estado se ha enviado un mensaje KEEPALIVE en respuesta al OPEN del vecino y se espera un KEEPALIVE/NOTIFICATION del vecino.
- **Established** Se ha establecido correctamente la conexión BGP y se puede iniciar ahora el intercambio de mensajes UPDATE.

BGP-ID Especifica el número de identificación del vecino.

AS Especifica el número de AS del vecino.

Upd# Especifica el número de secuencia del último mensaje UPDATE enviado al vecino.

dirección-internet
Utilice el mandato **neighbor** para mostrar datos detallados de un determinado vecino 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 BGP **parameter** para mostrar 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 BGP **paths** para mostrar las vías de acceso almacenadas en la base de datos de descripción de las 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 la vía de acceso

NextHop Dirección del direccionador utilizada como dirección de reenvío en destinos accesibles a través de una determinada vía de acceso.

MED Valor discriminador de varias salidas, utilizado para discriminar entre varios puntos de entrada/salida hacia el mismo AS.

AAG Indica si la vía de acceso ha agrupado "atómicamente", es decir, que el direccionador que anuncia la vía de acceso especificada haya seleccionado una ruta menos específica de la ruta más específica cuando se presenta con rutas solapadas.

AGRAS Indica el número de AS del emisor BGP que ha agrupado las rutas.

RefCnt Indica el número de las entidades de la vía de acceso que se refieren al descriptor.

ORG Especifica el originador de los destinos anunciados en la vía de acceso especificada: EGP, IGP o Incomplete (originado por otros medios no conocidos).

AS Path Enumeración de los sistemas anónimos de la vía de acceso.

- **seq:** Secuencia de sistemas autónomos de la vía de acceso en orden.
- **set:** Conjunto de sistemas autónomos de la vía de acceso.

Ping

Para obtener una explicación detallada del mandato **ping**, consulte el mandato Ping en el capítulo “Configuración y supervisión de IP” de la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 1*.

Policy-List

Utilice el mandato **policy-list** para visualizar la política actualmente instalada para vecinos específicos y las estadísticas utilizadas en cada política.

Ejemplo: policy-list

```
Neighbor address[0.0.0.0]? 192.0.251.167
Policy Type(Receive/Send/Origin)[All]?Receive
```

Presentación de la configuración de política basada en vecino:

```
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
```

Presentación de la configuración de 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
```

Presentación de la configuración de política basada en vecino:

```
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
```

Presentación de la configuración de 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 vecino BGP especificado, basándose en los parámetros de configuración del vecino que están almacenados en la memoria de configuración.

Sintaxis:

reset neighbor *dirección-ip*

Ejemplo: **reset neighbor**

```
Neighbor address[0.0.0.0]? 128.185.250.167
```

Sizes

Utilice el mandato BGP **sizes** para mostrar el número de entradas almacenadas en distintas 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 elegibles para todos los direccionadores de la tabla de direccionamiento BGP.

Path descriptors
Número total de descriptores de la vía de acceso de la base de datos utilizada para mantener la información de la vía de acceso común.

Update sequence#
Indica el número de la secuencia actualizada actual.

Routing tbl entries (allocated)
Indica el número de entradas de la tabla de direccionamiento BGP.

Current tbl entries (not imported)
Indica el número de rutas BGP no importadas al IGP.

Current tbl entries(imported to IGP)
Indica el número de rutas BGP importadas al IGP.

Traceroute

Para obtener una explicación completa del mandato **traceroute**, consulte "Configuración y supervisión de IP" en la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 2*.

Soporte de reconfiguración dinámica de BGP4

En este apartado se describe el modo en que la reconfiguración dinámica (DR) afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

BPG4 da soporte al mandato **delete interface** de CONFIG (Talk 6) con la matización siguiente:

Suprime los vecinos externos BPG configurados si la dirección de vecino tiene en la interfaz un número de red común con una dirección IP suprimida. Esto significa que la relación de par BGP se forma mediante una interfaz suprimida.

Mandato activate interface de GWCON (Talk 5)

El mandato **activate interface** de GWCON (Talk 5) no es aplicable a BGP4. BGP no tiene ningún registro de SRAM asociado con una interfaz.

Mandato reset interface de GWCON (Talk 5)

El mandato **reset interface** de GWCON (Talk 5) no es aplicable a BGP4. BGP no tiene ningún registro de SRAM asociado con una interfaz.

Mandatos de restablecimiento de componente de GWCON (Talk 5)

BGP4 da soporte a los mandatos **reset** de GWCON (Talk 5) específicos de BGP4 siguientes:

Mandato GWCON, protocol bgp, reset neighbor

Descripción: Añade o suprime un vecino BGP. Cambia políticas y parámetros de vecino.

Efecto en la red: Las rutas averiguadas y de conexión de vecino se actualizan tomando como base el cambio de configuración.

Limitaciones: Ninguna.

En la tabla siguiente se resumen los cambios de configuración de BPG4 que se activan cuando se invoca el mandato **GWCON, protocol bgp, reset neighbor**:

Mandatos cuyos cambios los activa el mandato GWCON, protocol bgp, reset neighbor
CONFIG, protocol BGP, add neighbor
CONFIG, protocol BGP, change neighbor
CONFIG, protocol BGP, delete neighbor
CONFIG, protocol BGP, attach policy-to-neighbor
CONFIG, protocol BGP, change policy-to-neighbor
CONFIG, protocol BGP, delete policy-to-neighbor
CONFIG, protocol BGP, add policy-list
CONFIG, protocol BGP, update policy-list

Mandatos de cambio temporal de GWCON (Talk 5)

BGP4 da soporte a los mandatos de GWCON que cambian de forma temporal el estado operativo del dispositivo indicados más abajo. Los cambios se pierden cada vez que se vuelve a cargar o iniciar el dispositivo o que se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
GWCON, protocol BGP, enable neighbor
GWCON, protocol BGP, disable neighbor

Mandatos no reconfigurables dinámicamente

En la tabla siguiente figuran los mandatos de configuración de BPG4 que no pueden cambiarse dinámicamente. Para activar estos mandatos, es necesario volver a cargar o a arrancar el dispositivo.

Mandatos
CONFIG, protocol BGP, enable/disable bgp
CONFIG, protocol BGP, add/delete no-receive
CONFIG, protocol BGP, add/change/delete/move aggregate
CONFIG, protocol BGP, add/change/delete/move originate-policy
CONFIG, protocol BGP, add/change/delete/move receive-policy
CONFIG, protocol BGP, add/change/delete/move send-policy
CONFIG, protocol BGP, enable/diable compare-med-from-diff-as
CONFIG, protocol BGP, enable/disable classless-bgp
CONFIG, protocol BGP, set ip-route-table-scan-timer

Configuración y supervisión de DVMRP

En este capítulo se describe la configuración y supervisión de la actividad del protocolo DVMRP (Distance Vector Multicast Routing Protocol). Consta de los apartados siguientes:

Acceso al entorno de configuración de DVMRP

Para acceder al entorno de configuración de DVMRP, escriba el siguiente mandato en el indicador `Config>`:

```
Config> protocol dvmrp
Distance Vector Multicast Routing Protocol config monitoring
DVMRP Config>
```

Mandatos de configuración de DVMRP

En este apartado se describen los mandatos de configuración de DVMRP. Dichos mandatos se teclean en el indicador `DVMRP Config>`.

Tabla 26. Resumen de los mandatos de configuración de DVMRP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado "Cómo obtener ayuda" en la página xxx.
Add	Añade más información a la información DVMRP ya existente. Puede añadir una interfaz física o una interfaz de túnel IP-IP.
Change	Cambia la información DVMRP en SRAM. Puede cambiar el coste o el umbral de una interfaz física, un túnel IP-IP, la interfaz MOSPF o los extremos de un túnel IP-IP.
Delete	Elimina información DVMRP de la configuración estática.
Disable	Inhabilita el protocolo DVMRP completo o la interfaz MOSPF.
Enable	Habilita 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 xxxi.

Add

Utilice el mandato **add** para añadir más información a la información DVMRP existente. Puede añadir una interfaz física o un túnel IP-IP.

Sintaxis:

add interface *dirección-ip coste umbral*

tunnel *origen-túnel destino-túnel coste 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 cuenta de saltos) producido al utilizar la interfaz.

Valores válidos: Cualquier entero mayor que 0

Valor por omisión: 1

umbral Especifica el tiempo de vida necesario para alcanzar al vecino más cercano de la interfaz.

Valores válidos: Cualquier entero mayor que 0

Valor por omisión: 1

tunnel Añade o actualiza un túnel IP-IP en una red que no sea multidifusión. Hay que configurar los túneles cuando el tráfico multidifusión necesite atravesar una red que no de soporte a datagramas multidifusión o no ejecute un protocolo de direccionamiento multidifusión.

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 cuenta de saltos) producido al utilizar el túnel.

Valores válidos: Cualquier entero mayor que 0

Valor por omisión: 1

umbral Especifica el tiempo de vida necesario para alcanzar al vecino 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 DVMRP existente. Puede modificar los valores del coste o del umbral de la interfaz física, los túneles IP-IP o la interfaz MOSPF.

Sintaxis:

change interface *dirección-ip coste umbral*

tunnel *origen-túnel destino-túnel coste umbral*

mospf *coste umbral*

interface Cambia una interfaz DVMRP

dirección-ip

Valores válidos: Cualquier dirección IP válida

Valor por omisión: Ninguno

coste Especifica el coste (en términos de cuenta de saltos) producido al utilizar la interfaz.

Valores válidos: Cualquier entero mayor que 0

Valor por omisión: 1

umbral Especifica el tiempo de vida necesario para alcanzar al vecino más cercano de la interfaz.

Valores válidos: Cualquier entero mayor que 0

Valor por omisión: 1

tunnel Cambia 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 cuenta de saltos) producido al utilizar la interfaz.

Valores válidos: Cualquier entero mayor que 0

Valor por omisión: 1

umbral Especifica el tiempo de vida necesario para alcanzar al vecino más cercano de la interfaz.

Valores válidos: Cualquier entero mayor que 0

Valor por omisión: 1

mospf Cambia una interfaz MOSPF.

coste Especifica el coste (en términos de cuenta de saltos) producido al utilizar la interfaz.

Valores válidos: Cualquier entero mayor que 0

Valor por omisión: 1

umbral Especifica el tiempo de vida necesario para alcanzar al vecino más cercano de la interfaz.

Valores válidos: Cualquier entero mayor que 0

Valor por omisión: 1

Delete

Utilice el mandato **delete** para eliminar información 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 inhabilitar la interfaz MOSPF o todo el protocolo DVMRP.

Sintaxis:

di**sable** dvmrp

mospf

dvmrp Inhabilita el protocolo DVMRP. Cuando se inhabilita, el dispositivo no participará como direccionador multidifusión DVMRP.

mospf Inhabilita el protocolo de direccionamiento MOSPF de la interfaz. Cuando está inhabilitado, el protocolo DVMRP no reenviará/recibirá datagramas multidifusión hacia/desde el protocolo de direccionamiento MOSPF.

Enable

Utilice el mandato **enable** para habilitar la interfaz MOSPF o todo el protocolo DVMRP.

Sintaxis:

enable dvmrp

mospf *coste umbral*

dvmrp Habilita el protocolo DVMRP. Se habilitan todas las interfaces configuradas para IP que no tienen habilitado el MOSPF y la interfaz MOSPF.

mospf Habilita el protocolo de direccionamiento MOSPF de la interfaz para DVMRP. Esta interfaz permite que DVMRP reenvíe datagramas multidifusión al protocolo de direccionamiento MOSPF. Esta interfaz es tratada como interfaz física.

coste Especifica el coste (en términos de cuenta de saltos) producido al utilizar la interfaz.

Valores válidos: Cualquier entero mayor que 0

Valor por omisión: 1

umbral Especifica el tiempo de vida necesario para alcanzar al vecino más cercano de la interfaz.

Valores válidos: Cualquier entero mayor que 0

Valor por omisión: 1

List

Utilice el mandato **list** para mostrar la configuración de DVMRP actual. La salida muestra el estado actual de DVMRP (habilitado o inhabilitado), información sobre la configuración de la interfaz física, información sobre la configuración del túnel e información sobre la configuración del 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 aparece en cada interfaz listada:

Protocolo DVMRP
Muestra si DVMRP está habilitado o no

Interfaces físicas DVMRP
En cada interfaz física, se muestran la dirección IP y los valores para el coste y el umbral.

Interfacez de túnel DVMRP
En cada interfaz de túnel, se muestran el umbral, el coste y los extremos del túnel configurados.

Interfaces MOSPF DVMRP
En cada interfaz MOSPF, se muestran el coste y el umbral.

Mandatos de supervisión de DVMRP

Los mandatos de supervisión de DVMRP permiten ver los parámetros y estadísticas de las redes que tienen habilitado DVMRP.

Escriba los mandatos de supervisión de DVMRP en el indicador **DVMRP>**.

Tabla 27. Resumen de los mandatos de supervisión de DVMRP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Dump routing tables	Muestra las rutas DVMRP contenidas en la tabla de direccionamiento.
Interface summary	Muestra las estadísticas y parámetros de la interfaz DVMRP.
Join	Configura el direccionador para que pertenezca a uno o más grupos multidifusión.
Leave	Quita al direccionador de entre los miembros de un grupo multidifusión.
Mcache	Muestra una lista de las entradas de antememoria de reenvío multidifusión actualmente activas.
Mgroups	Muestra los miembros de grupos de las interfaces conectadas del direccionador.
Mstats	Muestra diferentes estadísticas de direccionamiento multidifusión.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Dump Routing Tables

Utilice el mandato **dump routing tables** para mostrar el conjunto de orígenes multidifusión DVMRP conocido. Cada origen aparece junto con el direccionador DVMRP, 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 multidifusión (por ejemplo, DVMRP)

Origin-Subnet
Muestra la dirección IP de la subred de origen.

From-Gateway
Muestra la dirección IP de la pasarela por la que ha pasado la entrada.

Metric Muestra el coste asociado a esa ruta.

Age Muestra la edad de la entrada de la tabla de direccionamiento en número de segundos transcurridos desde que se renovó la entrada de la tabla de direccionamiento.

In Muestra el DVMRP VIF que el datagrama multidifusión procedente del origen debe recibir.

Out-Vifs Muestra los VIF que enviarán los datagramas multidifusión. Los VIF marcados con un asterisco indican que sólo se reenviará un datagrama si existen miembros de grupos en la red conectada.

Interface Summary

Utilice el mandato **interface summary** para mostrar 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). A cada VIF se le asigna un número que se utiliza para identificar el VIF en otros mandatos.

Local Address
Especifica la dirección IP local de la interfaz DVMRP.

Metric Coste asociado de la ruta.

Threshold
Refleja la capacidad de una red para controlar el flujo de paquetes multidifusión externos a la red.

Flags Muestra si VIF está desactivado o si el direccionador es el remitente de las consultas de miembros del sistema principal IGMP.

Join

Utilice el mandato **join** para establecer el direccionador como miembro de un grupo multidifusión.

Este mandato es parecido al mandato join utilizado para la supervisión de la configuración OSPF pero con dos diferencias:

- El efecto en el grupo es inmediato cuando los mandatos se dan desde el monitor (por ejemplo, no es necesario reiniciar/recargar).

- El mandato hace un seguimiento del número de veces que se “une” un determinado grupo.

Cuando el direccionador es miembro de un grupo multidifusión, responde a las consultas PING y SNMP enviadas a la dirección del grupo.

Sintaxis:

join *dirección-grupo-multidifusión*

Ejemplo: `join 224.185.00.00`

Leave

Utilice el mandato **leave** para eliminar un miembro del direccionador que se encuentre en un grupo multidifusión. Se evitará de esta forma que el direccionador responda a las consultas PING y SNMP enviadas a la dirección del grupo.

Este mandato es parecido al mandato **leave** del proceso de supervisión de la configuración OSPF pero con dos diferencias:

- El efecto en el grupo es inmediato cuando los mandatos se dan desde el monitor (por ejemplo, no es necesario reiniciar/recargar).
- El mandato no eliminará el miembro de un grupo hasta que el número de “leaves” ejecutados iguale al número de “joins” previamente ejecutados.

Sintaxis:

leave *dirección-grupo-multidifusión*

Ejemplo: `leave 224.185.00.00`

Mcache

Utilice el mandato **mcache** para mostrar una lista de las entradas de antememoria multidifusión activas actualmente. Las entradas de antememoria multidifusión se crean a petición, siempre que se reciba el primer datagrama multidifusión coincidente. No existe una entrada de antememoria distinta (y, por lo tanto, una ruta distinta) para cada combinación de grupo de destino y red origen del datagrama.

Las entradas de antememoria se borran en cambios topológicos (por ejemplo, una línea punto a punto del sistema DVMRP activada o no) y en cambios de miembros de grupo.

Nota: Los números mostrados en la leyenda situada en la parte superior de la salida NO se refieren directamente a los VIF, sino que se refieren a las interfaces físicas (que pueden ejecutar DVMRP o MOSPF) y a los 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 Subred/red de origen de datagramas coincidentes.

Destination
Grupo de destino de los datagramas coincidentes.

Count Muestra el número de entradas procesadas para el grupo multidifusión.

Upstream
Muestra el direccionador/red vecino/a desde el/la que los datagramas se deben recibir para ser reenviados. Cuando el valor es “none”, los datagramas nunca se reenviarán.

Downstream
Muestra el número total de vecinos/interfaces descendentes a los que se reenviará el datagrama. Cuando el valor es *none*, los datagramas nunca se reenviarán.

Existe más información en una entrada de antememoria de reenvío multidifusión. Una entrada de antememoria se puede visualizar al detalle proporcionando el origen y el destino del datagrama coincidente en la línea de mandatos. Si la entrada de antememoria coincidente no se encuentra, 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 mostrada en la forma abreviada del mandato mcache, aparecen los siguientes campos:

Upstream Type Indica el tipo de nodo desde el que se debe recibir el datagrama para que sea reenviado. Los posibles valores para este campo son “none” (que indica que el datagrama no se reenviará), “router” (que indica que el datagrama se recibirá a través de una conexión punto a punto), “transit network”, “stub network” y “external” (que indica que se espera que el datagrama proceda de otro sistema autónomo).

Downstream Imprime una línea distinta en cada interfaz o vecino al que se envía el datagrama. Se proporciona también un valor TTL que indica que los datagramas reenviados fuera de la interfaz o a la interfaz deben tener especificado al menos el valor TTL de su

cabecera IP. Cuando el direccionador es miembro del grupo multidifusión, una línea en la que se especifica *internal application* aparece como uno de los vecinos/interfaces descencentes.

Mgroups

Utilice el mandato **mgroups** para mostrar los miembros de grupos de las interfaces conectadas del direccionador. Sólo aparecen los miembros de grupo de interfaces en las que el direccionador esté designado o 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 de grupo tal y como se ha anunciado (a través de IGMP) en una interfaz.

Interface Muestra la dirección de la interfaz en la que se ha anunciado la dirección de grupo (a través de IGMP).

Los miembros del grupo interno del direccionador se indican mediante el valor “internal”. En estas entradas, el campo de tiempo de vida (véase más arriba) indica el número de aplicaciones que han solicitado ser miembro de un grupo determinado.

Lifetime Muestra el número de segundos durante los que la entrada persiste si un grupo determinado deja de oír los informes de miembros en la interfaz.

Mstats

Utilice el mandato **mstats** para mostrar diferentes estadísticas de direccionamiento multidifusión. El mandato indica si el direccionamiento multidifusión se habilita y si el direccionador es un reenviador multidifusión entre sistemas autónomos y/o entre áreas.

Sintaxis:

mstats

Ejemplo:

```
mstats

              MOSPF forwarding:       Disabled
              Inter-area forwarding:  Disabled
              DVMRP forwarding:       Enabled
              PIM forwarding:         Disabled

Datagrams received:           10143  Datagrams fwd (multicast):  10219
Datagrams fwd (unicast):          0  Locally delivered:              0
Unreachable source:               0  Unallocated cache entries:      0
Off multicast tree:               0  Unexpected DL multicast:   0
Buffer alloc failure:             0  TTL scoping:               0
Administrative filtering:       235

# DVMRP routing entries:          5  # DVMRP entries freed:          0
# fwd cache alloc:                1  # fwd cache freed:              0
# fwd cache GC:                   0  # local group DB alloc:         0
# local group DB free:            0
```

MOSPF forwarding Muestra si el direccionador reenviará datagramas multidifusión IP.

Inter-area forwarding Muestra si el direccionador reenviará datagramas multidifusión IP entre áreas.

DVMRP forwarding Muestra si el direccionador reenviará datagramas multidifusión IP.

Datagrams received Muestra el número de datagramas multidifusión recibidos por el direccionador (en este total no se incluyen los datagramas cuyo grupo de destino está en el rango que va del valor 224.0.0.1 al 224.0.0.255).

Datagrams (ext source) Muestra el número de datagramas recibidos cuyo origen está fuera del sistema autónomo (AS).

Datagrams fwd (multicast) Muestra el número de datagramas que se han reenviado como difusiones múltiples del enlace de datos (esto incluye réplicas de paquetes, llegado el caso, y por lo tanto el recuento puede ser mayor que el número de paquetes recibidos).

Datagrams fwd (unicast) Muestra el número de datagramas reenviados como difusiones únicas del enlace de datos.

Locally delivered Muestra el número de datagramas reenviados a las aplicaciones internas.

No matching rcv interface Muestra el número total de datagramas recibidos por un reenviador multidifusión que no esté entre AS en una interfaz que no sea MOSPF.

Unreachable source Muestra el número total de datagramas a cuya dirección de origen no se ha podido acceder.

Unallocated cache entries Muestra el número total de datagramas cuyas entradas de antememoria no se han podido crear debido a una falta de recursos.

Off multicast tree Muestra el número total de aquellos datagramas que no se han reenviado porque no existía vecino ascendente o vecinos/interfaces descendentes en la entrada de antememoria coincidente.

Unexpected DL multicast Muestra el total de datagramas recibidos como difusiones múltiples del enlace de datos en aquellas interfaces que se han configurado para la unidifusión del enlace de datos.

Buffer alloc failure Muestra el total de datagramas a los que no se pudo dar réplica debido a una falta de almacenamiento intermedio.

TTL scoping Indica los datagramas que no se han reenviado porque su TTL indicaba que nunca alcanzarían un miembro de grupo.

Administrative filtering Visualiza el número de datagramas descartados a causa del filtrado de salida.

DVMRP routing entries: Muestra el número de entradas de direccionamiento DVMRP.

DVMRP entries freed: Indica el número de entradas DVMRP liberadas. 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 de la antememoria de reenvío actual es el número de entradas asignadas ("# fwd cache alloc") menos el número de entradas de antememoria liberadas ("# fwd cache freed").

 # fwd cache freed Indica el número de entradas de antememoria liberadas. El tamaño de la antememoria de reenvío actual es el número de entradas asignadas ("# fwd cache alloc") menos el número de entradas de antememoria liberadas ("# fwd cache freed").

 # fwd cache GC Indica el número de entradas de antememoria borradas debido a que no se han utilizado recientemente y la antememoria se ha desbordado.

 # local group DB alloc Indica el número de entradas de la base de datos del grupo local asignadas. El número asignado ("# local group DB alloc") menos el número liberado (" # local group DB free") da lugar al tamaño actual de la base de datos del grupo local.

 # local group DB free Indica el número de entradas de la base de datos del grupo local liberadas. El número asignado ("# local group DB alloc") menos el número liberado (" # local group DB free") da lugar al tamaño actual de la base de datos del grupo local.

El número de aciertos de la antememoria se puede calcular de la siguiente forma: número de datagramas recibidos ("Datagrams received") menos el total de datagramas descartados por razones de "No matching rcv interface," "Unreachable source" y "Unallocated cache entries" menos "# local group DB alloc." El número de pérdidas de la antememoria es "# local group DB alloc"+.

Soporte de reconfiguración dinámica de DVMRP

En este apartado se describe el modo en que la reconfiguración dinámica (DR) afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

DVMRP da soporte al mandato **delete interface** de CONFIG (Talk 6) sin restricciones.

Mandato activate interface de GWCON (Talk 5)

DVMRP da soporte al mandato **activate interface** de GWCON (Talk 5) con la matización siguiente:

> Para poder activar DVMRP en una interfaz de red, debe estar habilitado globalmente.

Todos los mandatos específicos de interfaz DVMRP están soportados por el mandato **activate interface** de GWCON (Talk 5).

Mandato reset interface de GWCON (Talk 5)

DVMRP da soporte al mandato **reset interface** de GWCON (Talk 5) con la matización siguiente:

> Para poder activar DVMRP en una interfaz de red, debe estar habilitado globalmente.

Todos los mandatos específicos de interfaz DVMRP están soportados por el mandato **reset interface** de GWCON (Talk 5).

Mandatos no reconfigurables dinámicamente

Todos los parámetros de configuración de DVMRP pueden cambiarse dinámicamente.

Utilización de RSVP

RSVP (Resource ReSerVation Protocol) es un protocolo de señalización IP que utilizan las aplicaciones para señalizar sus necesidades de calidad de servicio (QoS). Está diseñado para dar soporte a sesiones de varios emisores a varios receptores. Cuando la señalización RSVP desencadena gestión del tráfico, el resultado es una reserva dinámica de los recursos de la red (por ejemplo, el ancho de banda y el almacenamiento intermedio) que completa la QoS deseada para una entrega de paquete. RSVP está orientado hacia el receptor, esto es, la aplicación que recibe el flujo QoS es responsable de iniciar la señalización RSVP que reserva los recursos de la red. De esta forma, la QoS de RSVP se realiza mediante la estabilización de reservas en cada salto de la vía de acceso del receptor al emisor. Una reserva está formada por un conjunto de parámetros que determinan la QoS para un flujo de tráfico. El emisor y el receptor, que son aplicaciones del sistema principal en las que RSVP está habilitado, crean la reserva mediante el envío de mensajes RSVP a otro. Una mejora de IBM permite que el direccionador de primer salto de algunas aplicaciones que no tienen habilitado RSVP realicen la señalización RSVP en su lugar. El RSVP se ejecuta en IPv4 en los direccionadores IBM y admite tráfico IP unidifusión y multidifusión. Encontrará una descripción completa de RSVP en el documento RFC 2205.

A todo flujo de tráfico IP para el que se haya establecido una reserva, RSVP, al estar implementado en el 2212, le proporciona una calidad de servicio de la carga controlada. La QoS de carga controlada se define en el modelo de servicios integrados de la IETF (Internet Engineering Task Force) (RFC 2211). Incluso en caso de atasco en la red, la QoS de carga controlada continúa proporcionando el nivel de servicio que el flujo de tráfico recibe cuando la red no está atascada.

Este capítulo consta de los siguientes apartados:

- "Cómo funciona RSVP"
- "Tipos de enlace soportados por RSVP" en la página 491
- "Ejemplo de configuración" en la página 492

Cómo funciona RSVP

La Figura 36 muestra la secuencia de mensajes que RSVp utiliza para establecer una reserva que proporcione una QoS a un determinado flujo de tráfico. En este ejemplo, los flujos de tráfico IP optimizados están ya establecidos en los direccionadores.

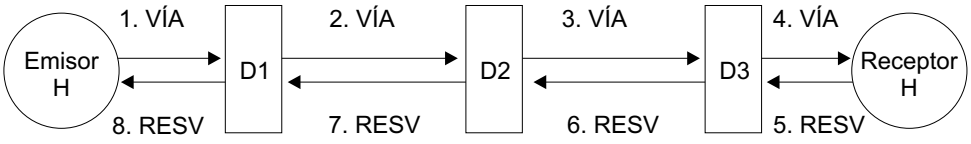


Figura 36. Reservas RSVP-Todos los direccionadores dan soporte al RSVP

El establecimiento de una reserva RSVP empieza cuando un emisor con RSVP habilitado envía mensajes *PATH* a os 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 (observando el campo de la opción

de alerta de la cabecera IP), establecen un estado dinámico y lo mantienen para el mensaje PATH. Un direccionador RSVP marcará también el mensaje PATH que se envía al destino con su propia dirección IP, denominado salto previo o "salto p". Un receptor con RSVP habilitado puede responder a uno de los mensajes PATH devolviéndole un mensaje *RESV*. El mensaje RESV solicita recursos de la red, como el ancho de banda, para reservarlos en cada enlace de la vía de acceso. El mensaje RESV se envía a través de la vía de acceso de reserva que el mensaje PATH atraviesa. El primer direccionador recibe el mensaje RESV (direccionador D3) que se encuentra en la vía de acceso de reserva. El direccionador intenta reservar recursos de la interfaz de salida, esto es, en el enlace que se encuentra entre D3 y el sistema principal del receptor. Si los recursos solicitados se encuentran disponibles, entonces se reservan para este flujo y la cantidad de recursos disponibles disminuye en la cantidad que le corresponde. Si los recursos solicitados no se encuentran disponibles, la reserva falla en ese nodo y el mensaje RESVERR puede volver a fluir al sistema principal del receptor. Por ahora, se dará por hecho que la reserva se ha realizado satisfactoriamente.

El direccionador D3 envía el mensaje RESV al siguiente direccionador (D2) de la vía de acceso de vuelta al emisor. D2 establece una reserva en el enlace que se encuentra entre éste y D3 y envía el mensaje RESV a D1. D1 establece una reserva en el enlace que se encuentra entre éste y D2 y envía el mensaje RESV al sistema principal del emisor. En este ejemplo, el sistema principal del emisor da soporte al RSVP, y establece una reserva en el enlace que se encuentra entre éste y D1. La vía de acceso de los enlaces reservados forma ahora una reserva que se establece del emisor al receptor.

Ahora, tengamos en cuenta una red en la que no todos los nodos den soporte al RSVP, tal y como se muestra en la Figura 37.

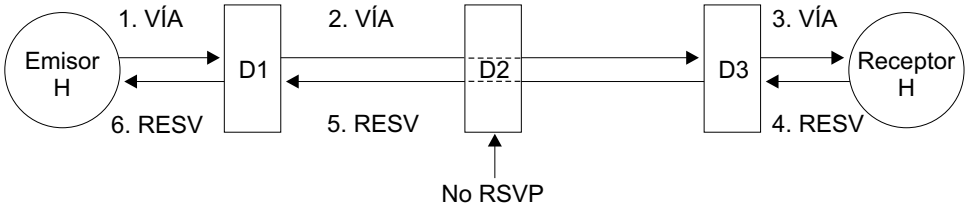


Figura 37. Reservas RSVP-No todos los direccionadores dan soporte al RSVP

Suponga, en concreto, que D2 no da soporte al RSVP. Cuando D2 recibe el mensaje PATH, lo trata como un paquete ordinario y lo reenvía a D3. D2 no cambia el "salto p" contenido en el mensaje PATH

Como en el caso anterior, cuando el mensaje PATH alcanza el sistema principal del receptor, inicial el proceso de reserva enviando un mensaje RESV a D3. El salto previo que D3 ve en el mensaje RESV es la dirección de D1 porque D2 no suministraba su salto previo en el mensaje PATH. D3 envía el mensaje RESV a D1 y hace la reserva en el enlace que se encuentra entre aquel y el sistema principal del receptor. Cuando D1 recibe el mensaje RESV de D3, hace la reserva desde él mismo a D3. Ahora, las reservas (de la dirección del emisor) existen en el emisor, D1 y D3. Los paquetes pasarán a través de D2 como paquetes optimizados ordinarios. En este caso, RSVP se puede utilizar en una red en la que no todos los direccionadores den soporte al RSVP.

Gestor de recursos del circuito virtual

El gestor de recursos del circuitos virtual (VCRM) es una función que se habilita al habilitar RSVP. Basándose en la solicitud de reserva de RSVP, el VCRM crea la conexión para el flujo de datos de la interfaz física. Para hacer esto, el VCRM debe primero determinar si existe suficiente ancho de banda para acomodar la reserva.

Nota: Si utiliza interfaces WAN como Frame Relay o la X.25, necesita establecer la velocidad de línea de forma que el VCRM conozca el ancho de banda del que se dispone. El procedimiento para establecer la velocidad de línea se describe en los capítulos de configuración de las interfaces X.25 y Frame Relay de la *Access Integration Services Guía del usuario de software* .

Si un enlace subrayado es WAN con DiffServ habilitado, el VCRM pedirá a DiffServ que asigne el recurso de enlace a los flujos DOS, y que añada las marcas TOS DiffServ como flujos de tráfico en el dispositivo.

Para obtener más información sobre el VCRM, consulte “Configuración y supervisión del VCRM” en *Utilización y configuración de las funciones*.

Flujos de tráfico y sesiones RSVP

El estado dinámico de la reserva y la vía de acceso de un direccionador define la existencia de una reserva RSVP y que el flujo de tráfico se transmite según la reserva. Una sesión RSVP se compone de todos los flujos de tráfico de uno o más emisores que se han dirigido a través de vías de acceso reservadas a la misma dirección de sesión IP, que puede ser una dirección IP unidifusión o multidifusión. Por ejemplo, en la Figura 39 en la página 490 la sesión incluye los flujos de tráfico del emisor E1 al receptor Rec 1, así como los flujos de tráfico del emisor E2 al receptor Rec 1. La dirección IP del receptor Rec 1 identifica a esta sesión.

Los emisores y los receptores mantienen la existencia de cada vía de acceso y de cada reserva de la sesión mediante el envío de mensajes de renovación que ratifican la existencia del flujo de tráfico reservado. Estos mensajes de renovación son sólo copias de los mensajes RESV y PATH. Los temporizadores configurables esperarán y harán que los nodos que mantienen el estado dinámico desmantelen la reserva si el nodo no recibe un mensaje de renovación en un periodo de tiempo determinado.

Existen dos tipos de mensajes de desmantelación: RSVTEAR y PATHTEAR. Los mensajes RSVTEAR, enviado por el receptor, desmantela la reserva pero no el flujo de tráfico, que continúa con el servicio optimizado. Los PATHTEAR desmantelan la vía de acceso del emisor a la dirección de la sesión. Los PATHTEAR desmantelan el estado dinámico de la vía de acceso y la reserva. El tráfico optimizado puede, sin embargo, fluir.

Estilos de reserva

La Figura 36 en la página 487 muestra el establecimiento de una reserva RSVP que reserva enlaces para una corriente de tráfico procedente de un emisor particular a un receptor particular. Si varios emisores envían al mismo receptor, habrá varios flujos de tráfico IP (uno de cada emisor a cada receptor). En este caso, los distintos emisores pueden compartir o no reservas a través de algunos enlaces con el receptor, según el *estilo de reserva* seleccionado.

La Figura 38 en la página 490 muestra dos emisores (E1 y E2) para los que el receptor a solicitado un estilo de reserva de filtro fijo (FF). En este estilo de reserva, a cada emisor se le proporciona su propia reserva individual. El sistema principal E3 no participa en RSVP, pero recibe tráfico optimizado.

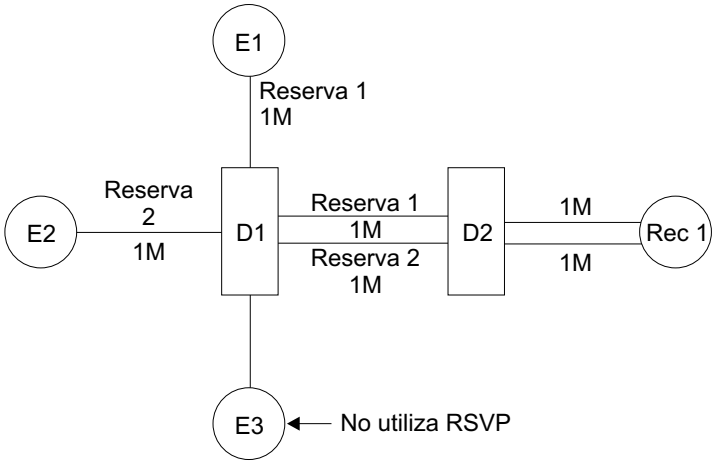


Figura 38. Estilo de reserva de filtro fijo

En el estilo de reserva explícitamente compartida (SE), los emisores identificados como miembros de un determinado grupo comparten algunos de los enlaces reservados. Los emisores que se encuentran dentro de un grupo son definidos por el receptor según la información enviada en el mensaje PATH, caso de las direcciones IP de los emisores. En la Figura 39, el emisor E1 y el emisor E2 han sido incluidos en la sesión RSVP identificada por la dirección de destino del receptor Rec 1. Los emisores del grupo comparten la reserva en cuanto las vías de acceso enviadas de los emisores a los receptores se fusionan. En este caso, la reserva común se amplía del direccionador D1 al receptor.

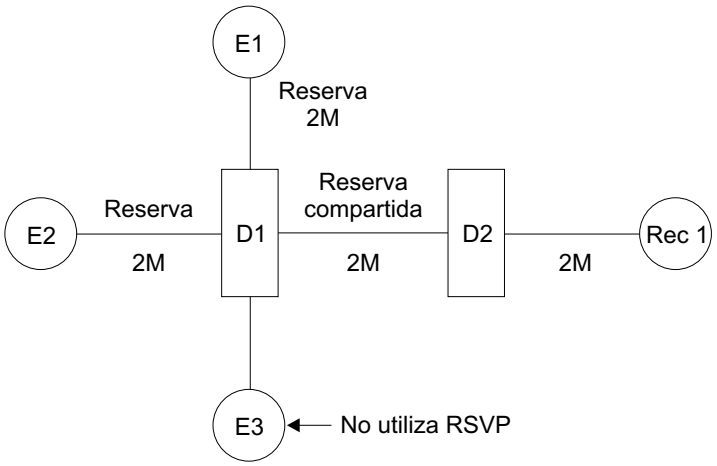


Figura 39. Estilo de reserva explícitamente compartida

En el tercer estilo de reserva, denominado filtro comodín (WF) todos los emisores que envían mensajes *PATH* a la dirección de sesión comparten la misma reserva, tal y como se ilustra en la Figura 40 en la página 491.

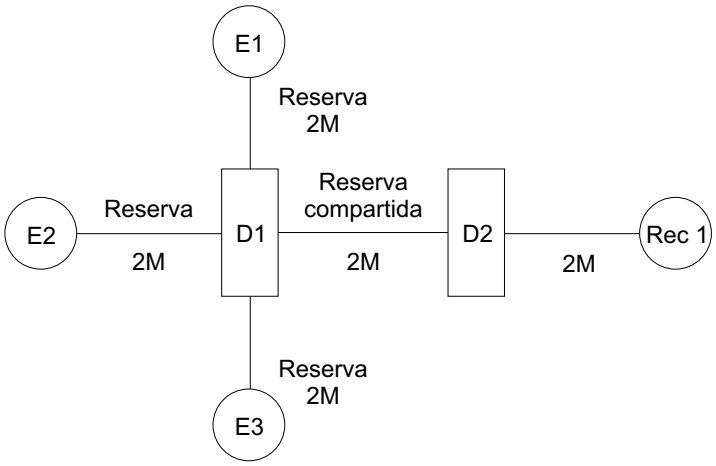


Figura 40. Estilo de reserva de filtro comodín

OPWA

OPWA (One-Path With Advertising) es un función opcional de RSVP. Permite al receptor obtener anotaciones de todos los valores QoS, como el ancho de banda, que se encuentran disponibles desde cada enlace de la vía de acceso de la reserva. Por ejemplo, si los direccionadores D1 y D3 mostrados en la Figura 36 en la página 487 se configuran para OPWA, se les tendrá que decir las características de cada enlace. Esta información les permite ajustar la información del mensaje PATH según la capacidad del enlace con menos recursos.

Por ejemplo, en el contexto de la Figura 36 en la página 487, suponga que un emisor inicia el envío de mensajes PATH a un receptor con una velocidad media de 1 Mbps y una velocidad pico de 10 Mbps. A continuación, suponga que el enlace entre el direccionador D2 y D3 es un enlace PPP con una velocidad de línea de 2 Mbps. La función OPWA de D2 alterará la velocidad pico del mensaje PATH para que disminuya a 2 Mbps, ya que no existen ninguna razón para que ningún nodo descendente reserve una velocidad pico mayor que 2 Mbps.

Tipos de enlace soportados por RSVP

RSVP da soporte a los siguientes tipos de enlace:

- Enlaces PPP. RSVP admite PPP en todos los tipos de enlace admitidos, como el V.35, T1/E1 y RDSI, que están en una base de conexión permanente. Los enlaces utilizados en configuraciones de llamada a petición, restauración de la WAN y de las modalidades de retención corta o equilibrado de la carga no se deben utilizar con RSVP.
- Frame relay PVC. Como en el caso de PPP, todos los tipos de enlace admitidos darán soporte al RSVP, pero sólo los enlaces que estén en una base de conexión permanente se podrán utilizar con RSVP. Los enlaces utilizados en configuraciones de llamada a petición, restauración de la WAN y de las modalidades de retención corta o equilibrado de la carga no se deben utilizar con RSVP.
- Frame relay SVC. Se le da el mismo soporte que a Frame relay PVC; esto es, RSVP no puede configurar DLCI para tráfico QoS, pero utilizará parte del DLCI por omisión para la ubicación del ancho de banda QoS.

- Todos los enlaces LAN:
  - Ethernet
  - Red en anillo (Token Ring)
  - Fast Ethernet

  Nota: En redes de medio compartido como la LAN, se necesitan otros métodos, como la ingeniería de tráfico, para coordinar el compartimiento ancho de banda LAN. RSVP controla el uso del ancho de banda de un direccionador determinado, pero no coordina el uso del ancho de banda cuando se trata de varios direccionadores y sistemas principales.
- X.25. Se le da soporte como a PPP y Frame relay PVC. RSVP no puede configurar distintos VC para el tráfico QoS y utiliza parte del VC por omisión para la ubicación del ancho de banda QoS.

Notas:

1. Para evitar conflictos, RSVP se inhabilita en enlaces PPP o FR que se han configurado para el Sistema de reserva del ancho de banda (BRS).
2. RSVP puede utilizar las funciones de programación y cola de DiffServ con enlaces PPP o FR que se han configurado para DiffServ.

Ejemplo de configuración

A título orientativo, se incluye un ejemplo de la configuración de la interfaz de la línea de mandatos talk 6. Consulte “Configuración y supervisión de RSVP” en la página 497 para obtener la descripción de los parámetros y mandatos RSVP. A través de los siguientes pasos, se describe un ejemplo para la configuración de RSVP:

1. Habilite RSVP en el direccionador con el mandato talk 6 **enable rsvp** del indicador `RSVP config>`. RSVP se puede habilitar sólo en interfaces configuradas para IP. Este mandato establece los parámetros del direccionador RSVP en los valores por omisión, incluido el 0 como el ancho de banda por omisión de las interfaces. Necesitará habilitar determinadas interfaces y establecerles el ancho de banda antes de que RSVP se pueda ejecutar en esas interfaces.
2. Utilice el mandato **enable interface** para habilitar todas las interfaces de RSVP.
3. Utilice el mandato talk 5 **reset interface** si desea que RSVP se active inmediatamente en la interfaz.
4. Se le solicitará el establecimiento del ancho de banda para cada interfaz. Si el ancho de banda de una determinada interfaz está en 0 (el valor por omisión), no se podrán hacer reservas RSVP en la interfaz.
5. Utilice el mandato **enable opwa-all** si desea habilitar el OPWA de todas las interfaces que tengan habilitado RSVP. Utilice el mandato **enable opwa** y el número de interfaz si desea habilitar el OPWA de cada interfaz. Asegúrese de habilitar RSVP en la interfaz antes de habilitar el OPWA. Si intenta habilitar el OPWA en una interfaz que no se haya habilitado para RSVP, aparecerá el mensaje `Cannot find RSVP i/f rec`.
6. Los demás parámetros son opcionales y RSVP se puede ejecutar con los valores por omisión.

7. Si lo desea, puede utilizar los mandatos **add sender** y **add receiver** para crear receptores o emisores estáticos para el direccionador. El receptor y el emisor estáticos generarán la señalización RSVP para la aplicación del sistema principal que no utilice RSVP. El puerto y la dirección IP configurados para el receptor y el emisor estáticos identifican el origen y el destino del flujo de tráfico IP al que el direccionador enviará mensajes RSVP. En caso de no configurar ningún emisor o receptor estático, el direccionador reenviará los mensajes RSVP y establecerá los enlaces de reserva pero no originará mensajes RSVP. Consulte “Ejemplo de configuración de un receptor y un emisor estáticos” en la página 494 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 completada la configuración, puede activar RSVP utilizando los mandatos **reset rsvp** o **reset interface** o reiniciando el direccionador.

Ejemplo de configuración de un receptor y un emisor estáticos

Si configura RSVP, tal y como se describe en “Ejemplo de configuración” en la página 492, las aplicaciones con RSVP habilitado de los sistemas principales conectados al direccionador establecerán de forma dinámica las sesiones y los flujos de tráfico RSVP. Cuando hay una aplicación del sistema principal que no esté habilitada para RSVP y que envíe paquetes a un puerto y a una dirección IP conocidos, se pueden configurar un emisor y un receptor estáticos para que el direccionador genere señalización RSVP para ese flujo.

Primero, configure el emisor con el mandato **add sender** del 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 unidifusión, la dirección IP de la sesión es la dirección unidifusión del receptor del flujo de tráfico IP. Si el flujo de tráfico es multidifusión, la dirección IP de la sesión es la dirección multidifusión del destino del flujo de tráfico IP.

2 La dirección IP del emisor es la dirección unidifusión del emisor del flujo de tráfico IP. Si el emisor y el receptor no son direccionadores, habrá sistemas principales conectados a los direccionadores. Los direccionadores, en este caso, actúan como proxy de 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 direccionador remoto segundo que actúe como receptor. En el ejemplo, el direccionador emisor tiene la dirección IP 5.0.27.27 y el direccionador receptor la 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 el protocolo, el puerto y la dirección de la sesión IP del receptor coinciden con el protocolo, el puerto y la dirección de la sesión IP del emisor. El emisor y el receptor deben identificar el mismo flujo de tráfico. El receptor, y no el emisor, determina el ancho de banda que los direccionadores situados en la vía de acceso intentarán establecer en cada enlace.

2 Las letras *wf* asignan al filtro comodín. Éste es uno de los tres estilos de reserva de RSVP. Consulte “Estilos de reserva” en la página 489 para obtener más información.

Configuración y supervisión de RSVP

En este capítulo se describe la forma de configurar y supervisar RSVP así como la forma de utilizar los mandatos de supervisión de RSVP. Consta de los siguientes apartados:

- "Acceso al entorno de configuración de RSVP"
- "Mandatos de configuración de RSVP"
- "Acceso al entorno de supervisión de RSVP" en la página 507
- "Mandatos de supervisión de RSVP" en la página 507

Acceso al entorno de configuración de RSVP

Para acceder al entorno de configuración de RSVP, escriba el siguiente mandato en el indicador `Config>`:

```
Config> protocol rsvp
Resource ReSerVation Protocol config console
RSVP Config>
```

Mandatos de configuración de RSVP

En este apartado se describen los mandatos de configuración de RSVP. Escriba estos mandatos en el indicador `RSVP Config>`.

Tabla 28. Resumen de los mandatos de configuración de RSVP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado "Cómo obtener ayuda" en la página xxx.
Add	Añade emisor y receptor.
Delete	Elimina emisor y receptor.
Disable	Inhabilita RSVP o bien OPWA (One-Path With Advertising).
Enable	Habilita RSVP o bien OPWA (One-Path With Advertising).
List	Lista la información sobre la configuración RSVP.
Set	Establece los 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 xxxi.

Add

Utilice el mandato **add** para añadir receptores y emisores RSVP estáticos al direccionador. Los receptores o emisores estáticos permiten que el direccionador envíe o reciba mensajes RSVP. En la mayoría de los casos, si el direccionador envía y recibe mensajes RSVP, actúa como proxy de la aplicación de un sistema principal que no esté configurada para RSVP. En tal caso, la dirección IP del emisor es la dirección de la aplicación del sistema principal y la dirección IP de la sesión la dirección de destino del flujo de datos. Si no se ha configurado emisor o receptor estático para el direccionador, éste reenviará dinámicamente mensajes

RSVP, configurará reservas y proporcionará QoS, pero no producirá mensajes RSVP.

Las definiciones de los emisores y los receptores se guardan en la configuración como registros SRAM numerados. El mandato **activate** de Talk 5 se puede utilizar para activar cada registro.

Sintaxis:

add sender ...

receiver ...

sender
Clave utilizada para especificar que los parámetros que siguen a este término se aplican al emisor del mensaje RSVP *path*.

receiver
Clave utilizada para especificar que los parámetros que siguen a este término se aplican al receptor que devuelve el mensaje RSVP *resv* al emisor.

La mayoría de los parámetros que aparecen a continuación se especifican tanto para el emisor como para el receptor. Los parámetros que sean únicos para el receptor o para el emisor se especifican en su descripción.

session-ip-address
Se trata de la dirección IP de destino multidifusión o unidifusión de los flujos de datos IP procedentes de uno o más emisores. Cuando los flujos de tráfico son unidifusión, esta dirección es la dirección del receptor; cuando los flujos de tráfico son multidifusión, la dirección será multidifusión. El receptor debe ser miembro del grupo identificado por la dirección de multidifusión. Los emisores y el receptor utilizan la dirección IP de la sesión junto con el número de puerto de la sesión y el protocolo para identificar la sesión RSVP para la que se han establecido las QoS.

Valores válidos: dirección IPv4 válida. No puede ser 0.0.0.0. Cuando RSVP está activado, esta dirección debe ser accesible para el emisor y el receptor.

Valor por omisión: ninguno

session-port
Número de puerto IP de la sesión reservada por RSVP. Se trata del número de puerto UDP o del número de zócalo TCP de la aplicación de destino.

Valores válidos: 0 - 65535

Valor por omisión: 1

session-protocol
UDP oTCP.

Valores válidos: UDP o TCP

Valor por omisión: UDP

sender-ip-address
Dirección del emisor, que es la aplicación emisora que produce el flujo de datos que se va a reservar. Este parámetro debe ser una dirección de unidifusión.

Valores válidos: dirección IPv4 válida.

Valor por omisión: ninguno

sender-port
Número del puerto IP del emisor del flujo IP reservado para las QoS. Se trata del número de puerto UDP o del número de zócalo TCP de la aplicación emisora.

Valores válidos: 0 - 65535

Valor por omisión: 1

receiver-ip-address
Dirección IP del receptor que emite el mensaje *resv*. En el caso de las sesiones unidifusión, esta dirección es la misma que la dirección IP de la sesión. En el caso de las sesiones multidifusión, esta dirección es la dirección de unidifusión de la aplicación que hace la reserva para la dirección de la sesión multidifusión. Si se trata de una sesión multidifusión, el receptor debe pertenecer al grupo multidifusión representado por esta dirección de multidifusión.

Valores válidos: dirección IPv4 válida.

Valor por omisión: ninguno

peak-rate
Especifica la velocidad pico de los datos de la sesión IP. Esta velocidad se establece en la velocidad pico de la generación del tráfico, si se conocen y se controla, en la velocidad de línea de la interfaz física, si se conoce, o en ilimitado (X'FFFFFFFF', en decimal 4 294 967 295) si no no se dispone de un valor mejor. La velocidad pico del tráfico debe establecerse en un valor mayor o igual que el promedio de la velocidad del tráfico.

Si el receptor solicita una velocidad pico de los datos diferente de la velocidad que le ofrece el emisor, el direccionador intentará complacer al emisor.

Valores válidos: 1 - 4 294 967 295 bytes/segundo

Valor por omisión: 250 000

average-rate
Especifica el promedio de la velocidad de los datos que el emisor debe enviar o que el receptor debe recibir en la sesión IP. Esta velocidad se establece en la velocidad media de generación del tráfico del emisor, si se conoce, o en 000 bytes/ segundo por omisión.

Si el receptor solicita un promedio de la velocidad de los datos diferente del que le ofrece el emisor, el direccionador intentará complacer al emisor.

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 pico el promedio de velocidad. Por ejemplo, si la velocidad pico es de 50 000 bytes/segundo y el tamaño de la ráfaga de datos es 2000, se pueden enviar 2000 bytes en una instancia determinada incluso si la ráfaga puede hacer que la velocidad pico se amplíe a 50 000 bytes/segundo en dicha instancia.

Si el receptor solicita una velocidad diferente de la que le ofrece el emisor, el direccionador intentará complacer al emisor.

Valores válidos: 1 - 4 294 967 295 bytes

Valor por omisión: 2000

max-packet-size

Especifica el máximo tamaño 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 establecer en el tamaño del mayor paquete generado por la aplicación emisora. Para el receptor, se debe establecer en la MTU más pequeña de la ruta, que el receptor obtiene de la información que llega en los paquetes OPWA o de otros modos.

Si el tamaño máximo de paquete es mayor que la MTU de un enlace de la ruta, la petición de reserva será rechazada. Por ejemplo, si un enlace de la ruta de las reservas tiene una MTU de 1500 y el tamaño máximo de paquete solicitado es 2000, la petición de reserva será rechazada.

Si el receptor solicita un tamaño máximo de paquete distinto que el emisor, el direccionador tratará de complacer al receptor.

El tamaño máximo de paquete se debe configurar con un valor que no sea más pequeño que el tamaño mínimo de paquete. Por ejemplo, si el tamaño mínimo de paquete es 64 bytes, el tamaño máximo de paquete debe ser mayor o igual que el valor 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 establecer en el tamaño más pequeño del paquete generado por la aplicación emisora.

Este tamaño de paquete no debe ser mayor que el tamaño máximo de paquete. Por ejemplo, si el tamaño máximo de paquete es de 1500 bytes, el tamaño mínimo de paquete debe ser menor o igual que 1500. Este tamaño de paquete incluye los datos de la aplicación y todas las cabeceras de protocolo del nivel IP o superiores, caso de IP, TCP o UDP, pero no incluye las cabeceras del nivel de enlace.

Nota: Este valor se utiliza para calcular la actividad general de la reserva de recursos. Cuanto más pequeño es el tamaño mínimo de paquete, mayor es la actividad general de la reserva.

Valores válidos: 1 - 4 294 967 295 bytes

Valor por omisión: 48

reservation-style

Este parámetro sólo se configura para los receptores. Especifica el estilo de reserva que el receptor recibirá en el flujo IP. Una reserva RSVP garantiza un manejo especial de los paquetes existentes en un flujo de tráfico IP para proporcionar una determinada QoS en cada enlace o serie de enlaces que forman una vía de acceso desde el emisor al receptor. Los tres estilos de reserva ofrecidos son los siguientes:

Fixed-Filter (FF)

Especifica que el receptor recibirá un determinado tráfico de datos del emisor en el flujo IP. Se establece una reserva por emisor.

Shared-Explicit (SE)
Especifica que el receptor recibirá tráfico de datos de un grupo de emisores del mismo grupo, definido por el receptor. Los miembros de este grupo comparten la reserva. Cada emisor del grupo puede compartir la reserva en cuanto su enlace se fusione con una vía de acceso común para el receptor.

Wildcard-Filter (WF)
Especifica que el receptor recibirá tráfico de datos procedente de todos los emisores. Cada emisor del grupo puede compartir la reserva en cuanto su enlace se fusione con una vía de acceso común para el receptor.

Consulte “Estilos de reserva” en la página 489 para obtener más información acerca de esto.

Valores válidos: FF, SE y WF

Valor por omisión: FF

confirm-reservation
Especifica si el receptor desea recibir un mensaje de *confirmación de la reserva*. Este mensaje se vuelve a enviar al receptor que lo envía cuando la solicitud se fusiona con una reserva existente más grande o se entrega a la aplicación del emisor.

Valores válidos: Yes o No

Valor por defecto: No

Delete

Utilice el mandato **delete** para eliminar un emisor o un receptor.

Sintaxis:

de**lete**
sender *registro-sram*

receiver *registro-sram*

sender or receiver *registro-sram*
Cada emisor o receptor se identifica mediante un registro SRAM que aparece al utilizar el mandato **delete**. Al especificar el número de registro SRAM del emisor o receptor para que se elimine, se elimina también el emisor o el receptor de la configuración.

Disable

Utilice el mandato **disable** para inhabilitar RSVP o bien OPWA en una interfaz o en todas las interfaces.

Sintaxis:

di**sable**
interface
opwa
opwa-all
rsvp

interface *número-interfaz*
Inhabilita la función RSVP de una determinada interfaz. Los mensajes de control RSVP pueden fluir a través de esta interfaz, pero no se realizarán reservas RSVP en la misma. Este mandato inhabilita también la posibilidad de que esta interfaz pueda configurar QoS.

Valores válidos: cualquier número de interfaz válido.

Valor por omisión: 0

OPWA *número-interfaz*
Inhabilita OPWA en una determinada interfaz.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

OPWA-all
Inhabilita OPWA en todas las interfaces

RSVP Inhabilita la función RSVP dentro del direccionador. Por omisión, RSVP está inhabilitado.

Enable

Utilice el mandato **enable** para habilitar RSVP o bien OPWA en una interfaz o en todas las interfaces.

Sintaxis:

e**nable**
interface
opwa
opwa-all
rsvp

interface *número-interfaz*
Habilita la función RSVP de una determinada interfaz. Este mandato habilita la interfaz para responder a mensajes RSVP y reenviarlos, pero no para producirlos. Para producir mensajes RSVP, es necesario configurar emisores y receptores estáticos.

Se le solicitará el establecimiento del ancho de banda para la interfaz habilitada. Puede utilizar también el mandato **set bandwidth** más tarde para cambiar el valor del ancho de banda. Este mandato funciona sólo si el direccionador está habilitado para RSVP y la interfaz especificada está habilitada y configurada para IP.

Consulte “Tipos de enlace soportados por RSVP” en la página 491 para obtener una lista de los enlaces que admiten RSVP.

Valores válidos: cualquier número de interfaz válido.

Valor por omisión: 0

OPWA *número-interfaz*
Habilita OPWA en una determinada interfaz. OPWA informa 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. Sólo se permite esta operación si la interfaz está habilitada para RSVP.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

OPWA-all

Habilita OPWA en todas las interfaces Para que este mandato tenga efecto, RSVP se debe habilitar en el direccionador.

RSVP Habilita la función RSVP en del direccionador. Si es la primera vez que habilita RSVP, se iniciarán también un conjunto de parámetros por omisión para RSVP.

La habilitación de RSVP no lo activa. Para activar RSVP en el direccionador debe utilizar el mandato **set bandwidth** y, de esta forma, establecer el ancho de banda en al menos una de las interfaces que utilicen RSVP. A continuación, debe reiniciar el direccionador para RSVP. Para hacerlo, puede utilizar el mandato **reset rsvp** de Talk 5, o rearrancar el direccionador. Consulte el mandato **reset rsvp** de Talk 5 para obtener más información.

List

Utilice el mandato **list** para listar los parámetros RSVP. Estos grupos de parámetros se pueden listar por separado:

- Todos los parámetros
- Parámetros de la interfaz
- Valores OPWA para todas las interfaces
- Registros del emisor o del receptor
- Parámetros RSVP del nivel sistema

Nota: El mandato **list** muestra los registros del emisor y del receptor que se han configurado. Estos registros no identifican los flujos de tráfico RSVP activos, definidos por la dirección del emisor y la del receptor. Utilice el mandato **show rsvp flows** de Talk 5 para ver los flujos RSVP que están 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 mostrada es la dirección de la sesión IP. Consulte el mandato **add session-ip-address** de Talk 6 para obtener una definición de la dirección de la sesión IP.

Set

Establece los parámetros del sistema RSVP. Consulte el ejemplo del mandato **list all** de Talk 6 para obtener una visión de algunos valores típicos para estos parámetros.

Sintaxis:

set ...
- allowed-successive-msg-loss ...
- bandwidth ...
- default
- encapsulation ...
- lifetime ...
- max-msg-size ...
- refresh-interval ...
- slew ...
- total ...

allowed-successive-msg-loss *pérdidas-mensajes*
Este parámetro define el número de mensajes "sucessive path" y "matching resv refresh" que se pueden perder antes de que RSVP exceda el tiempo del

estado de reserva y vía de acceso definido para el flujo de tráfico RSVP. Cuando RSVP excede el tiempo de espera del estado de reserva y vía de acceso para un flujo de tráfico determinado, dicho flujo no proporcionará más QoS. El emisor y el receptor deben restablecer la reserva.

Valores válidos: 1 - 9999

Valor por omisión: 3

bandwidth *interfaz bps*

Este parámetro define el ancho de banda reservable de una interfaz. Por lo general, el ancho de banda reservable debe ser una pequeña parte del ancho de banda total del enlace. Una buena medida es menos del 30%. El ancho de banda reservable sólo se puede establecer en una interfaz que esté habilitada para RSVP.

Este mandato de Talk 6 puede opcionalmente tener efecto inmediatamente y dinámicamente sin que afecte a los valores de otros parámetros.

interfaz

Número de interfaz de la red.

Valores válidos: cualquier número de interfaz de la red válido.

Valor por omisión: 0

bps Bps del ancho de banda que se puede reservar en esta interfaz.

Valores válidos: 1 - 4 294 967 295 bps (representa ilimitado)

Valor por omisión: 0

default

Este parámetro establece todos los parámetros RSVP en los valores por omisión originales que existen al utilizar el mandato **enable rsvp**. El mandato **set default** graba encima cualquier valor de parámetro que configurado anteriormente en las interfaces individuales. Al ser 0 el valor por omisión del ancho de banda de cada interfaz, lo que significa que las reservas RSVP no se establecerán en dicha interfaz, debe utilizar el mandato **set bandwidth** en cada interfaz que utilice RSVP para preparar de nuevo la ejecución del mismo.

encapsulation *interfaz estilo*

Este parámetro establece el estilo de encapsulación de los mensajes RSVP de una interfaz en IP, UDP o ambos. Por lo general, los mensajes de control de RSVP, como es el caso de los mensajes "path" y "resv", se encapsulan en tramas IP nativas con protocolo tipo 46. En el caso de que un sistema principal conectado al direccionador sólo pueda utilizar paquetes UDP para enviar mensajes RSVP, el estilo de la encapsulación a través de la interfaz conectada al sistema principal se debe establecer en UDP. Si algunos sistemas principales que utilizan IP y algunos que utilizan UDP están enviando mensajes RSVP a través del mismo enlace, debe establecer el estilo de encapsulación en "Both" (ambos). Sólo se permite esta operación si RSVP está habilitado en la interfaz especificada.

Este mandato de Talk 6 puede opcionalmente tener efecto inmediatamente y dinámicamente sin que afecte a los valores de otros parámetros.

interfaz

Número de interfaz de la red.

Valores válidos: cualquier número de interfaz de la red válido.

Valor por omisión: 0

estilo

Estilo de encapsulación de los mensajes RSVP.

Valores válidos: IP, UDP o ambos

Valor por omisión: IP

lifetime

Este parámetro define el tiempo de vida en segundos de un estado de la reserva y la vía de acceso, 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 especificado mediante el valor del parámetro de pérdidas sucesivas de mensajes permitidas. Para calcular correctamente este tiempo, utilice la fórmula: 1.5 x intervalo de renovación x (pérdidas sucesivas de mensajes permitidas + 0.5).

Si el estado de reserva excede su tiempo, pero no el de estado de la vía de acceso, la reserva se desactiva y el flujo de tráfico IP continúa con el servicio optimizado. Si el estado de la vía de acceso excede su tiempo de espera, tanto la reserva como el flujo de tráfico IP finalizan.

Este mandato de Talk 6 puede opcionalmente tener efecto inmediatamente y dinámicamente sin que afecte a los valores de otros parámetros. Se espera que el valor por omisión de este parámetro funcione sin necesidad de sufrir modificaciones.

Valores válidos: 1 - 2 147 483 647 segundos

Valor por omisión: 158 segundos

max-msg-size

Este parámetro define el tamaño máximo del total de mensajes de control RSVP en el direccionador. Este valor no debe ser mayor que la MTU de menor tamaño a la que dan soporte las interfaces con RSVP habilitado que se encuentra en la vía de acceso. Se espera que el valor por omisión de este parámetro funcione sin necesidad de sufrir modificaciones.

Valores válidos:64 - 2 147 483 647 bytes (representa ilimitado)

Valor por omisión: 1500 bytes

refresh-interval

Este parámetro define el intervalo de tiempo en segundos que transcurre entre los mensajes de renovación para mantener un estado de reserva y vía de acceso (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 cuántas veces el intervalo de renovación se puede cambiar dentro de un ciclo de renovación. Se espera que el valor por omisión de este parámetro funcione sin necesidad de sufrir modificaciones. No obstante, puede que sea necesario modificar el valor de este parámetro para evitar errores de cronometraje.

Por ejemplo, si slew-max es 30% y el intervalo de renovación es de 30 segundos, puede cambiar el intervalo de renovación un máximo de 9 segundos (30% de 30) dentro del intervalo de renovación. Para realizar un

cambio más grande, debe cambiar el intervalo de renovación otra vez. Por ejemplo, una vez que el intervalo de renovación sea 39, puede cambiarlo a más o menos 11 dentro de un intervalo de renovación. Si no, puede aumentar el "slew-max" y, a continuación, realizar el cambio. Por ejemplo, si el intervalo de renovación es 30 y desea cambiarlo a 50, primero puede aumentar el "slew-max" al 70% (proporcionándole la posibilidad de cambiar 30 en más o menos 21) y, a continuación, aumentar el intervalo de renovación a 50.

Este mandato de Talk 6 puede opcionalmente tener efecto inmediatamente y dinámicamente sin que afecte a los valores de otros parámetros.

Valores válidos: 0 - 100%

Valor por omisión: 30%

total

Debido a que la agrupación de los ancho de banda de los enlaces de todas las interfaces puede ser mayor que el rendimiento total del direccionador, puede que sea necesario establecer un límite al total de ancho de banda reservable del direccionador. Por ejemplo, la suma del ancho de banda de los enlaces agrupados puede sumar hasta 250 000 000 bps, mientras que el rendimiento total del direccionador puede ser de 200 000 000 bps. Si el total de ancho de banda reservable está establecido en 200 000 000 bps y 200 000 000 bps están actualmente reservados en todas las interfaces, no se podrán establecer más reservas IP RSVP hasta que algunas se desactiven.

Este mandato de Talk 6 puede opcionalmente tener efecto inmediatamente y dinámicamente sin que afecte a los valores de otros parámetros.

Valores válidos: de 1 a 4 294 967 295 bps

Valor por omisión: 4 294 967 295 bps (representa ilimitado)

Acceso al entorno de supervisión de RSVP

Para acceder al entorno de supervisión de RSVP, escriba **t 5** en el indicador OPCON (*):

```
* t 5
```

A continuación, escriba el siguiente mandato en el indicador **+**:

```
+ protocol rsvp
RSVP>
```

Mandatos de supervisión de RSVP

En este apartado se describen los mandatos de supervisión de RSVP. Escriba estos mandatos en el indicador RSVP>.

Tabla 29. Resumen de los mandatos de supervisión de RSVP	
Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Activate	Activa un emisor o receptor definido estáticamente.
List	Muestra la información sobre RSVP.
Reset	Restablece dinámicamente RSVP y sus características.
Send	Envía distintos mensajes RSVP, entre los que se encuentran *data-packet, ip ping, path, ptear, resv* y *rtear*.
Show	Muestra la información de los flujos RSVP activos.
Stop-RSVP	Detiene la función RSVP del direccionador.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Activate

Utilice el mandato **activate** para activar dinámicamente un receptor o emisor configurado.

Sintaxis:

a**ctivate**
número-registro

Este mandato permite activar dinámicamente los receptores o emisores que se hayan definido con los mandatos Talk 6 **add sender** y **add receiver** y que hayan sido habilitados con los mandatos correctos Talk 6 **enable**.

número-registro

Al utilizar el mandato **activate**, los receptores y emisores actualmente configurados y habilitados aparecerán y cada uno se identificará con un número de registro. Cuando especifique un número de registro, el receptor o emisor se activarán dinámicamente. Un emisor o receptor activado se puede detener en Talk 5 con el mandato **send ptear**, **send rtear** o **reset rsvp**, o al reiniciar el direccionador.

Para aprender a configurar emisores y receptores estáticos, consulte “Mandatos de configuración de RSVP” en la página 497 para obtener una descripción de los mandatos **add sender**, **add receiver** y **enable** de Talk 6.

List

Utilice el mandato **list** para mostrar la configuración RSVP actual.

Nota: Utilice el mandato **show rsvp flow** de Talk 5 para ver los flujos RSVP existentes.

Sintaxis:

l**ist** interface

opwa
sender/receiver-records-in-sram
system

interface Este mandato muestra las interfaces RSVP y su estado actual. El estado *bwCtrl* designa un enlace que está bajo el control del ancho de banda de RSVP; el ancho de banda se puede reservar para RSVP en esta interfaz. El estado *notCnf* indica un enlace que no está configurado para RSVP. El estado *up* indica que un enlace que hay configurado un enlace para RSVP pero que el ancho de banda está bajo el control de una función QoS del nivel de enlace (como la función de servicios diferenciados).

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 las 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 configurados estáticamente.

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 de los parámetros del sistema RSVP que se están ejecutando actualmente, valores que serán diferentes de aquellos en SRAM si se ha alterado alguno de ellos con los mandatos 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 distintos aspectos de la configuración RSVP. El mandato **reset** escribe encima de cualquier parámetro configurado dinámicamente con Talk 5 y en su lugar se utilizan los valores configurados más recientemente con Talk 6.

Sintaxis:

r**eset**
- interface
- queue-stat
- rsvp
- system-parameters

interface Actualiza los parámetros de la interfaz RSVP con los datos de la configuración almacenados en SRAM. El mandato le solicitará el número de interfaz.

Las reservas de la interfaz se perderán y se restablecerán durante el siguiente el periodo de renovación de los mensajes "resv" y "path", según la disponibilidad de recursos. Existe el riesgo de que algunas reservas se puedan perder si los recursos para renovarlas, como el ancho de banda, ya no se encuentran disponibles.

queue-stat
Vacía las colas de control de flujo en todas las interfaces configuradas para RSVP.

rsvp Detiene RSVP del direccionador y reinicia RSVP si éste está habilitado en SRAM.

Todos los mensajes "resv" y "path" del direccionador se borrarán cuando RSVP se detenga. Al reiniciarse RSVP, las reservas se reiniciarán durante el siguiente periodo de renovación de los mensajes "resv" y "path", según la disponibilidad de recursos. Existe el riesgo de que algunas reservas se puedan perder si los recursos para renovarlas, como el ancho de banda, ya no se encuentran disponibles.

system-parameters
Actualiza los parámetros del sistema RSVP con los datos de configuración creados en Talk 6 y almacenados en SRAM. Los parámetros del sistema RSVP son los que se han configurado con el mandato **set** de Talk 6.

Send

Utilice el mandato **send** para enviar dinámicamente mensajes RSVP y ping de IP.

Sintaxis:

se**nd**
- data-packet
- ip-ping
- path
- ptear
- resv
- rtear

data-packet

Este mandato sirve para enviar datos de prueba a través de un flujo IP definido. Puede enviar varios paquetes por segundo, según la velocidad del direccionador y las limitaciones de los recursos. Cada vez que se envíe el décimo paquete aparecerá un mensaje.

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 (eco ICMP). Consulte el mandato **ping** del capítulo “Configuración y supervisión de IP” en *Configuración y supervisión de protocolos - Manual de consulta, volumen 1*.

path

Envía un mensaje RSVP *path*, para sí mismo o como proxy para otro sistema principal. El formato de salida para el mandato es el mismo que para el mandato **add sender** de Talk 6. Consulte el mandato **add sender** de Talk 6 para obtener una descripción de los parámetros necesarios.

Por omisión, estos mensajes se envían cada 30 segundos. La vía de acceso permanece activa hasta que se elimina con el mandato **send ptear** o se restablece RSVP.

Este mandato puede añadir dinámicamente un emisor a la configuración. Puede utilizar Talk 2 para ver el rastreo ELS de las renovaciones de la vía de acceso.

ptear

Envía un mensaje RSVP *ptear*, para sí mismo o como proxy para otro sistema principal. La eliminación de una vía de acceso mediante el mandato **send ptear** suprime el flujo de tráfico y la reserva. Se le solicitarán los parámetros que identifican a una vía de acceso, por ejemplo, la dirección de destino IP y la dirección de la sesión IP. Consulte el mandato **add** de Talk 6 para obtener una descripción de los parámetros necesarios.

El estado de la vía de acceso especificado en el mandato **send ptear** debe existir o, de lo contrario, se generará un mensaje de error de ELS. Puede utilizar Talk 2 para ver los mensajes ELS relacionados con este mandato.

resv

Envía un mensaje RSVP *resv*, para sí mismo o como proxy para otro sistema principal. Se le solicitarán los parámetros que identifican a una vía de acceso, por ejemplo, la dirección de destino IP y la dirección de la sesión IP. Consulte el mandato **add** de Talk 6 para obtener una descripción de los parámetros necesarios. Puede utilizar Talk 2 para ver los mensajes ELS relacionados con este mandato. Para ver los mensajes de rastreo, debe habilitarlos con estos mandatos desde el indicador Talk 6 o Talk 5:

Ejemplo:

```
Config>event
ELS config>disp sub rsvp all
```

Si intenta ejecutar este mandato para un receptor que no tenga configurada la sesión RSVP, aparecerá el mensaje `Inputting session does not exist`. Utilice el mandato **show rsvp flow** para mostrar 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 solicitante debe ser una dirección de unidifusión IP.

2 La dirección de la sesión IP, que es la dirección de destino de la sesión, puede ser una dirección de unidifusión IP del receptor o una dirección de multidifusión IP de un grupo multidifusión del que el receptor sea miembro.

3 Observe que el campo *Rsvd* (Reservado) de la entrada del flujo cambia de N (No) a Y (Sí) después de realizar la reserva. Si este valor es N, existirá un flujo, pero no habrá reserva. El flujo se enviará con QoS optimizado.

4 El rastreo ELS de Talk 2 muestra las renovaciones de la reserva enviadas por omisión cada 30 segundos.

rtear

Envía un mensaje RSVP *rsvtear*, para sí mismo o como proxy para otro sistema principal. Este mandato sirve para desconectar un flujo de tráfico RSVP pero no para eliminar la vía de acceso del emisor, por lo tanto el flujo de tráfico IP continuará con QoS optimizado. El mandato le solicitará los parámetros que identifican a un flujo de tráfico RSVP, por ejemplo, la dirección de la sesión IP y la dirección de destino del receptor. Consulte el mandato **add** de Talk 6 para obtener una descripción de los parámetros necesarios.

El flujo de tráfico IP especificado en el mandato **send rtear** debe existir o, de lo contrario, se generará un mensaje de error de ELS. Puede utilizar Talk 2 para ver los mensajes ELS relacionados con este mandato.

Show

Utilice el mandato **show** para mostrar distintos aspectos de RSVP.

Sintaxis:

s**how**

- adspec
- classifier
- ds
- flowspec
- queue
- rsvp
  - flows
  - senders
  - sessions
  - reservations
  - requests
- vc

adspec

Muestra el spec de anuncio (adspec) de todos los flujos. Adspec es la salida de OPWA y muestra la información sobre los parámetros reservados en cada enlace de la ruta de la sesión RSVP activa.

classifier

Muestra todas las entradas del flujo QoS del clasificador de paquetes RSVP y/o la antememoria IP.

ds Muestra las reservas actuales de los enlaces de servicios diferenciados (DS). El campo streamID permite que el usuario correlacione las reservas con las que muestra el mandato **show stream** de la función DS.

flowspec

Muestra el tspec del emisor, el tspec de la reserva y el tspec de petición que se encuentran actualmente en las tablas de estado RSVP.

queue

Muestra las estadísticas actuales de las colas de software de RSVP.

rsvp

Muestra aspectos del estado de conexión RSVP actual.

flows Muestra los flujos de tráfico RSVP activos. Consulte el ejemplo del mandato **send resv** de Talk 5 para obtener un ejemplo de este mandato.

senders Muestra los emisores RSVP. Los emisores pueden estar configurados pero no necesariamente activados.

sessions Muestra las sesiones RSVP, tanto las sesiones activas que tienen reservados flujos como las inactivas existentes pero sin reservas por el momento.

reservations
Muestra las reservas RSVP.

requests Muestra las peticiones RSVP.

Stop-RSVP

Utilice el mandato **stop-rsvp** para detener la función RSVP del direccionador.

Sintaxis:

stop
rsvp

Utilización de SNMP

En este capítulo se describe SNMP. Consta de los siguientes apartados:

- "Gestión de red"
- "Gestión SNMP"

Gestión de red

En la publicación *IBM 2212 Guía de introducción y planificación* hallará información sobre la gestión de red.

Gestión SNMP

El IBM 2212 proporciona una interfaz SNMP (protocolo simple de gestión de red) destinada a aplicaciones y plataformas de gestión de red tales como los productos Nways Campus Manager.

El protocolo SNMP se utiliza para supervisar y gestionar sistemas principales IP de una red IP y funciona a través de un software denominado agente SNMP que permite que los sistemas principales de la red lean y modifiquen algunos parámetros operativos del IBM 2212. De este modo, SNMP establece la gestión de red para la comunidad IP.

Es necesario tener en cuenta los siguientes aspectos a la hora de configurar SNMP en el IBM 2212.

Comunidad
La comunidad le permite definir la dirección IP de la estación de gestión SNMP a la que se permite acceder a la información contenida en la Base de información de gestión (MIB) del agente SNMP. El nombre de la comunidad se define para utilizarlo al acceder a MIB.

Autenticación
El nombre de la comunidad se utiliza como método de autenticación para evitar que los usuarios no autorizados accedan a la información de un agente SNMP o modifiquen sus características.

Este método incluye la definición de uno o más conjuntos de datos MIB (denominados vistas MIB) y la asociación de un privilegio de acceso (sólo-lectura, sólo-escritura), una máscara IP y un nombre de comunidad con cada vista MIB. La máscara IP establece qué direcciones IP pueden originar peticiones de acceso para una determinada vista y el nombre de la comunidad sirve como contraseña que debe coincidir con las peticiones SNMP. El nombre de la comunidad viene incluido en cada mensaje SNMP y es verificado por el agente SNMP del IBM 2212. Una petición SNMP es rechazada cuando no proporciona el nombre de comunidad correcto, cuando no coincide con la máscara IP o cuando intenta un acceso que no concuerda con el privilegio de acceso asignado.

Contraseña SNMP
La contraseña SNMP se utiliza para cifrar y autenticar objetos MIB que deben protegerse, tales como una contraseña o clave de cifrado en la sección del perfil de usuario de la función de autenticación. El establecimiento de una

contraseña SNMP de longitud cero indica que no se puede acceder a los datos confidenciales. Cuando la contraseña SNMP se establece en *clear*, los datos son accesibles a través de SNMP sin cifrado. Cuando la contraseña SNMP se establece en otros valores, los datos se podrán recuperar con cifrado y autenticación usando una clave derivada de la contraseña SNMP. Para obtener más información, consulte la definición de MIB.

Soporte MIB

Una MIB es un almacén de información virtual que proporciona acceso a información de gestión. Esta información se define como objetos MIB a los que se puede acceder y, en algunos casos, modificables con herramientas de gestión de la red.

El IBM 2212 proporciona un conjunto completo de objetos MIB estándar, de objetos MIB para supervisar y gestionar recursos específicos de la empresa, y de archivos README

Los archivos README que que constituyen la documentación del soporte MIB del IBM 2212 se hallan en la World Wide Web; para consultarlos, se debe acceder al directorio del release pertinente en el URL siguiente:

ftp://ftp.nways.raleigh.ibm.com/pub/netmgmt/2212/

Para recibir una copia de una MIB específica, escriba 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.

Desde el sitio ftp, puede acceder a la siguiente información:

- MIB estándar
- MIB de empresa
- Capturas genéricas SNMP
- MIB específicas de empresa
- Valores definibles

Las capturas genéricas SNMP, las MIB de empresa y los valores definibles se encuentran en los archivos README.

Todos los objetos MIB se implementan como objetos de sólo-lectura, aunque su cláusula de acceso esté definida como de lectura-escritura o de lectura-creación, excepto aquellos objetos MIB identificados en el archivo README que admitan SET a objetos que tengan su cláusula de acceso definida como de lectura-escritura o de lectura-creación.

Mensajes de captura

Los mensajes de captura son mensajes no solicitados enviados desde el agente SNMP del dispositivo a un gestor SNMP en respuesta a un problema de red o dispositivo, caso de la recarga del dispositivo o de la desactivación de la red.

Configuración y supervisión de SNMP

En este capítulo se describen los mandatos de configuración y supervisión de SNMP. Consta de los siguientes apartados:

Acceso al entorno de configuración de SNMP

Para acceder al entorno de configuración de SNMP, escriba el siguiente mandato en el indicador `Config>`:

```
Config> protocol snmp
SNMP user configuration
SNMP Config>
```

Mandatos de configuración de SNMP

En este apartado se describen los mandatos de configuración de SNMP.

En la Tabla 30 en la página 518 se listan los mandatos de configuración de SNMP. Los mandatos de configuración de SNMP le permiten especificar parámetros que sirven para definir la relación entre el agente SNMP y la estación de gestión de la red. La información especificada tiene efecto inmediatamente después del reinicio o recarga del IBM 2212.

Especifique los mandatos de configuración de SNMP en el indicador `SNMP Config>`.

Tabla 30. Resumen de los mandatos de configuración de SNMP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
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	Inhabilita el protocolo SNMP y las capturas relacionadas con las comunidades nombradas.
Enable	Habilita el protocolo SNMP y las capturas relacionadas con las comunidades nombradas.
List	Muestra las comunidades actuales con sus modalidades de acceso asociadas, las capturas habilitadas, las direcciones IP y las vistas. Muestra también todas las vistas y sus subárboles de MIB asociados.
Set	Establece la vista o modalidad de acceso de una comunidad. La modalidad de acceso de una comunidad puede ser una de las siguientes: Lectura y generación de captura Lectura, escritura y generación de captura Sólo generación de captura Este mandato se utiliza también para establecer un puerto UDP de captura y para establecer la contraseña utilizada para cifrar y autenticar los datos confidenciales.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Tabla 31 (Página 1 de 2). Resumen de las opciones de los mandatos de configuración de SNMP

MANDATO	PARÁMETRO 1	PARÁMETRO 2	PARÁMETRO 3	PARÁMETRO 4	VALOR POR OMISIÓN
add	community	<nomb_comunid>			Ninguno
	address	<nomb_comunid>	<dir_IP>	<másc_IP>	
	sub_tree	<nombre_vista>	<oid>		
delete	community	<nomb_comunid>			
	address	<nomb_comunid>	<dir_IP>	<másc_IP>	
	sub_tree	<nombre_vista>	<oid>		
disable	snmp				
	trap	all	<nomb_comunid>		
		cold_start	<nomb_comunid>		
		link_down	<nomb_comunid>		
		link_up	<nomb_comunid>		

Tabla 31 (Página 2 de 2). Resumen de las opciones de los mandatos de configuración de SNMP

MANDATO	PARÁMETRO 1	PARÁMETRO 2	PARÁMETRO 3	PARÁMETRO 4	VALOR POR OMISIÓN
		auth_fail	<nomb_comunid>		
		enterprise	<nomb_comunid>		
enable	snmp				
	trap	all	<nomb_comunid>		
		cold_start	<nomb_comunid>		
		link_down	<nomb_comunid>		
		link_up	<nomb_comunid>		
		auth_fail	<nomb_comunid>		
		enterprise	<nomb_comunid>		
list	all				
	community	access			access
		traps			
		address			255.255.255.255
		view			all
	views				
set	community	access	read_trap	<nomb_comunid>	
			write_read_trap	<nomb_comunid>	
			trap_only	<nomb_comunid>	
		view	<comunidad>	all	all
				<nombre_vista>	
	trap_port	<puerto_udp>			
	password				
exit					

Add

Utilice el mandato **add** para añadir un nombre de comunidad a la lista de comunidades SNMP, añadir una dirección a una comunidad o 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 un acceso read_trap, una vista de todas las capturas inhabilitadas y todas las direcciones IP permitidas.

Nota: Para seleccionar un tipo de acceso o control de captura, utilice el mandato **set community access** para asignar tipos de acceso a comunidades SNMP existentes y utilice el mandato **enable trap** o **disable trap** para el control de las capturas.

community name

Proporciona el 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 por el parámetro Community IP address.

Valores válidos: una serie de 1 a 31 caracteres alfanuméricos. No se admitirán caracteres tales como espacios, tabuladores o secuencias de la tecla <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 la comunidad la dirección de una estación de gestión de red autorizada para comunicarse con esta unidad. Debe proporcionar el nombre de la comunidad y la dirección de red (en notación a.b.c.d estándar). Puede también proporcionar una máscara de red para restringir el acceso a un sistema principal individual (máscara = 255.255.255.255) o a una red de sistemas principales. Se puede añadir más de una dirección a una comunidad, para ello, escriba el mandato cada vez que desee añadir otra dirección.

Si no especifica una dirección para la comunidad, se manejarán solicitudes desde cualquier sistema principal.

Las direcciones también especifican sistemas principales que reciben las capturas. Si no se ha especificado ninguna dirección, no se producirá ninguna captura.

community name

Valores válidos: una serie de 1 a 31 caracteres alfanuméricos. No se admitirán caracteres tales como espacios, tabuladores o secuencias de la tecla <ESC>.

Valor por omisión: ninguno

IP address

Valores válidos: cualquier dirección IP válida

Valor por omisión: 0.0.0.0

IP mask Puede también proporcionar una máscara de red para restringir el acceso a un sistema principal individual (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 nueva vista. El valor por omisión es toda la MIB. El mandato **add sub_tree** se utiliza para gestionar vistas MIB. Se puede añadir más de un subárbol a una vista definida por <nombre_vista>.

view name

Especifica el nombre de la vista que se va a crear.

Valores válidos: Cualquier serie de hasta 31 caracteres alfanuméricos de longitud. No se admitirán caracteres tales como espacios, tabuladores o secuencias de la tecla <Esc>.

Valor por omisión: ninguno

Nota: Debe asignar una vista a una o más comunidades con el mandato **set community view** para hacer que tenga efecto. Las definiciones de los subárboles están incluidas, es decir, el OID del subárbol especificado y cualquier OID que sea lexicográficamente mayor que el OID especificado se considera parte de la vista MIB.

Si se añade una comunidad con el mandato **add community**, todas las vistas MIB admitidas se asignarán a la comunidad a menos que se utilice el mandato **set community view** para asignar vistas específicas a la comunidad.

MIB OID name

Especifica el ID de objeto MIB para el subárbol. Se debe especificar como valor numérico y no como valor simbólico.

Este parámetro contiene un nombre de subárbol MID incluido en la vista definida con el parámetro View name. Todos los hijos de un subárbol MIB especificado están también incluidos en la vista.

Por ejemplo, para proporcionar una vista que diese acceso al grupo del sistema en MIB-II, especifique **1.3.6.1.2.1.1**.

Valores válidos:

Un identificador de objetos en la forma <elemento1>.<elemento2>.<elemento3>. . ., donde:

- Necesita un mínimo de 1 elemento. Como todos los OID de la MIB empiezan por *1.3.6.1*, el número mínimo de elementos que es necesario proporcionar para que la vista difiera de *todos*, es 5 (1.3.6.1.X).
- Puede definir un máximo de 31 caracteres, incluidos los puntos (.) usados como separadores.
- Todos los elementos que vienen después de los cuatro primeros (*1.3.6.1*) son enteros entre 0 y 127.

Nota: Este valor debe ser numérico en notación punteada, y *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 eliminar una comunidad y todas sus direcciones, una dirección específica o un subárbol de una vista.

Sintaxis:

delete community
address
sub_tree

community

Elimina una comunidad y sus direcciones 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 por el parámetro Community IP address.

Valores válidos: una serie de 1 a 31 caracteres alfanuméricos. No se admitirán caracteres tales como espacios, tabuladores o secuencias de la tecla <ESC>.

Valor por omisión: ninguno

Ejemplo:

```
SNMP Config> delete community
Community Name []?
```

address Elimina una dirección de una comunidad. Debe proporcionar el nombre.

community name

Especifica el nombre de la comunidad de la que se eliminará 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 por el parámetro Community IP address.

Valores válidos: una serie de 1 a 31 caracteres alfanuméricos. No se admitirán caracteres tales como espacios, tabuladores o secuencias de la tecla <ESC>.

Valor por omisión: public

IP address

Especifica la dirección IP que se va a eliminar.

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 proporcionar el nombre del subárbol. Si se eliminan todos los subárboles, la vista de la MIB también se suprime y se eliminan todas las referencias a ella hechas desde cualquier comunidad SNMP asociada.

view name

Especifica la vista utilizada por la comunidad definida en el parámetro **community name**. Esta vista determina los objetos MIB a los que esta comunidad puede acceder. Si no se ha especificado ninguna vista, la comunidad puede acceder a todos los objetos conocidos por el agente SNMP del dispositivo.

Se debe responder a este parámetro si decide restringir a una comunidad el acceso a toda la MIB gestionada por el agente SNMP del dispositivo.

Valor por omisión: ninguno

MIB OID name

Especifica el ID de objeto MIB para el subárbol. Se debe especificar como valor numérico y no como valor simbólico.

Este parámetro contiene un nombre de subárbol MID incluido en la vista definida con el parámetro View name. Todos los hijos de un subárbol MIB especificado están también incluidos en la vista.

Valores válidos: Un identificador de objetos en la forma <elemento1>.<elemento2>.<elemento3>. . ., donde:

- Necesita un mínimo de 1 elemento. Como todos los OID de la MIB empiezan por *1.3.6.1*, el número mínimo de elementos que es necesario proporcionar para que la vista difiera de *todos*, es 5 (1.3.6.1.X).
- Puede definir un máximo de 31 caracteres, incluidos los puntos (.) usados como separadores.
- Todos los elementos que vienen después de los cuatro primeros (*1.3.6.1*) son enteros entre 0 y 127.

Valor por omisión: ninguno

Ejemplo:

```
SNMP Config> delete sub_tree
View name[]?
MIB OID[]?
```

Disable

Utilice el mandato **disable** para inhabilitar el protocolo SNMP o determinadas capturas del dispositivo.

Sintaxis:

disable snmp

trap
sram-write

snmp Inhabilita SNMP.

Ejemplo: `disable snmp`

trap *tipo-captura*
Inhabilita capturas especificadas o todas las capturas.

tipo-captura
Especifica el tipo de captura que se debe inhabilitar. Los tipos de capturas válidas aparecen en la Tabla 32.

community name

Valores válidos: una serie de 1 a 31 caracteres alfanuméricos. No se admitirán caracteres tales como espacios, tabuladores o secuencias de la tecla <ESC>.

Valor por omisión: ninguno

Ejemplo:

```
SNMP Config> disable trap link_up
Community name []?
```

sram-write

Tabla 32. Tipos de capturas SNMP

Tipo de captura	Descripción
all	Especifica todas las capturas de una comunidad especificada.
cold_start	Una captura "cold start" significa que el dispositivo transmisor se está reinicializando y que se puede haber modificado la implementación de la entidad del protocolo o la configuración del agente.
link_down	Una captura "link_down" reconoce un error en uno de los enlaces de comunicación representados en la configuración del agente. La PDU-captura "link_down" contiene el nombre y el valor de las instancias iflndex para el enlace en cuestión como primer elemento de sus enlaces-variables.
link_up	Una captura "link_up" reconoce que se ha activado un enlace anteriormente inactivo en la red. La PDU-captura "link_up" contiene el nombre y el valor de las instancias iflndex para el enlace en cuestión como primer elemento de sus enlaces-variables.
auth_fail	Las capturas "auth_fail" indican que el remitente de la petición SNMP no posee el permiso correcto para comunicarse con el agente SNMP de esta unidad.
enterprise	Las capturas específicas de empresa indican que se ha producido algún suceso específico de empresa. El campo de captura específica identifica la captura particular que se haya producido. Por ejemplo, cuando se configuran con este fin, los mensajes de sucesos de ELS se envían en capturas específicas de empresa.

Enable

Utilice el mandato **enable** para habilitar el protocolo SNMP o las capturas especificadas del dispositivo.

Sintaxis:

enable snmp

trap

sram-write

snmp Habilita SNMP

Ejemplo: `enable snmp`

trap *tipo-captura*
Habilita capturas especificadas o todas las capturas.

tipo-captura
Especifica el tipo de captura habilitada. Los tipos de capturas válidas aparecen en la Tabla 32 en la página 524.

community name

Valores válidos: una serie de 1 a 31 caracteres alfanuméricos. No se admitirán caracteres tales como espacios, tabuladores o secuencias de la tecla <ESC>.

Valor por omisión: ninguno

sram-write

List

Utilice el mandato **list** para mostrar la configuración actual de las comunidades SNMP, las modalidades de acceso, las capturas, las direcciones de red y las vistas.

Sintaxis:

list all

community

views

list all Muestra la configuración actual de las comunidades SNMP para las opciones Access, Traps, Address y View. Consulte la descripción del mandato **list community** para obtener información detallada 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 acceso, dirección, capturas y vista.

Opción	Descripción
Access	Muestra las modalidades de acceso de la comunidad.
Address	Muestra la dirección de red de la comunidad.
Traps	Muestra los tipos de capturas generados para la comunidad.
View	Muestra la vista MIB para 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 de la 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 establecer el número de puerto de captura UDP de SNMP o para establecer la modalidad de acceso de la comunidad o la 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 proporcionar el nombre de la comunidad y el tipo de acceso.

opciones Elija una opción de la lista siguiente:

read_trap

Permite el acceso de lectura y de generación de capturas a la comunidad nombrada.

write_read_trap

Permite el acceso de lectura y escritura y de generación de capturas a la comunidad especificada.

trap_only

Indica que la comunidad sólo se utiliza al enviar una captura SNMP.

nomb_comunid

El **nombre de la comunidad** tiene:

Valores válidos: una serie de 1 a 31 caracteres alfanuméricos.

No se admitirán caracteres tales como espacios, tabuladores o secuencias de la tecla <ESC>.
Valor por omisión: ninguno

Ejemplo: `set community access <opciones> nomb_comunid`

community view

Utilice el mandato **set community view** para asignar una vista MIB a una comunidad.

nomb_comunid

Valores válidos: una serie de 1 a 31 caracteres alfanuméricos. No se admitirán caracteres tales como espacios, tabuladores o secuencias de la tecla <ESC>.

Valor por omisión: ninguno

all Permite acceder a todos los objetos MIB de la comunidad nombrada. El valor por omisión es "all" (todos).

nombre_vista

Asigna una vista MIB especificada a la comunidad nombrada.

Ejemplo: `set community view nomb_comunid <all o nombre_vista>`

trap_port Utilice el mandato **set trap_port** para especificar un número de puerto UDP, distinto del puerto 162 estándar predeterminado, al que enviar capturas.

Valor por omisión: standard port (puerto estándar)

Ejemplo: `set trap_port puerto_udp`

UDP Port Number

Especifica un protocolo de datagrama de usuario distinto del puerto UDP estándar.

Valor por omisión: 162

password

Utilice el mandato set password para especificar la contraseña para cifrar y autenticar los objetos MIB confidenciales definidos en la MIB. El establecimiento de la contraseña en una serie de longitud cero proporciona la máxima seguridad al impedir cualquier acceso o definición de objetos MIB confidenciales. El establecimiento de la contraseña en "clear" proporciona el nivel mínimo de seguridad al permitir que los datos fluyan sin autenticación. El establecimiento de la contraseña en cualquier otro valor permite el acceso y la definición de objetos MIB confidenciales que están cifrados y autenticados con esta contraseña.

Ejemplos:

(a) establecer la contraseña en 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) establecer la contraseña en "clear":

```
SNMP Config>set pa
Password:
to verify Enter password again:
Password is set to "clear". (WARNING: security data flow in clear)
```

(c) establecer la contraseña en "test":

```
SNMP Config>set pa
Password:
to verify Enter password again:
Password is set. (security data flow encrypted)
```

Acceso al entorno de supervisión de SNMP

Para acceder al entorno de supervisión de SNMP, escriba **t 5** en el indicador OPCON (*):

```
* talk 5
```

A continuación, escriba el siguiente mandato en el indicador **+**:

```
+ protocol snmp
SNMP>
```

Mandatos de supervisión de SNMP

En este apartado se describen los mandatos de supervisión de SNMP.

En la Tabla 33 en la página 530 aparecen los mandatos de supervisión de SNMP. Los mandatos de supervisión de SNMP le permiten ver los parámetros de la configuración de SNMP y visualizar algunas estadísticas relacionadas con el agente SNMP.

Se pueden realizar cambios temporales en los parámetros SNMP de ejecución mediante el proceso de supervisión. Estos cambios afectarán inmediatamente al funcionamiento del agente SNMP. Si desea hacer que los cambios temporales sean permanentes, utilice entonces el mandato SAVE. Si necesita restaurar la configuración de SNMP original, utilice el mandato **reset**. Este mandato le permite alterar de forma temporal el comportamiento del agente SNMP, sin necesidad de cambiar permanentemente la configuración. Para que los cambios temporales tengan efecto, debe SALIR (EXIT) del proceso de supervisión de SNMP.

Escriba los mandatos de supervisión de SNMP en el indicador SNMP>.

Tabla 33. Resumen de los mandatos de supervisión de SNMP	
Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
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	Inhabilita las capturas relacionadas con las comunidades especificadas. La inhabilitación de SNMP o SRAM_write se debe realizar con el entorno de configuración `SNMP Config>`.
Enable	Habilita las capturas relacionadas con las comunidades especificadas. La habilitación de SNMP o SRAM_write se debe realizar a través del entorno de configuración `SNMP Config>`.
List	Muestra la configuración actual de las comunidades SNMP, las vistas, las modalidades de acceso, las capturas y las direcciones de red.
Reset	Actualiza la configuración de SNMP con los valores de la configuración de SNMP almacenada actualmente.
Save	Toma los cambios especificados y los guarda en la configuración de SNMP de forma permanente.
Set	Establece la vista o modalidad de acceso de una comunidad. La modalidad de acceso de una comunidad puede ser una de las siguientes: • Lectura y generación de captura • Lectura, escritura y generación de captura • Sólo generación de captura Permite también establecer la contraseña y el puerto UDP. Consulte 528 para obtener más información.
Statistics	Muestra las estadísticas del agente SNMP.
Reset	Actualizar la configuración de SNMP con los valores de la configuración de SNMP almacenada actualmente.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Add

Utilice el mandato **add** para añadir un nombre de comunidad a la lista de comunidades SNMP, añadir una dirección a una comunidad o asignar una parte de la MIB (subárbol) a una vista.

Para obtener información sobre cómo utilizar el mandato **add**, consulte “Add” en la página 519.

Delete

Utilice el mandato **delete** para eliminar:

- Una dirección específica.
- Una comunidad y todas sus direcciones.
- Un subárbol de una vista.

Para obtener información sobre cómo utilizar el mandato **delete**, consulte “Delete” en la página 522.

Disable

Utilice el mandato **disable** para inhabilitar capturas especificadas del dispositivo.

Para obtener información sobre cómo utilizar el mandato **disable**, consulte “Disable” en la página 523.

Enable

Utilice el mandato **enable** para habilitar capturas especificadas del dispositivo.

Para obtener información sobre cómo utilizar el mandato **enable**, consulte “Enable” en la página 525.

List

Utilice el mandato **list** para visualizar la configuración actual de las direcciones de red, las capturas, las modalidades de acceso, las vistas y las comunidades SNMP.

Sintaxis:

list	all
	community
	views

Para obtener información sobre cómo utilizar el mandato **list**, consulte “List” en la página 525.

Reset

Utilice el mandato SNMP **reset** para actualizar la configuración de SNMP con los valores de la configuración de SNMP almacenada actualmente. Esta acción permite realizar cambios en la configuración de SNMP actual al reiniciar o recargar el dispositivo.

Save

Utilice el mandato **save** para guardar permanentemente los cambios especificados.

Set

Para obtener más información sobre cómo utilizar el mandato **set**, consulte “Set” en la página 527.

Statistics

Utilice el mandato **statistics** para visualizar las estadísticas del agente SNMP.

Sintaxis:

statistics

Ejemplo: `statistics`

```
                Max       Current    Current
               Alloc      Alloc       In Use

SNMP agent:   512000      181144     133120

SNMP MIBs:   1048576       57976      19712
```

Aparecerá la siguiente información:

Max Alloc
Cantidad máxima de memoria (en bytes) reservada para el componente SNMP.

Current Alloc
Cuando se necesita memoria, se toma de la agrupación reservada (designada como MAX ALLOC) y se traslada a una agrupación de memoria "activa". El tamaño de esta agrupación de memoria "activa" se indica mediante el valor CURRENT ALLOC.

Current In Use
Este valor representa la memoria actualmente asignada a partir de la agrupación de memoria "activa" (designada como CURRENT ALLOC) que está utilizando el componente SNMP.

Soporte de reconfiguración dinámica de SNMP

En este apartado se describe el modo en que la reconfiguración dinámica (DR) afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

SNMP da soporte al mandato **delete interface** de CONFIG (Talk 6) con la matización siguiente:

Cuando se suprima la interfaz de red, se eliminarán todas las filas de las tablas MIB indexadas por la instancia ifIndex asociada.

Mandato activate interface de GWCON (Talk 5)

SNMP da soporte al mandato **activate interface** de GWCON (Talk 5) con la matización siguiente:

Cuando se suprima la interfaz de red, se crearán todas las filas de las tablas MIB indexadas por la instancia ifIndex asociada.

Todos los mandatos específicos de interfaz SNMP están soportados por el mandato **activate interface** de GWCON (Talk 5).

Mandato reset interface de GWCON (Talk 5)

SNMP da soporte al mandato **reset interface** de GWCON (Talk 5) con la matización siguiente:

> Cuando se restablezca la interfaz de red, se conservarán todas las filas de las tablas MIB indexadas por la instancia ifIndex asociada, pero los valores de objeto pueden ser diferentes.

Todos los mandatos específicos de interfaz de SNMP están soportados por el mandato **reset interface** de GWCON (Talk 5).

Mandatos de restablecimiento de componente de GWCON (Talk 5)

SNMP da soporte a los mandatos **reset** de GWCON (Talk 5) específicos de SNMP siguientes:

Mandato GWCON, protocol SNMP, reset

Descripción: El agente SNMP activa todos los valores de configuración de SNMP cambiados.

Efecto en la red: El acceso al agente SNMP puede eliminarse o restringirse en función de la nueva configuración.

Limitaciones:

- No es posible utilizar el mandato **reset** para habilitar SNMP si se ha inhabilitado anteriormente. Es necesario rearrancar.

En la tabla siguiente se resumen los cambios de configuración de SNMP que se activan cuando se invoca el mandato **GWCON, protocol SNMP, reset**:

Mandatos cuyos cambios los activa el mandato GWCON, protocol SNMP, reset
CONFIG, protocol SNMP, add address
CONFIG, protocol SNMP, add community
CONFIG, protocol SNMP, add sub_tree
CONFIG, protocol SNMP, delete address
CONFIG, protocol SNMP, delete community
CONFIG, protocol SNMP, delete sub_tree
CONFIG, protocol SNMP, disable trap
CONFIG, protocol SNMP, disable snmp
CONFIG, protocol SNMP, set community
CONFIG, protocol SNMP, set password
CONFIG, protocol SNMP, set trap_port

Mandatos de cambio temporal de GWCON (Talk 5)

SNMP da soporte a los mandatos de GWCON que cambian de forma temporal el estado operativo del dispositivo indicados más abajo. Los cambios se pierden cada vez que se vuelve a cargar o iniciar el dispositivo o que se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
GWCON, protocol SNMP, add address
GWCON, protocol SNMP, add community
GWCON, protocol SNMP, add sub_tree
GWCON, protocol SNMP, delete address
GWCON, protocol SNMP, delete community
GWCON, protocol SNMP, delete sub_tree
GWCON, protocol SNMP, disable trap
GWCON, protocol SNMP, disable snmp
GWCON, protocol SNMP, set community
GWCON, protocol SNMP, set password

Mandatos no reconfigurables dinámicamente

En la tabla siguiente figuran los mandatos de configuración de SNMP que no pueden cambiarse dinámicamente. Para activar estos mandatos, es necesario volver a cargar o a arrancar el dispositivo.

Mandatos
CONFIG, protocol SNMP, enable snmp

Utilización de DLSw

En este capítulo se describe el protocolo DLSw (Data Link Switching) y su implementación. Las modificaciones realizadas en el indicador `Config>` no tienen efecto de forma inmediata, pero forman parte de la configuración de SRAM utilizada para los subsiguientes reinicios del direccionador. Para obtener una descripción de las modificaciones de configuración temporales, pero inmediatas, consulte la página 606.

El 2212 ofrece una gran variedad de funciones que le permiten integrar tráfico NetBIOS (Network Basic Input/Output System) y SNA (Arquitectura de red de sistemas) 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 puenteo del direccionador, en el protocolo SSP (Switch-to-Switch Protocol) y en TCP/IP para proporcionar un transporte fiable de tráfico SNA sobre una interred. DLSw no proporciona funciones completas de direccionamiento, pero proporciona conmutación en la capa de enlace de datos. En lugar de enviar tramas LLC2 por puente, DLSw encapsula sus datos en tramas TCP y reenvía los mensajes resultantes a través del enlace WAN hacia un direccionador DLSw asociado, para entregarlos a las direcciones de estación final previstas.

Cómo funciona DLSw

LLC2, SDLC y QLLC son protocolos orientados a la conexión. DLSw proporciona las características dinámicas de los protocolos direccionables ***y*** preserva las características de control y fiabilidad de extremo a extremo para una comunicación eficiente.

Problemas de la solución de puenteo

La Figura 41 en la página 536 ilustra el enfoque tradicional del puenteo de tramas LLC2 a través de enlaces WAN. Con el enfoque tradicional, los retrasos de red se producen con mucha más frecuencia en la WAN que en una LAN. Estos retrasos pueden ser producidos por simple congestión de la red, por velocidades de línea más bajas, o por otros factores. Sea cual sea la causa, estos retrasos incrementan las posibilidades de tiempos excedidos de sesión y de que los datos no lleguen a su destino.

Además, los protocolos de LAN, como LLC2, utilizan tiempos de respuesta/retransmisión bastante más cortos que las redes WAN. Por esto las conexiones de extremo a extremo a través de una WAN son muy difíciles de mantener y tiempos excedidos de sesión mucho más probables.

Además de tiempos excedidos de sesión, surge un problema importante cuando los datos se retrasan al cruzar la WAN. Una estación emisora puede reenviar datos que se han retrasado (pero no perdido); como consecuencia de esto, puede suceder que estaciones finales LLC2 reciban datos duplicados. Los datos duplicados pueden causar confusión a los procedimientos LLC2 en el lado receptor, que a su vez pueden provocar un uso ineficiente del enlace WAN.

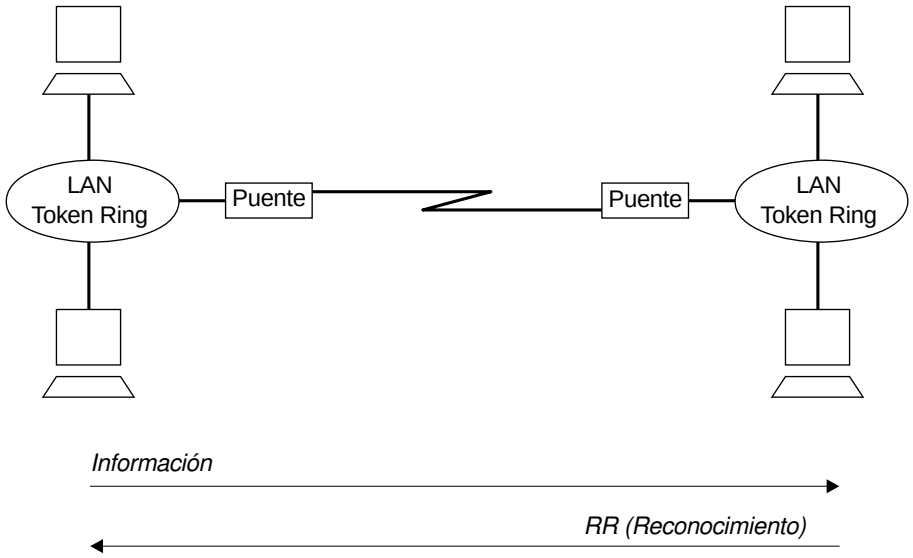


Figura 41. Enfoque tradicional del puenteo a través de enlaces WAN

El ejemplo anterior muestra un puenteo tradicional con control de enlace de datos de extremo a extremo. Al tratarse de un protocolo sin conexión, el puenteo no asegura la integridad del tráfico LLC en la WAN.

Suplantación de protocolo

Para reducir la posibilidad de tiempos excedidos de sesión, y para mantener el aspecto de conectividad de extremo a extremo para las estaciones emisoras, DLSw finaliza o “suplanta” conexiones LLC2 en el direccionador local. Al recibir una trama LLC2, el direccionador envía un acuse de recibo a la estación emisora. Este acuse de recibo indica al emisor que se han recibido los datos transmitidos previamente.

El acuse de recibo evita que la estación vuelva a transmitir los datos. A partir de este punto, es responsabilidad del software DLSw que los datos lleguen a su destino. El software cumple con esta misión encapsulando los datos en tramas IP direccionables, y transportándolas a continuación (a través de TCP) hacia un DLSw asociado. El direccionador DLSw asociado elimina las cabeceras TCP, determina la dirección del destino de los datos y establece una nueva conexión LLC2 con la estación final.

La Figura 42 en la página 537 ilustra la relación entre dos direccionadores DLSw asociados, cada uno conectado a una red en anillo.

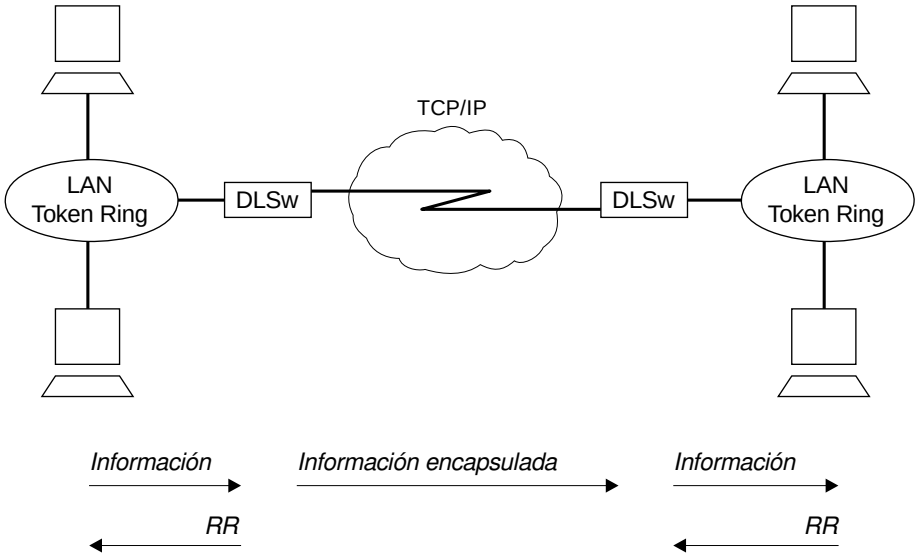


Figura 42. Conmutación de enlace de datos sobre la WAN

DLSw finaliza la conexión LLC2 en el direccionador. Esto significa que las conexiones LLC2 no cruzan la red de área amplia. Esto reduce los tiempos excedidos de sesión y los acuses de recibo (RR) que de otra forma atravesarían los enlaces de área amplia.

Ventajas de DLSw

Debido a que DLSw finaliza la conexión DLC en el dispositivo local (ver la Figura 42), DLSw es especialmente efectivo para eliminar tiempos excedidos de sesión SNA y reducir la actividad general de WAN en circuitos compartidos. El protocolo tiene las siguientes ventajas principales:

- Reduce la posibilidad de tiempos excedidos de sesión finalizando el tráfico de control LLC2, SDLC y QLLC en el dispositivo local.
- Reduce la actividad general de WAN eliminando la necesidad de transmitir acuses de recibo (RR) a través del área amplia. Los RR se confinan a la LAN de forma local para cada direccionador DLSw.
- Proporciona control de flujo y de congestión, y control de difusión de paquetes de búsqueda, entre direccionadores DLSw y sus estaciones finales conectadas.
- Incrementa los límites de cuenta de saltos del puenteo de direccionamiento en origen.
- Permite la conversión de protocolo entre LLC2, SDLC y QLLC.
- Da soporte al tráfico NetBIOS.

Utilización de las funciones de DLSw

Las siguientes secciones describen la utilización de varias funciones de DLSw:

- “Conexiones TCP, descubrimiento de vecinos y exploración de multidifusión” en la página 538
- “Soporte de dispositivos LLC” en la página 541
- “Soporte de dispositivos SDLC” en la página 541

- "Soporte de dispositivos QLLC" en la página 545
- "Soporte de interfaz APPN" en la página 551
- "Utilización de la función de prioridad de vecino" en la página 552
- "Reparto del tráfico SNA y NetBIOS" en la página 553

Conexiones TCP, descubrimiento de vecinos y exploración de multidifusión

DLSw utiliza TCP para proporcionar una entrega fiable y ordenada de información de usuario final a través de una red IP. Los formatos de mensaje DLSw permiten transportar múltiples sesiones de estación final o múltiples circuitos a través de una única conexión de transporte TCP. Hay tres formas de configurar qué direccionadores con capacidad de DLSw deben tener conexiones de transporte TCP entre ellos para permitir la conectividad deseada de estación final:

- Configurar las direcciones IP del direccionador vecino en uno o en los dos direccionadores de cada par. Este es el método más básico y está soportado por todos los proveedores de direccionadores DLSw.
- Configurar la pertenencia a grupos de multidifusión en cada direccionador, permitiendo a los direccionadores descubrir las direcciones IP de los demás de forma dinámica. Esta es una función especial de DLSw de este producto, para facilitar la pesada tarea de configurar direcciones IP de vecino.

Configuración de vecinos TCP

Para configurar una dirección IP de vecino en un direccionador, utilice el mandato **add tcp** una vez para cada vecino de dicho direccionador. No es necesario configurar para cada uno de los dos direccionadores vecinos la dirección IP del otro. Sólo es necesario que un direccionador tenga la dirección del otro, y el otro direccionador puede configurarse para aceptar conexiones TCP dinámicas desde vecinos no configurados. Utilice el mandato **enable dynamic-neighbors** para configurar este comportamiento, y utilice el mandato **set dynamic-tcp** para configurar los parámetros utilizados para estas conexiones dinámicas. El habilitar conexiones TCP dinámicas puede ser particularmente útil para aquellos direccionadores "concentradores" que no desea reconfigurar al configurar nuevos direccionadores de sucursal remotos con conexión a dichos concentradores.

Además de la dirección IP, el mandato **add tcp** le permite configurar una serie de parámetros para el vecino y para la propia conexión TCP. El parámetro *Keepalive* controla si la capa TCP sondeará de forma ocasional su capa TCP igual en ausencia de tráfico de datos de usuario. La habilitación de mensajes Keepalive proporciona una notificación más oportuna de anomalías de conexión TCP, pero puede incrementar la actividad general de WAN y provocar el informe de anomalías que podrían haber sido satisfactoriamente redireccionadas.

El parámetro de simulación NetBIOS SessionAlive controla si se reenvían o no las tramas NetBIOS SessionAlive al DLSw asociado. Este parámetro es importante cuando se han establecido sesiones NetBIOS entre los DLSw asociados a través de un enlace RDSI. Si se habilita este parámetro y se inhabilita el parámetro Keepalive, no habrá paso de tráfico DLSw entre los DLSw asociados si se establecen sesiones NetBIOS desocupadas entre los DLSw asociados. Esto permitiría la conclusión de una conexión RDSI subyacente manteniendo una sesión NetBIOS desocupada sobre DLSw.

El parámetro *connectivity setup type* controla cuándo DLSw establece y concluye la conexión TCP. Cuando uno o ambos vecinos tienen CST establecido en *active*, DLSw intenta establecer la conexión durante el arranque del sistema y a intervalos regulares hasta que se establezca. Una vez se ha establecido la conexión TCP, DLSw procura mantenerla siempre activa, intentando restablecerla siempre que ésta se interrumpa debido a alguna anomalía. Si ambos vecinos tienen CST establecido en *passive*, DLSw establece la conexión TCP sólo cuando sea realmente necesaria para establecer una sesión de estación final de DLSw. Cuando concluye la última sesión DLSw y no se arranca ninguna nueva sesión durante un período de tiempo configurable (el *temporizador de inactividad de vecino*), DLSw desconecta la conexión TCP y libera los recursos internos asociados.

Configuración de grupos para el descubrimiento de vecinos

Para evitar la configuración de direcciones IP de vecino en uno o ambos direccionadores de cada par de direccionadores vecinos, configure DLSw para utilizar IP de multidifusión para descubrir la dirección IP de los vecinos con los que debe conectar. Utilice el mandato **join-group** en cada direccionador para convertirlo en miembro de uno o más grupos DLSw y para asignarle un cometido dentro del grupo. El cometido puede ser el de “cliente”, “servidor” o “igual”. DLSw utiliza IP de multidifusión para descubrir las direcciones IP de todos los direccionadores DLSw que son miembros de los mismos grupos y que tienen un cometido complementario (es decir, clientes descubren servidores dentro de un grupo y viceversa, e iguales descubren otros iguales).

Cuando DLSw averigua las direcciones IP de sus vecinos de cada grupo, utiliza el parámetro “connectivity setup type” de su pertenencia al grupo y el de cada vecino de grupo para determinar cuándo debe establecerse una conexión TCP con dicho vecino. Al igual que con vecinos individuales configurados, cuando cualquiera de los dos CST es *active*, DLSw establece la conexión TCP con el vecino descubierto tan pronto como sea posible, e intenta mantenerla activa durante todo el tiempo. Cuando ambos CST son *passive*, DLSw establece la conexión TCP sólo cuando se requieren sesiones DLSw, y utiliza el *temporizador de inactividad de vecino* para desconectar la conexión TCP cuando no se utiliza.

Exploración de multidifusión y reenvío de tramas

DLSw utiliza servicios IP de multidifusión para algo más que para descubrir las direcciones IP de direccionadores vecinos. Utiliza los mismos servicios para reenviar mensajes DLSw buscando recursos de estación final (por ejemplo, direcciones MAC o nombres NetBIOS), y para reenviar tráfico de datagrama NetBIOS. Esta función puede incrementar en gran medida la capacidad de crecimiento de las redes DLSw porque no hay la necesidad de conexiones TCP estáticas con todos los vecinos para llevar mensajes de datagrama y de búsqueda. Además, DLSw no necesita enviar una copia diferente de cada mensaje de difusión en cada conexión TCP, sino que puede enviar una única copia que se replica dentro de la infraestructura IP de multidifusión.

Para utilizar IP de multidifusión para el reenvío de tramas y exploración, ejecute el mandato **join-group** y establezca el parámetro *connectivity setup type* en *passive*. DLSw determina automáticamente qué otros miembros del grupo tienen capacidad de multidifusión, y cuales están utilizando su pertenencia al grupo simplemente para descubrir direcciones IP de vecino y establecer conexiones TCP estáticas. DLSw trabaja de forma simultánea con ambos tipos de vecinos cuando busca recursos de estación final, reenvía datagramas NetBIOS y establece sesiones DLSw.

Al ejecutar el mandato **join-group**, se selecciona uno de los dos métodos de direccionamiento para describir el grupo al que se va a unir. Al proporcionar un ID de grupo y el cometido de cliente/servidor/igual descrito previamente, el direccionador construye las correspondientes direcciones IP de multidifusión y puede comunicar con otros direccionadores IBM que utilicen este método. También tiene la opción de especificar las direcciones IP de multidifusión que se van a utilizar y si cada una de ellas debe ser de lectura, de grabación, o de ambas cosas. Este método se introdujo para dar soporte a RFC 2166 y para permitir la interoperatividad de multidifusión con otros productos de DLSw Versión 2.

Un direccionador determinado puede ser miembro de grupos tradicionales y leer y escribir en direcciones de multidifusión de DLSw Versión 2. Las nuevas direcciones de multidifusión también pueden utilizarse para el descubrimiento de vecinos, pero debe asegurarse de que en cada par de direccionadores que vayan a formar una conexión TCP, un direccionador tenga el parámetro *connectivity setup type* en *active* en una dirección con capacidad de escritura en la que el otro direccionador esté leyendo. Independientemente de si va a realizar descubrimiento de vecinos o no, la especificación de direcciones de multidifusión requiere una planificación de la configuración más minuciosa, para asegurar su accesibilidad, que en el caso de la utilización de ID y el modelo cliente/servidor/igual.

Reducción del tráfico explorador: Si el volumen de tráfico explorador que se reenvía entre vecinos DLSw es demasiado grande, existen varias posibilidades de reducirlo.

SAP abiertos de DLSw
: Cada DLSw envía una lista de todos los SAP abiertos en cualquier interfaz a sus vecinos DLSw a través del intercambio de posibilidades DLSw. Los vecinos DLSw pueden utilizar esta lista de SAP para limitar el tráfico explorador enviado a esta DLSw.

listas de direcciones MAC de DLSw
: Cada DLSw puede configurar una lista de direcciones MAC locales. Esta lista está definida como exclusiva (representa todas las direcciones MAC accesibles a través de esta DLSw) o como no exclusiva (representa un conjunto de direcciones MAC accesibles vía esta DLSw). Cada entrada de la lista contiene una máscara de direcciones MAC y un valor de dirección MAC. La lista completa de direcciones MAC y el tipo de exclusividad se envían a todos los vecinos DLSw a través del intercambio de posibilidades DLSw. Los vecinos DLSw pueden utilizar esta lista de direcciones MAC para limitar el tráfico explorador enviado a esta DLSw.

  Las listas de direcciones MAC funcionan de un modo parecido a las listas de nombres NetBIOS. Para obtener información acerca de las listas de nombres NetBIOS, consulte “Listas de nombres de NetBIOS” en la página 156.

entradas de antememoria MAC de DLSw
: Una DLSw puede configurar entradas de antememoria MAC individuales que correlacionan una dirección MAC determinada con un vecino DLSw determinado. Pueden utilizarse múltiples entradas de antememoria MAC para correlacionar una dirección MAC determinada con múltiples vecinos DLSw. La DLSw utiliza esta lista de forma local para limitar dónde se envían los exploradores DLSw destinados a una dirección MAC configurada.

filtros de direcciones MAC
: Los filtros de direcciones MAC configurados para la interfaz de red de puente se aplican al tráfico DLSw. Estos filtros de direcciones MAC de entrada

pueden utilizarse para limitar el tráfico entregado a DLSw, limitando de esta forma el tráfico explorador enviado a asociados DLSw. Para obtener más información acerca de los filtros MAC, consulte “Utilización y configuración del filtrado Mac” y “Supervisión del filtrado MAC”en el manual *Access Integration Services Guía del usuario de software*.

Limitación de exploradores por cola de transporte

De forma ocasional, el rendimiento de una sesión TCP con un asociado DLSw puede verse sustancialmente afectado por una acumulación de tráfico o un problema en la red. En estos casos, DLSw puede poner en cola tráfico explorador (SNA y NetBIOS) en espera de ser enviado al asociado DLSw. Si la cantidad de datos en la cola aumenta excesivamente puede tener un efecto negativo en la memoria. Para reducir este impacto, DLSw dispone de dos parámetros de configuración que controlan cuántas tramas exploradoras SNA pueden ponerse en cola de forma simultánea en un único asociado DLSw, y cuántas tramas exploradoras NetBIOS pueden ponerse en cola de forma simultánea en un único 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 a través de interfaces LAN y WAN de puenteo remoto. Tanto las estaciones finales como el direccionador ejecutan el Control de enlace lógico (LLC), estándar ISO 8802-2 (IEEE 802.2), para proporcionar control de secuencia de datos y una entrega fiable. El direccionador da soporte actualmente al tráfico LLC que circula por puerte en los siguientes tipos de interfaz, y todos pueden utilizarse para el flujo de datos entre estaciones finales DLSw y LLC:

- Red en anillo
- Ethernet/802.3
- Frame Relay (con los formatos de trama descritos en el documento RFC 1490/2427)
- PPP
- Circuitos de marcación que utilizan tramas PPP o FR (por ejemplo, RDSI)

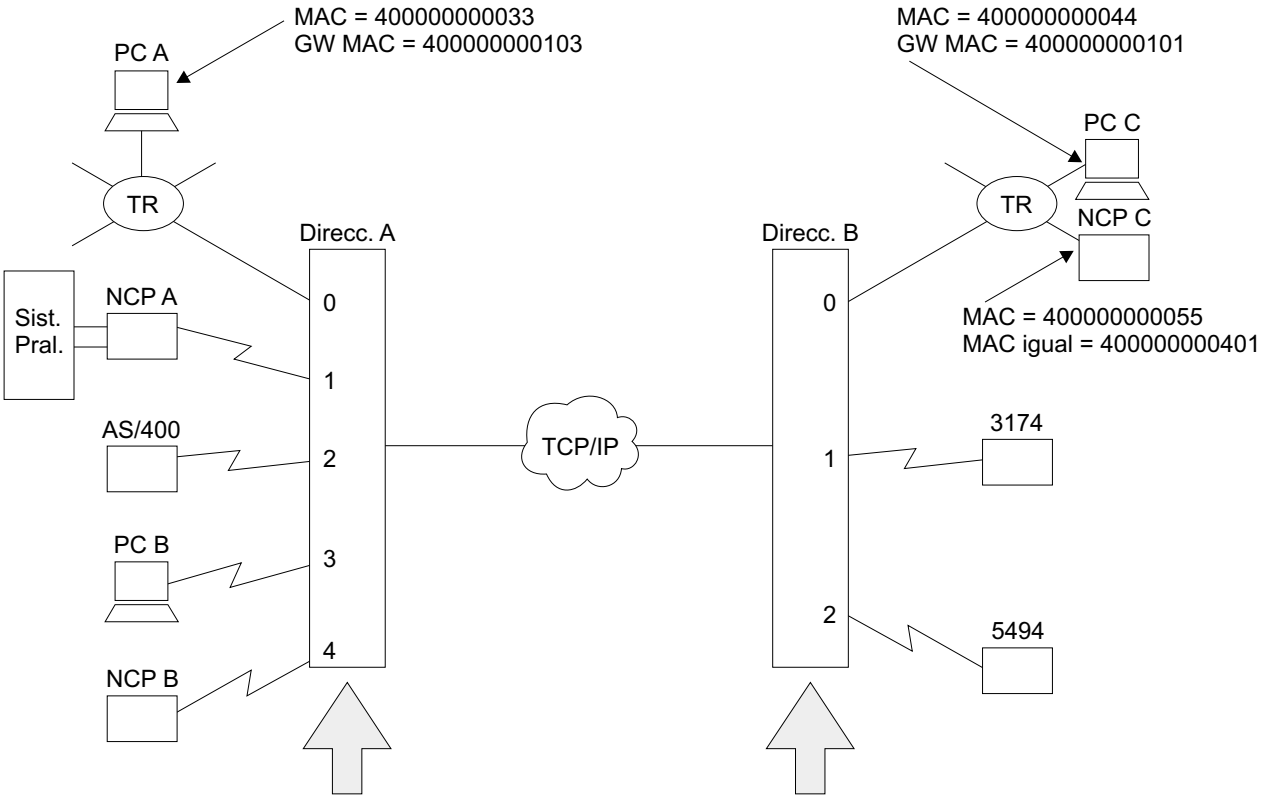
Debido a que DLSw utiliza las direcciones MAC y SAP disponibles en enviadas por puente, no es necesario configurar en DLSw ninguna información acerca de estaciones finales LLC individuales. DLSw recibe tráfico de difusión enviado por estas estaciones finales, y utiliza métodos normales de difusión por LAN/puente para establecer el primer contacto con ellas. Sin embargo, debe configurarse el soporte de puenteo para cualquier interfaz que DLSw vaya a utilizar, y configurar dentro de DLSw los SAP que va a utilizar en cada interfaz.

Soporte de dispositivos SDLC

DLSw da soporte a estaciones finales SDLC que pueden ser unidades físicas (PU) SNA de los tipos 1, 2.0, 2.1, 4 (para tráfico NCP-NCP) o4/5 (un sistema principal o NCP realizando la función de límite SNA). El direccionador puede servir como estación de enlace SDLC primaria o secundaria, en función del cometido configurado para la interfaz SDLC, o en función de la negociación XID SNA. Como estación primaria, el direccionador puede dar soporte a múltiples dispositivos SDLC de diferentes tipos de PU en la misma línea SDLC multipunto física. Como estación secundaria, el direccionador puede representar múltiples estaciones

secundarias SDLC en una única interfaz SDLC física. También da soporte a la función de sondeo de grupo IBM 3174 como estación secundaria.

Nota: DLSw da soporte a dispositivos PU1 SDLC que comunican con dispositivos conectados por SDLC o por LAN que a su vez dan soporte a dispositivos PU1 (por ejemplo, 3745). También da soporte a dispositivos PU1 que comunican con dispositivos que no dan soporte a dispositivos PU1; para ello, emula el dispositivo PU1 como dispositivo PU2.0 para el sistema principal.



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 43. Ejemplo de configuraciones SDLC de DLSw

La Figura 43 ilustra algunas de las configuraciones SDLC soportadas por DLSw, y muestra un subconjunto de la configuración DLSw necesaria para correlacionar entre direcciones SDLC y DLSw (MAC y SAP). El diagrama muestra sesiones DLSw *locales* (con un único direccionador) y *remotas* (entre dos direccionadores y una red IP).

Se han configurado las siguientes sesiones DLSw:

- NCP A con los PC A, B y C, y con 3174

  Para que el NCP A pueda comunicar con estas 4 PU, el direccionador A debe tener configurada en la interfaz 1 una estación de enlace secundaria para cada PU. Esta interfaz debe configurarse en SDLC como secundaria, dúplex y punto

a punto. Se recomienda el sondeo de grupo siempre que hayan varias estaciones secundarias en la misma interfaz, para reducir el sondeo no productivo.

En este ejemplo, el NCP A comunica con el PC C a través de la dirección de estación SDLC 01, con 3174 a través de la dirección 02, con PC A a través de la dirección 03 y con PC B a través de la dirección 04. Observe que las sesiones de los PC A y C implican la conversión SDLC a LLC en una configuración local y remota, respectivamente. La sesión del PC B es una sesión local SDLC a SDLC, cosa poco habitual.

Para las estaciones de enlace secundarias definidas en el direccionador A, el tipo de PU 5 indica que el dispositivo SDLC es un sistema principal (en este caso con un controlador como componente frontal) que realiza la función BNN de SNA para un dispositivo PU2.0 descendente. El tipo de PU 2 indica que el FEP/sistema principal SDLC actúa como nodo T2.1 que se comunica con otro nodo T2.1 de la red DLSw.

- AS/400® cone 5494

  En este caso, estos dispositivos funcionan como nodos T2.1 y los enlaces SDLC de sus respectivos direccionadores están configurados como negociables (los nodos T2.1 también están soportados en enlaces de cometido fijo, y DLSw restringe la negociación de cometidos de forma oportuna). La estaciones realizarán una negociación XID completa, incluyendo la determinación de cometidos y la resolución de direcciones SDLC (si el direccionador y la estación final de un mismo enlace están configurados cada uno con una dirección de estación SDLC diferente). Observe que no hay ninguna relación en configuraciones SDLC-SDLC remotas entre las direcciones de estación SDLC utilizadas en los dos enlaces SDLC diferentes. Las sesiones SDLC-LLC remotas también están soportadas entre dispositivos T2.1.

- NCP B con NCP C

  El NCP B está configurado como PU de tipo 4, indicando que esta sesión DLS conducirá tráfico de subárea INN entre los NCP, y no tráfico BNN desde un NCP a un dispositivo PU 2. El ejemplo muestra una sesión SDLC-LLC remota, pero también se da soporte a sesiones de igual a igual. La función INN de DLSw no da soporte a los TG multienlace ni a las funciones de carga/vuelco remotas.

Correlación de direcciones

La configuración de DLSw proporciona una correlación entre direcciones de estación SDLC de un único byte y los SAP y direcciones MAC con los que DLSw identifica las estaciones finales. La dirección MAC de origen de una estación SDLC representa el dispositivo SDLC para el resto de la red DLSw. Es la dirección de origen de las tramas procedentes del dispositivo y la dirección de destino de las tramas que se dirigen al dispositivo. Se requiere una dirección MAC de origen para que el dispositivo SDLC pueda comunicar a través de DLSw.

La dirección MAC de destino especifica la estación final de la red DLSw a la que debe conectarse este dispositivo SDLC al empezar la comunicación. Los dispositivos SDLC que actuarán siempre como destino de sesiones nuevas y nunca como iniciadores deben tener una dirección MAC de destino igual a cero. Cuando el direccionador se configura como estación de enlace secundaria, es importante definir una dirección MAC de destino para que las conexiones de salida de sistema principal puedan realizarse satisfactoriamente. Esto se debe a que una estación de

enlace secundaria no puede establecer contacto con el sistema principal en nombre de una estación final DLSw remota que se está conectando, sino que debe esperar a ser sondeada. Debe tenerse en cuenta que cuando la estación final DLSw remota es al mismo tiempo una estación SDLC (por ejemplo, el 3174 en el direccionador B de la Figura 43 en la página 542) y se empareja con una estación local secundaria, la estación remota debe tener una dirección MAC de destino igual a cero para reflejar esta dependencia en una conexión de salida de sistema principal.

Configuración de DLSw y configuración de SDLC

Para utilizar DLSw sobre una interfaz SDLC, debe configurar la correlación de direcciones como parte de la configuración de DLSw, y configura además cierta información como parte de la configuración de SDLC. En el caso de SDLC, debe como mínimo establecer la interfaz para que sea SDLC y configurar otros parámetros de nivel de interfaz como por ejemplo el cometido del enlace. Los parámetros de interfaz SDLC proporcionan valores por omisión para todas las estaciones de enlace SDLC de dicha interfaz, pero si desea tener valores exclusivos para una estación, puede configurar información para las estaciones SDLC de forma individual.

La pareja de direcciones *número de interfaz, dirección de estación SDLC* es la clave común que enlaza la información de correlación de direcciones de 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 DLSw especifica, SDLC crea una definición de estación de enlace de forma dinámica y utiliza los valores por omisión de los parámetros definidos en SDLC para dicha interfaz.

Relación con la función de retransmisión de SDLC

La retransmisión SDLC es una función de direccionador que encapsula tramas SDLC completas en paquetes IP, y los direcciona a continuación hacia otro direccionador que también da soporte a la retransmisión SDLC. El direccionador de destino separa la cabecera IP y entrega las tramas SDLC sin modificar a un enlace SDLC de destino.

Esta función difiere del soporte SDLC de DLSw en los siguientes puntos:

- Con la retransmisión SDLC, no existe ninguna estación de enlace SDLC dentro del direccionador. Las tramas de control (por ejemplo, RR) fluyen a través de la red IP. Con DLSw, el soporte SDLC del direccionador finaliza la conexión SDLC. Sólo los datos de las tramas SDLC fluyen a través de la red IP. Como consecuencia, DLSw puede proporcionar una mejor utilización del ancho de banda de la WAN, y es menos sensible a los tiempos excedidos de enlace debido a retrasos en la WAN.
- Las tramas de control y de datos SDLC pasan de forma transparente a través de la retransmisión SDLC, mientras que DLSw necesita interpretar y modificar algunas de las tramas. Junto con el hecho que DLSw finaliza la conexión SDLC, esto significa que DLSw no da soporte a ciertas funciones y configuraciones de producto (por ejemplo, los TG multienlace entre los NCP).
- La retransmisión SDLC requiere que el tipo de datos de ambas estaciones finales en comunicación sea SDLC. DLSw proporciona una función de conversión de protocolos para que el tipo de datos de la otra estación final pueda ser

LLC, SDLC, QLLC o cualquier otro tipo de datos soportado por los productos DLSw.

- DLSw es un estándar desarrollado por APPN Implementers Workshop y descrito en un documento RFC de la IETF. Como tal, está soportado por muchos proveedores. Actualmente se da soporte a la retransmisión SDLC sólo en ciertos productos direccionadores 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) para que fluya fuera de la red IP

Debe utilizar la retransmisión SDLC cuando:

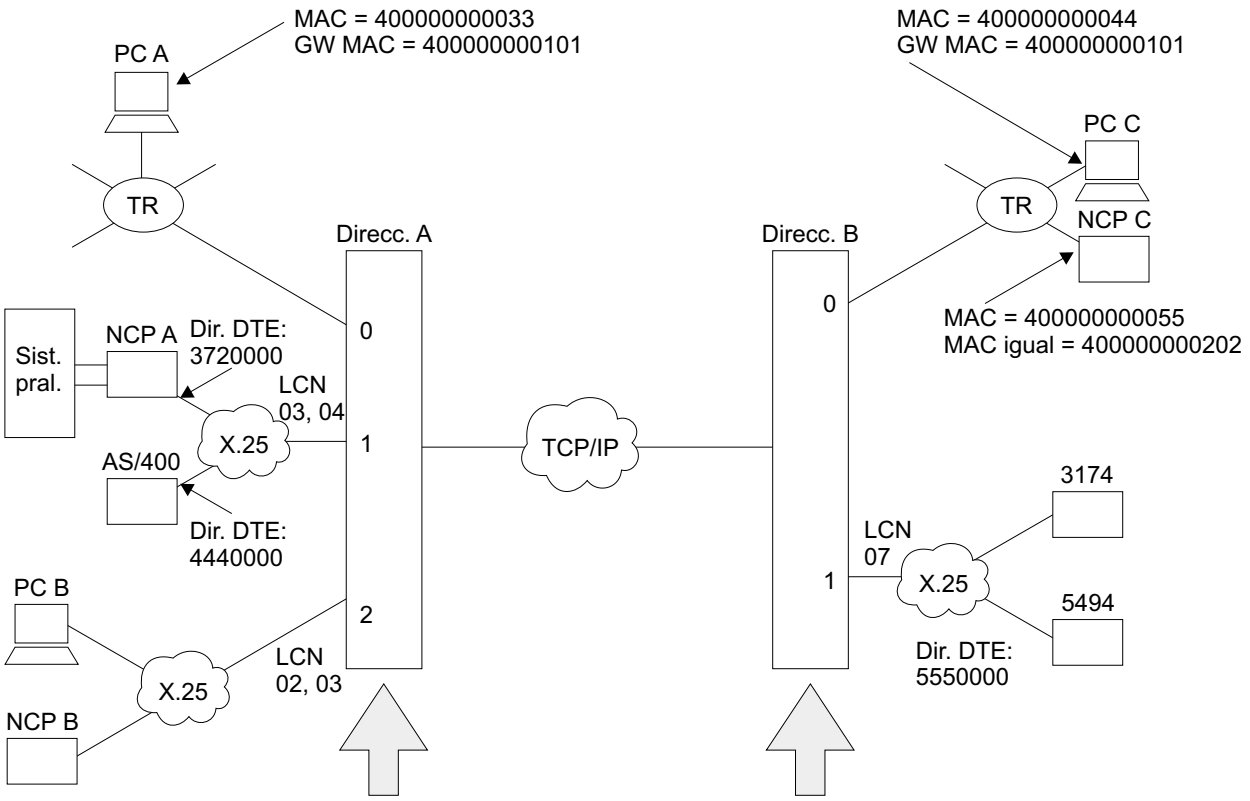
- Necesite una de las funciones o configuraciones SDLC-SDLC a las que DLSw no de soporte actualmente

En otras configuraciones SDLC-SDLC, elija la función que cubra mejor sus necesidades en cuanto a facilidad de configuración, utilización de WAN y soporte para su entorno actual de estación final. Para obtener más información acerca de la retransmisión SDLC, consulte la publicación *Guía del usuario de software*.

Soporte de dispositivos QLLC

QLLC es un protocolo que opera sobre el protocolo de capa de paquetes de X.25 para proporcionar un aspecto de estación SDLC a los dispositivos SNA en redes X.25. QLLC da soporte a una única PU SNA por cada circuito virtual (PVC o SVC). La multiplexación de canales X.25 permite la conexión de varios circuitos virtuales o varias PU a la red X.25 a través de una única interfaz física. La arquitectura QLLC define los cometidos primario, secundario y igual, aunque éstos son menos importantes que en SDLC porque no afectan a la transmisión de datos de usuario final. Los datos de todos los circuitos virtuales de una interfaz fluyen a través de una única conexión de enlace de capa2 de LAPB, que funciona de forma equilibrada. Cada extremo tiene permiso para enviar en todo momento mientras el enlace está conectado.

DLSw da soporte a estaciones finales QLLC que pueden ser unidades físicas (PU) SNA de los tipos 2.0, 2.1, 4 (para tráfico NCP-NCP), o4/5 (un sistema principal o un NCP desempeñando la función de límite de SNA). Pueden conectarse estaciones finales a través de PVC configurados, SVC configurados o SVC dinámicos como resultado de una llamada de entrada. El direccionador puede actuar como estación de enlace QLLC primaria o secundaria, en función del cometido configurado para la interfaz X.25 y en función de la negociación de XID SNA. Pueden coexistir diferentes tipos de PU en diferentes circuitos virtuales dentro de la misma interfaz física, pero sólo se da soporte a un cometido de estación de enlace por cada interfaz.



Interfaz	Tipo VC	Dirección 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 habilitadas para llamadas de entrada
1

ID conexión	MAC dest.
PCA	400000000033
PCC	400000000044

Interfaz	Tipo VC	Dirección LCN/DTE	Tipo PU	MAC origen	MAC dest.
1 (pri)	PVC	07	2	401111110101	400000000102

Interfaces habilitadas para llamadas de entrada
1

ID conexión	MAC dest.
AS400	400000000104

Figura 44. Ejemplo de configuraciones QLLC de DLSw

La Figura 44 ilustra algunas de las configuraciones QLLC soportadas por DLSw, y muestra un subconjunto de la configuración DLSw necesaria para correlacionar entre direcciones QLLC y DLSw (MAC y SAP). El diagrama muestra sesiones DLSw *locales* (con un único direccionador) y *remotas* (entre dos direccionadores y una red IP). No se muestra ningún emparejamiento QLLC-SDLC, pero se les da soporte en ambas configuraciones, local y remota.

Se han configurado las siguientes sesiones DLSw:

- NCP A con los PC A, B y C, y con 3174

  El NCP A está conectado a la interfaz 1 del direccionador A a través de dos PVC y dos SVC, representando cada circuito virtual 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 en SDLC, la configuración de DLSw correlaciona estas

direcciones DLC "nativas" (dirección LCN o DTE) con direcciones DLSw (MAC y SAP).

En este ejemplo, el NCP A comunica con el 3174 (QLLC-QLLC remota) a través del PVC 03, y con el PC B (QLLC-QLLC local) a través del PVC 04. Estos LCN son en realidad locales para el direccionador A; el NCP puede utilizar diferentes LCN para sus PVC correspondientes en la red X.25. El direccionador A conecta el NCP A con el PC C (QLLC-LLC remota) y con el PC A (QLLC-LLC local) mediante dos SVC entre la dirección DTE 3720000 para el NCP A y la dirección DTE para la interfaz 1 del direccionador A. Debido a que el direccionador A debe poder aceptar llamadas del NCP A, tiene la interfaz 1 habilitada para llamadas de entrada en DLSw. El NCP A utiliza los *ID de conexión*, mencionados más abajo, para conectar con los PC A y C.

El PC C no está configurado en el direccionador B porque tiene una conexión LLC/LAN. El 3174 está conectado a través del LCN 07 de la interfaz 1, que no tiene relación con el número de LCN o de interfaz utilizado en el direccionador A.

- AS/400 con 5494

  Además del NCP A, el AS/400 también está conectado al direccionador A a través de la interfaz 1. A diferencia de SDLC, no hay mejora de rendimiento al limitar el número de estaciones de una determinada interfaz. Pueden haber múltiples estaciones en un enlace independientemente del cometido del enlace. Si el cometido es negociable y las estaciones son nodos T2.1 o PU4, cada estación puede negociar el convertirse en primaria o secundaria independientemente.

  El AS/400 no tiene dirección MAC de destino configurada en el direccionador A, y por lo tanto no puede conectarse al 5494. El 5494 no está configurado en el direccionador B, y por lo tanto 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 habilitada para llamadas de entrada en DLSw para que pueda recibir llamadas del 5494.

- NCP B con NCP C

  El NCP B está configurado como PU de tipo 4, indicando que esta sesión DLS conducirá tráfico de subárea INN entre los NCP, y no tráfico BNN desde un NCP a un dispositivo PU 2. El ejemplo muestra una sesión QLLC-LLC remota, pero también se da soporte a sesiones de igual a igual y sesiones que impliquen SDLC. La función INN de DLSw no da soporte a los TG multienlace ni a las funciones de carga/vuelco remotas.

Correlación de direcciones

DLSw proporciona una correlación entre pares MAC/SAP utilizados para direccionar entidades de estación final en el dominio DLSw, y los pares *interfaz, LCN* (PVC) o *interfaz, dirección DTE* (SVC) utilizados en el dominio X.25. Esta correlación tiene lugar en el momento del establecimiento de la conexión, pero utiliza información de direccionamiento configurada en el direccionador y en los productos de estación final.

Conexión de salida (a estaciones QLLC)

DLSw recibe un mensaje CUR_ex o CUR_cs direccionado a un MAC y SAP de destino concretos. Busca entre sus estaciones finales QLLC una estación cuyo SMAC y SSAP (SAP sólo se comprueba para CUR_cs) coincida con este MAC/SAP de destino. Puede haber una coincidencia o bien ninguna, ya que los SMAC son exclusivos para cada direccionador.

Si se produce una coincidencia, DLSw inicia la conexión con la estación QLLC utilizando la interfaz y LCN correspondientes en el caso de un PVC, o la interfaz y el número de teléfono si se trata de un SVC. DLSw puede emitir múltiples llamadas de salida a la misma dirección DTE utilizando una única definición (SVC) de estación QLLC. Esto permite la conexión de muchos dispositivos DLSw al mismo destino con un trabajo de configuración mínimo.

Conexión de entrada (desde estaciones QLLC)

Para los **PVC**, QLLC recibe una trama que inicia el establecimiento del circuito desde la estación final conectada. QLLC y DLSw comparan la interfaz y el LCN en los que se recibió la trama con las entradas de la lista de estaciones QLLC. Puede producirse una coincidencia o bien ninguna, ya que los LCN deben ser exclusivos para cada interfaz. Si no hay ninguna coincidencia o la entrada no tiene ningún DMAC/DSAP definido, la conexión de entrada fallará. De lo contrario, se establecerá una conexión con el DMAC/DSAP definido. El MAC/SAP de origen para la conexión es el SMAC/SSAP de la misma entrada de lista.

En el caso de los **SVC**, DLSw obtiene direcciones MAC/SAP utilizando la dirección de la parte llamante X.25, o un *id de conexión* (bytes 4-11) del campo de datos de usuario de llamada del paquete Call_Request recibido. Si está disponible la dirección de la parte llamante, DLSw la compara con todas las direcciones DTE SVC configuradas para la interfaz llamada. Puede producirse una coincidencia o bien ninguna, ya que las direcciones DTE deben ser exclusivas para cada interfaz. Si se produce una coincidencia y la entrada de la lista de estaciones QLLC tiene un DMAC/DSAP diferente de cero, DLSw utiliza este DMAC/DSAP como dirección de destino para establecer la conexión. El MAC/SAP de origen para la conexión es el SMAC/SSAP de la misma entrada de lista.

Si no hay disponible ninguna dirección de la parte llamante, o hay una pero coincide con una entrada para la que no se ha definido un DMAC/DSAP, o 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 es interpretado como una serie alfanumérica EBCDIC de hasta 8 caracteres.

Si hay una coincidencia de CID, DLSw utiliza el DMAC/DSAP asociado del registro de destino como dirección de destino para establecer el circuito. Si ha habido también una coincidencia de dirección de parte llamante (sin DMAC/DSAP definido), DLSw utiliza el SMAC/SSAP de la entrada coincidente de la lista de estaciones. En caso contrario, DLSw asigna de forma dinámica el SMAC y el SSAP. En el caso del SMAC, DLSw elige la siguiente dirección MAC disponible (de forma rotativa) contenida en el rango definido por los parámetros globales de configuración de DLSw *QLLC base MAC address* y *Max dynamic addresses*. El SSAP seleccionado dinámicamente es siempre 0x04.

Si no hay ninguna dirección de parte llamante ni ningún ID de conexión coincidentes, DLSw no recoge la llamada. Debe tenerse en cuenta que los CID son la

única forma de que una dirección de parte llamante pueda emitir llamadas a múltiples destinos.

APPN y DLSw pueden aceptar ambos llamadas QLLC de la misma dirección de parte llamante. DLSw obtiene el acceso a la llamada en primer lugar porque es más restrictiva en cuanto a las llamadas que va a aceptar. Si DLSw no encuentra ninguna coincidencia de parte llamante o de ID de conexión, no finaliza la llamada, sino que permite que ésta se presente a APPN.

Por tanto, para poder aceptar una llamada de entrada debe definirse en DLSw una dirección de parte llamante o un ID de conexión. Esto es necesario en primer lugar para proporcionar correlación de direcciones, pero también proporciona un elemento de seguridad contra llamadas de entrada de partes no autorizadas. Otras posibles medidas de seguridad son el no habilitar una interfaz para las llamadas de entrada en DLSw, y establecer en cero el número de posibles direcciones MAC dinámicas de origen. Lo primero evitará todas las llamadas de entrada en dicha interfaz, incluso las procedentes de direcciones DTE configuradas en DLSw. Lo segundo evitará sólo las llamadas dinámicas de entrada procedentes de direcciones DTE no configuradas.

Para que DLSw pueda aceptar cualquier parte llamante X.25 (independientemente de la dirección DTE o del CID) y relacionarla con un DMAC y DSAP específicos (uno por unidad), puede configurar un registro de destino QLLC con un valor de CID igual a "ANYCALL" y los DMAC y DSAP deseados. DLSw asigna de forma dinámica el SMAC y el SSAP. Si se utiliza esta característica, DLSw acepta todas las llamadas. No se presentará ninguna llamada a APPN y se evitan todas las características de seguridad asociadas con la correlación de direcciones.

Configuración de DLSw y de X.25

Para utilizar el soporte QLLC de DLSw sobre una determinada interfaz X.25, debe configurar la correlación de direcciones como parte de la configuración de DLSw, y debe además configurar la siguiente información como parte de la configuración de la interfaz X.25. Consulte el apartado “Configuración de interfaces X.25” en la página 559 como ejemplo de estos pasos, y consulte el capítulo “Utilización de la interfaz de red X.25” de la publicación *Access Integration Services Guía del usuario de software* para obtener información adicional.

1. Configure la interfaz para que sea X.25, y configure sus parámetros base de interfaz X.25.
2. Añada DLS como protocolo soportado.
3. Configure los PVC que DLSw va a utilizar, y asócielos con DLSw.
4. Configure las direcciones DTE SVC estáticas que DLSw va a utilizar y asócielas con DLSw. Son las mismas direcciones configuradas en DLSw. No es necesario configurar las direcciones DTE de las estaciones finales QLLC que pueden realizar llamadas de entrada de forma dinámica.

A diferencia de SDLC, X.25 no puede crear de forma dinámica una definición (circuito virtual) de estación de enlace basándose en la información configurada en DLSw.

Relación con la función XTP

El protocolo de transporte X.25 (XTP) es una función de direccionamiento que recoge paquetes de circuitos virtuales X.25 y los transporta a través de TCP/IP hacia otro direccionador que también da soporte a XTP. A continuación el direccionador de destino quita la información de cabecera XTP y entrega los paquetes a otro circuito virtual X.25 de destino.

Esta función es comparable con el soporte QLLC de DLSw en los siguientes puntos:

- Ambas funciones utilizan TCP/IP para comunicar entre direccionadores iguales, y pueden multiplexar información de múltiples circuitos virtuales (o sesiones DLSw) en una única conexión TCP.
- En ambas funciones el direccionador finaliza las conexiones de capa de paquetes layer-3 y LAPB layer-2 con la estación final X.25. Las tramas de control LAPB no fluyen a través de TCP/IP.
- XTP da soporte a la comunicación sólo entre dos estaciones finales X.25. DLSw realiza la conversión de protocolos entre los tipos de datos LLC (puenteado de forma remota o en una LAN), SDLC, QLLC y cualquier otro tipo de datos soportado por los productos DLSw.
- XTP no es sensible al tipo de LLC (por ejemplo, QLLC o PAD) cuando opera sobre la capa de paquetes. Siempre que las dos estaciones finales X.25 den soporte al mismo tipo de LLC, podrán comunicar a través de XTP. El soporte QLLC de DLSw puede comunicar sólo con estaciones finales SNA que ejecuten QLLC.
- En XTP existe una relación configurada entre un circuito virtual de una red X.25, un direccionador asociado y un circuito virtual de otra red X.25. Sólo en el caso de los SVC es posible definir múltiples direccionadores asociados e intentar establecer una conexión a través de un direccionador secundario en caso de que el direccionador primario no estuviera disponible, pero XTP no realiza intentos de establecimiento de conexión ni búsquedas en paralelo. En cambio, DLSw correlaciona un circuito virtual con una dirección MAC y SAP, y efectúa a continuación una búsqueda totalmente dinámica entre múltiples nodos para localizar la estación de destino. Con el soporte de multidifusión de DLSw, incluso no es necesario configurar las direcciones IP de nodos individuales que se van a buscar.
- XTP puede correlacionar un PVC sólo con otro PVC, y un SVC sólo con otro SVC. En configuraciones QLLC-QLLC de DLSw, es posible correlacionar un PVC con un SVC. En la práctica esto puede resultar poco útil, ya que DLSw intentará activar el SVC siempre que el protocolo QLLC esté activo en el PVC.
- En el caso de XTP que utiliza los SVC, las llamadas se emiten hacia y desde las direcciones DTE de las estaciones finales X.25. Tal vez sea necesario configurar un conmutador X.25 o subscripción de red para que el direccionador pueda representar múltiples direcciones DTE. Con DLSw, las llamadas se emiten desde estaciones finales a la dirección DTE de la interfaz del direccionador y viceversa.
- DLSw es un estándar desarrollado por APPN Implementers Workshop y descrito en un documento RFC de la IETF. Como tal, está soportado por muchos proveedores. Actualmente se da soporte a XTP sólo en ciertos direccionadores IBM y productos compatibles.

Debe utilizar DLSw cuando:

- Necesite una conversión de protocolos de QLLC a SDLC o LLC
- Necesite múltiples rutas concurrentes hacia un destino

Debe utilizar XTP cuando:

- Vaya a ejecutar un protocolo que no sea QLLC sobre X.25

En otras configuraciones QLLC-QLLC, elija el protocolo que mejor se adapte a las necesidades de su red. Para obtener más información sobre XTP, consulte el capítulo titulado “Utilización, configuración y supervisión de XTP” en la publicación *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. No es necesario que los direccionadores remotos den soporte a APPN, lo cual puede reducir la cantidad de memoria que necesitan. Tal como se muestra en la Figura 45, esta interfaz interna equivale a colapsar una conexión DLC (por ejemplo, LLC sobre una LAN) para formar una única interfaz de software.

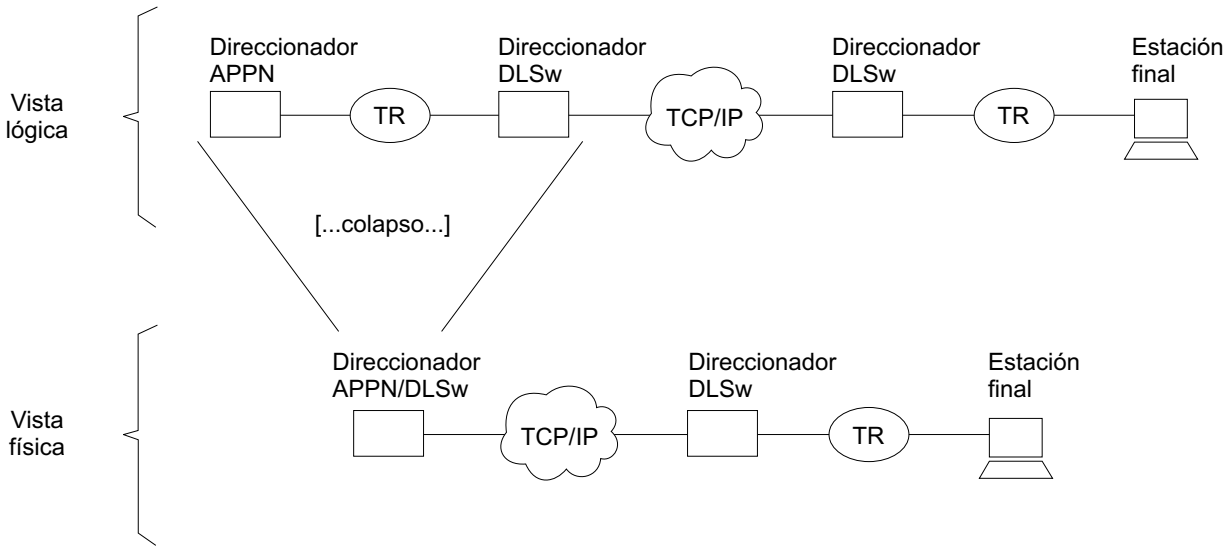


Figura 45. Interfaz de software APPN-DLSw

APPN no puede utilizar la interfaz de software DLSw para acceder a las estaciones finales que están conectadas localmente al direccionador APPN/DLSw. Debe utilizar este soporte DLC nativo para comunicar con estos dispositivos.

No se requiere ninguna configuración adicional de DLSw para dar soporte a la interfaz APPN. Debe habilitar los mensajes Keepalive de TCP en el direccionador remoto DLSw para habilitar la detección de la pérdida de estaciones de enlace en el puerto DLSw. Debe configurar APPN para que utilice una interfaz virtual DLSw y puede acceder a una determinada estación final. Para obtener más información acerca de la implementación de APPN utilizando DLSw, consulte el capítulo acerca de la configuración de APPN en la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 2.*

Utilización de la función de prioridad de vecino

Muchas configuraciones de red de DLSw proporcionan múltiples rutas desde un direccionador DLSw de origen a estaciones finales de destino convirtiendo las estaciones finales en locales para más de un direccionador DLSw de destino. Para proporcionar un control adicional sobre qué direccionador DLSw remoto se utiliza para los nuevos circuitos, puede asignar una prioridad (alta, media o baja) a cada vecino definido. Aunque los valores asignables son similares, la prioridad de vecino ***no*** es la misma que las prioridades para equilibrar el tráfico SNA y NetBIOS, descrito en “Reparto del tráfico SNA y NetBIOS” en la página 553.

En el caso de la prioridad de vecino, asigna una prioridad al definir un vecino mediante los mandatos **add tcp** o **join group**. La prioridad de un grupo se traspasa a todas las conexiones de transporte establecidas dentro de dicho grupo.

Cuando DLSw crea un circuito y detecta que la dirección MAC de destino o el nombre NetBIOS es accesible por múltiples direccionadores DLSw remotos, establece el circuito a través del vecino que posee la prioridad más alta. Si existen múltiples direccionadores remotos que comparten la prioridad más alta, DLSw utiliza un método “rotativo” para asignar nuevos circuitos entre dichos direccionadores.

Mediante la prioridad de vecino, puede establecer una relación primario/reserva entre los direccionadores remotos. No se utilizará un direccionador con prioridad más baja a menos que el direccionador con prioridad más alta pierda su disponibilidad. Además, el método rotativo proporciona un equilibrado de la carga entre los direccionadores de igual prioridad.

Notas:

1. Cuando se recibe una trama SNA destinada a una dirección MAC que no tiene información en antememoria con la que los vecinos puedan alcanzar la dirección MAC, se envía un mensaje explorador SNA a todos los vecinos DLSw. Se recopilarán respuestas al mensaje explorador SNA durante el periodo de tiempo especificado con el “temporizador de espera de prioridad de vecino”. Después de este periodo de tiempo, la entrada de antememoria de la dirección MAC se actualiza con la información procedente de las respuestas de los vecinos que tengan la prioridad más alta. Se escoge a uno de estos vecinos para manejar el circuito SNA, y se envía una respuesta a la trama SNA original recibida. Las subsiguientes peticiones de circuito SNA correspondientes a esta dirección MAC utilizarán uno de los vecinos de prioridad más alta almacenado en antememoria para activar el circuito.
2. Cuando se recibe una trama NetBIOS destinada a un nombre NetBIOS que no tiene información en antememoria para este nombre NetBIOS, se envía un mensaje explorador NetBIOS a todos los vecinos DLSw que den soporte a NetBIOS. A diferencia del caso SNA, las respuestas se recopilan durante un periodo de tiempo especificado antes de enviar la respuesta a la trama original NetBIOS. Los temporizadores de estación final normalmente no permiten ningún retraso en el direccionador.

   Por este motivo se guarda la primera respuesta al mensaje explorador NetBIOS. Este vecino se utiliza para activar el circuito NetBIOS, y se envía una respuesta a la trama NetBIOS original recibida. Mientras tanto, las subsiguientes respuestas al mensaje explorador NetBIOS se utilizan para actualizar la antememoria de nombres NetBIOS.

- Si se recibe una respuesta de un vecino de igual prioridad que la información almacenada actualmente en antememoria, se añade a la antememoria.
- Si se recibe una respuesta de un vecino con prioridad más alta que la información almacenada actualmente en antememoria, se elimina la información almacenada en antememoria y se añade la información del vecino de prioridad más alta.
- Si se recibe una respuesta de un vecino con prioridad inferior a la información almacenada actualmente en antememoria, se ignora. Las subsiguientes peticiones de circuito NetBIOS correspondientes a este nombre NetBIOS utilizarán uno de los vecinos de prioridad más alta almacenado actualmente en antememoria para activar el circuito.

Es posible inhabilitar la función de prioridad de vecino en todas las direcciones MAC o en ciertos conjuntos de direcciones MAC. Para inhabilitarla en todas las direcciones MAC, establezca el *temporizador de espera de prioridad de vecino* en 0. Para inhabilitarla en un conjunto de direcciones MAC, cree una alteración temporal de explorador de antememoria MAC y establezca su *temporizador de espera de prioridad de vecino* en 0.

Si se inhabilita la función de prioridad de vecino, no se almacenará en antememoria la información de asociado DLSw para la dirección MAC. Los exploradores SNA y NetBIOS se envían siempre a todos los asociados DLSw aplicables, y el primer asociado DLSw en responder se utiliza para establecer la sesión DLSw (independientemente de su prioridad).

Reparto del tráfico SNA y NetBIOS

Con la introducción del soporte DLSw para el tráfico NetBIOS, necesita controlar la mezcla de tráfico SNA y NetBIOS dentro de conexiones de transporte DLSw. Sin este control, las transferencias de archivos NetBIOS tienen una tendencia a excluir el tráfico SNA interactivo durante periodos de tiempo excesivamente largos, especialmente si las conexiones TCP se establecen sobre enlaces WAN relativamente lentos. Puede controlar esta mezcla de tráfico utilizando los parámetros de configuración del mandato **set priority**. Mediante estos parámetros puede:

- Establecer una proporción del número de tramas de cada protocolo transmitidas a través de una conexión TCP durante periodos de congestión
- Establecer un tamaño de trama máximo para tramas NetBIOS de forma que las tramas grandes no colapsen los enlaces WAN lentos.

Para establecer una relación de tramas SNA y NetBIOS, seleccione globalmente uno de los cuatro valores de prioridad (crítica, alta, media o baja) 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 la prioridad de cada nuevo circuito con el valor del protocolo que va a utilizar el circuito. El direccionador DLSw que inicie el circuito escogerá la prioridad de circuito a utilizar. Si el direccionador DLSw local inicia el circuito, la prioridad de circuito que escoge está basada en los valores por omisión de prioridad de circuito y en alteraciones temporales de prioridad de circuito. Si el que inicia el circuito es el direccionador DLSw remoto, el direccionador DLSw local informará al direccionador DLSw remoto sobre la necesidad de utilizar una prioridad de circuito basada en los valores por omisión y alteraciones temporales configurados, pero el direccionador DLSw remoto puede escoger un valor diferente. En todo caso, el

direccionador que ha iniciado el establecimiento del circuito asigna una de las cuatro prioridades al circuito.

Durante periodos de congestión TCP, el direccionador pone en cola tramas (procedentes de circuitos con datos a transmitir) en una de las cuatro colas - una cola para cada posible prioridad de circuito. Las tramas se ponen 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 dicte el parámetro “message allocation by priority” (asignación de mensajes por prioridad). Éste toma el valor por omisión 4/3/2/1, lo que significa que como máximo se tomarán cuatro mensajes de la cola de prioridad crítica, seguidos por un máximo de tres mensajes de la cola de prioridad media, y así sucesivamente. Si una cola está vacía perderá su turno dentro de este ciclo.

Para evitar que una trama NetBIOS de gran tamaño domine un enlace lento durante mucho tiempo, puede utilizar el parámetro “NetBIOS maximum frame size” (tamaño máximo de trama NetBIOS) para proporcionar un límite superior al tamaño de las tramas NetBIOS. Este valor se pasa a ambas estaciones finales NetBIOS durante el establecimiento del circuito mediante los bits LF (Largest Frame) de la cabecera MAC de direccionamiento en origen. Las estaciones finales NetBIOS de direccionamiento en origen deben considerar los valores LF y no generar tramas más grandes que el valor especificado.

Pueden configurarse cuatro prioridades de circuito por omisión:

- Prioridad de circuito de tráfico explorador SNA por omisión
- Prioridad de circuito de tráfico de sesión SNA por omisión
- Prioridad de circuito de tráfico explorador NetBIOS por omisión
- Prioridad de circuito de tráfico de sesión NetBIOS por omisión

Estos diferentes valores permiten asignar diferentes proporciones de tráfico de sesión y de explorador SNA y NetBIOS.

Puede haber casos en los que desee asignar una cierta prioridad de circuito a un tráfico específico. Por ejemplo, tal vez desee asignar al tráfico destinado a una determinada dirección MAC SNA una prioridad más alta que el resto del tráfico. Esto puede lograrse utilizando el mandato de alteraciones temporales de prioridad de circuito (**add priority**). Esto permite asignar una prioridad de circuito de sesión y de explorador a un rango específico de SAP y direcciones MAC de origen y de SAP y direcciones MAC de destino. Estas alteraciones temporales de prioridad de circuito se evalúan en el orden en que se han configurado. La prioridad de circuito se establece en el valor de la primera coincidencia de alteración temporal de prioridad de circuito encontrada. Si no se encuentra ninguna coincidencia de alteración temporal de prioridad de circuito se utiliza la prioridad de circuito por omisión.

Configuración de DLSw

Las secciones siguientes explican los procedimientos de configuración de DLSw:

Además también se incluye un ejemplo de configuración de DLSw con notas explicativas (consulte la Figura 46 en la página 561).

Requisitos de configuración de DLSw

Para utilizar DLSw, configure los siguientes protocolos: ASRT, IP y DLSw. Tal vez necesite configurar también los protocolos listados en la Tabla 34.

Tabla 34. Protocolos opcionales de DLSw

Protocolo opcional	Cuándo se utiliza
LLC2	Cuando son necesarios parámetros LLC2 diferentes de los parámetros por omisión
SDLC	Para conectar a dispositivos que utilizan SDLC
OSPF	Para el direccionamiento dinámico o para utilizar grupos de multidifusión de DLSw
X.25	Para conectar a dispositivos que utilizan QLLC

Las secciones siguientes explican paso a paso cómo configurar los protocolos requeridos y opcionales.

Definición de almacenamientos intermedios globales

Al ejecutar DLSw en un 2212 con 4 MB de DRAM, puede ser necesario permitir más memoria para DLSw reduciendo el número de almacenamientos intermedios de paquetes globales. Entre el mandato **set global** en el indicador `Config>`, y entre a continuación el número de almacenamientos intermedios de paquetes globales.

Configuración de ASRT para DLSw

Debido a que el direccionador DLSw aparece como un puente a las estaciones finales conectadas, es necesario configurar el puenteo de ruta en origen. Para hacerlo siga los pasos siguientes:

1. Entre en el proceso de configuración de ASRT. Utilice el mandato **protocol asrt** desde el indicador `Config>`.
2. Habilite el puenteo en el direccionador mediante el mandato **enable bridge**. Cada puente debe tener una dirección de puente exclusiva en cada DLSw.
3. Añada un puerto de puente con el mandato **add port**. La pantalla le solicita un número de interfaz y un número de puerto.
   - ***Para las interfaces red en anillo:***

     La ejecución de DLSw sobre red en anillo requiere que sólo esté presente el puenteo de ruta en origen en el puerto de puente designado. Por este motivo debe inhabilitar el puenteo transparente. Para hacerlo utilice el mandato **disable transparent**. A continuación ejecute el mandato **enable source routing** para activar el direccionamiento en origen para el puerto de puente.
   - ***Para interfaces Ethernet:***

Asegúrese de que el puenteo transparente está habilitado en el puerto de puente. Ejecute el mandato **enable transparent**.

4. Si va a configurar el direccionador para ***DLSw y puenteo concurrente:***

   Cree un filtro de protocolos contra los SAP (puntos de acceso a servicio) que quiere que DLSw utilice. Es esencial hacer esto si el direccionador va a realizar operaciones de puenteo y a reenviar paquetes vía DLSw. Si no lo hace, los paquetes DLSw recibidos por el puente serán reenviados por DLSw y enviados por puente por el direccionador. La idea es evitar el reenvío (envío por puente) de los paquetes DLSw en paralelo con el direccionamiento DLSw.

   Para crear un filtro de SAP, ejecute 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 igual a 4 en el puerto designado para DLSw (tenga en cuenta que esto asume que ha escogido un SAP igual a 4 para el tráfico DLSw. Esto es algo que realiza durante la configuración de DLSw).

5. Habilite DLSw mediante el mandato **enable dls**.Esto habilita el protocolo de DLSw en el puerto de puente que ha designado.

6. Verifique la configuración de ASRT. No es necesario hacerlo, pero es una buena idea comprobar la configuración del puente antes de continuar. Utilice el mandato **list bridge** para verificar la configuración del protocolo ASRT. El ejemplo siguiente muestra los resultados del mandato list bridge después de la configuración de 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 de IP para DLSw

Necesita configurar IP para que el direccionador local DLSw pueda establecer conexiones TCP con otros iguales DLSw. Para hacerlo:

1. Entre en el proceso de configuración de IP mediante 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 va a utilizar para conectar con el otro igual DLSw.
3. Habilite el direccionamiento dinámico. Debe asegurarse de que los asociados DLSw tienen una ruta hacia la dirección interna del otro. La forma más sencilla de conseguirlo es habilitar el direccionamiento dinámico utilizando RIP u OSPF como protocolo de direccionamiento. Se recomienda utilizar OSPF, ya que normalmente requiere menos actividad general de red que RIP.
   - Para habilitar OSPF, consulte el apartado “Configuración de OSPF para DLSw” para habilitar OSPF.
   - Para habilitar RIP, entre **enable RIP** en el indicador `IP Config>` para habilitar RIP.
4. Defina la dirección IP interna. Utilice el mandato **set internal-ip-address** para definir la dirección que pertenece al direccionador en su totalidad, y no a cualquier interfaz en particular. El direccionador utiliza la dirección IP interna al establecer la conexión TCP con el otro igual DLSw.
   - Si utiliza RIP, la dirección interna puede anunciarse si se anuncian las rutas de sistema principal. Para habilitar el anuncio del sistema principal en las rutas RIP, utilice el mandato **enable sending host-routes** de configuración de IP.
   - Si utiliza OSPF, la dirección interna se anuncia automáticamente.

Configuración de OSPF para DLSw

Si desea utilizar OSPF como protocolo de direccionamiento, debe configurarlo de la forma siguiente:

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 va a utilizar para conectar con el otro igual DLSw.
3. *Habilite el direccionamiento dinámico*. Utilice el mandato **enable ospf** para habilitar el direccionamiento. Si va a utilizar la función de grupos de DLSw, debe habilitar el protocolo de direccionamiento de OSPF y el direccionamiento de multidifusión de OSPF desde el indicador `Config>` de OSPF. Todos los valores por omisión de OSPF funcionan correctamente. Sólo necesita habilitar OSPF y OSPF de multidifusión después de utilizar el mandato **join-group** en lugar de utilizar la adición de vecino TCP 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 para V.25bis, no pueden definirse los parámetros de enlace físico a nivel de SDLC ya que deben configurarse a nivel de V.25bis. En este caso no debe configurar los siguientes parámetros SDLC:

- Role (Cometido) - Debe ser primario.
- Group (Grupo) - No puede definir una dirección de sondeo de grupo.
- Type (Tipo) - Debe ser punto a punto.
- Duplex (Dúplex)
- Idle state (Estado desocupado)
- Clocking (Cronometraje)
- Speed (Velocidad)
- Cable (Cable)
- Encoding (Codificación)
- Inter-frame delay (Retraso entre tramas)

Debe configurar enlaces SDLC si tiene previsto dar soporte a SDLC sobre DLSw. Esta sección explica como acceder a la consola de configuración de SDLC, y describe los mandatos relacionados con SDLC.

Si hay conectado directamente un dispositivo SDLC, configure el protocolo SDLC de la forma siguiente:

1. Establezca el enlace de datos en SDLC: En el indicador `Config>`, utilice el mandato **set data-link SDLC** para configurar el tipo de enlace de datos para 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 usted añade estaciones SDLC y el software asigna los siguientes valores por omisión a las estaciones:
   - El BTU máximo es el máximo asignable por la interfaz
   - Las ventanas Tx y Rx son 7 para Mod 8, y 127 para Mod 128
4. El cometido del enlace es primario por omisión. Si es necesario, cambie el cometido del enlace a secundario o a negociable mediante el mandato **set link role**.
5. Puede configurar el sondeo de grupo para estaciones secundarias en el enlace. Para hacerlo, defina la dirección de sondeo de grupo mediante 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 grupo.
6. Defina el origen de cronometraje del enlace (Opcional): Si desea conectar directamente 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 línea (Opcional): Si va a utilizar cronometraje interno, utilice el mandato **set link speed** para escoger la velocidad de cronometraje de esta línea.

Nota: Si va a utilizar SDLC para conectar desde un PC, debe también definir la codificación (NRZ/NRZI), y el dúplex (completo/medio) para que coincidan con la configuración del PC.

8. Defina el cable de enlace en RS-232, X.21, V.35, o V.36.
9. Verifique la configuración de SDLC: Utilice el mandato **list link** para verificar la configuración de la interfaz SDLC.

Configuración de interfaces X.25

Configure la interfaz X.25 si tiene previsto utilizar el soporte de DLSw para los dispositivos QLLC. Siga los pasos siguientes:

1. Defina la interfaz para que sea 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** en el indicador `Config>`. Se le solicitará un número de interfaz, y a partir de aquí entrará una serie de mandatos en el indicador `X.25>`.
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 correspondiente a los números de canal lógico que se utilizarán para los PVC y que estarán disponibles para que los SVC los utilicen. Cualquier PVC que defina en la configuración de DLSw debe tener números de canal comprendidos en el rango que ha definido aquí. En el caso de los SVC, debe asegurarse de que el número de canales disponibles para las llamadas de entrada y de salida es suficiente para el número de llamadas simultáneas que espera que DLSw pueda emitir o contestar.
5. Utilice el mandato **add protocol** para añadir "dls" como el protocolo que operará sobre X.25 en esta interfaz. X.25 entiende que este hecho implica el soporte QLLC, y solicita una serie de parámetros QLLC convencionales cuyo valor se aplicará a todos los circuitos virtuales DLSw de esta interfaz.
6. Utilice el mandato **add pvc** para asociar un determinado número de canal lógico PVC al protocolo DLSw. Debe hacer esto para cada PVC de esta interfaz que DLSw vaya a utilizar (es decir, cada PVC para el que ejecuta el mandato **add qllc station** de configuración de DLSw). El número de canal lógico es la clave que se utilizará para contrastar la configuración de DLSw de esta estación con esta definición de PVC X.25.
7. Utilice el mandato **add address** para crear una lista de direcciones DTE X.25 para todos los PVC y SVC definidos en la configuración de DLSw. Tenga presente que DLSw no utiliza direcciones DTE para los PVC, pero son necesarias dentro de la configuración de X.25. No es necesario añadir las direcciones DTE de las estaciones finales QLLC que pueden realizar llamadas dinámicas de entrada a DLSw y no están configuradas en DLSw.
8. Establezca las características de personalidad nacional y las capas físicas necesarias para la conexión a la red X.25. En el capítulo dedicado a la configuración de la interfaz X.25 de la publicación *Access Integration Services Guía del usuario de software* hallará la descripción de los parámetros configurables de X.25.

Configuración de DLSw

Antes de configurar DLSw, entre el mandato **list device** en el indicador `Config>` para listar los números de interfaz de diferentes dispositivos.

Para configurar el protocolo DLSw:

1. En el indicador `Config>`, entre el mandato **protocol dls**. Esto hace aparecer el mandato `DLSw config>`.
2. En el mandato `DLSw config>`, entre el mandato **enable dls** para habilitar DLSw en el direccionador.
3. Entre el mandato **set srb** para designar el número de segmento SRB (puenteo de ruta en origen) para el direccionador DLS.

   Este número de segmento SRB debe ser el mismo para todos los direccionadores DLSw conectados a la misma LAN, y debe ser exclusivo en el dominio del puente de ruta en origen. El puente utiliza este número en el Campo de información de direccionamiento (RIF) cuando se envían las tramas en la LAN. El número de segmento es la clave para evitar los bucles.
4. Entre el mandato **open-sap** para cada SAP que desee que DLSw conmute. El direccionador solicitará números de interfaz. Para abrir los SAP de SNA más utilizados normalmente (4, 8 y C), especifique SNA. Como mínimo, abra los SAP 0 y 4. Para abrir el SAP de 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 igual DLSw que desee configurar. Si desea que el direccionador acepte conexiones procedentes de iguales no configurados, utilice el mandato **enable-dynamic neighbor**. Las conexiones TCP también pueden establecerse utilizando OSPF de multidifusión y el mandato **join-group**.

   Nota: Un direccionador puede participar en un grupo ***sólo*** si su direccionador igual es una plataforma basada en AIS que ejecuta DLSw. Si configura un direccionador para un grupo, debe habilitar OSPF y MOSPF en todos los direccionadores DLSw del grupo.
6. Para que su configuración de DLSw dé soporte a SDLC, debe añadir una estación de enlace SDLC mediante el mandato **add sdlc**.
7. Para que su configuración de DLSw dé soporte a QLLC, añada una estación de enlace QLLC con el mandato **add qllc station**.

   O si desea dar soporte a los SVC dinámicos, habilite interfaces X.25 para llamadas de entrada con el mandato **enable qllc callin**, y defina destinos DLSw con el mandato **add qllc destination**.

Ejemplo de configuración DLSw

El siguiente ejemplo de configuración DLSw asume que no se ha configurado el dispositivo para ningún otro protocolo ni enlace de datos. Por este motivo, las secuencia de pasos empieza con el indicador `Config (only)>`, en lugar de `Config>`.

Diagrama de ejemplo

Este ejemplo está basado en la información mostrada en Figura 46.

El direccionador DLSw que se va a configurar (R1 en el diagrama) da soporte a una conexión SDLC y una LLC con su igual DLSw (R2). La conexión TCP entre los dos direccionadores se realiza sobre una línea serie.

La configuración de R1 para DLSw requiere toda la información mostrada. Esta información incluye:

- La dirección IP interna de R1 y R2
- La dirección IP de cada puerto utilizado para mantener la conexión TCP entre los direccionadores
- Los números de interfaz asignados a los dispositivos SDLC y de red en anillo, que se utilizan para la conexión TCP
- La dirección MAC del dispositivo SDLC conectado
- La dirección MAC del dispositivo QLLC conectado
- El número de segmento del puente de ruta en origen del dispositivo de red en anillo conectado

El ejemplo indica dónde se proporciona esta información a lo largo del procedimiento de configuración.

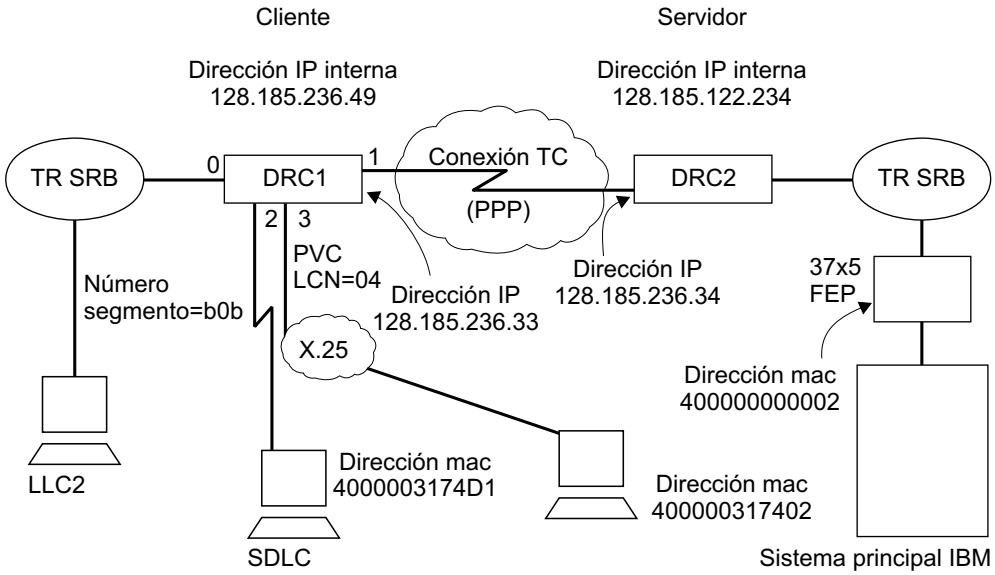


Figura 46. Ejemplo de diagrama para la configuración de DLSw

Ejemplos de mandatos de configuración

Esta sección proporciona ejemplos de lo siguiente:

Paso 1: Añadir dispositivos

Los dispositivos que va a añadir son de red en anillo, SDLC o QLLC. Tal vez añada también Ethernet como puerto de puente transparente. Para una mejor ilustración, este ejemplo de configuración de DLSw da soporte a SDLC, LLC y QLLC. Si embargo, sólo es necesario dar soporte a uno de estos enlaces de datos en una configuración real.

En el caso de SDLC y QLLC, debe establecer de forma explícita el enlace de datos, ya que la interfaz también da soporte a otros enlaces de datos como por ejemplo FR, X.25 y SDLC Relay.

```
Config (only)>set data-link sdlc 2
Config (only)>set data-link x25 3
```

Después de añadir los dispositivos, puede listarlos para verificar que se han asignado a las interfaces de direccionador adecuadas.

Entre el mandato **list device** en el indicador `config>` para visualizar un alista 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 el 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. Normalmente se utiliza el valor de 16 Mbps con cables UTP, así que es lo que se ha hecho en este caso. El mandato **list** mostrado en estos procedimientos no es necesario en este punto ni en ningún momento durante 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 WAN (TCP/IP). El enlace de datos seleccionado para el 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 debe 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 cronometraje 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 cronometraje, puede comprobar la configuración con el mandato **list hdlc** talcomo 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 va a configurar DLSw para que de soporte a SDLC, el siguiente paso es configurar SDLC. La mayoría de elementos configurables no necesitan modificación.

   Para acceder a la configuración de SDLC, utilice el mandato **network** y el número de la interfaz a la que se ha asignado un dispositivo SDLC (en este caso, 2).

```
Config>network 2
SDLC user configuration
```

   La mayoría de información que añade al configurar SDLC está relacionada con el hardware.

   El ejemplo empieza con un mandato **list link**. El mandato **list** no altera la configuración, simplemente muestra los valores que están asociados actualmente con el enlace SDLC.

   Si va a configurar un IBM 2212 Access Utility:

```
SDLC 2 Config>list link
Link configuration for: LINK_2   (ENABLED)

Role:         PRIMARY          Type:        POINT-TO-POINT
Modulo        8                Frame Size   2048

Timers:    XID/TEST response:  2.0 sec
           SNRM response:      2.0 sec
           Poll response:      0.5 sec
           Inter-poll delay:   0.2 sec
Counters:  XID/TEST retry:  4
           SNRM retry:      6
           Poll retry:      10
```

Tal como se hizo en la configuración de un dispositivo de red en anillo, deben modificarse el tipo de cronometraje y la velocidad de línea para el dispositivo SDLC. Si va a utilizar un eliminador de módem externo, no es necesario que realice este paso.

```
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***

   Para dar soporte a la estación QLLC mostrada en la Figura 46 en la página 561, debe configurar la interfaz 3 para que sea X.25 y tener soporte QLLC para DLSw en el PVC indicado. El siguiente ejemplo empieza desde el principio con una interfaz serie que no es X.25. El siguiente ejemplo de configuración muestra el soporte 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. Registrar el número de la interfaz y utilizarlo en el mandato set data-link para configurar X.25 en la interfaz.

   En el ejemplo, se configura X.25 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: La dirección DTE “4444” utilizada para el PVC con el número de canal lógico “4” no lo utiliza DLSw, sino que sólo lo utiliza X.25 para correlacionar información de configuración. Así mismo, la dirección del protocolo DLSw (“Chicago” en este ejemplo), no tiene ningún significado para DLSw, y se utiliza sólo ayuda de referencia a las diferentes direcciones DTE que DLSw puede utilizar. A diferencia de otros protocolos que se ejecutan en X.25, la conversión de direcciones DLSw se define como parte de la configuración de DLSw y no en la configuración de X.25.

Paso 2: Configurar los protocolos

Una vez se ha completado la configuración de dispositivos, debe configurar los protocolos necesarios. Para la ejecución sobre DLSw, debe configurar los protocolos IP, OSPF (o RIP), ASRT y DLSw.

1. ***Configure IP***

   Este ejemplo empieza por la configuración de 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 acerca de este importante protocolo, consulte “Utilización de IP” en la página 235.

   - La primera cosa que se debe hacer es añadir una dirección de internet y asignarla a una interfaz por la que tiene previsto transportar 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. Esta es la dirección que utilizan los direccionadores remotos para conectar con el 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
```

- El subsiguiente uso del mandato **list** visualiza la nueva información añadida.

```
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 usar cualquiera de estos protocolos de direccionamiento. Sin embargo, si utiliza RIP, no podrá utilizar la función de grupos de DLSw.

   En primer lugar, entre un mandato **list**. El mandato visualiza la configuración por omisión de OSPF. Debe modificar esta configuración para ejecutar 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, habilite OSPF y estime el número de direccionadores externos y direccionadores OSPF.

```
OSPF Config>enable ospf
Estimated # external routes [0]? 100
Estimated # OSPF routers [0]? 25
```

- Como este ejemplo implementa la función de grupos de DLSw, debe habilitar OSPF de multidifusión, tal como se indica:

```
OSPF Config> enable multicast
Inter-area multicasting enabled? [No]:
```

- Ejecute el mandato **set interface** para cada interfaz IP física que vaya a utilizar OSPF. Este ejemplo asume que la red troncal es el área OSPF (0.0.0.0). Hasta este punto sólo 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 ejemplo siguiente muestra la pantalla 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 por omisión de OSPF 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 del puenteo de ruta en origen y habilite el puerto tal como se indica:

```
Config (only)>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>enable bridge
```

- El mandato **list port** muestra que el puerto toma el valor por omisión de puenteo transparente. El puenteo transparente es lo que desea si el dispositivo conectado es Ethernet, pero no funcionará si el dispositivo es de red en anillo. Observe que el número de puerto 1 es el puerto 1 de la interfaz 0. En otras palabras, el puerto 1 es el puerto de puente lógico de la interfaz física configurada para la red en anillo (consulte la Figura 46 en la página 561).

```
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 la ejecución sobre un enlace de datos LLC (como por ejemplo una red en anillo), DLSw necesita SRB (puenteo de ruta en origen). En este caso, la primera cosa a realizar es inhabilitar el puenteo transparente en el puerto.

  ```
  ASRT config>disable transparent
  Port Number [1]?

  ASRT config>enable source-routing
  ```

- Ahora, asigne un número de segmento al puerto. Sólo tiene que asignar números de segmento cuando configure un dispositivo de puente de ruta en origen, como por de ejemplo red en anillo. En este ejemplo (consulte Figura 46 en la página 561) **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]?
  ```

  A continuación habilite DLSw en el puerto de puente.

  ```
  ASRT config>enable dls
  ```

Una vez completados estos pasos, habilite DLSw tal como se muestra. El listado de la configuración del puente confirmará 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:Implementar el filtrado de protocolos

Este es un paso importante que se omite a menudo al configurar DLSw.

Dado que se utilizará DLSw, en lugar de puentes, para reenviar el tráfico en los SAP (puntos de acceso a servicio) 04, 08, 0C, debe añadirse un filtro de protocolo especial en la configuración de puente.

Nota: Sólo necesita implementar el filtro aquí descrito si se ha configurado el puenteo, además de DLSw, en los enlaces de WAN. Este no es el caso de este ejemplo. En este ejemplo, el procedimiento de creación de un filtro de SAP se indica sólo como referencia.

El objeto del filtro es evitar que el puente reenvíe a otros puertos paquetes que deben ser manejados por DLSw únicamente. No es apropiado que DLSw y la función de puenteo reenvíen los mismos paquetes. Cuando esto ocurre, se desarrollan condiciones de actualización que pueden provocar la disminución del rendimiento de la red.

Este mandato crea un filtro que funciona en todos los paquetes que tengan el SAP de destino 4. La posterior ejecución del mandato **list** visualiza 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 establecido el filtro que necesita, abandone la configuración de ASRT.

```
ASRT config>exit
```

Paso 4: Configurar DLSw

El paso final es la configuración del protocolo DLSw. El siguiente mandato **list** muestra los valores pr 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
```

Habilite DLSw y defina el número de segmento SRB. El número de segmento hace referencia al dispositivo de red en anillo, tal como se muestra en la Figura 46 en la página 561.

```
DLSw config>enable dls
DLSw config>set srb 020
```

Configuración de grupos DLSw y sesiones estáticas: Este ejemplo define un grupo y una sesión TCP configurada. La configuración de DLSw no requiere este paso. Sin embargo, debe definir una de las dos cosas (o bien un grupo DLSw o una sesión TCP configurada) para realizar conexiones de salida a un direccionador DLSw vecino. Si desea poder realizar conexiones de entrada de direccionadores no configurados, ejecute el mandato **enable dynamic-neighbors**.

El mandato Join-Group: El mandato **join-group** se utiliza para crear un grupo DLSw. Designe cada miembro del grupo como cliente/servidor o como igual. Igual es el valor por omisión.

En este caso, se ejecuta el mandato **join-group** para R1 (consulte la Figura 46 en la página 561), designando este direccionador DLSw como un cliente del grupo 1. Para unirse a este grupo, R2 debería ser añadido como servidor además de la ejecución del 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** se utiliza para definir vecinos de DLSw configurados de forma explícita. La dirección IP DLSw del vecino añadida aquí es la dirección interna IP del direccionador DLSw igual (llamado R2 en la Figura 46 en la página 561). También puede configurar R2 con la dirección IP de vecino de R1, o puede configurar R2 para que acepte vecinos 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), SNRM (S), or DELAYED SNRM (D) [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 de cada PVC y de cada SVC configurado. En el ejemplo de configuración, sólo existe 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 los puntos de acceso a servicio: La siguiente cosa a realizar es abrir los puntos de acceso a servicio (SAP) en cada interfaz de puenteo.

Los números de SAP 0, 4, 8 y C son SAP SNA utilizados comúnmente. Para abrir todos estos SAP, utilice la opción SNA con el mandato **open-sap** tal como se indica. Para abrir los SAP para NetBIOS, escoja la opción NB. Si lo prefiere, también puede entrar los SAP de forma individual entrando 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 después de 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 finalizado la configuración de DLSw, salga de la misma y reinicie 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

Es este capítulo se describe la manera de configurar y supervisar el protocolo DLSw (Data Link Switching). Incluye las secciones siguientes:

Acceso al entorno de configuración de DLSw

El proceso CONFIG sirve para cambiar la configuración del direccionador. La configuración nueva entra en vigor cuando se reinicia el dispositivo.

Para entrar el proceso de configuración, entre **talk 6** (o **t 6**), en el indicador OPCON (*). Con ello, aparecerá el indicador `CONFIG>` tal y como se muestra en el ejemplo siguiente:

```
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 de forma inmediata, pulse de nuevo la tecla **Intro**.

Los mandatos de configuración de DLSw se entran en el indicador `DLS config>`. Para acceder a este indicador, entre el mandato **protocol DLSw** como se indica a continuación:

```
Config>protocol dls
DLSw protocol user configuration
DLSw config>
```

Requisitos de preconfiguración

Antes de dar comienzo a los procedimientos de configuración, utilice el mandato **list device** en el indicador **config** para elaborar una lista de los números de interfaz de los diferentes dispositivos. Si necesita alguna explicación más de los mandatos de configuración, consulte los mandatos de configuración que se describen en este capítulo.

Mandatos de configuración de DLSw

En este apartado se resumen y explican los mandatos de configuración de DLSw. Éstos permiten crear o modificar una configuración DLSw. En la Tabla 35 en la página 576 se da un breve resumen de cada uno de los mandatos. Los mandatos de configuración de DLSw deben entrarse a continuación del indicador `DLSw Config>`. Los valores por omisión de los mandatos y sus parámetros van entre corchetes inmediatamente después del indicador.

Los cambios efectuados en la configuración del direccionador no entran en vigor de manera inmediata, sino que pasan a formar parte de la configuración SRAM del direccionador cuando éste se reinicia.

Tabla 35. Resumen de los mandatos de configuración de DLSw

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Add	Añade una estación de enlace SDLC, una dirección IP de vecino TCP, un destino o estación QLLC, entradas de antememoria, entradas de lista de direcciones MAC, alteraciones temporales de prioridad de circuito o alteraciones temporales de explorador de antememoria MAC.
Ban	Permite el acceso al indicador BAN (nodo de acceso de límites) a fin de que se puedan entrar los mandatos de configuración de BAN.
Close-Sap	Cierra el SAP (punto de acceso a servicio) abierto actualmente. DLSw utiliza los SAP para las comunicaciones en interfaces que dan soporte a LLC.
Delete	Elimina una estación de enlace SDLC configurada, una conexión TCP, un destino o estación QLLC, entradas de antememoria, entradas de lista de direcciones MAC, alteraciones temporales de prioridad de circuito o alteraciones temporales de explorador de antememoria MAC.
Disable	Inhabilita el protocolo DLSw, la estación de enlace SDLC, la función de desconexión LLC, los vecinos dinámicos, una interfaz o estación QLLC, o bien la utilización de listas de direcciones MAC remotas y locales.
Enable	Habilita el protocolo DLSw, la estación de enlace SDLC, la función de desconexión LLC, los vecinos dinámicos, una interfaz o estación QLLC, la utilización de listas de direcciones MAC remotas y locales, o bien el establecimiento de los bits de precedencia DLSw IPv4.
Join-Group	Permite que los vecinos DLSw se hallen dinámicamente unos a otros.
Leave-Group	Retira al direccionador del grupo DLSw especificado.
List	Visualiza información correspondiente a las estaciones de enlace SDLC, los SAP, la prioridad de circuito, los grupos DLSw, la información global DLSw, las interfaces, estaciones y destinos QLLC, las entradas de antemoria o las entradas de lista de direcciones MAC. También facilita información detallada sobre las conexiones TCP.
NetBIOS	Proporciona acceso al indicador de configuración NetBIOS.
Open-SAP	Permite que DLSw transmita datos a través del SAP especificado. DLSw utiliza los SAP para las comunicaciones en interfaces que dan soporte a LLC.
Set	Configura los parámetros LLC2, el número máximo de sesiones DLSw, el número de segmento de SRB, el tamaño de antememoria TCP, la asignación de memoria, los temporizadores de protocolo, la prioridad de circuito, los parámetros de los vecinos dinámicos, los parámetros de funcionamiento de QLLC y los 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 xxxi.

Add

El mandato **add** sirve para configurar una estación de enlace SDLC, una dirección IP de vecino TCP, un destino o estación QLLC, entradas de antememoria, entradas de lista de direcciones MAC, alteraciones temporales de prioridad de circuito y alteraciones temporales de explorador de antememoria MAC.

Sintaxis:

a**dd**	cache-entry
	explorer-override
	mac-list
	priority
	gllc...
	sdlc
	tcp

cache-entry

Añade una entrada de antememoria MAC configurada. Esta entrada de antememoria correlaciona una dirección MAC determinada con un igual DLSw concreto. Una dirección MAC puede estar correlacionada con varios iguales DLSw; para ello, basta con añadir varias entradas de 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 alteración temporal de explorador de antememoria MAC. Esta alteración temporal permite que un conjunto de direcciones MAC posea características diferentes de flujo de explorador y antememoria MAC. Cuando se crea una entrada de antememoria MAC, se realiza una búsqueda en la lista alteraciones temporales de explorador siguiendo el orden en que están configuradas. Si se halla una coincidencia, se utilizan los parámetros relacionados con el explorador y la antememoria MAC procedentes de la primera alteración temporal de explorador coincidente. Si no se encuentra ninguna coincidencia, se utilizan los valores relacionados con el explorador y la antememoria MAC globales.

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

Combinados, estos dos campos representan un conjunto de direcciones MAC. Para determinar si, en el caso de una dirección MAC específica, se debe utilizar un registro de alteración temporal de explorador de antememoria MAC configurado junto con el valor y la máscara dados, se utiliza el algoritmo siguiente:

```
si ((<dirección MAC específica>Y<máscara de la alteración temporal>)
== <valor de la alteración temporal>)
se encuentra una coincidencia para la alteración temporal de explorador;
se debe utilizar el valor de la alteración temporal
```

Database age timeout
: Especifica por cuánto tiempo se conservan las entradas DLSw no utilizadas. Las entradas de base de datos correlacionan las direcciones MAC de destino con el conjunto de iguales DLSw que pueden llegar hasta ellas.

  El valor cero indica que la antigüedad de las entradas de esta base de datos es indiferente. Esto puede resultar útil cuando se ejecutan conexiones TCP de vecino en interfaces de marcación, pero no suele ser recomendable porque inhabilita otras funciones DLSw.

Max wait timer ICANREACH
: Especifica por cuánto tiempo se ha de esperar a recibir una respuesta ICANREACH a un mensaje CANUREACH transmitido con anterioridad.

Neighbor priority wait timer
: Especifica el tiempo que ha de esperarse mientras dura la exploración antes de seleccionar un vecino. Esto permite seleccionar un vecino de mayor prioridad, aunque éste no sea el primero en responder con un mensaje ICANREACH.

  El valor cero indica que no se utilizará la función de prioridad de vecino. No habrá información de igual DLSw en antememoria para la dirección MAC. Se envía siempre CANREACH y se utiliza el primer igual DLSw que envíe ICANREACH (con independencia de cuál sea su prioridad).

Delay sending TEST response
: Tiempo que ha de esperarse una vez realizada la exploración en busca de una dirección MAC antes de enviar una respuesta TEST. Esto resulta útil si hay dos 2212 DLSw en una misma red puenteada capaces de llegar a la misma dirección MAC a través de iguales DLSw. Si uno de los 2212 DLSw tiene mayor preferencia, se puede retardar la respuesta TEST del 2212 DLSw con menor preferencia.

Forwarding explorers
: Especifica si los exploradores han de reenviarse a todos los iguales DLSw pertinentes, únicamente en la conexión TCP local o bien no se han de reenviar en absoluto.

Position in explorer override list to insert new entry
: Dado que se utiliza la primera coincidencia de alteración temporal de explorador de antememoria MAC, el orden en que están configuradas las entradas de alteración temporal de explorador es importante. Este campo especifica dónde se ha de insertar la entrada nueva en la lista actual de alteraciones temporales. Para ver esta lista, se puede utilizar el mandato **list explorer-override**. Si el valor de esta campo es cero, indica que la entrada nueva se ha de añadir al final de la lista actual.

mac-list Añade una entrada de lista de direcciones MAC locales. Todas las entradas de lista de direcciones MAC locales añadidas forman la lista de direcciones MAC locales. Esta lista de envía a cada uno de los

iguales DLSw para indicar cuál es el conjunto de direcciones MAC a las que se pueden llegar 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
: Combinados, estos dos campos representan un conjunto de direcciones MAC a las que se puede llegar utilizando este DLSw. Si se recibe una trama en un DLSw igual, se utilizan ambos campos en el algoritmo siguiente:

```
si ( (<dirección MAC de destino de la trama> Y <MAC Address Mask>)
     == <MAC Address Value> )
se encuentra una coincidencia en la lista de direcciones MAC; se reenvía la trama a este DLSw
```

priority Añade una entrada de alteración temporal de prioridad de circuito. Cuando se establece una sesión DLSw, se realiza una búsqueda en la lista alteraciones temporales de prioridad de circuito siguiendo el orden en que están configuradas. Si se halla una coincidencia del rango SAP de origen y rango de direcciones MAC de origen y del rango SAP de destino y rango de direcciones MAC de destino, se utilizan las prioridades de explorador y sesión de la entrada de alteración temporal de prioridad de circuito coincidente. Si no se encuentra ninguna coincidencia con una entrada de alteración temporal de prioridad de circuito, se utilizan los valores de prioridad de circuito por omisión.

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
: Combinados, estos dos campos representan el rango de SAP de origen asignado a esta alteración temporal de prioridad de circuito. Si el valor del SAP de origen no importa, especifique el rango completo de valores de SAP de origen (lower source sap value = 0 y upper source sap value = fe).

Lower source MAC address

Upper source MAC address
: Combinados, estos dos campos representan el rango de direcciones MAC de origen asignado a esta alteración temporal de prioridad de circuito. Si el valor de la dirección MAC de origen no importa, especifique el rango completo de valores de dirección MAC de origen (lower source MAC address = 000000000000 y upper source MAC address = ffffffffffff).

Lower destination sap value

Upper destination sap value
: Combinados, estos dos campos representan el rango de SAP de destino asignado a esta alteración temporal de prioridad de circuito. Si el valor del SAP de destino no importa, 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
: Combinados, estos dos campos representan el rango de direcciones MAC de destino asignado a esta alteración temporal de prioridad de circuito. Si el valor de la dirección MAC de destino no importa, especifique el rango completo de valores de dirección MAC de destino (lower destination MAC address = 000000000000 y upper destination MAC address = ffffffffffff).

Priority for session traffic
: Prioridad de circuito que debe asignarse al tráfico de sesiones 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 alteración temporal de prioridad de circuito.

Priority for explorer traffic
: Prioridad de circuito que debe asignarse al tráfico de exploradores 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 alteración temporal de prioridad de circuito.

Position in circuit priority override list to insert new entry
: Dado que se utiliza la primera coincidencia de alteración temporal de prioridad de circuito, el orden en que están configuradas las entradas de alteración temporal de prioridad de circuito es importante. Este campo especifica dónde se ha de insertar la entrada nueva en la lista actual de alteraciones temporales de prioridad de circuito. Para ver esta lista, se puede utilizar el mandato **list priority**. Si el valor de esta campo es cero, indica que la entrada nueva se ha de añadir al final de la lista actual.

qllc Añade soporte para una estación QLLC de una red X.25 o para un destino DLSw de estaciones QLLC. Una estación QLLC es la estación de enlace local que representa un dispositivo QLLC conectado al direccionador por medio de una interfaz X.25. Un destino QLLC es una correlación de dirección que apunta a un dispositivo de la red DLSw. Dicho dispositivo está conectado a un direccionador DLSw vecino por medio de cualquiera de los tipos de DLC soportados y, a menudo, no es un dispositivo QLLC en sí.

Sintaxis:

a**ddq**l**lc**	destination 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 con la que deben coincidir los bytes 4-11 de los datos de usuario de llamada de los paquetes Call_Request entrantes. En muchos productos QLLC, este valor está configurado como contraseña.

  PRECAUCIÓN:
  Si un registro QLLC Destination está configurado con "ANYCALL", DLSw aceptará todas las llamadas (con independencia de la dirección de DTE o del ID de conexión). Conviene tenerlo presente, puesto que aceptar todas las llamadas entrantes entraña un riesgo para la seguridad.

Destination MAC address
: Dirección MAC que debe utilizarse como destino de las sesiones iniciadas por una llamada QLLC entrante en la que el paquete Call_Request coincida con el ID de conexión anterior.

Destination SAP
: SAP de destino que debe utilizarse 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 #
: Número de la interfaz X.25 por la que el dispositivo QLLC está conectado al direccionador.

PVC or SVC
: Tipo de circuito virtual (permanente o conmutado) por el que se ha de conectar el dispositivo QLLC.

Logical channel number
: Para PVC, número de canal X.25 al que está abonada la estación QLLC. Este campo no es aplicable a los SVC, que utilizan números de canal asignados dinámicamente.

DTE address
: Para SVC, número “de teléfono” por el que la red X.15 conoce a la estación QLLC. Es la dirección de la parte que recibe la llamada, si se trata de llamadas efectuadas por el direccionador, y la dirección de la parte que realiza la llamada, si se trata de llamadas procedentes de la estación QLLC. Este campo no es aplicable a los PVC, que pueden identificarse de forma exclusiva mediante un número de canal lógico fijo.

Source MAC address
: Dirección MAC (control de acceso al medio) que representa esta estación QLLC en el resto de la red DLSw. Es la dirección de origen de las sesiones DLSw iniciadas por la estación QLLC y la dirección de destino de las sesiones iniciadas por otros dispositivos de la red DLSw.

  Esta dirección es obligatoria para cada una de las estaciones y debe ser exclusiva entre todas las direcciones MAC de origen de los dispositivos SDLC y QLLC configurados en el direccionador. Para que funcione de forma fiable, también debe ser exclusiva entre todas las direcciones MAC de estación final de la red DLSw. El valor por omisión se construye de manera que sea exclusivo, con toda probabilidad, dentro de la red. El formato de ésta y todas las direcciones MAC DLSw sigue el orden de bits (de red en anillo) no canónico.

Source SAP
: Dirección SAP (punto de acceso a servicio) que forma pareja con la dirección MAC de origen. Se utiliza de la misma forma.

Destination MAC address
: Dirección MAC (control de acceso al medio) que representa esta la estación QLLC de la red DLSw a la que se ha de conectar el dispositivo QLLC. Para PVC, DLSw intenta iniciar una sesión en esta dirección de destino en cuanto se establece contacto de manera satisfactoria con el dispositivo QLLC. Para SVC, DLSw intenta iniciar una sesión en esta dirección de destino en cuanto el dispositivo QLLC efectúa una llamada entrante.

  Esta dirección no es obligatoria. Si no la configura, la estación QLLC sólo puede ser el destino de una sesión DLSw en lugar del origen.

Destination SAP
: Dirección SAP (punto de acceso a servicio) que forma pareja con la dirección MAC de destino. Se utiliza de la misma forma. Tanto la dirección MAC de destino como el SAP de destino deben ser distintos de cero para que DLSw los utilice como destino de una sesión DLSw.

PU type
: Tipo de PU (unidad física) SNA de la estación QLLC. Puede tener uno de los valores siguientes:

  2 Nodo PU 2.0 o T2.1. También puede representar dispositivos que envían XID_1s como respuesta a un sondeo XID_null.

  4 Controlador SNA intermedio que realiza funciones de direccionamiento SNA de subárea. Normalmente, éstas ejecutan el software NCP de IBM en modalidad INN (nodo intermedio de red) para otro NCP y ***no*** sirven para las conexiones de función de límite NCP con dispositivos PU 2.

  5 Sistema principal, con o sin procesador front-end (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 efectúa una conexión con un dispositivo T2.1 de la red DLSw, es preferible, pero no obligatorio, configurar el sistema

principal en sí como dispositivo T2.1 (es decir, PU type=2, XID0 block/id num=0).

XID0 block num
: Campo de número de bloque XID que debe utilizar el direccionador cuando construya XID_0 en nombre de la estación QLLC. Este campo es aplicable, y se solicita, sólo si el tipo de PU es 2. Para los dispositivos T2.1 y los dispositivos PU 2.0 que puedan responder por sí mismos a un sondeo XID_null, este campo es opcional y debe dejarse a cero. Si no está seguro, lo mejor es cumplimentarlo para todos los dispositivos QLLC PU2.0 QLLC y dejarlo a cero para todos los dispositivos T2.1. Si es distinto de cero, debe coincidir con el campo de dirección de PU correspondiente de la configuración de nodo principal conmutado NCP de IBM de la estación de enlace.

XID0 id num
: Campo de número identificador XID que va junto con el campo de número de bloque XID0. Se utiliza con la misma finalidad y se necesita en las misma situaciones.

sdlc Añade información SDLC específicamente para añadir una estación de enlace SDLC a la configuración de una interfaz serie SDLC dada. El mandato **sdlc** debe utilizarse 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 #
: Número de la interfaz SDLC por la que el dispositivo SDLC está conectado al direccionador.

SDLC Address
: Dirección SDLC de la estación de enlace que va a conectar; está comprendida entre 01 y FE o bien es “sw”. “Sw” indica que se trata de un circuito de llamada entrante SDLC conmutado.

Source MAC address
: Dirección MAC de esta PU SDLC. Este valor identifica la estación SDLC conectada dentro del dominio DLSw. Debe ser exclusivo dentro de las estaciones SDLC y QLLC conectadas al direccionador, así como también entre todas las redes LAN, SDLC y QLLC.

Source SAP in hex
: Junto con la dirección MAC de origen, representa la estación final SDLC dentro del dominio DLSw.

Destination MAC Address
: Dirección MAC de la estación de enlace remota a la que va a conectarse. El formato sigue el orden de bits (de red en anillo) no

canónico. Esto se cumple aunque la estación final remota sea Ethernet. Utilice el mandato de supervisión de ASRT **flip** a modo de ayuda para darle la vuelta la dirección MAC, en tales casos.

Nota: La dirección de destino no puede tener el valor 0 si se trata de un circuito de llamada entrante SDLC conmutado (lo que viene indicado por “sw” como dirección SDLC).

Destination SAP in hex
Define el SAP que ha de utilizarse al intentar automáticamente establecer una conexión cuando se activa la estación de enlace. Si este SAP es 0, entonces la estación de enlace está en modalidad pasiva y no inicia el establecimiento de línea. En tal caso, se hace caso omiso de la dirección MAC de destino.

Nota: El SAP de destino no puede tener el valor 0 si se trata de un circuito de llamada entrante SDLC conmutado (lo que viene indicado por “sw” como dirección SDLC).

PU type
Tipo de PU (unidad física) SNA de la estación SDLC. Puede tener uno de los valores siguientes:

1 Nodo PU1. Si se selecciona el tipo de PU 1, se le pedirá al usuario que seleccione si se comunica con el dispositivo PU4/5 por medio de SDLC, por LAN, o como emulación de 2.0. Esto permite al usuario elegir la manera en que el dispositivo PU1 conectado a SDLC se comunica con el dispositivo PU4/5.

2 Nodo PU 2.0 o T2.1.

4 Controlador SNA intermedio que realiza funciones de direccionamiento SNA de subárea. Normalmente, éstas ejecutan el software NCP de IBM en modalidad INN (nodo intermedio de red) para otro NCP y *no* sirven para las conexiones de función de límite NCP con dispositivos PU 2.

5 Sistema principal, con o sin procesador front-end (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 sistema principal efectúa una conexión con un dispositivo T2.1 de la red DLSw, debe configurar el sistema principal en sí como dispositivo T2.1 (es decir, PU type=2, XID0 block/id num=0).

El dispositivo PU1 se comunica con el dispositivo PU4/5 Si se elige el tipo de PU 1, se elige también el método por el que el dispositivo PU1 se comunica con el dispositivo PU4/5. Las opciones son:

SDLC El dispositivo PU1 conectado a SDLC se comunica con un dispositivo PU4/5 conectado a SDLC que da soporte a dispositivos PU1 conectados a SDLC.

LAN El dispositivo PU1 conectado a SDLC se comunica con un dispositivo PU4/5 conectado a LAN que da soporte a dispositivos PU1 conectados a LAN. Esta opción se utiliza muy pocas veces.

as Emulated 2.0
El dispositivo PU1 conectado a SDLC se comunica con un dispositivo PU4/5 conectado a LAN que no da soporte a dispositivos PU1 conectados a LAN. Esto se consigue emulando el dispositivo PU1 como si fuese un dispositivo PU2.0 para el sistema principal (éste debe tener definido el tipo de PU como 2). Esta opción sirve también para que un dispositivo PU1 conectado a SDLC se comunique con un dispositivo conectado a canal, a SDLC o a QLLC.

Nota: No puede establecer este parámetro para un circuito de llamada entrante SDLC conmutado. Se supone que el tipo de PU es 2.0.

XID0 block num
Campo de número de bloque XID que debe utilizar el direccionador cuando construya XID_0 en nombre de la estación SDLC. Este campo es aplicable, y se solicita, sólo si el tipo de PU es 1 o 2. Para los dispositivos T2.1 y los dispositivos PU 2.0 que puedan responder por sí mismos a un sondeo XID_null, este campo es opcional y debe dejarse a cero. Si no está seguro, lo mejor es cumplimentarlo para todos los dispositivos SDLC PU2.0 y dejarlo a cero para todos los dispositivos T2.1. También debe dejarse a cero para los dispositivos PU1 que se comunican dispositivos conectados a SDLC que dan soporte a dispositivos PU1. Si es distinto de cero, debe coincidir con el campo de dirección de PU correspondiente de la configuración de nodo principal conmutado NCP de IBM de la estación de enlace.

Nota: Si ha definido este parámetro como un valor distinto de cero para un circuito de llamada entrante SDLC conmutado, la información configurada se coloca en XID_0. Para un circuito de llamada entrante SDLC conmutado, el número de bloque XID_0 configurado se utiliza de una manera distinta. El software supone que la estación de llamada entrante construirá siempre un XID_0 propio. Si se define este parámetro como un valor distinto de cero, se modifica el XID_0 de la estación con el valor configurado. Si se define este parámetro como cero, no se modifica el XID_0If de la estación.

XID0 id num
Campo de número identificador XID que va junto con el campo de número de bloque XID0. Se utiliza con la misma finalidad y se necesita en las misma situaciones.

Poll type
Define cómo y cuándo se debe sondear el dispositivo SDLC:

TEST Sondear el dispositivo SDLC con la trama TEST al activarse la interfaz.

SNRM Sondear el dispositivo SDLC con una trama SNRM al activarse la interfaz.

DELAYED SNRM
Sondear el dispositivo SDLC con una trama SNRM cuando se ha establecido la sesión DLSw y está activa la interfaz.

tcp Añade la dirección interna de un igual 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 igual DLSw remoto de la red IP con el que desea realizar una conexión.

Connectivity setup type
Indica si la conexión TCP con este DLSw debe realizarse al iniciarse el direccionador (Active) o según convenga (Passive). Si desea ver una visión general de esta opciones, consulte el apartado “Conexiones TCP, descubrimiento de vecinos y exploración de multidifusión” en la página 538.

Transmit Buffer Size
Tamaño del almacenamiento intermedio de transmisión de paquetes, comprendido entre 1024 y 32768. El valor por omisión es 5120.

Receive Buffer Size
Tamaño del almacenamiento intermedio de recepción de paquetes, comprendido entre 1024 y 32768. El tamaño por omisión es 5120.

Maximum Segment Size
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 (Disable).

Enable/Disable NetBIOS SessionAlive Spoofing (E/D)
Indica si desea descartar las tramas I SessionAlive de NetBIOS (no reenviar al asociado DLSw). El valor por omisión es D (Disable), que significa no descartar la trama.

Neighbor Priority
Permite especificar la prioridad de vecino como High (alta), Medium (media) o Low (baja). Si a una estación de destino se puede llegar a través de varios direccionadores vecinos que tienen diferentes prioridades, DLSw intenta establecer circuitos que lleven a dicha estación por medio del vecino cuya prioridad sea mayor.

BAN

El mandato **ban** sirve para acceder al indicador de configuración BAN (nodo de acceso de límites). Los mandatos BAN se entran en el indicador de configuración BAN (`BAN config>`). En el apartado “BAN” en la página 86 hallará la explicación de cada uno de ellos.

Sintaxis:

b**an**

Close-Sap

El mandato **close-sap** sirve para inhabilitar la conmutación DLSw para el SAP (punto de acceso a servicio) especificado. Los SAP los utiliza LLC a efectos de 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 #

Número de interfaz utilizado por el SAP abierto.

Enter SAP

Se puede entrar SAP individuales en hexadecimal o bien se puede entrar SNA, NB (NetBIOS) o LNM (LAN Network Manager).

Si entra SAP en hexadecimal, el rango es de 0 a 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

El mandato **delete** sirve para eliminar una estación de enlace SDLC, una dirección IP de vecino TCP, un destino o estación QLLC, entradas de antememoria, entradas de direcció MAC, alteraciones temporales de prioridad de circuito y alteraciones temporales de explorador de 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 antememoria MAC configurada.

Ejemplo: `delete cache-entry`

```
Enter mac cache record number [1]? 1
MAC cache entry has been deleted
```

mac cache record number

Número de registro de la entrada de antememoria MAC que se ha de suprimir. El número de registro puede determinarse utilizando el mandato de configuración **list cache all**.

explorer-override

Elimina una entrada de alteración temporal de explorador de antememoria MAC.

Ejemplo: `delete explorer-override`

```
Enter explorer override record number [1]?
Explorer override record has been deleted.
```

Explorer override record number

Número de registro de la entrada de alteración temporal de explorador de antememoria MAC que se ha de suprimir. El número de registro puede determinarse utilizando el mandato de configuración **list explorer-override** desde *talk 6*.

mac-list Elimina una entrada de lista de direcciones MAC locales.

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

Número de registro de la entrada de lista MAC que se ha de suprimir. El número de registro puede determinarse utilizando el mandato de configuración **list mac-list all**.

priority Elimina una entrada de alteración temporal 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

Número de registro de la entrada de alteración temporal de prioridad de circuito que se ha de suprimir. El número de registro puede determinarse utilizando el mandato de configuración **list priority all**.

qllc Elimina soporte para una estación QLLC de una red X.25 o para un destino DLSw de estaciones QLLC.

Sintaxis:

del**ete** q**llc** d**estination**
s**tation**

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 prestar servicios cuando se reinicia el direccionador.

Sintaxis:

del**ete** s**dlc**

Ejemplo: `delete sdlc`

```
Interface #[0]? 1
SDLC Address or 'sw' (switched dial-in) [C1]?
Record deleted
```

Interface #
Número de interfaz del direccionador que se conecta a la estación de enlace SDLC.

SDLC Address
Dirección SDLC de la estación de enlace remota que va a suprimir. Los valores son 01–FE o “sw” para un circuito de llamada entrante conmutado.

tcp Elimina la dirección IP (*dirección_ip*) del igual DLSw con el que puede efectuar una conexión TCP.

Sintaxis:

del**ete** t**cp** *dirección_ip*

Ejemplo: `delete tcp`

```
IP Address [0.0.0.0]? 128.185.14.1
```

Disable

El mandato **disable** sirve para inhabilitar el protocolo DLSw, una estación de enlace SDLC, la función de desconexión LLC, vecinos dinámicos, una interfaz o estación QLLC, o bien la utilización de listas de direcciones MAC remotas y locales.

Sintaxis:

di**sable**
- dls
- dynamic-neighbors
- llc
- mac-list
- qllc...
- sdlc

dls Impide que el direccionador que actúa de puente lleve a cabo funciones DLSw en todas las interface DLSw configuradas.

Ejemplo: `disable dls`

dynamic-neighbors
Impide que el direccionador acepte conexiones TCP DLSw entrantes procedentes de direcciones IP *que no sean* las de aquellos vecinos DLSw que se han configurado con el mandato **add tcp**.

Ejemplo: `disable dy`

llc Impide que el direccionador termine de forma activa una conexión LLC emitiendo una trama DISC LLC. En cambio, termina las conexiones LLC de forma pasiva. Esto hace que la conxión LLC de la estación final detecte la terminación del enlace. El sistema principal IBM responde a las desconexiones activas de manera diferente a como lo hace a las pasiva.

Este mandato no afecta a la función de conmutación de LLC en DLSw. Para detener la función de conmutación LLC, utilice el mandato **close-sap**.

Ejemplo: `disable llc`

mac-list Inhabilita la utilización de listas de direcciones MAC locales o remotas.

Sintaxis:

m**ac-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 se especifica “callin”, se impide que DLSw acepte las llamadas entrantes QLLC en la interfaz X.25 especificada. Éste es el estado por omisión; para permitir las llamadas entrantes a DLSw, se debe habilitar de forma específica una interfaz.

Si se especifica “station”, se impide que una estación QLLC configurada pueda ser el origen o el destino de las sesiones DLSw.

Sintaxis:

q**llc**	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 Impide que se realicen 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

El mandato **enable** sirve para habilitar el protocolo DLSw, una estación de enlace SDLC, la función de desconexión LLC, vecinos dinámicos, una interfaz o estación QLLC, o bien la utilización de listas de direcciones MAC remotas y locales.

Sintaxis:

enable dls
dynamic-neighbors
ipv4 dlsw precedence
llc
mac-list
qllc...
sdlc

dls Habilita el funcionamiento de DLSw en el direccionador.

Ejemplo: `enable dls`

dynamic-neighbors
Define el direccionador para que acepte conexiones TCP DLSw entrantes procedentes de direcciones IP *que no sean* las de aquellos vecinos configurados con el mandato **add tcp**. Éste es el estado por omisión.

ipv4 dlsw precedence
Define el direccionador para que establezca los bits de precedencia IP para IP versión 4. Estos bits los lee la característica BRS del direccionador con el fin de priorizar el tráfico DLSw.

Ejemplo:

```
enable IPv4 DLSw Precedence
IPv4 Precedence is now enabled.
```

llc Permite que el direccionador termine una conexión LLC tras producirse la pérdida de la conexión TCP.

mac-list Inhabilita la utilización 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 Especificar “callin” hace que DLSw acepte las llamadas entrantes QLLC en la interfaz X.25 especificada.

Si se especifica “station”, se permite que una estación QLLC configurada pueda ser el origen o el destino de las sesiones DLSw. Éste es el estado por omisión de todas las estaciones QLLC configuradas.

Sintaxis:

gllc 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 que se realicen 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

El mandato **join-group** sirve para permitir que los vecinos DLSw realicen búsquedas de forma dinámica y creen sesiones TCP entre sí y para habilitar la exploración de multidifusión y la retransmisión de tramas. Si desea ver una visión general de esta funciones, consulte el apartado “Conexiones TCP, descubrimiento de vecinos y exploración de multidifusión” en la página 538. Para utilizar este mandato, la red IP que se utilice debe dar soporte al direccionamiento de multidifusión y se debe configurar OSPF y MOSPF desde el indicadore `OSPF Config>`.

A la hora de añadir un direccionador DLSw a un grupo, debe indicar si desea utilizar el modelo de identificación de grupo por ID de grupo (en el que el direccionador construye las correspondientes direcciones de multidifusión) o bien especificar las direrccciones de multidifusión usted mismo. El modelo por ID de grupo es más sencillo de configurar, pero si desea tener conectividad con productos que no sean IBM DLSw Versión 2, deberá especificar las direcciones de multidifusión usted mismo. Un direccionador puede ser miembro de ambos estilos de grupo a la vez.

Con el modelo por ID de grupo, se puede formar parte de 64 grupos como máximo. Al asignar un direccionador DLSw a un grupo, el protocolo DLSw añade automáticamente una dirección, elegida entre dos, al número de grupo para componer una dirección de multidifusión. El direccionador transmite la dirección de multidifusión para identificarse ante los demás miembros del grupo y les transmite los paquetes. Las dos direcciones que se añaden al número de grupo son 225.0.1.0 para los iguales y los clientes DLSw y 225.0.1.64 para los servidores DLSw. Por ejemplo, la dirección de multidifusión para un cliente del grupo 2 sería 225.0.1.2.

Sintaxis:

jo**in-group**

Ejemplo:

El ejemplo siguiente corresponde al valor por omisión [G]. Las descripciones dadas a continuación del ejemplo contienen información referente a (G) y a (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
Especifica si desea que el direccionador construya las direcciones de multidifusión o bien si desea proporcionarlas usted.

Multicast IP address
La dirección IP de multidifusión es una dirección IP de multidifusión conforme con DLSw Versión 2 comprendida entre 224.0.10.0 y 224.0.10.191 que se utiliza para enviar y/o recibir el tráfico de explorador DLSw.

Read Only , Write Only o Read Write
Este parámetro indica si la dirección IP de multidifusión configurada debe utilizarse únicamente para recibir el tráfico de explorador (Read Only), para enviarlo (Send Only) o para ambas cosas (Read Write).

Group ID Número del grupo del que desea que forme parte este direccionador.

Client/Server or Peer Group Member
Cometido que debe desempeñar el direccionador dentro del grupo: C significa cliente, S servidor y P igual.

Connectivity setup type
Indica si el direccionador debe unirse al grupo en calidad de mimebro activo o pasivo. Esto controla cuándo se establecen conexiones TCP con otros mimebros del grupo, según lo descrito en el apartado “Conexiones TCP, descubrimiento de vecinos y exploración de multidifusión” en la página 538.

Transmit Buffer Size
Tamaño del almacenamiento intermedio de transmisión de paquetes, comprendido entre 1024 y 32768. El valor por omisión es 5120.

Receive Buffer Size
Tamaño del almacenamiento intermedio de recepción de paquetes, comprendido entre 1024 y 32768. El tamaño por omisión es 5120.

Maximum Segment Size
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 en las conexiones abiertas dentro de este grupo. El valor por omisión es D (Disable).

Enable/Disable NetBIOS SessionAlive Spoofing (E/D)
Indica si desea descartar las tramas I SessionAlive de NetBIOS (no reenviar a los asociados DLSw de este grupo). El valor por omisión es D (Disable), que significa no descartar las tramas.

Neighbor Priority (H/M/L) [M]?
Permite especificar la prioridad de vecino como High (alta), Medium (media) o Low (baja). Si a una estación final de destino se puede llegar a través de varios direccionadores vecinos que tienen diferentes prioridades, DLSw intenta establecer circuitos que lleven a dicha estación final por medio del vecino cuya prioridad sea mayor.

Leave-Group

El mandato **leave-group** sirve para retirar el direccionador de un grupo configurado con el mandato **join-group** o para dejar de utilizar una dirección de multidifusión configurada.

Leave-group no afecta a las conexiones TCP existentes que pertenecen al grupo especificado.

Sintaxis:

le**ave-group**

Ejemplo: leave-group

```
Configure group member (G) or specific multicast address (M) -  [G]?
Group ID (1-64 Decimal) [1]? 2
```

List

El mandato **list** sirve para visualizar información DLSw referente a las estaciones de enlace SDLC, la prioridad de circuito, los SAP, los vecinos TCP, los grupos, los vecinos dinámicos, las estaciones QLLC, los destinos, las interfaces, las entradas de antememoria, las entradas de lista de direcciones MAC, las alteraciones temporales de circuito y las alteraciones temporales de explorador de antememoria MAC.

Sintaxis:

li**st**	cache dls explorer-override groups llc2 mac-list open priority qllc... sdlc tcp timers

cache Elabora una relación de las entradas de antememoria de direcciones MAC configuradas.

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 Visualiza la información configurada con los mandatos **enable** y **set**.

Ejemplo: `list dls`

(La salida del mandato **list dls** es la misma que la salida del mandato **list dls global**. En la página 612 hallará un ejemplo de ella.)

explorer-override
Visualiza las alteraciones temporales de explorador de antememoria MAC configuradas.

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
```

llc2 Visualiza los parámetros LLC2 configurados con el mandato **set llc2**. (Si desea una explicación completa de estos parámetros, consulte el mandato **set llc2** en la página 601.) Estos parámetros se definen por interfaz. Si no se han realizado cambios en los parámetros LLC2 con el mandato **set llc2**, no se generará salida alguna.

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 respuesta.

t2 Temporizador de acuse de recibo de recepción.

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 incrementar Ww.

acc La implementación actual de LLC2 no utiliza la prioridad de acceso. Como resultado, este parámetro se siempre 0 por omisión.

mac-list Elabora una relación de las entradas de lista de direcciones MAC configuradas.

Sintaxis:

m**ac** a**ll**

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 Visualiza todos los SAP abiertos y sus interfaces asociadas.

Ejemplo: `list open`

```
Interface   SAP(s)
    0        0  4
    1        0  4  8  C
```

priority Elabora una relación de las prioridades de circuito seleccionadas para los circuitos SNA y NetBIOS, las relaciones de transmisión entre los diversos circuitos y el tamaño mayor de trama 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 (máxima), High (alta), Medium (media) y Low (baja). El direccionador utiliza el valor de prioridad que usted asigne para limitar de manera selectiva la longitud de las ráfagas de los tipos concretos de tráfico. Por ejemplo, si asigna al tráfico SNA la prioridad Critical y al tráfico de las sesiones NetBIOS la prioridad Medium, siendo la asignación de mensajes 4/3/2/1, el direccionador procesará 4 tramas de sesión SNA antes de procesar 2 tramas NetBIOS y así sucesivamente. En este ejemplo, dos tercios del ancho de banda disponible están dedicados al tráfico SNA. Cuando el direccionador asigna el ancho de banda utilizando las prioridades que usted especifique, *cuenta tramas en lugar de bytes.*.

qllc... Elabora una relación de las estaciones, destinos o interfaces QLLC.

Sintaxis:

qllc callin
destination

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
```

Si desea obtener una descripción de los parámetros, consulte el apartado dedicado al mandato **add qllc destination** en la página 581.

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 de la lista anterior están explicados en la página 581. “E/D” indica si se ha inhabilitado la estación mediante el mandato **disable qllc station**.

sdlc Visualiza la información de estación de enlace SDLC configurada con el mandato **add sdlc link station**.

Nota: Los circuitos de llamada entrante SDLC conmutados se indican por medio de “FF(sw)” en el campo Addr.

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 Número de identificación de la interfaz que se conecta a la estación de enlace SDLC.

Addr Dirección SDLC, comprendida entre 01 y FE o bien “FF(sw)” para un circuito de llamada entrante conmutado, de la estación de enlace que se conecta.

Status Estado, Enabled (habilitada) o Disabled (inhabilitada), de la estación de enlace.

Source SAP/MAC
SAP LLC y las direcciones MAC representan para el dominio DLSw la estación SDLC conectada.

Dest SAP/MAC
SAP LLC y las direcciones MAC de una estación final remota en la que la estación SDLC conectada iniciará el establecimiento de circuito cuando se active la estación SDLC.

PU Tipo de PU SNA del dispositivo SDLC conectado, que puede ser:

2 Nodo PU 2.0 o T2.1

4 PU 4 que realiza el direccionamiento de subárea INN a otra PU 4 (es decir de NCP a NCP)

5 Sistema principal, con o sin procesador front-end (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
Número de bloque XID0 y número de identificación que utiliza el direccionador para generar XID0 en nombre del dispositivo SDLC conectado. Este campo se visualiza sólo para los dispositivos cuyo tipo de PU es 2.

PollType Tipo de trama SDLC que utiliza el direccionador para establecer el contacto inicial con la estación SDLC; puede ser una trama TEST, una trama SNRM o una trama SNRM retardada (una trama SNRM enviada una vez establecida la sesión DLSw). Este campo se visualiza sólo para los dispositivos cuyo tipo de PU es 2.

tcp Visualiza los vecinos TCP DLSw configurados. Los vecinos 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 Dirección IP del vecino TCP

CST Tipo de configuración de la conectividad; puede ser Active (activa) o Passive (pasiva).

Xmit Bufsize
Tamaño del almacenamiento intermedio de transmisión de paquetes, comprendido entre 1024 y 32768. El valor por omisión es 5120.

Rcv Bufsize
Tamaño del almacenamiento intermedio de recepción de paquetes, comprendido entre 1024 y 32768. El valor por omisión es 5120.

Max Segsize
Tamaño máximo del segmento TCP, comprendido entre 64 y 16384. El valor por omisión es 1024.

Keepalive
Estado de la función Keepalive; puede ser Enabled (habilitada) o Disabled (inhabilitada).

SesAlive Spoofing
Estado de la función SesAlive Spoofing de NetBIOS; puede ser Enabled (habilitada) o Disabled (inhabilitada).

Priority Prioridad del direccionador vecino en el proceso de selección. La prioridad de vecino es High (alta), Medium (media) y Low (baja).

timers Tiempo, especificado por usuario, que debe esperarse a que se produzcan 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
```

For additional information, refer to the **list timers** command.

NetBIOS

Visualiza el indicador de configuración NetBIOS.

En el apartado “Mandatos de NetBIOS” en la página 174 hallará la descripción de los mandatos NetBIOS.

Sintaxis:

n**etbios**

Open-Sap

Emita el mandato **open-sap** para todos los SAP que desee que utilice DLSw, ya sea como origen o destino de los circuitos DLSw. Los valores de SAP SNA habituales son 00, 04, 08 y 0C; todos estos SAP pueden abrirse juntos con el mnemotécnico “SNA”. El SAP NetBIOS es F0 y puede denominarse “NB”. Los SAP relacionados con la función LAN Network Manager reciben colectivamente el nombre de “LNM”. Abra los SAP que correspondan a los protocolos que seleccione, en las interfaces a través de las que DLSw llegará a 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 #
Número de la interfaz a través de la que desea abrir el SAP.

Enter SAP in hex
Puede entrar SAP individuales en hexadecimal o bien se puede entrar SNA, NB (para NetBIOS) o LNM (para LAN Network Manager).

Si entra SAP en hexadecimal, el rango es de 0 a FE y el SAP debe ser un número par. Si entra SAP 4, 8 o C sin haber abierto previamente el SAP 0 en la misma interfaz, el SAP 0 se abrirá de manera automática.

Si entra SNA, los SAP 0, 4, 8 y C se abren.

Si entra NB, el SAP F0 se abre.

Si entra LNM, los SAP 0, 2, D4, F2, F4, F8 y FC se abren.

Set

El mandato **set** sirve para configurar el tamaño de la antememoria de correlación de direcciones MAC con direcciones IP, los parámetros LLC2, el número máximo de sesiones DLSw, el número de segmento de SRB, los temporizadores de protocolo, el tamaño de almacenamiento intermedio de recepción, los vecinos dinámicos TCP, los parámetros de funcionamiento de QLLC, los parámetros relacionados con la lista de direcciones MAC y las alteraciones temporales 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** permite especificar el tamaño de la antememoria de correlación de direcciones MAC con direcciones IP.

DLSw utiliza la información almacenada en esta antememoria para descubrir las rutas de las estaciones remotas. Cuanto más grande sea la antememoria, más posibilidades tiene DLSw de encontrar la estación remota deseada sin enviar tramas CANUREACH a todos los vecionos TCP/IP conocidos.

No obstante, conviene evitar la definición de un tamaño de antememoria excesivo. Si lo hace, consumirá la memoria del direccionador y se entrometerá en la memoria que se necesita para las sesiones DLSw reales. El efecto será una disminución del número sesiones DLSw que puede manejar el direccionador.

Ejemplo: `set cache`

```
MAC  IP cache size (4 - 65535) [128]?
```

dynamic-tcp

Permite especificar diversos parámetros TCP para las conexiones TCP de vecinos dinámicos (es decir, las conexiones de entrada desde vecinos no definidos por el mandato **add tcp** command). DLSw utiliza estos valores sólo si los vecinos dinámicos están habilitados.

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]?
```

Si desea obtener una descripción de los parámetros que figuran en la lista anterior, consulte el apartado dedicado al mandato **add tcp** en la página 586.

explorer-limit

Permite poner límites al número de tramas exploradoras SNA y NetBIOS que pueden estar 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

Número máximo de tramas exploradoras SNA que pueden estar en cola simultáneamente para ser enviadas a un asociado DLSw individual.

Max NB explorers per transport queue

Número máximo de tramas exploradoras NetBIOS que pueden estar en cola simultáneamente para ser enviadas a un asociado DLSw individual.

llc2 Permite configurar atributos LLC2 concretos para un SAP determinado.

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

Número de SAP que desea ajustar. Los valores están comprendidos entre 0 y FE.

Reply timer (T1)

Este temporizador caduca cuando el igual LLC2 no recibe del otro igual LLC2 un acuse de recibo o respuesta obligatorios.

Receive Ack timer (T2)

Tiempo, en milisegundos, que tarda en enviarse un acuse de recibo de una trama de formato I recibida.

Inactivity Timer (Ti)

Este temporizador caduca cuando LLC no recibe una trama durante un período de tiempo especificado. Cuando caduca este temporizador, el igual LLC2 transmite un señal RR hasta que el igual LLC2 responde o se rebasa el número total de reintentos N2. El valor por omisión es 30 segundos.

Transmit Window (Tw)

Número máximo de tramas I que pueden enviarse antes de recibir una señal RR. Los valores están comprendidos entre 1 y 127. 0 establece Tw en el valor por omisión, que es 2.

Receive Window (Rw)

Número máximo de tramas I con numeración consecutiva y sin acuse de recibo que puede recibir un igual LLC2 de un sistema principal remoto.

Acks needed to increment Ww (Nw)

Afecta a la manera en que funciona el algoritmo de ventanas dinámicas. Especifica el número de acuses de recibo tras producirse una condición de error. El valor por omisión es 1. Ww (ventana de trabajo) es una réplica que cambia dinámicamente de Tw (ventana de transmisión). Una vez detectado un error LLC, 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 para que incremente Ww en uno. Ww seguirá incrementándose de esta forma hasta que Ww = Tw.

Max Retry value (N2)

Número máximo de veces que el igual LLC2 trasnmite una señal 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 junto con el temporizador T2 para reducir el tráfico de acuses de recibo de las tramas I recibidas. Este contador se establece en un valor determinado y disminuye cada vez que se recibe una trama I. Cuando llega a 0 o caduca el temporizador T2, se envía un acuse de recibo.

Para garantizar un buen rendimiento, establezca N3 en un valor inferior a Tw del igual LLC remoto. El valor por omisión es 1.

mac-list Modifica la exclusividad de la lista de direcciones MAC locales.

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 MAC local exclusiva (representa todas las direcciones MAC accesibles mediante este DLSw) o no exclusiva (es un conjunto de direcciones MAC accesibles mediante este DLSw).

maximum

Establece el número máximo de sesiones DLSw al que puede dar soporte el protocolo DLSw. Esto incluye las sesiones (circuitos) SNA y NetBIOS.

Ejemplo: `set maximum`

```
Maximum number of DLSw sessions (1-60000) [1000]?
```

memory Permite especificar el total de memoria de que dispone DLSw, así como la memoria de que disponen cada una de las sesiones DLSw y las tramas UI NetBIOS. El direccionador utiliza los valores por sesión y trama UI para fijar límites que indican a los algoritmos de control de flujo cuándo deben empezar a, o dejar de, ejercer presión regresiva sobre los orígenes de datos, así como cuándo deben empezar a, o dejar de, descartar el tráfico de tramas UI.

El direccionador no utiliza actualmente el valor de asignación DLSw general, así que puede dejarse el valor por omisión. Los mensajes DLS.161 que hagan referencia a las agrupaciones de transmisión y recepción globales (no a la agrupación de tramas UI NetBIOS) puesen pasarse por alto. En lugar de utilizar estas agrupaciones lógicas, los algoritmos de avance DLSw utilizan el estado de la memoria física para determinar cuáles son los tamaños de ventana que deben anunciar.

Los valores de asignación de sesión LLC, SDLC y QLLC proporcionan límites por circuito (par de estación final) al almacenamiento intermedio de los datos que fluyen desde dispositivos conectados a LLC, SDLC y QLLC, respectivamente, a TCP. Cuando el direccionador llega a estos límites, envía señales RNR/RR a las estaciones finales oportunas. El estado de las agrupaciones por sesión resulta visible desde el mandato de supervisión **list dlsw memory** 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 NetBios controla cuántas tramas UI (incluido NetBIOS DATAGRAM, NAME_QUERY, ADD_NAME_QUERY, etc.) puede colocar DLSw en el almacenamiento intermedio en un momento determinado. Cuando se alcanza este límite, DLSw descarta las tramas UI NetBIOS recibidas y la estación final que las ha originado deberá volver a transmitirlas. Así pues, si el límite que se fija es demasiado bajo, pueden surgir anomalías intermitentes en los intentos de establecer un circuito NetBIOS. El direccionador informa de una condición de descarte de tramas por medio del mensaje ELS DLS.161 (referente a la agrupación de tramas UI NetBIOS global).

priority

Permite especificar las prioridades que deben utilizarse para los circuitos SNA y NetBIOS, así como la relación de tráfico *entre* dichas prioridades. El mandato **set priority** sirve para especificar la prioridad de circuito como Critical, High, Medium o Low (en orden descendente de Critical a Low). El direccionador utiliza los valores de prioridad que usted asigne para limitar de manera selectiva la longitud de las ráfagas de los tipos concretos de tráfico que transmite a sus vecinos.

Esta función entra en marcha sólo en períodos de aglomeración, cuando los mensajes DLSw hacen cola antes de ser enviados a TCP. Supongamos, por ejemplo, que asigna al tráfico SNA la prioridad de explorador y sesión Critical, que por omisión se corresponde con el valor de asignación de mensajes 4. Si, a continuación, asigna al tráfico de explorador y sesión NetBIOS la prioridad Medium, que se corresponde con la asignación de mensajes 2, el direccionador transmitirá 4 tramas SNA antes de transmitir 2 tramas NetBIOS. Cuando procese las 2 tramas NetBIOS, procesará de nuevo 4 tramas SNA, y así sucesivamente. Cuando el direccionador asigna el ancho de banda en función de las prioridades que usted ha asignado, cuenta tramas en lugar de bytes. Asimismo, la prioridad de un circuito concreto se negocia con el direccionador vecino en el momento de activarse el cir-

cuito; por lo tanto, el direccionador vecino puede establecer una nueva prioridad del circuito utilizando una política distinta de la basada en los valores de configuración que usted haya especificado para este direccionador. Tal vez le interese además asignar diferentes prioridades al tráfico de explorador y sesión SNA y NetBIOS.

El mandato **set priority** sirve también para establecer un tamaño máximo de trama para todos los circuitos que pasen por este direccionador. Las estaciones finales NetBIOS tienden a generar las tramas más grandes permitidas, lo que da como resultado la existencia, en un enlace de baja velocidad, de un sola trama que ocupa el enlace durante varios segundos y que, de esta forma, incide negativamente en el tráfico SNA interactivo. Para disminuir el alcance de este efecto, se puede establecer un valor de tamaño máximo de trama más pequeño, que el direccionador hará saber a las estaciones finales NetBIOS por medio de los mecanismos estándar de puente origen-ruta. Si tiene en la red segmentos TB (puenteados de forma transparente) que ejecutan NetBIOS, establezca el tamaño máximo de trama NetBIOS en 1470 como mínimo.

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 Permite especificar un rango de direcciones MAC asignadas dinámicamente que se utiliza como dirección MAC de origen para las llamadas QLLC dinámicas entrantes.

Para especificar el rango, debe dar una dirección MAC base “X” y un número máximo “N” direcciones dinámicas. DLSw elije las 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 Establece el número de segmento de SRB (puente de direccionamiento en origen) que identifica DLSw en redes en anillo. Especifique el número de segmento en forma de valor hexadecimal de tres dígitos.

Ejemplo: `set srb`

```
Enter segment number hex (1-FFF) [5]?
```

timers Establece 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 por cuánto tiempo se conservan las entradas DLSw no utilizadas. Las entradas de base de datos correlacionan las direcciones MAC de destino con el conjunto de iguales DLSw que pueden llegar hasta ellas.

El valor cero indica que la antigüedad de las entradas de esta base de datos es indiferente. Esto puede resultar útil cuando se ejecutan conexiones TCP de vecino en interfaces de marcación, pero no suele ser recomendable porque inhabilita otras funciones DLSw.

Max wait timer
Especifica por cuánto tiempo se ha de esperar a recibir una respuesta ICANREACH a un mensaje CANUREACH transmitido con anterioridad.

Wait timer LLC test response
Especifica por cuánto tiempo se ha de esperar a recibir una respuesta TEST LLC antes de abandonar.

Wait timer SDLC test response
Especifica por cuánto tiempo se ha de esperar a recibir una respuesta TEST SDLC antes de abandonar.

QLLC session retry timer
Tiempo que espera el direccionador antes de intentar de nuevo establecer contacto con una estación QLLC para iniciar una sesión DLSw.

Group join timer interval
Tiempo que espera el direccionador antes de difundir cúmulos de mensajes de anuncio de grupo. Esto puede afectar al tiempo que tardan las funciones DLSw basadas en grupo en recuperarse tras producirse una anomalía del direccionador intermedio, así como al volumen de actividad general que se necesita para que esté en marcha la función de multidifusión. Este valor no se utiliza si se configuran conexionex TCP en lugar de utilizar las características de multidifusión IP de DLSw.

Neighbor priority wait timer
Tiempo que ha de esperarse mientras dura la exploración antes de seleccionar un vecino. Esto permite seleccionar un vecino de mayor prioridad, aunque éste no sea el primero en responder con un mensaje ICANREACH.

El valor cero indica que no se utilizará la función de prioridad de vecino. No habrá información de igual DLSw en antememoria para cada dirección MAC. Se envía siempre CANUREACH y se utiliza el primer igual DLSw que envíe ICANREACH (con independencia de cuál sea su prioridad).

Inactive neighbor termination timer
Tiempo que DLSw espera antes de desactivar una conexión TCP pasiva (cero sesiones) inactiva.

Delay sending TEST response

Tiempo que ha de esperarse una vez realizada la exploración en busca de una dirección MAC antes de enviar una respuesta TEST. Esto resulta útil si hay dos 2212 DLSw en una misma red puenteada capaces de llegar a la misma dirección MAC a través de iguales DLSw. Si uno de los 2212 DLSw tiene mayor preferencia, se puede retardar la respuesta TEST del 2212 con menor preferencia.

Mandatos de supervisión de DLSw

En este apartado se describen los mandatos de supervisión de DLSw. Estos mandatos entran en vigor de manera inmediata, pero no forman parte de la configuración SRAM del direccionador. Así pues, mientras que los mandatos de supervisión permiten realizar cambios en tiempo real en la configuración del direccionador, sobre ellos prevalece la configuración SRAM cuando se reinicia el direccionador. La supervisión consiste las acciones siguientes:

- La supervisión de los protocolos y las interfaces de red que utiliza actualmente el direccionador.
- La visualización de mensajes de ELS (sistema para el registro cronológico de sucesos) relacionados con el rendimiento y las actividades del direccionador.
- La realización en tiempo real de cambios en la configuración DLSw sin afectar de manera permanente a la configuración SRAM.

Acceso 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 y como se muestra en el ejemplo siguiente:

```
MOS Operator Console

For help using the Command Line Interface, press ESCAPE, then '?'

* talk 5
+ protocol dls
DLS>
```

Mandatos de supervisión de DLSw

En este apartado se describen los mandatos de supervisión de DLSw que figuran en la Tabla 36. Utilice estos mandatos para reunir información de la base de datos.

Tabla 36 (Página 1 de 2). Resumen de los mandatos de supervisión de DLSw

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.

Tabla 36 (Página 2 de 2). Resumen de los mandatos de supervisión de DLSw

Mandato	Función
Add	Añade dinámicamente una estación de enlace SDLC, una dirección IP de vecino TCP, un destino o estación QLLC, entradas de antememoria, entradas de lista de direcciones MAC, alteraciones temporales de prioridad de circuito o alteraciones temporales de explorador de antememoria MAC.
BAN	Permite acceder al indicador de consola BAN (nodo de acceso de límites) para entrar mandatos de consola BAN concretos. En el apartado “Utilización de la función de nodo de acceso de límites (BAN)” en la página 59 hallará una descripción detallada.
Close-Sap	Cierra de forma dinámica un SAP LLC abierto actualmente. Las interfaces LLC utilizan los SAP para las comunicaciones en la red.
Delete	Elimina dinámicamente una estación de enlace SDLC, una sesión DLSw, una dirección IP de vecino TCP, un destino o estación QLLC, entradas de antememoria, entradas de lista de direcciones MAC, alteraciones temporales de prioridad de circuito y alteraciones temporales de explorador de antememoria MAC.
Disable	Inhabilita dinámicamente la función de conmutación LLC, una estación de enlace SDLC, los vecinos dinámicos, una interfaz o estación QLLC, , o bien la utilización de listas de direcciones MAC remotas y locales.
Enable	Habilita dinámicamente la función de conmutación LLC, una estación de enlace SDLC, los vecinos dinámicos, una interfaz o estación QLLC, , o bien la utilización de listas de direcciones MAC remotas y locales.
Join-Group	Añade dinámicamente el direccionador a un grupo DLSw que sea distinto de la configuración SRAM.
Leave-Group	Retira dinámicamente al direccionador del grupo DLSw especificado.
List	Visualiza información correspondiente a las estaciones de enlace SDLC, los SAP, la prioridad de circuito, los grupos DLSw, las sesiones DLSw, las sesiones de las interfaces, estaciones y destinos QLLC, las entradas de antemoria y las entradas de lista de direcciones MAC. También facilita información detallada sobre las estadísticas, las conexiones y las posibilidades TCP.
NetBIOS	Proporciona acceso al indicador de soporte NetBIOS.
Open-SAP	Abre de manera dinámica un SAP LLC.
Set	Cambia dinámicamente los parámetros LLC2, el número máximo de sesiones DLSw, la asignación de memoria, los temporizadores de protocolo, la prioridad de circuito, los parámetros de los vecinos dinámicos, los parámetros de funcionamiento de QLLC o los parámetros relacionados con la lista de direcciones MAC.
Test	Coteja direcciones MAC concretas con las listas de direcciones MAC y la antememoria de direcciones MAC actuales.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Add

Utilice el mandato **add** para configurar dinámicamente una estación de enlace SDLC, una dirección IP de vecino TCP, un destino o estación QLLC, entradas de antememoria, entradas de lista de direcciones MAC, alteraciones temporales de prioridad de circuito y alteraciones temporales de explorador de antememoria MAC sin afectar a la configuración SRAM.

Sintaxis:

a**dd**	cache-entry explorer-override mac-list priority qllc... sdlc tcp

En el apartado dedicado al mandato **add** del capítulo de configuración, apartado “Add” en la página 577, hallará ejemplos y la descripción de los campos.

BAN

El mandato **ban** sirve para acceder al indicador de supervisión de BAN (nodo de acceso de límites). El mandato **ban** se entra en el indicador `DLS>`.

Sintaxis:

b**an**

Una vez haya accedido al indicador de supervisión de BAN, ya puede entrar los mandatos de supervisión de BAN específicos. En el “Utilización de la función de nodo de acceso de límites (BAN)” en la página 59 hallará la explicación de ellos.

Para volver al indicador `DLSw>` en cualquier momento, entre el mandato **exit**.

Close-SAP

El mandato **close-sap** sirve para inhabilitar dinámicamente la utilización que DLSw hace del SAP especificado sin afectar a la configuración 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
```

(En la página 587 hallará la explicación de los parámetros de **close-sap**.)

Delete

El mandato **delete** sirve para eliminar dinámicamente una estación de enlace SDLC, una sesión DLSw, una dirección IP de vecino TCP, un destino o estación QLLC, entradas de antememoria, entradas de lista de direcciones MAC, alteraciones temporales de prioridad de circuito o alteraciones temporales de explorador de antememoria MAC sin afectar a la configuración SRAM de DLSw. Si se utiliza este mandato, se termina cualquier sesión existente.

Sintaxis:

delete cache-entry
dls
explorer-override
mac-list
priority
qllc...
sdlc
tcp

cache-entry
Suprime la entrada de antememoria especificada

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 activa actualmente.

Ejemplo: `delete dls`

```
Session identifier [1]?
```

explorer-override
Elimina la entrada de alteración temporal de explorador de antememoria MAC especificada.

Ejemplo: delete explorer-override

```
Enter explorer override record number [1]?
Explorer override record has been deleted.
```

mac-list Suprime la entrada de lista de direcciones MAC locales especificada.

Ejemplo: `delete mac-list`

```
Enter mac list record number [1]?

Local MAC list entry 10005A000000 / FFFFFF000000 has been deleted.
```

priority Suprime la entrada de alteración temporal de prioridad de circuito especificada.

Ejemplo: `delete priority`

```
Enter circuit priority override record number [1]?
Circuit priority override record has been deleted.
```

qllc Elimina el soporte para una estación o destino QLLC. Si suprime una estación que esté activa actualmente, DLSw verifica si desea desactivar la conexión antes de proceder. 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
```

Ejemplo: `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 activo actualmente sin afectar a la información de configuración de estación de enlace SDLC.

Ejemplo: `delete sdlc`

```
Interface #[0]? 1
SDLC Address or 'sw' (switched dial-in) [C1]?
Link closed
```

Interface #
Número de interfaz del direccionador que se conecta a la estación de enlace SDLC.

SDLC Address
Dirección SDLC de la estación de enlace remoto que va a suprimir; está comprendida entre The SDLC address of the remote link 01 y FE o bien es “sw” para un circuito de llamada entrante SDLC conmutado.

tcp Elimina la dirección IP (*dirección_ip*) del igual DLSw con el que se efectúa una conexión TCP. La conexión TCP se cierra.

Ejemplo: `delete tcp`

```
IP Address [0.0.0.0]? 128.185.14.1
```

Disable

El mandato **disable** sirve para inhabilitar dinámicamente la función de desconexión LLC, el protocolo DLSw, estación de enlace SDLC, los vecinos dinámicos, una interfaz o estación QLLC, o bien la utilización de listas de direcciones MAC remotas y locales sin afectar a la configuración SRAM de DLSw. Inhabilitar la supervisión en ***la totalidad de*** la función DLSw no está soportado..

Sintaxis:

di**sable**	dynamic-neighbors llc mac-list qllc... sdlc

(A partir de la página 589 hallará ejemplos de la utilización de los parámetros del mandato **disable**.)

Enable

El mandato **enable** sirve para habilitar dinámicamente la función de desconexión LLC, una estación de enlace SDLC, los vecinos dinámicos, una interfaz o estación QLLC, o bien la utilización de listas de direcciones MAC remotas y locales sin afectar a la configuración SRAM de DLSw.

Sintaxis:

en**able**	dynamic-neighbors llc mac-list qllc... sdlc

(A partir de la página 591 hallará ejemplos de la utilización de los parámetros del mandato **enable**.)

Join-Group

El mandato **join-group** sirve para obligar a DLSw a iniciar la realización de las funciones de descubrimiento de vecino, exploración de multidifusión y reenvío de tramas de multidifusión.

En el capítulo “Utilización de DLSw” en la página 535 hallará más información y un ejemplo.

Sintaxis:

jo**in-group**

Leave-Group

El mandato **leave-group** sirve para obligar a DLSw a dejar de realizar las funciones de descubrimiento de vecino, exploración de multidifusión y reenvío de tramas de multidifusión en el grupo especificado o utilizar la dirección de multidifusión especificada. Este cambio se efectúa sin afectar a la configuración SRAM de DLSw. **Leave-group** termina las conexiones TCP existentes activadas en el grupo o la dirección de multidifusión especificados. En el capítulo “Utilización de DLSw” en la página 535 hallará más información y un ejemplo.

Sintaxis:

le**ave-group**

Ejemplo:

```
Configure group member (G) or specific multicast address (M) -  [G]?
Group ID (1-64 Decimal) [1]? 2
```

List

El mandato **list** sirve para visualizar información DLSw referente a las estaciones de enlace SDLC, la prioridad de circuito, los SAP, los vecinos TCP, los grupos, los vecinos dinámicos, las interfaces, destinos y estaciones QLLC, las entradas de antememoria configuradas, las entradas de lista de direcciones MAC y las alteraciones temporales de explorador de antememoria MAC.

Sintaxis:

li**st**	dls... explorer-override groups... llc2... mac-list priority... qllc...

sdlc...
tcp...
timers

dls Visualiza información que pertenece al protocolo DLSw. Las opciones (global, memory, sessions y cache) de los parámetros DLSw se describen más abajo y en las páginas siguientes.

Global Visualiza los valores operativos de los parámetros DLSw generales configurados.

Memory Visualiza la informacón de memoria DLS configurado y el grado de utilización de memoria actual.

Sessions Visualiza la información de sesión DLS actual, que incluye el origen, el destino, el estado, los distintivos, la dirección IP de destino y un ID de sesión.

cache Elabora una relación de las direcciones que figuran en la antememoria de direcciones MAC de DLSw.

dls global

Visualiza información global referente a los parámetros 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; puede ser Enabled (habilitado) o Disabled (inhabilitado).

LLC2 send disconnect is
Estado de impedir que el direccionador termine una conexión LLC2 tras producirse la pérdida de la conexión TCP. Los valores son Enabled o Disabled.

Dynamic Neighbors
Indica si DLSw acepta los intentos de conexión TCP entrante procedentes de direccionadores DLSw que no están configurados (es decir, con el mandato **add tcp**).

SRB Segment number
Número de segmento de 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
Número máximo de sesiones DLSw al que puede dar soporte el protocolo DLSw (tanto sesiones SNA como NetBIOS).

DLSw global memory allotment
Máximo de memoria que tiene permitido DLSw.

LLC per-session memory allotment
Máximo de memoria permitido por sesión DLSw LLC.

SDLC per-session memory allotment
Máximo de memoria permitido por cada sesión DLSw SDLC.

QLLC per-session memory allotment
Máximo de memoria permitido por cada sesión DLSw QLLC.

NetBIOS UI-frame memory allotment
Máximo de memoria permitido para todas las tramas UI NetBIOS que reenvía DLSw.

Dynamic Neighbor Transmit Buffer Size
Tamaño del almacenamiento intermedio de transmisión TCP para las conexiones TCP dinámicas.

Dynamic Neighbor Receive Buffer Size
Tamaño del almacenamiento intermedio de recepción TCP para las conexiones TCP dinámicas.

Dynamic Neighbor Maximum Segment Size
Tamaño máximo de segmento TCP para las conexiones dinámicas.

Dynamic Neighbor Keep Alive
Si se han de enviar mensajes Keep Alive TCP al establecerse nuevas conexiones TCP dinámicas.

Dynamic Neighbor NetBIOS SessionAlive Spoofing
Si se reenvían tramas I SessionAlive de NetBIOS a los iguales DLSw establecidos al producirse nuevas conexiones TCP dinámicas.

Dynamic Neighbor Priority
Prioridad de vecino que debe utilizarse para todas las nuevas conexiones TCP dinámicas.

QLLC base source MAC address
Dirección MAC más baja del rango utilizado como direcciones MAC de origen para las llamadas QLLC de entrada dinámicas (SVC).

QLLC maximum dynamic addresses
Número máximo de direcciones MAC de origen dinámicas que pueden utilizarse a un mismo tiempo para las llamadas QLLC de entrada dinámicas.

dls sessions all

Visualiza la información actual de sesión DLS.

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 Dirección MAC de origen y SAP de la sesión. Si se trata de sesiones con un origen SDLC, QLLC o APPN, la dirección MAC se sustituye por las series de caracteres siguientes, de manera que estas sesiones puedan identificarse con facilidad:

Tipo DLC	Caracteres	Contenido
SDLC	1-5	"SDLC "
	6-7	Número de interfaz
	8	"-"
	9-10	Dirección de estación SDLC
	11-12	" "
QLLC	1-5	"QLLC "
	6-7	Número de interfaz
	8	"P" de PVC o "S" de SVC
	9-12	LCN para PVC o los 4 últimos bytes de la dirección DTE para SVC
APPN	1-4	"APPN"
	5-12	" "

Destination

Dirección MAC de destino de la sesión.

State Estado de la sesión. Se pueden visualizar los estados siguientes:

DISCONECT

Indica el estado inicial sin ningún circuito ni conexión establecidos.

RSLV_PEND

Indica que el DLSw destino está a la espera de una indicación SSP_STARTED o bien sigue una petición SSP_START.

CIRC_PEND

Indica que el DLSw destino está a la espera de 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 a la espera del reinicio del enlace de datos y de una respuesta SSP_RESTARTED a un mensaje SSP_RESTART.

CONN_PEND

Indica que el DLSw origen está a la espera de una respuesta SSP_CONTACTED a un mensaje SSP_CONTACT.

CONT_PEND

Indica que el DLSw destino está a la espera de una confirmación SSP_CONTACTED a un mensaje SSP_CONTACT.

CONNECTED

Indica que el circuito está totalmente activo para la transferencia de datos orientados a la conexión.

DISC_PEND
Indica que el DLSw que ha originado la desconexión está a la espera de una respuesta SSP_HALTED a un mensaje SSP_HALT.

HALT_PEND
Indica que el DLSw remoto está a la espera de una indicación SSP_HALTED a continuación de una petición SSP_HALT.

REST_PEND
Indica que el DLSw local ha recibido RESTART_DL pero no ha devuelto todavía DL_RESTARTED.

CIRC_STRT
Indica que el DLSw local ha enviado CANUREACH_cs pero no ha recibido todavía ICANREACH_cs.

HLT_NOACK
Indica que el DLSw local ha recibido HALT_DL_NOACK pero no ha acabado de cerrar la estación de enlace.

Flags Puede uno de los siguientes:

A - CONTACT MSG PENDING

B - SAP RESOLVE PENDING

C - EXIT BUSY EXPECTED

D - TCP BUSY

E - DELETE PENDING

F - CIRCUIT INACTIVE

Dest. IP Addr
Dirección IP del igual DLSw remoto.

Id Número utilizado para identificar la sesión. Utilice este número en cualquier mandato que requiera el ID de sesión.

dls sessions appn
Visualiza información de sesión DLS referente a las sesiones que tienen APPN como punto final en este direccionador.

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
Visualiza la información actual sobre las sesiones BAN.

Ejemplo: `list dls session ban`

```
BAN port number (user 0 for all ports) [0]?
No active sessions
```

dls sessions dest
Visualiza la información de sesión DLS ordenada 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

Visualiza información detallada de sesión 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

Iniciador (ORIGINATOR) o destinatario (TARGET) de la conexión.

XIDs sent, XIDs rcvd

Número total de XID que este igual DLSw ha enviado y recibido del igual DLSw remoto.

Datagrams sent, Datagrams rcvd

Número total de datagramas que este igual DLSw ha enviado y recibido del igual DLSw remoto.

Info frames sent, Info frames rcvd

Número total de tramas I que este igual DLSw ha enviado y recibido del igual DLSw remoto.

RIF Información incluida en el campo RIF de la trama TEST LLC.

Local CID

ID de circuito DLSw que ha asignado este direccionador.

Remote CID

ID de circuito DLSw que ha asignado el direccionador vecino.

Priority Prioridad de circuito DLSw establecida para este circuito al iniciarse.

dls sessions ip

Visualiza las sesiones DLS de un vecino conectado a TCP especificado.

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

Elabora una relación de información sobre los circuitos activos actuales 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

Rango de sesiones DLS que desea visualizar. Este número está situado 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

Visualiza la información de sesión DLS ordenada 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 está correlacionada con el nombre “SDLC 04”. Si no sabe cuál es la dirección MAC de origen que se requiere como parámetro de este mandato, entre el mandato **list SDLC config all** para obtener la información.

dls sessions state

Visualiza todas las sesiones DLS que están en un estado especificado.

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** elabora una relación de las entradas que hay en la antememoria de direcciones MAC de DLSw. Esta antememoria contiene una base de datos de las conversiones más recientes de dirección MAC a vecino IP. Proporciona la dirección MAC, el tiempo de vida (en segundos) en la antememoria y la dirección IP del vecino.

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

Visualiza las entradas de antememoria MAC configuradas 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

Visualiza la información correspondiente a un rango especificado de entradas de 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 elebora una relación de todas las sesiones DLSw existentes y de la memoria que utiliza cada una de ellas.

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 el total de memoria asignada actualmente por DLS. En él se incluye todas las asignaciones de sesión y los mensajes de control.

El campo “Congest State” proporciona información sobre el control de flujo y en él puede figurar lo siguiente:

Ready Indica que no hay aglomeraciones en la sesión.

Session Indica que la sesión ha utilizado la mayor parte de su asignación y ha efectuado un control de flujo del enlace de datos.

Global Indicates que hay una aglomeración en la sesión debido a una falta de memoria en el direccionador.

Ses/gbl Indicates que hay una aglomeración en la sesión debido a una falta de memoria global y de sesión.

El campo “DLC Xmits Queued” muestra el número total de tramas en cola para su transmisión de DLS a LLC o SDLC, más el número de las que están en cola en DLC y a la espera de que llegue el acuse de recibo por parte de la estación final conectada.

explorer-override

Elabora una relación de las alteraciones temporales de explorador de antememoria MAC configuradas.

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

Visualiza todas las entradas de 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

Visualiza todas las entradas de lista de direcciones MAC configuradas localmente.

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

Visualiza todas las entradas de lista de direcciones MAC locales activas.

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

Visualiza TODAS las entradas de lista de direcciones MAC remotas activas de un igual DLSw determinado.

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

Visualiza la información de grupo referente al este igual DLSw 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
Si se trata de grupos cliente/servidor/igual, es el número del grupo. Si se trata de grupos DLSw Versión 2, la dirección de multidifusión está configurada para lectura o grabación.

Role Si se trata de grupos cliente/servidor/igual, es el cometido para el que está configurado el direccionador dentro del grupo. Si se trata de grupos DLSw Versión 2, es el cometido de lectura/grabación de la dirección de multidifusión configurada: Read-only (sólo lectura), Write-only (sólo grabación) o Read-write (lectura-grabación).

CST Tipo de configuración de conectividad que utiliza el direccionador dentro del grupo; puede ser a (activa) o p (pasiva).

Xmit Bufsize
Tamaño del almacenamiento intermedio de transmisión de paquetes, comprendido entre 1024 y 32768. El valor por omisión es 5120.

Rcv Bufsize
Tamaño del almacenamiento intermedio de recepción de paquetes, comprendido entre 1024 y 32768. El valor por omisión es 5120.

Max Segsize
Tamaño máximo del segmento TCP, comprendido entre 64 y 16384. El valor por omisión es 1024.

Keepalive
Visualiza el estado de la función Keepalive; puede ser Enabled (habilitada) o Disabled (inhabilitada).

SesAlive Spoofing
Visualiza el estado de la función SesAlive Spoofing de NetBIOS; puede ser Enabled (habilitada) o Disabled (inhabilitada).

Priority Visualiza la prioridad del direccionador vecino en el proceso de selección. La prioridad de vecino es High (alta), Medium (media) y Low (baja).

groups config
Visualiza la información de grupo referente al este igual DLSw configurado con el mandato **join-group**.

Ejemplo: `list groups config`

```
   Group# /                      Xmit     Rcv      Max
Mcast IP Addr    Role       CST  Bufsize  Bufsize  Segsize  Keepalive
Priority

224.0.10.0       READ/WRITE   p    5120     5120     1024    DISABLED   MEDIUM
   1             CLIENT       p    5120     5120     1024    DISABLED   MEDIUM
```

Group # / Mcast IP Addr
Si se trata de grupos cliente/servidor/igual, es el número del grupo. Si se trata de grupos DLSw Versión 2, la dirección de multidifusión está configurada para lectura o grabación.

Role Si se trata de grupos cliente/servidor/igual, es el cometido para el que está configurado el direccionador dentro del grupo. Si se trata de grupos DLSw Versión 2, es el cometido de lectura/grabación de la dirección de multidifusión configurada: Read-only (sólo lectura), Write-only (sólo grabación) o Read-write (lectura-grabación).

CST Tipo de configuración de conectividad que utiliza el direccionador dentro del grupo; puede ser a (activa) o p (pasiva).

Xmit Bufsize
Tamaño del almacenamiento intermedio de transmisión de paquetes, comprendido entre 1024 y 32768. El valor por omisión es 5120.

Rcv Bufsize
Tamaño del almacenamiento intermedio de recepción de paquetes, comprendido entre 1024 y 32768. El valor por omisión es 5120.

Max Segsize
Tamaño máximo del segmento TCP, comprendido entre 64 y 16384. El valor por omisión es 1024.

Keepalive
Visualiza el estado de la función Keepalive; puede ser Enabled (habilitada) o Disabled (inhabilitada).

Priority Visualiza la prioridad del direccionador vecino en el proceso de selección. La prioridad de vecino es High (alta), Medium (media) y Low (baja).

groups statistics
Visualiza las estadísticas de uso de los grupos DLSw con fines de tráfico de explorador desde el último reinicio del direccionador o la creación del 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
Visualiza información correspondiente a todos los SAP abiertos actualmente de las interfaces existentes entre los iguales LLC2.

Ejemplo: `list llc2 open`

```
Interface   SAP(s)
    0        0  4
    1        0  4  8  C
```

llc2 SAP parameters
Visualiza información de configuración referente a los parámetros LLC2. Sólo se visualizarán las configuraciones que hayan sufrido cambios. Si no se ha utilizado el mandato **set llc2**, no se generará salida alguna.

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

Visualiza la información actual correspondiente a 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 Estado de la sesión LLC. Se pueden visualizar los estados siguientes:

DISCONNECTED

Indica que existe la estructura de control de enlace de datos, pero no se ha establecido ningún enlace de datos.

CONNECT_PEND

Se entra en este estado cuando cuando se recibe una trama de mandato TEST enviada para NULL SAP o bien cuando se recibe un mandato DLC_START_DL desde DLS.

RESOLVE_PEND

Se entra en este estado cuando se ha enviado un mandato DLC_RESOLVE_C a DLS.

CONNECTED

Se trata de un estado estable en el que los servicios de nivel tipo 1 LLC están disponibles a través de DLS. Se entra en este estado cuando se recibe un mandato DLC_RESOLVE_R desde DLS o cuando se recibe una trama de respuesta TEST desde la red.

CONTACT_PEND

Se entra en este estado cada vez que hay una respuesta pendiente a un SABME transmitido o recibido.

CONTACTED

Se trata de un estado estable en el que se entra cada vez que se recibe una respuesta UA a un SABME transmitido o se transmite UA para un SABME recibido. En este estado, las tramas informativas LLC2 se intercambian a través de DLS.

DISCONNECT_PENDING

Se entra en este estado cada vez que se transmite o recibe un mandato DISC o bien cuando se ha recibido DLC_HALT desde DLS.

llc2 sessions ban

Visualiza la información actual correspondiente a las sesiones LLC2 en las que interviene la función BAN.

llc2 sessions nb

Visualiza la información actual correspondiente a las sesiones LLC2 que llevan el tráfico del protocolo NetBIOS.

llc2 sessions range

Visualiza la 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 Visualiza la información de 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... Elabora una relación de las estaciones, destinos o interfaces QLLC que están habilitados.

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
```

Si desea obtener la descripción de los campos configurables de esta pantalla, consulte el apartado dedicado al mandato **add qllc** del capítulo “Utilización de DLSw” en la página 535. El campo *Hits* indica el número de veces que DLSw ha utilizado una coincidencia entre el ID de conexión de un paquete Call_Request QLLC entrante 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
```

Si desea obtener la descripción de los campos configurables de esta pantalla, consulte el apartado dedicado al mandato **add qllc** del capítulo “Utilización de DLSw” en la página 535.

El campo *Type* tiene los valores siguientes:

PERM (Permanent)
Esta definición de estación formaba parte de la configuración del direccionador la última vez que se inició el direccionador.

STAT (Static)
Esta definición de estación la ha añadido el usuario dentro de la función de supervisión de DLSw una vez iniciado el direccionador por última vez.

DYNM (Dynamic)
DLSw ha creado de forma dinámica esta definición de estación como resultado de una llamada entrante o de la necesidad de efectuar varias llamadas salientes a un sola dirección de DTE remota.

La línea de resumen que hay en la parte inferior de la lista de sesiones muestra cuántas sesiones existen actualmente de cada tipo.

El campo *State* indica el estado de la conexión DLSw desde el punto de vista de QLLC. Estos estados son distintos de los estados DLS principales visualizados con los mandatos **list dls sess** y añaden información sobre lo que ocurre en la interfaz QLLC. Los valores posibles son:

NET_DOWN
La interfaz X.25 está actualmente desactivada.

PLC_DOWN
La capa de paquetes X.25 está actualmente desactivada.

DISCONNECTED
Para este estado y los siguientes, la interfaz X.25 y la capa de paquetes están activadas. En este estado, DLSw está a la espera de que una estación final inicie el establecimiento de conexión.

XID_POLL
DLSw sondea a la estación final QLLC con QXID (XID_null) en un intento de contactar inicialmente con el dispositivo o de recuperar una conexión perdida.

SETMODE_POLL
DLSw sondea a la estación final QLLC con QSM en un intento de contactar inicialmente con el dispositivo o de recuperar una conexión perdida.

SENT_EX
DLSw ha tenido noticias de la estación final QLLC y realiza una exploración para hallar el destino adecuado en la red DLSw.

CS_PEND
Se ha efectuado la exploración de DLSw y se ha iniciado una petición de inicio de circuito (sent CUR_cs).

CALL_REQ_PEND
DLSw ha cursado una petición de llamada en la estación final y está a la espera para ver si se responde satisfactoriamente a la llamada.

ESTABLISHED
El circuito DLSw está en estado “circuito establecido”; está disponible para enviar y recibir XID SNA.

CONTACT_PEND
DLSw ha enviado QSM a la estación final QLLC y está a la espera de QUA.

CONNECTED
El circuito DLSw está totalmente activado y puede transportar datos de usuario final de tramas I.

DISC_PEND
DLSw ha solicitado una desconexión de circuito a la estación QLLC y está a la espera del acuse de recibo.

RESET_PEND
DLSw ha solicitado a la estación QLLC un restablecimiento de PVC o que se borre la llamada de SVC y está a la espera del 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
```

Si desea obtener la descripción de los campos configurables de esta pantalla, consulte el apartado dedicado al mandato **add qllc** del capítulo “Utilización de DLSw” en la página 535. El campo “E/D” indica si la estación está actualmente habililitada. El campo “Type” tiene los mismos valores descritos anteriormente para el mandato **list qllc sessions**.

sdlc config
Visualiza los parámetros configurados de 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
Visualiza 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
```

Dado que DLSw y SDLC tienen la facultad de realizar una negociación de XID completa, es posible que la estación de enlace SDLC conectada establezca el enlace en una dirección de estación SDLC distinta de la configurada en el direccionador. Cuando esto sucede, las dos direcciones de estación SDLC figuran en la columna “Addr” de esta 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 supervisión para hacer referencia a esta estación de enlace. La dirección operativa actual establecida por el dis-

positivo SDLC conectado es el valor yy que aparece a la derecha entre paréntesis.

tcp capabilities

Visualiza la información recibida de un direccionador DLSw asociado en el mensaje de intercambio de posibilidades.

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 2212 AIS 2212-AIS

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

Identificador exclusivo de organización (OUI) de IEEE del proveedor del DLSw vecino. El OUI de IBM es X'10005A'.

Vendor version

Serie de texto que el DLSw vecino ha enviado para describirse. “(not available)” indica que la implementación de vecino no ha enviado la serie.

Initial pacing window

Número de mensaje SSP que le está permitido enviar a este DLSw al DLSw vecino tras recibir el permiso inicial de avance para cada circuito nuevo.

Preferred TCP connections

Número de conexiones TCP (1 o 2) que desearía tener este vecino. IBM 2212 se ajusta al número solicitado y tendrá sólo 1 conexión TCP dúplex con los vecinos que lo soliciten.

Supported SAPs

Lista de SAP que el DLWs vecino ha abierto, o abrirá automáticamente, en cualquiera de las interfaces de LAN o que representan las estaciones SDLC conectadas.

MAC List Exclusivity

Indica si la lista de direcciones MAC enviada por este vecino ha de considerarse que es una lista parcial o completa de las direcciones MAC que son locales para el vecino. La respuesta “(not supplied)” indica que el vecino no ha enviado una lista de direcciones MAC como parte de sus posibilidades.

MAC List Visualiza todas las máscaras y valores de lista MAC que este vecino ha enviado en la lista de direcciones MAC. La respuesta “(none supplied)” indica que el vecino no ha enviado una lista de direcciones MAC como parte de sus posibilidades.

NetBIOS Exclusivity
Indica si la lista de nombre NetBIOS enviada por este vecino ha de considerarse que es una lista parcial o completa de los nombres NetBIOS que son locales para el vecino. La respuesta “(not supplied)” indica que el vecino no ha enviado una lista de nombres NetBIOS como parte de sus posibilidades.

NetBIOS Name List
Visualiza todos los calificadores de nombre NetBIOS que este vecino ha enviado en la lista de nombres NetBIOS. La respuesta “(none supplied)” indica que el vecino no ha enviado una lista de nombres NetBIOS como parte de sus posibilidades.

Multicast Version
Indica la versión de multidifusión a la que da soporte este vecino según lo definido en el estándar AIW. La respuesta *not supplied* indica que el vecino no ha enviado una versión de multidifusión como parte de sus posibilidades.

IBM CST Indica el tipo de configuración de conectividad (CST) IBM que ha configurado este vecino. La respuesta *not supplied* indica que el vecino no ha enviado un CST IBM como parte de sus posibilidades.

IBM Multicast
Indica si determinadas funciones de multidifusión de IBM están disponibles o no en este vecino. La respuesta *not supplied* indica que el vecino no ha enviado la multidifusión de IBM como parte de sus posibilidades.

IBM Capex Correlator
Indica el valor del último correlacionador CAPEX de IBM recibido de este vecino. La respuesta *not supplied* indica que el vecino no ha enviado un correlacionador CAPEX IBM como parte de sus posibilidades.

tcp config
Visualiza los parámetros de configuración correspondientes a todas las conexiones TCP con direccionadores DLSw iguales configuradas.

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
Visualiza el estado de todas las sesiones TCP conocidas con direccionadores DLSw iguales.

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 Grupo a través del que se ha descubierto el vecino, si procede.

IP Address

Dirección IP de vecino utilizada para DLSw

Conn State

Estado de la conexión de transporte (que puede estar formada por 1 o 2 conexiones TCP) con este vecino. Los estados válidos son:

DOWN Sesión TCP no establecida; no se produce el intercambio de posibilidades (sólo asociados pasivos).

CAPEX FAILED

Intento de intercambio de posibilidades fallido; se desactiva la sesión TCP.

Unicasting

Sesión TCP no establecida; se produce el intercambio de posibilidades (sólo asociados pasivos) (preparado para tráfico de explorador DLSw).

PENDING R/W

2212 ha intentado establecer una sesión TCP con el vecino.

RD EST/WR PEND

La sesión TCP entre el vecino y 2212 está activa, pero no así la sesión TCP entre 2212 y el vecino.

RD EST/WR PEND

La sesión TCP entre 2212 y el vecino está activa, pero no así la sesión TCP entre el vecino y 2212.

CAPEX PENDING

Sesión TCP establecida; intercambio de posibilidades en curso.

ESTABLISHED

Sesión TCP establecida; se ha producido el intercambio de posibilidades (preparado para utilizar sesiones DLSw).

CLOSING

Se procede a desactivar la sesión.

RECONNECT WAIT

Sesión TCP no establecida; se está a la espera de que caduque el temporizador a fin de intentar establecer de nuevo la sesión TCP.

CST Tipo de configuración de conectividad actual; puede ser:

```
a - Configurado localmente como activo
p - Configurado localmente como pasivo
A - Configurado localmente como pasivo, pero funciona en modalidad
    activa debido a los requisitos de vecino
D - No está configurado localmente, sino que se trata de una
    coenxión TCP de vecino dinámico
```

Version Nivel de protocolo DLSw del vecino. Puede ser AIW VnRm para direccionadores conformes al estándar AIW, RFC1434+ para implementaciones anteriores a AIW V1R0 o UNKNOWN.

Active Sess

Número actual de sesiones (circuitos) DLSW activas (en cualquier estado) que hay en esta conexión de transporte.

Sess Creates

Número total de sesiones (circuitos) DLSW que han entrado alguna vez en estado CIRC_EST desde el último reinicio del direccionador o “add tcp” de esta conexión de transporte.

tcp statistics

Visualiza las estadísticas de uso de las conexiones de transporte TCP desde el último reinicio del direccionador o “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 Tiempo, especificado por usuario, que debe esperarse a que se produzcan 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

Tiempo que se han de conservar las entradas de base de datos dirección MAC-dirección IP sin referencias. El valor cero indica que no se mide el tiempo que llevan las entradas en esta base de datos.

Max wait timer for ICANREACH

Tiempo que el direccionador espera a ver si recibe una respuesta a un mensaje CANUREACH antes de decidir que la sesión no se activará.

Wait timer for LLC test response

Tiempo que el direccionador espera a ver si recibe una respuesta TEST LLC antes de volver a transmitir una trama TEST LLC.

Wait timer for SDLC test response

Tiempo que espera el direccionador antes de intentar de nuevo establecer contacto con una estación SDLC para iniciar una sesión DLSw.

QLLC session retry timer
Tiempo que espera el direccionador antes de intentar de nuevo establecer contacto con una estación QLLC para iniciar una sesión DLSw.

Join Group Interval
Tiempo que transcurre entre difusiones de anuncio de grupo DLSw.

Neighbor priority wait timer
Tiempo que espera DLSw antes de seleccionar un vecino durante un intento de establecimiento de sesión dado.

Neighbor Inactivity Timer
Tiempo que DLSw espera antes de desactivar una conexión TCP pasiva (cero sesiones) inactiva.

Delay sending TEST response
Tiempo que ha de esperarse una vez realizada la exploración en busca de una dirección MAC antes de enviar una respuesta TEST.

NetBIOS

Visualiza el indicador de supervisión NetBIOS.

Sintaxis:

n**etbios**

Ejemplo: `netbios`

```
NetBIOS Support User Configuration
NetBIOS config>
```

En el capítulo “Configuración y supervisión de NetBIOS” en la página 171 hallará la descripción de los mandatos NetBIOS.

Open-Sap

El mandato **open-sap** sirve para habilitar dinámicamente la conmutación DLSw para el SAP (punto de acceso a servicio) especificado sin afectar a la configuración SRAM de DLSw.

Sintaxis:

op**en-sap**

Ejemplo: `open-sap`

En el apartado “Open-Sap” en la página 599 hallará información adicional y la explicación de los parámetros de **open-sap**.

Set

El mandato **set** sirve para cambiar dinámicamente los parámetros LLC2, el número máximo de sesiones DLSw, los temporizadores de protocolo, los vecinos dinámicos, los parámetros operativos QLLC, los parámetros relacionados con la lista de direcciones MAC y los parámetros de prioridad de circuito sin afectar a la configuración SRAM de DLSw.

Sintaxis:

se**t**
- dynamic-tcp
- explorer-limit
- llc2
- mac-list
- memory
- priority
- qllc
- timers

dynamic-tcp

Permite especificar diversos parámetros TCP para las conexiones TCP de vecinos dinámicos (es decir, las conexiones de entrada desde vecinos no definidos por el mandato **add tcp** command). DLSw utiliza estos valores sólo si los vecinos dinámicos están habilitados.

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]?
```

Si desea obtener una descripción de estos parámetros, consulte el apartado dedicado al mandato **add tcp** del capítulo “Utilización de DLSw” en la página 535.

explorer-limit

Permite poner límites al número de tramas exploradoras SNA y NetBIOS que pueden estar 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

Número máximo de tramas exploradoras SNA que pueden estar en cola simultáneamente para ser enviadas a un asociado DLSw individual.

Max NB explorers per transport queue

Número máximo de tramas exploradoras NetBIOS que pueden estar en cola simultáneamente para ser enviadas a un asociado DLSw individual.

llc2 Permite configurar atributos LLC2 concretos para un SAP determinado.

Ejemplo: `set llc2`

(En la página 601 hallará un ejemplo del mandato **set llc2**).

mac-list Permite establecer la exclusividad de dirección MAC local. Este mandato permite también comprometer todos los cambios realizados con anterioridad por medio de los mandatos de supervisión siguientes:

- 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 envian nuevas posiblidades de ejecución a todos los iguales DLSw a fin de comunicar 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 / FFFFFFFFFFF.
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 permite especificar dinámicamente el total de memoria que se asigna a DLSw, así como el total que se debe asignar a cada una de las sesiones DLSw.

Ejemplo: `set memory`

En la página 602 hallará un ejemplo del mandato **set memory**.

priority Permite especificar las prioridades que deben utilizarse para los circuitos SNA y NetBIOS. Puede configurar la prioridad de circuito como Critical, High, Medium o Low (en orden descendente de Critical a Low).

Este mandato también permite configurar las relaciones de las transmisiones de transporte para cada prioridad de circuito, así como establecer el tamaño máximo de trama que debe utilizarse para NetBIOS. Si la red contiene segmentos TB (puenteados de forma transparente), utilice un tamaño máximo de trama NetBIOS que sea 1470 como mínimo.

Ejemplo: `set priority`

Para obtener más información sobre el mandato **set priority**, consulte la página 603.

qllc Permite especificar un rango de direcciones MAC asignadas dinámicamente que se utiliza como dirección MAC de origen para las sesiones DLSw resultantes de las llamadas QLLC dinámicas entrantes.

Para especificar el rango, debe dar una dirección MAC base “X” y un número máximo “N” direcciones dinámicas. DLSw elije las 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 Establece los temporizadores del protocolo DLSw.

Ejemplo: `set timers`

En la página 604 hallará un ejemplo del mandato **set timers**.

Test

El mandato **test** sirve para realizar pruebas en la lista de direcciones MAC y la antememoria de direcciones MAC activas actualmente.

Sintaxis:

test cache
mac-list

cache Permite determinar cómo se reenviará una trama dirigida a una dirección MAC concreta tomando como base la información actual de igual DLSw y antememoria.

Sintaxis: cache

Example: `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 Permite cotejar una dirección MAC dada con todas las entradas de lista de direcciones MAC activas actualmente (locales y remotas). Esto resulta útil a la hora de resolver problemas derivados de conflictos con la lista 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
```

Soporte de reconfiguración dinámica de DLSw

En este apartado se describe el modo en que la reconfiguración dinámica (DR) afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

DLSw da soporte al mandato **delete interface** de CONFIG (Talk 6) con la matización siguiente:

Se suprimen las estaciones QLLC, las estaciones SDLC y los SAP DLSw de la interfaz suprimida.

Mandato activate interface de GWCON (Talk 5)

DLSw da soporte al mandato **activate interface** de GWCON (Talk 5) con la matización siguiente:

Para que se activen las estaciones QLLC, las estaciones SDLC y los SAP DLSw de la nueva interfaz, DLSw debe estar habilitado globalmente.

Todos los mandatos específicos de interfaz de DLSw están soportados por el mandato **activate interface** de GWCON (Talk 5).

Mandato reset interface de GWCON (Talk 5)

DLSw da soporte al mandato **reset interface** de GWCON (Talk 5) con la matización siguiente:

- Para que se modifiquen las estaciones QLLC, las estaciones SDLC y los SAP DLSw de la interfaz restablecida, DLSw debe estar habilitado globalmente.
- Los SAP DLSW de la interfaz restablecida se cierran y se vuelven a abrir, pero las sesiones DLSw actuales no se ven afectadas.
- Las estaciones SDLC y QLLC asociadas con la interfaz que se restablece se suprimen y, a continuación, se reinician, los que hace que las sesiones DLSw asociadas se desactiven y se vuelvan a establecer.

Todos los mandatos específicos de interfaz de DLSw están soportados por el mandato **reset interface** de GWCON (Talk 5).

Mandatos de cambio temporal de GWCON (Talk 5)

DLSw da soporte a los mandatos de GWCON que cambian de forma temporal el estado operativo del dispositivo indicados más abajo. Los cambios se pierden cada vez que se vuelve a cargar o iniciar el dispositivo o que se ejecuta un mandato reconfigurable dinámicamente.

Los mandatos relacionados a continuación no afectan a las funciones de DLSw ya activas en el momento de emitirse el mandato, salvo que se indique lo contrario.

Los cambios sí que se aplican al tráfico y a todas las operaciones de DLSw, las sesiones TCP, las sesiones DLSw y el tráfico DLSw posteriores.

Mandatos
GWCON, protocol dls, add cache-entry
GWCON, protocol dls, add explorer-override
GWCON, protocol dls, add mac-list
GWCON, protocol dls, add priority-override
GWCON, protocol dls, add qllc destination
GWCON, protocol dls, add qllc station
GWCON, protocol dls, add sdlc
GWCON, protocol dls, add tcp
GWCON, protocol dls, close-sap
GWCON, protocol dls, delete cache-entry
GWCON, protocol dls, delete explorer-override
GWCON, protocol dls, delete mac-list
GWCON, protocol dls, delete priority-override
GWCON, protocol dls, delete qllc destination
GWCON, protocol dls, delete qllc station **Nota:** Este mandato desactiva todas las sesiones DLSw asociadas.
GWCON, protocol dls, delete sdlc **Nota:** Este mandato desactiva todas las sesiones DLSw asociadas.
GWCON, protocol dls, delete tcp **Nota:** Este mandato desactiva todas las sesiones TCP y DLSw asociadas.
GWCON, protocol dls, disable dynamic-neighbors
GWCON, protocol dls, disable forwarding-explorers
GWCON, protocol dls, disable IPv4 DLSw Precedence
GWCON, protocol dls, disable LLC Disconnect
GWCON, protocol dls, disable mac-list
GWCON, protocol dls, disable qllc callin
GWCON, protocol dls, disable qllc station
GWCON, protocol dls, disable sdlc
GWCON, protocol dls, enable dynamic-neighbors
GWCON, protocol dls, enable forwarding-explorers
GWCON, protocol dls, enable IPv4 DLSw Precedence
GWCON, protocol dls, enable LLC Disconnect
GWCON, protocol dls, enable mac-list
GWCON, protocol dls, enable qllc callin
GWCON, protocol dls, enable qllc station
GWCON, protocol dls, enable sdlc
GWCON, protocol dls, join-group

GWCON, protocol dls, leave-group
GWCON, protocol dls, open-sap
GWCON, protocol dls, set dynamic-tcp
GWCON, protocol dls, set explorer-limit
GWCON, protocol dls, set llc2
GWCON, protocol dls, set mac-list
GWCON, protocol dls, set memory
GWCON, protocol dls, set priority
GWCON, protocol dls, set qllc
GWCON, protocol dls, set timers

Mandatos no reconfigurables dinámicamente

En la tabla siguiente figuran los mandatos de configuración de DLSw que no pueden cambiarse dinámicamente. Para activar estos mandatos, es necesario volver a cargar o a arrancar el dispositivo.

Mandatos
CONFIG, protocol dls, disable dlsw
CONFIG, protocol dls, enable dlsw
CONFIG, protocol dls, set cache
CONFIG, protocol dls, set maximum
CONFIG, protocol dls, set srb

Utilización de ARP

En este capítulo se describe la manera de utilizar los protocolos ARP (Address Resolution Protocol) y ARP inverso (Inverse Address Resolution Protocol) en el direccionador. Consta de los apartados siguientes:

Visión general de ARP

ARP es un protocolo de bajo nivel que correlaciona de forma dinámica las direcciones de la capa de red con direcciones MAC (control de acceso al medio) físicas. Dada la dirección de capa de red del sistema destino, ARP localiza la dirección MAC del sistema principal destino dentro del mismo segmento de red.

Por ejemplo, un direccionador recibe un paquete IP dirigido a un sistema principal conectado a una de las LAN. El paquete contiene sólo una dirección de destino IP de 32 bits. Para construir la cabecera de la capa de enlace de datos, el direccionador adquiere la dirección MAC física del sistema principal destino. A continuación, correlaciona esa dirección con la dirección IP de 32 bits. Esta función se denomina *resolución de dirección*. La Figura 47 en la página 638 ilustra la forma en que funciona ARP.

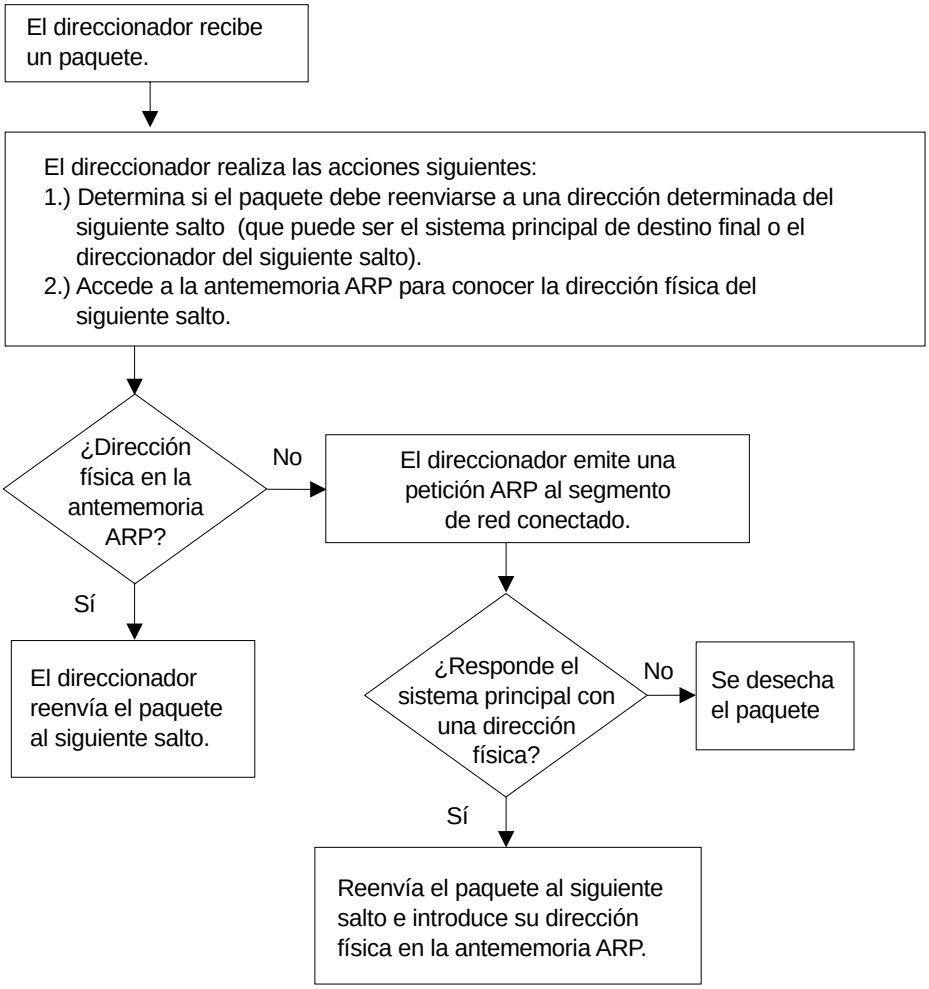


Figura 47. Difusión de la resolución de dirección ARP

Cuando un direccionador convierte una dirección de la capa de red en una dirección física, accede a la antememoria (de conversión) ARP. Ésta contiene la dirección MAC física que corresponde a la dirección de la capa de red. Si falta la dirección, el direccionador difunde una petición ARP a todos los sistemas principales del segmento de red conectado a fin de localizar la dirección MAC física correcta. El nodo que tiene la dirección MAC física correcta responde al direccionador. Éste envía entonces el paquete al nodo y entra la dirección MAC física en la antememoria de conversión para su uso en el futuro.

Visión general de ARP inverso

El protocolo ARP inverso, descrito en el documento RFC 1293/2390, se creó para redes Frame Relay. Este protocolo define un método para que los direccionadores de una red Frame Relay conozcan las direcciones de protocolo de otros direccionadores de manera que se reduzca muy eficientemente el tráfico suprimiendo la necesidad de difundir paquetes ARP con el fin de resolver la dirección. Para descubrir una dirección de protocolo, ARP inverso envía paquetes de petición de ARP inverso a la dirección de hardware (para los circuitos Frame Relay, el identificador de circuito es el equivalente Frame Relay de una dirección de hardware), en cuanto se activa el circuito. El direccionador remoto responde dando su direc-

ción de protocolo y la correlación resultante queda almacenada en la antememoria ARP.

Las entradas de dirección de protocolo-dirección de hardware que se averiguan por medio de ARP inverso no caducan cuando caduca el temporizador de renovación. Las correlaciones no pierden vigencia de ninguna manera, excepto cuando se desactiva el circuito Frame Relay. Esto significa que no es necesario que el direccionador transmita ninguna difusión ARP para actualizar la antememoria ARP. No obstante, el direccionador permite las actualizaciones de una entrada cuando el otro direccionador (remoto) cambia de dirección de protocolo.

El soporte a ARP y a ARP inverso mejora en buena medida la interoperabilidad del direccionador con los de otros proveedores en Frame Relay por lo que a la correlación dinámica de las direcciones de hardware y protocolo se refiere. Si hay otros direccionadores conectados a Frame Relay que den soporte a ARP inverso, las correlaciones se averiguan dinámicamente según lo descrito anteriormente. Si los direccionador conectados no dan soporte a ARP inverso sino al protocolo “tradicional” ARP sobre Frame Relay, las correlaciones se averiguan dinámicamente mediante intercambios ARP (consulte la Figura 47 en la página 638).

Si es necesario, las direcciones de protocolo de otros direccionadores se pueden configurar manualmente utilizando el mandato de configuración Frame Relay **add protocol-address**. Si desea obtener información adicional, consulte el capítulo dedicado a configuración y supervisión de interfaces Frame Relay de la publicación *Access Integration Services Guía del usuario de software*.

Configuración y supervisión de ARP

En este capítulo se describe cómo configurar y supervisar la actividad del protocolo ARP, y cómo utilizar los mandatos de supervisión de ARP. Incluye las secciones siguientes:

Acceso al entorno de configuración de ARP

Para obtener información sobre cómo acceder al entorno de configuración de ARP, consulte "Cómo empezar", en *Access Integration Services Guía del usuario de software*.

Para acceder al proceso de *configuración* de ARP, siga los pasos siguientes:

1. En el indicador de OPCON, escriba **talk 6**. (Para obtener más detalles sobre este mandato, consulte "Proceso OPCON y mandatos de OPCON", en el manual *Access Integration Services Guía del usuario de software*.) Por ejemplo:

   ```
   * talk 6
   Config>
   ```

   Cuando haya entrado el mandato **talk 6**, aparecerá en el terminal el indicador CONFIG (`Config>`). Si el indicador no aparece al entrar por primera vez en la configuración, pulse **Intro** de nuevo.

2. En el indicador CONFIG, entre el mandato **prot arp** para acceder al indicador `ARP Config>`.

Mandatos de configuración de ARP y de ARP inverso

En este apartado se describen los mandatos de configuración de ARP . En la Tabla 37 en la página 642 se listan los mandatos de configuración de ARP. Se puede acceder a los mandatos de configuración de ARP desde el indicador `ARP config>`.

Tabla 37. Resumen de los mandatos de configuración de ARP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Add Entry	Añade una entrada de conversión de dirección MAC.
Change Entry	Cambia una entrada de conversión de dirección MAC.
Delete Entry	Suprime una entrada de conversión de dirección MAC.
Disable Auto-refresh	Inhabilita la renovación automática de ARP.
Enable Auto-refresh	Habilita la renovación automática de ARP.
List	Lista los datos de configuración de ARP almacenados en memoria SRAM.
Set	Establece los tiempos de espera de utilización y de renovación.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Add Entry

Utilice el mandato **add entry** para añadir una entrada que “correlacione estáticamente direcciones hardware y direcciones del protocolo”. Actualmente este mandato sólo se admite para direcciones IP.

Sintaxis:

| **add entry** *número-interfaz tipo-protocolo dirección-protocolo dirección-MAC tipo-encapsulación-IP*

número-interfaz

Valores válidos: Cualquier interfaz ya definida

Valor por omisión: 0

tipo-protocolo

Valores válidos: Cualquier protocolo que admita ARP.

Valor por omisión: IP

dirección-protocolo

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0

dirección-MAC

Valores válidos: Cualquier dirección MAC válida

Valor por omisión: Ninguno

| **tipo-encapsulación-IP**

| Esta opción aparece sólo si se va a configurar una interfaz Ethernet. Debe seleccionarse el tipo de encapsulación IP que coincida con la calse de encapsulación que se efectúa el sistema principal. Consulte el apartado “Configuración y supervisión de la interfaz de red Ethernet” de

la publicación *Access Integration Services Guía del usuario de software* si desea obtener más información.

Valores válidos: **Ether** o **ieee-802.3**

Valor por omisión: **Ether**. El valor configurado entra en vigor sólo si la encapsulación de la interfaz de red es **both**. De lo contrario, este parámetro toma como valor por omisión el tipo de encapsulación que está configurado en la interfaz de red, independientemente de cuál sea el valor configurado para el sistema interfaz.

Ejemplo: **add entry**

```
Interface Number [0]?
Protocol [IP]?
IP Address [0.0.0.0]?
Mac Address []?
IP Encapsulation type (ETHER/IEE-802.3) [ETHER]?
```

Change Entry

Utilice el mandato **change entry** para cambiar una entrada que "correlacione estáticamente direcciones hardware y direcciones del protocolo". Actualmente este mandato sólo se admite para direcciones IP. El parámetro dirección hardware (dirección-MAC) debe ser la dirección del nodo que se va a cambiar.

Sintaxis:

c**hange** e**ntry** *número-interfaz tipo-protocolo dirección-protocolo dirección-MAC tipo-encapsulación-IP*

número-interfaz

Valores válidos: Cualquier interfaz ya definida

Valor por omisión: 0

tipo-protocolo

Valores válidos: Cualquier protocolo que admita ARP.

Valor por omisión: IP

dirección-protocolo

Valores válidos: Cualquier máscara IP válida

Valor por omisión: Ninguno

dirección-MAC

Valores válidos: Cualquier dirección MAC válida

Valor por omisión: Ninguno

tipo-encapsulación-IP

Esta opción aparece sólo si se va a configurar una interfaz Ethernet. Debe seleccionarse el tipo de encapsulación IP que coincida con la calse de encapsulación que se efectúa el sistema principal.

Valores válidos: **Ether** o **ieee-802.3**

Valor por omisión: **Ether**. El valor configurado entra en vigor sólo si la encapsulación de la red es **both**. De lo contrario, este parámetro toma como valor por omisión el tipo de encapsulación que está configurado en la interfaz de red, independientemente de cuál sea el valor configurado para el sistema interfaz.

Delete Entry

Utilice el mandato **delete entry** para suprimir una entrada que “correlacione estáticamente direcciones hardware y direcciones del protocolo”. Actualmente este mandato sólo se admite para direcciones IP.

Sintaxis:

d**elete** e**ntry** *número-interfaz tipo-protocolo dirección-protocolo*

número-interfaz

Valores válidos: Cualquier interfaz ya definida

Valor por omisión: 0

tipo-protocolo

Valores válidos: *IP* o *IPX*

Valor por omisión: IP

dirección-protocolo

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 renovación automática. La función de renovación automática permite que el direccionador envie una petición ARP basada en la entrada de la antememoria de conversión, antes de que se agote el tiempo del temporizador. La petición se envía directamente a la dirección hardware de la conversión actual, en lugar de difundirse de manera general. Si la función de renovación automática está inhabilitada, no se realizan peticiones ARP ‘preventivas’, se permite que se agote el tiempo del temporizador y, por último, la conversión ARP se depura en la tabla. El siguiente paquete de protocolo que se envíe a la dirección del protocolo de destino hará que se difunda una petición ARP nueva a toda 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 renovación automática. La función de renovación automática permite que el direccionador envie una petición ARP basada en la entrada de la antememoria de conversión, antes de que se agote el tiempo del temporizador. La petición se envía directamente a la dirección hardware de la conversión actual, en lugar de difundirse de manera general.

Si se habilita la función de renovación automática, puede ocurrir que la antememoria retenga algunas entradas, se utilicen o no. En redes que tengan un

gran número de nodos, esto puede llevar a que el número de entradas en la antememoria sea excesivo, lo que afectará negativamente al rendimiento del direccionador. Sin embargo, en redes con un número pequeño de nodos, esta opción es útil puesto que reduce el tráfico ARP que se difunde de manera general.

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 almacenada en memoria SRAM. El mandato list muestra la configuración actual de los tiempos de espera de los temporizadores de renovación y de utilización.

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: permanent
Auto Refresh: disabled

Mac address translation configuration
IF #           Prot #         Protocol --> Mac Address  IP-Encap 1
 0               0           2.2.2.1 --> 0000C90932EF  Ether
```

1 La encapsulación IP se visualiza sólo en el caso de las interfaces Ethernet configuradas estáticamente.

config Lista la configuración de los parámetros de ARP.

Ejemplo: `list config`

```
ARP configuration:

Refresh Timeout: 5 minutes
Auto refresh: disabled
```

entry Lista las entradas de ARP almacenadas en memoria 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:

s**et** refresh-timer

refresh-timer *minutos*

Cambiar el tiempo de espera del temporizador de renovación. Para cambiar el tiempo de espera del temporizador de renovación, escriba el tiempo de espera en minutos. Si el valor es cero (0), el temporizador de renovación se desactiva (inhabilita).

Este temporizador se utiliza para determinar cuándo debe renovarse una entrada de la antememoria de conversión de ARP, si la renovación automática está habilitada; o cuándo debe depurarse, si está inhabilitada. Al inhabilitar el temporizador, las entradas se retendrán hasta que la conversión de una dirección que se acaba de averiguar haga que se eliminen las entradas, hasta que las entradas se borren manualmente con el mandato de supervisión **clear** de ARP, o hasta que se vuelva a iniciar el direccionador.

Valores válidos: Un número entero de minutos, comprendido entre 0 y 65.535

Valor por omisión: 5 minutos

Ejemplo: `set refresh-timer 3`

Acceso al entorno de supervisión de ARP

Siga el procedimiento que se describe a continuación para acceder a los mandatos de supervisión de ARP. Este proceso permite acceder al proceso de *supervisión* de ARP.

1. Entre **talk 5** en el indicador de OPCON. (Para obtener más detalles sobre este mandato, consulte “Descripción del proceso OPCON”, en la publicación *Access Integration Services Guía del usuario de software*).Por ejemplo:

   ```
   * talk 5
   +
   ```

   Cuando haya entrado el mandato **talk 5**, aparecerá en el terminal el indicador de GWCON (+). Si el indicador no aparece al entrar por primera vez en la configuración, pulse **Intro** de nuevo.

2. En el indicador +, escriba el mandato **protocol arp** para acceder al indicador ARP>.

   Ejemplo:

   ```
   + prot arp
   ARP>
   ```

Mandatos de supervisión de ARP

En este apartado se describen los mandatos de supervisión de ARP. Se puede acceder a los mandatos de supervisión de ARP desde el indicador ARP>. En la Tabla 38 en la página 647 se muestran los mandatos.

Tabla 38. Resumen de los mandatos de supervisión de ARP	
Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Clear	Borra la antememoria de una interfaz determinada.
Dump	Muestra la antememoria de una interfaz determinada.
Hardware	Lista todas las redes configuradas para ARP.
Ping	Verifica la conexión entre el dispositivo y la estación final.
Protocol	Lista todos los protocolos configurados para ARP.
Statistics	Muestra información sobre ARP.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Clear

Utilice el mandato **clear** para vaciar la antememoria ARP de una interfaz de red concreta. El mandato **clear** puede utilizarse para forzar la supresión de transacciones incorrectas.

Para borrar una interfaz concreta escriba el número de interfaz o de red como parte del mandato. Para obtener el número de interfaz, utilice el mandato **list devices**, de CONFIG.

Sintaxis:

c**lear** *número-interfaz*

Ejemplo: `clear 1`

Dump

Utilice el mandato **dump** para visualizar la antememoria ARP de una combinación de red y protocolo concretas. Para visualizar la antememoria ARP de una interfaz concreta, escriba el número de interfaz o de red como parte del mandato. Para obtener el número de interfaz, utilice el mandato **list devices**, de CONFIG.

Si existe más de un protocolo para la red, también debe proporcionarse el número de protocolo. Esto hace que la función de supervisión muestre las correlaciones entre las direcciones hardware y del protocolo almacenadas en la base de datos. En el caso de que se esté utilizando ARP para un solo protocolo de la interfaz, el número de protocolo es opcional. Para obtener el número de protocolo, utilice el mandato **protocol** de CONFIG.

Para cada correlación, el mandato **dump** muestra la dirección hardware, la dirección del protocolo y el parámetro del temporizador de renovación.

Sintaxis:

d**ump** *número-interfaz número-protocolo*

Ejemplo: dump 2 ip

```
 ARP>du 2 ip
Hardware Address    IP Address  IP-Encap    Refresh
 02-07-01-00-00-01  1.1.1.1                 19
 a1-b2-c3-4d-5e-6f  1.1.1.2     ieee 802.3  Permanent
 100                1.1.1.3     ieee 802.3  Permanent
 16                 1.1.1.5                 Not Aging
```

Notas:

1. Los parámetros del temporizador de renovación válidos son los siguientes:

   Permanent
   Correlación configurada estáticamente entre la dirección de hardware y la dirección de protocolo (entrada mediante el mandato **add entry** de ARP, o **add protocol** de frame-relay, o **add address** de X.25). No se verifica la antigüedad de las entradas y las correlaciones averiguadas dinámicamente no pueden grabarse encima.

   minutos para caducar
   Minutos que transcurrirán hasta que expire la vigencia de esta correlación o hasta que se renueve (si está habilitada la función de renovación automática). Este parámetro se expresa como valor numérico.

   Not Aging
   Correlación fija de un SVC o un PVC averiguada mediante ARP inverso. Empiezará perder vigencia solamente cuando se desactive el circuito. Una dirección que se acaba de averiguar puede grabarse encima de la correlación, o se puede borrar ejecutando el mandato de supervisión **clear** de ARP.

2. La encapsulación IP se aplica sólo a las entradas ARP estáticas (las que tienen intervalos de renovación permanentes). Consulete el mandato **add entry** de Talk 6 si desea obtener más información.

Hardware

Utilice el mandato **hardware** para visualizar las redes registradas con ARP. El mandato **hardware** lista las redes registradas con ARP y muestra el espacio de direcciones hardware (Hardware AS) y las direcciones hardware locales 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 IPPN hace referencia a los túneles IP, siendo el campo dirección hardware la dirección IP del túnel IP.

Ping

Utilice el mandato **ping** para que el direccionador envíe peticiones ICMP de eco a un destino concreto. Para obtener más información sobre el mandato **ping**, consulte “Ping” en la página 350.

Protocol

Utilice el mandato **protocol** para mostrar (para cada red) los protocolos que tienen direcciones registradas con ARP. Este mandato muestra la red, el nombre y el número del protocolo, el espacio de direcciones del protocolo (en hexadecimal) y las direcciones locales del protocolo.

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 SR hacen referencia al direccionamiento en origen (la dirección del protocolo se utiliza para indicar la dirección MAC). Utilice el mandato **dump** de la interfaz de red en anillo para ver las entradas RIF reales.

Statistics

Utilice el mandato **statistics** para visualizar las estadísticas sobre el funcionamiento del módulo ARP.

Sintaxis:

s**tatistics**

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	Muestra los contadores que representan el número de paquetes ARP de entrada descartados porque la capa ARP estaba demasiado ocupada. Se muestra el número total por cada interfaz de red.
ARP cache meters	Consiste en varios medidores del funcionamiento de la antememoria ARP. Se muestra el número total por cada protocolo e interfaz.

Net	Muestra los números de interfaz.
Prot	Muestra los números de protocolo.
Max	Muestra la longitud máxima que ha tenido la cadena hash.
Cur	Muestra la longitud máxima actual de la cadena hash.
Cnt	Muestra el número total de entradas actualmente activas.
Alloc	Muestra el número total de entradas creadas.
Rfrsh:Tot	Muestra el número de peticiones de renovación enviadas para esta interfaz de red y protocolo.
Fail	Muestra el número de intentos de renovación automática que no han tenido éxito debido a la falta de disponibilidad de recursos internos. Este valor no está relacionado con el hecho de que se haya renovado una entrada o no.
TMOs:Rfrsh	Muestra el número total de entradas suprimidas a causa de que se ha cumplido el tiempo de espera del temporizador de renovación.

Utilización de IPX

En este capítulo se describe cómo utilizar el protocolo IPX en el 2212. Incluye las secciones siguientes:

Visión general de IPX

La implementación de IPX hecha por IBM permite que el direccionador funcione como un direccionador de interredes NetWare de Novell. Tiene las características siguientes:

- Compatibilidad con todos los entornos de las versiones anteriores de NetWare de Novell.
- Compatibilidad con la función de puenteo de un servidor de archivos NetWare, además de poder funcionar como un puente NetWare autónomo.
- Soporte del emulador NetBIOS de Novell.

Direcciones IPX

Los apartados siguientes describen las direcciones IPX.

Números de red

Un número de red IPX indica la ubicación de una red determinada dentro de una interred. Se pueden utilizar direcciones divididas en varias partes, como en el caso de la dirección de una carta, compuesta de ciudad, calle y piso. Por ejemplo, IPX hace mención a números de red (ciudad), números de sistema principal (calle) y números de socket (piso). Estas direcciones permiten la comunicación entre dos entidades pertenecientes a redes distintas.

Números de sistema principal

Cada circuito IPX necesita un número de sistema principal (nodo) de 6 bytes.

Los circuitos de red en anillo y Ethernet utilizan sus direcciones MAC como número de sistema principal y no pueden cambiarse.

Puesto que las líneas serie no tiene direcciones MAC de hardware, se debe especificar un número exclusivo de sistema principal. IPXWAN utiliza el identificador de nodo configurado, seguido de x'0000'.

Circuitos IPX

El software de direccionamiento de IPX representa a las interfaces de red como un solo circuito IPX de difusión general, como uno o más circuitos IPXWAN punto a punto, o como una combinación de ambos tipos de circuitos. El tipo de encapsulación, de direcciones IPX y los protocolos de direccionamiento utilizados para el circuito, dependen del DLC subyacente y de si el circuito IPX está configurado como de difusión general o como IPXWAN punto a punto.

Los circuitos IPX de difusión general tienen las características siguientes:

- Se utilizan en interfaces LAN
- Se utilizan en interfaces WAN, si IPXWAN no está configurado
- Están restringidos a un solo circuito IPX de difusión general por cada interfaz
- Se les debe asignar un número de red IPX distinto de cero
- Para interfaces LAN, utilizan la dirección MAC de la interfaz de red como número de nodo IPX del circuito.
- Para interfaces WAN, utilizan el número de sistema principal IPX configurado como número de nodo IPX del circuito.
- Permiten la utilización concurrente de RIP/SAP, y de rutas y servicios estáticos.

Los circuitos IPXWAN punto a punto tienen las características siguientes:

- Sólo pueden utilizarse en interfaces WAN
- Pueden no estar restringidos a un solo circuito IPXWAN punto a punto por cada interfaz
- Utilizan IPXWAN para negociar los parámetros
- Pueden no necesitar un número de red IPX
- Utilizan un ID de nodo IPXWAN seguido de 0000 como número de nodo IPX del circuito
- Están restringidos a negociar un sólo tipo de direccionamiento.

En los apartados siguientes se describe cómo se representan todos los tipos de interfaces de red admitidos.

Interfaces LAN (de red en anillo, Ethernet)

El software de direccionamiento de IPX representa a una interfaz LAN como un solo circuito IPX de difusión general.

Al circuito se le debe asignar un número de red IPX exclusivo y distinto de cero

La dirección MAC de la interfaz de red se utiliza como número de nodo IPX del circuito.

La dirección difundida a todas las estaciones de la LAN (x'FFFFFFFFFFFF') se utiliza para recibir y transmitir paquetes de difusión general, como por ejemplo paquetes de actualización RIP y SAP.

Se admiten los tipos de encapsulación normales para el tipo apropiado de interfaz LAN.

El tamaño máximo de un paquete IPX se calcula a partir de la MTU configurada para la interfaz.

Para interfaces de red en anillo, se puede habilitar el direccionamiento en origen para la interfaz, de forma que se permita al reenviador IPX acceder a las estaciones finales (y a otros direccionadores) a través de puentes de direccionamiento en origen.

Se puede utilizar uno de los tipos de direccionamiento siguientes para el circuito (o ambos):

- Rutas o servicios estáticos
- RIP/SAP (numerado)

Protocolo punto a punto (PPP)

El software de direccionamiento de IPX representa a una interfaz PPP como un solo circuito IPX de difusión general, o como un solo circuito IPXWAN punto a punto.

El tamaño máximo de un paquete IPX se calcula a partir de la MTU negociada por el DLC subyacente de PPP.

Circuito IPX de difusión general: Si se configura como un circuito de difusión general, se le debe asignar un número de red exclusivo y distinto de cero.

Puesto que no hay ninguna dirección MAC asociada con una interfaz PPP, se utiliza como número de nodo IPX del circuito un número de sistema principal configurado.

Se puede utilizar uno de los tipos de direccionamiento siguientes para el circuito (o ambos):

- Rutas o servicios estáticos
- RIP/SAP (numerado)

Circuito IPXWAN punto a punto: Si se configura como un circuito IPXWAN punto a punto, utilizará IPXWAN para negociar los parámetros de direccionamiento.

El tipo de direccionamiento RIP numerado de IPXWAN necesita que se le asigne al circuito un número de red exclusivo y distinto de cero. Los otros tipos de direccionamiento de IPXWAN (RIP no numerado o estático), no necesitan número de red (el valor es 0).

Puesto que no hay ninguna dirección MAC asociada con la interfaz PPP, el identificador de nodo IPXWAN seguido de 0000 se utiliza como número de nodo IPX del circuito.

El tipo de direccionamiento a negociar para el circuito es configurable. Si el direccionamiento estático está habilitado, no se podrá negociar ningún otro tipo de direccionamiento. Se puede habilitar uno de los otros tipos (o ambos) y se negociará el que se elegirá en orden descendente:

- RIP/SAP no numerado
- RIP/SAP numerado

Frame Relay

El software de direccionamiento de IPX representa a una interfaz Frame Relay como:

- un solo circuito IPX de difusión general, o
- un conjunto de uno o más circuitos IPXWAN punto a punto, o
- una combinación de ambos.

El tamaño máximo de un paquete IPX se calcula a partir de la MTU configurada para la interfaz.

El DLC subyacente de Frame Relay utiliza InARP para correlacionar las direcciones del nodo IPX de destino con el circuito Frame Relay virtual apropiado. Opcionalmente, las direcciones del nodo IPX de destino pueden configurarse estáticamente para los circuitos virtuales conectados a direccionadores que no admitan InArp.

Circuito IPX de difusión general: Todos los circuitos virtuales de la interfaz Frame Relay que no están configurados como circuitos IPXWAN punto a punto se agrupan juntos y se representan como un solo circuito IPX de difusión general, al que debe asignársele un número de red exclusivo y distinto de cero. Por lo tanto, los circuitos virtuales subyacentes definidos por el usuario para interconectar direccionadores en la red Frame Relay son transparentes para el software de direccionamiento de IPX.

Puesto que no hay ninguna dirección MAC asociada con una interfaz Frame Relay, se utiliza como número de nodo IPX del circuito un número de sistema principal configurado.

La dirección difundida a todas las estaciones de la LAN (x'FFFFFFFFFFFF') sirve como dirección IPX de difusión general del circuito. Los paquetes dirigidos a la dirección de difusión general se transmiten a todos los circuitos virtuales del circuito IPX de difusión general mediante el DLC subyacente de Frame Relay. Esta función de Frame Relay de difusión general del protocolo se activa al habilitar las opciones de configuración de Frame Relay siguientes:

- Difusión general del protocolo
- Emulación de multidifusión

Para admitir topologías Frame Relay que no son en malla completa, debe inhabilitarse el horizonte dividido para el circuito IPX de difusión general. Esto permite que RIP y SAP difundan información a todos los circuitos virtuales en el circuito IPX de difusión general, de forma que puede producirse un direccionamiento intermedio entre circuitos virtuales del mismo circuito IPX de difusión general.

No se necesita inhabilitar el horizonte dividido para las topologías Frame Relay en malla completa.

Se puede utilizar uno de los tipos de direccionamiento siguientes para el circuito (o ambos):

- Rutas o servicios estáticos
- RIP/SAP (numerado)

Circuito IPXWAN punto a punto: IPX puede configurarse para que funcione como circuitos IPXWAN punto a punto a través de circuitos PVC y SVC Frame Relay individuales. IPXWAN se utiliza para negociar los parámetros de direccionamiento.

El tipo de direccionamiento RIP numerado de IPXWAN necesita que se le asigne al circuito un número de red exclusivo y distinto de cero. Los otros tipos de direccionamiento de IPXWAN (RIP no numerado o estático) no necesitan número de red (el valor es 0).

Puesto que no hay ninguna dirección MAC asociada con la interfaz Frame Relay, el identificador de nodo IPXWAN seguido de 0000 se utiliza como número de nodo IPX del circuito.

El tipo de direccionamiento a negociar para el circuito es configurable. Si el direccionamiento estático está habilitado, no se podrá negociar ningún otro tipo de direccionamiento. Se puede habilitar uno de los otros tipos (o ambos) y se negociará el que se elegirá en orden descendente:

- RIP/SAP no numerado
- RIP/SAP numerado

X.25

El software de direccionamiento de IPX representa a una interfaz X.25 como un solo circuito IPX de difusión general. Por lo tanto, los circuitos virtuales subyacentes definidos por el usuario para interconectar direccionadores en la red X.25 son transparentes para el software de direccionamiento de IPX.

Al circuito se le debe asignar un número de red IPX exclusivo y distinto de cero

Puesto que no hay ninguna dirección MAC asociada con una interfaz X.25, se utiliza como número de nodo IPX del circuito un número de sistema principal configurado.

La dirección difundida a todas las estaciones de la LAN (x'FFFFFFFFFFFF') sirve como dirección IPX de difusión general del circuito. Los paquetes dirigidos a la dirección de difusión general se transmiten a todas las direcciones X.25 de destino del circuito IPX de difusión general mediante el DLC subyacente de X.25.

El tamaño máximo de un paquete IPX se calcula a partir de la MTU configurada para la interfaz.

Para admitir topologías X.25 que no son en malla completa, debe inhabilitarse el horizonte dividido para el circuito IPX de difusión general. Esto permite que SAP difunda información a todas las direcciones X.25 de destino en el circuito IPX de difusión general, de forma que puede producirse un direccionamiento intermedio entre circuitos virtuales del mismo circuito IPX de difusión general.

No se necesita inhabilitar el horizonte dividido para las topologías X.25 en malla completa.

Se puede utilizar uno de los tipos de direccionamiento siguientes para el circuito (o ambos):

- Rutas o servicios estáticos
- RIP/SAP (numerado)

Las direcciones del nodo IPX de destino deben configurarse estáticamente para todas las direcciones X.25 de destino, puesto que el DLC de X.25 no admite InArp.

Configuración de IPX

En este apartado se describe cómo configurar inicialmente IPX. En los apartados siguientes se describen los parámetros opcionales que pueden definirse.

1. Visualice el indicador de configuración de IPX, tal y como se muestra aquí:

```
* talk 6
Config> protocol ipx
IPX protocol user configuration
IPX config>
```

2. Habilite globalmente IPX.

```
IPX config> enable ipx
```

3. Añada un circuito de difusión general a una interfaz WAN o LAN, o un circuito IPXWAN a una interfaz 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 ? Cartagena
```

   Nota: El número de red IPX 0 sólo es válido en RIP o circuitos de direccionamiento estático no numerados 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 se ha habilitado IPX para que funcione en un circuito serie, asigne al direccionador un número exclusivo de sistema principal.

```
IPX config>set host-number
Host number for serial lines (in hex) []? 2
```

5. Opcionalmente, cambie el tipo de trama para Ethernet o red en anillo. No es necesario establecer el tipo de trama para otros circuitos distintos de Ethernet o red en anillo. Para obtener una descripción de los tipos de tramas disponibles, consulte “Frame” en la página 687.

   Los formatos de encapsulación por omisión son:

   - Ethernet - Ethernet_8023
   - Red en anillo - red en anillo MSB

   Utilice el mandato **frame** tal como se muestra a continuación:

```
IPX config> frame ethernet_8023 IPX circuit number [1]? 2
```

6. Opcionalmente, cambie los parámetros de IPXWAN para los que no quiera 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 los apartados siguientes se describe cómo ajustar los valores de configuración opcionales.

Especificación del tamaño de la tabla de redes RIP de IPX

La tabla de redes RIP de IPX contiene información sobre todas las redes IPX. El tamaño por omisión de la tabla es 32. Se puede configurar un tamaño de tabla de entre 1 y 2.048; sin embargo, es posible que las limitaciones de memoria del direccionador impidan utilizar el tamaño máximo de la tabla.

```
IPX config>set maximum networks
New Network table size [32]? 32
```

Especificación del intervalo de actualización RIP

IPX utiliza RIP para el mantenimiento de las rutas de sus tablas de direccionamiento. Una ruta indica la vía que ha de seguir un paquete. El intervalo de actualización RIP determina la frecuencia con que el direccionador difundirá las tablas de información de direccionamiento a sus circuitos. También determina durante cuanto tiempo permanecerá una entrada RIP, antes de considerar que ha perdido vigencia.

Las entradas válidas permanecen en las tablas de direccionamientos durante un período de tres veces el intervalo de actualización RIP, y el direccionador difunde sus tablas RIP cada vez que vence un 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 renueva mediante una actualización RIP, la ruta se marca con una cuenta de saltos infinita (16) y, a continuación, se suprime. Cada 60 segundos el direccionador difunde sus tablas RIP a los circuitos correspondientes.

Puede configurarse un intervalo RIP de entre 1 y 1.440 minutos (24 horas). Si se aumenta el intervalo RIP, se reduce el tráfico de las líneas WAN y de los circuitos de marcación. También se evita que los circuitos de marcación a petición tengan que marcar tan a menudo.

Nota: Aunque los anuncios RIP realizados se controlan mediante este intervalo, el direccionador sigue difundiendo los cambios ocurridos en la topología de la red a medida que los va averiguando.

El intervalo RIP no puede configurarse para servidores de archivos de 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 SAP de IPX

La tabla de servicios del Protocolo de anuncio de servicios (Service Advertising Protocol, SAP) de IPX es una base de datos distribuida que se utiliza para buscar servicios de NetWare, como por ejemplo, servidores de archivos. Los servicios se identifican exclusivamente gracias a un tipo numérico de 2 bytes y a un nombre de 47 caracteres. Cada suministrador de servicios anuncia sus servicios especificando el tipo, el nombre y la dirección del servicio. El direccionador acumula esta información en una tabla y se la envía a otros direccionadores. El tamaño por omisión de la tabla es 32.

Se puede configurar un tamaño de tabla de entre 1 y 2.048; sin embargo, puede ser que las restricciones de memoria del direccionador impidan utilizar el tamaño máximo de la tabla.

```
IPX config>set maximum services
New Service table size [32]? 32
```

Especificación del intervalo de actualización SAP

El intervalo del protocolo de anuncio de servicios (SAP) de IPX le permite configurar el tiempo que transcurrirá entre actualizaciones SAP de IPX para cada circuito. Todos los circuitos del direccionador que estén en la misma red, utilizarán el mismo intervalo SAP. Este intervalo determina tanto la vigencia de la información de la tabla, como el intervalo entre difusiones a los circuitos del direccionador.

Las entradas válidas permanecen en la tabla de servicios SAP durante un período de tres veces el intervalo de actualización SAP, y el direccionador difunde la información de su tabla de servicios SAP cada vez que vence un intervalo de actualización.

Puede configurarse un intervalo SAP de entre 1 y 1.440 minutos (24 horas). Si se aumenta el intervalo SAP, se reduce el tráfico de las líneas WAN y de los circuitos de marcación. También se evita que los circuitos de marcación a petición tengan que marcar tan a menudo.

Nota: Aunque los anuncios SAP realizados se controlan mediante este intervalo, el direccionador sigue difundiendo los cambios ocurridos en la topología de la red a medida que los va averiguando.

El intervalo SAP no puede configurarse para servidores de archivos de Novell.

```
IPX config>set sap-update
IPX circuit number [1]? 2
SAP timer value(minutes) [1]? 4
```

Filtrado de paquetes Keepalive y de serialización de IPX

IPX se puede configurar para evitar que los paquetes Keepalive y de serialización activen continuamente un enlace de marcación a petición o para minimizar el tráfico que pasa por un enlace de marcación a petición.

En la Figura 48, por ejemplo, si el cliente Novell se conecta con el servidor Novell y a continuación se mantiene inactivo, el servidor enviará periódicamente peticiones Keepalive al cliente y este le devolverá respuestas Keepalive. El filtrado de paquetes Keepalive hace que los direccionadores entren la primera respuesta Keepalive en sus tablas Keepalive y que después reenvíen la respuesta. A partir de entonces, los direccionadores ya no reenviarán el tráfico Keepalive de esa conexión cliente-servidor a través del enlace WAN. En vez de eso, el direccionador A responderá a las peticiones Keepalive que reciba del servidor, y el direccionador B enviará peticiones Keepalive al cliente Novell.

El filtrado de paquetes Keepalive también impide que los direccionadores reenvíen paquetes NetWare de serialización a través del enlace WAN.

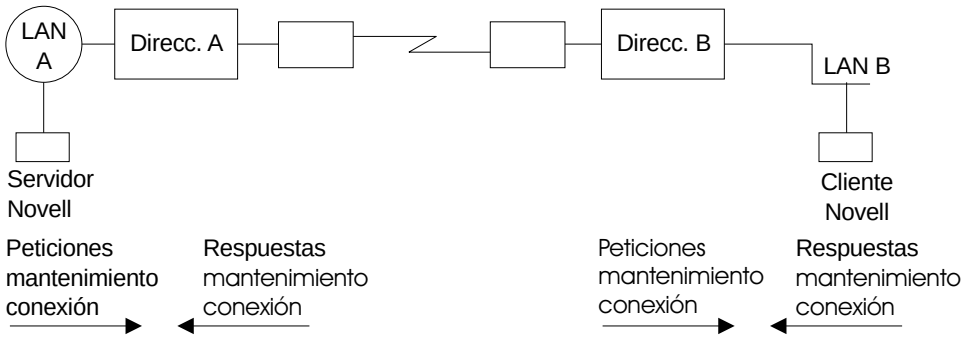


Figura 48. Filtrado Keepalive

Para establecer el filtrado Keepalive, habilítelo para los circuitos de marcación.

```
IPX Config> enable keepalive-filtering
IPX circuit number [1]? 5
```

Configuración de varias rutas

Se puede configurar IPX de forma que mantenga para la misma red de destino más de una entrada en la tabla de direccionamiento. La ventaja de esta función es que si se desactiva una ruta, se utilizará inmediatamente la ruta alternativa. El direccionador no tiene que esperar una difusión RIP, que puede tardar varios segundos (hasta un minuto), en averiguar la ruta nueva. El direccionador almacena en la tabla de direccionamiento solamente las vías que tienen el mismo coste.

Utilice el mandato siguiente para configurar el número máximo de rutas que se almacenarán en la tabla de direccionamiento para cada destino. El valor está comprendido entre 1 y 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 que se conservarán en la tabla de direccionamiento. El valor está comprendido entre 1 y 4.096. El valor por omisión es 32. El número de entradas debe ser al menos igual que el de la tabla de redes RIP (configure el tamaño de la tabla de redes RIP mediante el mandato **set maximum networks**, que se explica en este capítulo).

```
IPX config> set maximum total-route-entries
New route table size [32]? 40
```

Se puede configurar el coste (en ciclos) de un circuito RIP, para cada circuito IPX. El coste del circuito se tiene en cuenta a la hora de calcular el coste total de la ruta en los anuncios de ruta. Si existen varias rutas con el mismo destino, se puede influir en la selección de la ruta asignando un coste de ruta mayor a un circuito IPX que a otro. Utilice el mandato siguiente para establecer el coste de un circuito para una ruta determinada conectada directamente.

```
IPX config> set rip-ticks
IPX circuit number [1]? 2
RIP ticks value (in 55msec ticks [0]? 3
```

Configuración de rutas estáticas

Se puede configurar una ruta estática por cada número de red de destino. Cada ruta estática está asociada con un circuito y se instala en la tabla de direccionamiento cuando se activa el protocolo IPX para el circuito. La ruta estática se elimina de la tabla de direccionamiento cuando se desactiva el protocolo IPX para el circuito, cuando es el propio circuito el que se desactiva, o cuando se averigua dinámicamente una ruta a la red de destino. Las rutas que se averiguan dinámicamente (mediante RIP), siempre se graban encima de las rutas estáticas. La ruta estática se volverá a instalar en la tabla de direccionamiento cuando se vuelva a activar el protocolo IPX en el circuito, cuando el propio circuito vuelva a activarse, o cuando se pierdan todas las rutas RIP a la red de destino.

Las rutas estáticas son particularmente útiles en los circuitos de marcación a petición en los que RIP está inhabilitado y las rutas a las redes de destino están configuradas estáticamente para el circuito de marcación a petición.

Un circuito puede utilizar el direccionamiento estático solo o en combinación con RIP. La única excepción se da si el direccionamiento estático está habilitado para un circuito IPXWAN. En este caso, el direccionamiento estático es el único tipo de direccionamiento que negociará IPXWAN.

RIP anunciará las rutas estáticas, aunque dependerá del horizonte dividido y de los filtros aplicables.

Cuando se configuran varias rutas estáticas por cada red de destino, se utilizan las mismas normas para elegir las rutas RIP que las que se utilizan para determinar las rutas estáticas instaladas en la tabla de direccionamiento. En la tabla de direccionamiento se instalarán varias rutas estáticas a la misma red de destino, si tienen el mismo coste. En la tabla de direccionamiento se pueden almacenar concurrentemente tantas rutas por destino como se haya configurado.

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

Los servicios estáticos pueden configurarse por cada tipo de servicio o por nombre. Cada servicio estático está asociado con un circuito y se instala en la tabla de servicios SAP cuando se activa el protocolo IPX para el circuito y se conoce una ruta a la red del servicio (por un anuncio RIP o de ruta estática). El servicio estático se elimina de la tabla de servicios SAP cuando se desactiva el protocolo IPX para el circuito, cuando es el propio circuito el que se desactiva, cuando se pierde la ruta a la red del servidor, o cuando se averigua dinámicamente el mismo servicio. Mientras se conozca una ruta a la red del servidor, el servicio estático se volverá a instalar en la tabla de servicios cuando se vuelva a activar el protocolo IPX en el circuito, cuando el propio circuito vuelva a activarse o cuando se pierda el servicio SAP que se ha averiguado. Los servicios que se averiguan dinámicamente (mediante SAP), siempre se graban encima de los servicios estáticos.

Los servicios estáticos son particularmente útiles en los circuitos de marcación a petición en los que SAP está inhabilitado y los servicios están configurados estáticamente para el circuito de marcación a petición.

Un circuito puede utilizar los servicios estáticos solo o en combinación con RIP/SAP. La única excepción se da si el direccionamiento estático está habilitado para un circuito IPXWAN. En este caso, el direccionamiento estático es el único tipo de direccionamiento que negociará IPXWAN.

SAP anunciará los servicios estáticos, aunque dependerá del horizonte dividido y de los filtros aplicables.

Cuando se configuran varios servicios estáticos por cada nombre o tipo, se utilizan las mismas normas para elegir los servicios SAP que las que se utilizan para determinar los servicios estáticos instalados en la tabla de direccionamiento. Obsérvese que si entre los servicios configurados existe alguno con el mismo coste, se instalará en la tabla de servicios el que esté definido como ruta actual a la red del servidor para el mismo circuito.

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: []? SERVIDOR_ARCHIVOS01
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 RIP por omisión

La ruta por omisión es un caso especial de ruta estática. Se utiliza como último recurso como salto siguiente en el caso de redes de destino desconocidas.

La ruta por omisión es especialmente útil en los circuitos de marcación a petición en los que RIP está inhabilitado. Configurar la ruta por omisión para el circuito de marcación a petición permite que los clientes soliciten rutas y envíen paquetes a

redes de destino que están al otro extremo del circuito, sin tener que configurar una ruta estática para cada destino.

Manejo de RIP

Para los direccionadores que utilizan RIP, la ruta por omisión viene indicada por el número de red FFFFFFFE.

Cuando se anuncien las rutas RIP, se anunciará la ruta por omisión (como cualquier otra ruta estática), después de aplicar los filtros RIP y dependiendo el horizonte dividido.

El direccionador responderá a una petición RIP dirigida a una red de destino desconocida, solamente si existe una ruta por omisión en la tabla de direccionamiento.

Cuando se reenvían paquetes, si no se conoce la ruta a la red de destino, el reenviador reenviará el paquete al direccionador de salto siguiente que está anunciando la ruta por omisión (o al direccionador de salto siguiente indicado en la definición de ruta por omisión estática local, en caso de direccionamiento estático).

El ejemplo siguiente muestra cómo configurar una ruta RIP por omisión.

```
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

En general, los anuncios SAP se aceptan solamente si se conoce una ruta a la red del servidor. Si no se conoce ninguna ruta a la red del servidor, pero sí se conoce una ruta por omisión, también se aceptará el anuncio (después de aplicar los filtros SAP).

Los anuncios SAP que se acepten a consecuencia de la existencia de la ruta por omisión, se anunciarán en todos los circuitos IPX que sean distintos de aquél del que provenía el anuncio SAP aceptado (horizonte dividido). Naturalmente, antes de anunciarlo, se le aplicarán los filtros SAP. Las mismas normas se aplican a las respuestas a las peticiones SAP.

Configuración de filtros IPX globales (controles de acceso de IPX)

Los filtros IPX globales se aplican a todos los circuitos IPX. Pueden utilizarse para impedir que el direccionador reenvíe paquetes según su dirección IPX (red/sistema-principal/socket). Se pueden utilizar los filtros IPX globales para proporcionar seguridad o para detener el reenvío de paquetes más allá del área de interés por parte de aplicaciones “ruidosas”.

Los filtros IPX globales se basan en la dirección IPX de origen inicial y en la dirección IPX de destino final. Las direcciones de salto intermedias no tienen importancia.

Para un filtro global, una dirección IPX (origen o destino) consiste en un número de red IPX, un número de sistema principal IPX y un rango de números de socket IPX, especificados en hexadecimal. Se puede especificar que el número de red y

el de sistema principal sean 0, que es un comodín que coincide con todos los números de red y de sistema principal, respectivamente. Para los sockets, el comodín es definir un rango de 0 a FFFF.

La lista de filtro globales es una lista ordenada de entradas. Cada entrada de filtro global puede configurarse como incluyente o excluyente. El direccionador compara los paquetes que recibe con la lista de filtro globales.

- Si un paquete coincide con una entrada incluyente, el direccionador reenviará el paquete.
- Si un paquete coincide con una entrada excluyente, el direccionador descartará el paquete.
- Si el direccionador llega al final de la lista sin que ningún paquete coincida con una entrada, el direccionador descartará el paquete (lo que es equivalente a que la última entrada de la lista sea excluyente).

Si va a crear listas de filtro globales, tenga en cuenta los puntos siguientes sobre el protocolo IPX:

- En primer lugar, nunca bloquee los sockets RIP y SAP (X'0453' y X' 0452'). RIP y SAP son necesarios para reenviar correctamente los paquetes IPX.
- Recuerde que la lista de filtro globales se aplica a todos los circuitos. Para representar controles direccionales tendrá que utilizar números de red de origen o de destino en los filtros globales.
- Debe saber donde se encuentran los servicios que está intentando proteger. En el indicador `IPX>`, escriba el mandato **slist** para conocer la dirección de un servicio.

  Nota: Todos los servicios en un servidor de archivos de Novell (versión 3.0 o más reciente) están en la red interna del servidor, normalmente en el sistema principal 000000000001. Puesto que este número de la red interna es exclusivo para toda la red IPX, puede protegerla bloqueando todos los paquetes dirigidos a los sockets de la red interna que estén comprendidos entre 0 y FFFF. Para bloquear solamente el servidor de archivos, bloquee el socket 0451 (0451-0451).

- Cuando se extraen números de socket con el mandato **slist** para crear una lista de filtro globales, recuerde que algunos servicios tienen números de socket fijos y que otros tienen números dinámicos (temporales). Puesto que los sockets comprendidos entre 4000 y FFFF son dinámicos, no puede garantizarse que el servicio tenga el mismo número de socket la próxima vez que se vuelva a arrancar el servidor de archivos. Sin embargo, los números de socket comprendidos entre 8000 y FFFF los asigna Novell y, generalmente, son constantes.

Nota: Los filtros globales y los de circuitos son mutuamente excluyentes. Si se habilitan los filtros SAP globales, no se pueden habilitar los filtros SAP de circuitos (y viceversa). Si se habilitan los filtros IPX globales (*controles de acceso*), no se pueden habilitar los filtros IPX de circuitos (y viceversa).

El direccionador examina cada trama IPX para ver si coincide con alguna entrada de la lista de filtro globales. Se aplica el primer filtro que coincida, por lo que el orden de los filtros globales es muy importante. Estos son los criterios que sigue el direccionador para examinar los paquetes IPX:

1. Tipo de filtro global (dos tipos):

a. Incluyente, que indica que si el paquete coincide con el criterio siguiente, se reenviará
b. Excluyente, que indica que si el paquete coincide con el criterio siguiente, se descartará

2. Red de destino - se obtiene directamente del campo red IPX de destino, del paquete.
3. Sistema principal de destino - se obtiene directamente del campo sistema principal IPX de destino, del paquete.
4. Socket de destino inicial o final - se obtiene directamente del campo socket IPX de destino (no del campo sistema principal), del paquete. El número de socket es la ubicación en que el protocolo vincula el paquete con un servicio de aplicación.
5. Red de origen - se obtiene directamente del campo red IPX de origen, del paquete.
6. Sistema principal - se obtiene directamente del campo sistema principal IPX de origen, del paquete.
7. Socket de origen inicial o final - se obtiene directamente del campo socket IPX de origen, del paquete.

El resultado del ejemplo siguiente será reenviar solamente aquellos paquetes IPX provenientes de los clientes de la red IPX número 1871, con destino a la aplicación NCP, en el servidor de archivos de Novell 0000 C93A 0912, de la red 18730. El tráfico restante se descartará.

```
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 SAP globales

Los filtros SAP globales se aplican a todos los circuitos. Pueden utilizarse para impedir que el direccionador difunda información relacionada con el anuncio de servicios. Hay cuatro razones principales para utilizar filtros SAP globales:

- Se utilizan servidores con tamaños de bindery pequeños (por ejemplo, Netware versión 2.15 o anteriores) y debe limitar la cantidad de información en la base de datos SAP.
- No se quieren anunciar determinados servicios fuera del área local, puesto que no es conveniente que se acceda a ellos de forma remota.
- Se quiere poner orden en la tabla SAP.
- Se quieren reducir los anuncios SAP innecesarios en los enlaces WAN, puesto que los anuncios SAP pueden llegar a consumir una cantidad considerable del ancho de banda de la WAN.

Nota: Ninguna de estas razones menciona explícitamente la seguridad. Los filtros SAP globales no pueden proteger un servicio. Todo lo que hace SAP es proporcionar a los servicios una conversión de nombre a dirección. Si un

intruso potencial conociera la dirección del servicio, bloquear sus anuncios mediante los filtros SAP globales, no protegerá el servicio. Solamente los controles de acceso pueden proporcionar seguridad.

Los filtros SAP globales se basan en establecer una cuenta de saltos máxima para un servicio particular o para un grupo de servicios. La tabla SAP aceptará los anuncios de servicios que se reciban cuya cuenta de saltos sea igual o menor que la especificada. Los otros no se tendrán en cuenta. Los servicios de la base de datos SAP son los únicos que se volverán a anunciar o se utilizarán para responder consultas.

Nota: El direccionador sólo permite que se entren nombres de servicios en formato ASCII de 7 bits. Algunos nombres de servicios utilizan datos binarios, infringiendo las especificaciones SAP de Novell. No será posible filtrar estos servicios por nombre.

Un filtro SAP global puede aplicarse a todos los servicios de un tipo determinado. Novell asigna números de 4 dígitos hexadecimales para cada tipo de servicio. Alternativamente, un filtro SAP global puede aplicarse a un servicio concreto de un tipo determinado. Esto se hace especificando el nombre del servicio.

Pueden existir varios servidores del mismo tipo de servicio, cada uno con un nombre exclusivo de servicio. En este caso, se pueden configurar varios filtros SAP globales con el mismo tipo de servicio para filtrar los nombres exclusivos de servicios, o se puede configurar un solo filtro SAP que filtre el tipo de servicio para todos los nombres de servicios (filtro comodín).

Creación de filtros SAP globales

Para configurar filtros SAP globales:

1. Escriba **add filter** en el indicador `IPX Config>`. Se deben especificar varias entradas clave que normalmente se encuentran en las difusiones SAP:
   a. Número de saltos. Esta entrada indica la cuenta de saltos permitida para una entrada SAP (si es mayor, se descartará).
   b. Tipo de servicio
   c. Nombre de servicio
2. Escriba **set filter on** en el indicador `IPX Config>` para habilitar el filtro.

El ejemplo siguiente muestra la creación de un filtro SAP global para 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 SAP global hace que el direccionador haga caso omiso de los anuncios SAP provenientes del servidor de impresión (tipo de servicio 0047) llamado **rem-ptr1**, que esté a más de dos saltos de distancia. El filtro impide que el direccionador difunda los anuncios que cumplan estos criterios.

Determinación del tipo de servicio para un filtro SAP global

Para determinar el tipo de servicio SAP que se quiere establecer para un filtro, siga estos pasos:

1. En el indicador *, escriba **talk 5**. A continuación, en el indicador +, escriba **protocol ipx**.

   En el indicador `IPX>`, escriba **slist**. Apunte la entrada para los servicios que se quieren filtrar.

2. En el indicador `*`, escriba **talk 6**. A continuación, en el indicador `Config>`, escriba **protocol ipx**. Añada el filtro SAP global y la cuenta de saltos apropiados para el servicio que se quiere filtrar.

3. Después de crear el filtro, vuelva a iniciar el direccionador.

4. Si se ha conseguido filtrar el servicio, ya no debería aparecer en la lista. Para comprobar que el servicio ya no aparece en la lista, escriba **slist** en el indicador `IPX>`.

Filtros IPX de circuitos - Visión general

La característica de direccionamiento de IPX admite cuatro tipos de filtros dependientes del circuito: ROUTER, RIP, SAP e IPX. Para cada circuito puede definirse un *filtro de entrada* y un *filtro de salida*. Los criterios de filtrado, llamados *elementos*, se ensamblan en *listas de filtro* y a continuación se conectan con los filtros de entrada y salida. Una lista de filtro puede conectarse a más de un filtro. Esto evita tener que configurar los mismos criterios de filtrado para más de un circuito.

Nota: Los filtros globales y los de circuitos son mutuamente excluyentes. Si se habilitan los filtros SAP globales, no se pueden habilitar los filtros SAP de circuitos (y viceversa). Si se habilitan los filtros IPX globales (*controles de acceso*), no se pueden habilitar los filtros IPX de circuitos (y viceversa).

Configuración de filtros IPX de circuitos

Para configurar filtros IPX de circuitos:

1. Con el mandato **create list** Cree una lista de filtro y déle nombre.

2. Modifique la lista de filtro con el mandato **update** y, con sus submandatos, especifique los criterios de filtrado y si la lista de filtro es incluyente o excluyente.

3. Cree un filtro para el circuito que quiera mediante el mandato **create filter**, especificando si es un filtro de entrada o de salida.

4. Habilite los filtros IPX de circuitos con el mandato **enable all**.

5. Conecte al filtro las listas de filtro utilizando el mandato **attach**.

6. Establezca la acción por omisión del filtro, ejecutando el mandato **default**. Si no se da ninguna coincidencia con las listas de filtro conectadas, se llevará a cabo la acción por omisión.

También existen 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 de filtro de un filtro, cambiar el orden de las listas de filtro de un filtro (ya que las listas de filtro están ordenadas), listar un filtro, y establecer el tamaño de la antememoria de filtros (solamente para filtros IPX).

Filtros ROUTER

El filtro ROUTER se aplica a la cabecera IPX de todos los paquetes RIP de respuesta recibidos. No se admiten los filtros ROUTER de salida. Los filtros ROUTER pueden utilizarse para agrupar redes IPX individuales en varias interredes IPX diferentes, controlando los direccionadores a los que se permite intercambiar información de direccionamiento.

Los filtros ROUTER de RIP se guardan en listas de elementos ordenadas por circuito. Los elementos se aplican por orden a cada paquete RIP de respuesta recibido. Si se da una coincidencia, se realizará la acción especificada en la lista de filtro coincidente (Excluir = se descarta el paquete, Incluir = se recibe el paquete para proceso). Puesto que los paquetes Excluidos se descartan, la información contenida en sus entradas de red, no se entra en las tablas de direccionamientos RIP. Si no se da ninguna coincidencia, se llevará a cabo la acción por omisión del filtro que se haya especificado.

Filtros RIP

El filtro RIP se aplica a las entradas de red de los paquetes RIP de respuesta. Puede utilizarse para controlar a qué distancia se ha diseminado la información de direccionamiento sobre las redes seleccionadas. Como filtro de *entrada*, puede impedir que se *almacene* información de direccionamiento sobre las redes seleccionadas. Esto impide que ***ninguna*** de las otras redes pueda obtener información sobre las redes seleccionadas (al menos, a través de este direccionador).

Los filtros RIP (de entrada) se guardan en listas de elementos ordenadas por circuito. Los elementos se aplican por orden a cada entrada de red de cada paquete RIP de respuesta recibido. Si se da una coincidencia, se realizará la acción especificada en la lista de filtro coincidente (Excluir = no se tendrá en cuenta la entrada de red, Incluir = se procesará la entrada de red). Puesto que las entradas de red Excluidas no se tienen en cuenta, no se entrarán en las tablas de direccionamientos RIP. Si no se da ninguna coincidencia, se llevará a cabo la acción por omisión del filtro que se haya especificado.

Como filtro de *salida*, puede impedir que se *anuncie* (opuesto a que se almacene) la información de direccionamiento sobre las redes seleccionadas. Esto impide que *alguna* (opuesto a todas) red obtenga información sobre las redes seleccionadas (al menos, a través de este direccionador).

Los filtros RIP (de salida) se guardan en listas de elementos ordenadas por circuito. Los elementos se aplican por orden a cada entrada de red de los paquetes RIP de respuesta que se vayan a transmitir. Si se da una coincidencia, se realizará la acción especificada en la lista de filtro coincidente (Excluir = se excluye del paquete la entrada de red, Incluir = se incluye en el paquete la entrada de red). Este filtro no afecta al contenido de las tablas de direccionamientos RIP. Si no se da ninguna coincidencia, se llevará a cabo la acción por omisión del filtro que se haya especificado.

Filtros SAP

El filtro SAP se aplica a las entradas de servidor de todos los paquetes SAP de respuesta. Puede utilizarse para controlar a qué distancia se ha diseminado la información sobre los servicios y puede reducir el tráfico SAP en redes WAN lentas.

Como filtro de *entrada*, puede impedir que se *almacene* información relativa a los servicios sobre los servidores seleccionados. Esto impide que ***ninguna*** de las otras redes pueda obtener información sobre los servidores seleccionados (al menos, a través de este direccionador).

Los filtros SAP (de entrada) se guardan en listas de elementos ordenadas por circuito. Los elementos se aplican por orden a cada entrada de servidor de cada paquete SAP de respuesta recibido. Si se da una coincidencia, se realizará la acción especificada en la lista de filtro coincidente (Excluir = no se tendrá en cuenta la entrada de servidor, Incluir = se procesará la entrada de servidor). Puesto que las entradas de servidor Excluidas no se tienen en cuenta, no se entrarán en las tablas de servicios SAP. Si no se da ninguna coincidencia, se llevará a cabo la acción por omisión del filtro que se haya especificado.

Como filtro de *salida*, puede impedir que se *anuncie* (opuesto a que se almacene) la información de servicios sobre los servidores seleccionados. Esto impide que *algunas* (opuesto a todas) redes obtengan información sobre los servidores seleccionados (al menos, a través de este direccionador).

Los filtros SAP (de salida) se guardan en listas de elementos ordenadas por circuito. Los elementos se aplican por orden a cada entrada de servidor de cada paquete SAP de respuesta que se vaya a transmitir. Si se da una coincidencia, se realizará la acción especificada en la lista de filtro coincidente (Excluir = se excluye en el paquete la entrada de servidor, Incluir = se incluye en el paquete la entrada de servidor). Este filtro no afecta al contenido de la tabla de servicios SAP. Si no se da ninguna coincidencia, se llevará a cabo la acción por omisión del filtro que se haya especificado.

Filtros IPX

El filtro IPX se aplica a la cabecera IPX de los paquetes IPX. Puede utilizarse para controlar a qué distancia podrán comunicarse los servidores y estaciones de trabajo seleccionados con otros servidores y estaciones de trabajo seleccionados, dependiendo de los campos red de origen y de destino, nodo y socket, así como del tipo de protocolo y cuenta de saltos.

Como filtro de *entrada*, una coincidencia que indique que el paquete debe descartarse impide que éste se transmita para ***todos*** los circuitos.

Los filtros IPX (de entrada) se guardan en listas de elementos ordenadas por circuito. Los elementos se aplican por orden a cada paquete IPX recibido. Si se da una coincidencia, se realizará la acción especificada en la lista de filtro coincidente (Excluir = se descarta el paquete, Incluir = se recibe el paquete para proceso o se reenvía). Si no se da ninguna coincidencia, se llevará a cabo la acción por omisión del filtro que se haya especificado.

Como filtro de *salida*, la decisión de reenviar el paquete o no se toma dependiendo del circuito de salida y, por lo tanto, se puede permitir que un paquete recibido sea reenviado a un circuito, pero no a otro.

Los filtros IPX (de salida) se guardan en listas de elementos ordenadas por circuito. Los elementos se aplican por orden a cada paquete IPX que se vaya a transmitir. Si se da una coincidencia, se realizará la acción especificada en la lista de filtro coincidente (Excluir = se descarta el paquete, Incluir = se transmite el

paquete). Si no se da ninguna coincidencia, se llevará a cabo la acción por omisión del filtro que se haya especificado.

Puesto que los filtros IPX se invocan para cada paquete recibido, es recomendable utilizarlos solamente donde es necesario un alto grado de especificidad (es decir, donde no puedan utilizarse los filtros ROUTER, RIP y SAP). En general, los filtros RIP se ocupan de las interredes formadas por ***todas*** las estaciones de un determinado conjunto de redes; los filtros SAP controlan a qué servidores pueden acceder las estaciones de trabajo de la interred; los filtros IPX se ocupan de las interredes formadas por estaciones de trabajo ***individuales*** (o aplicaciones individuales de estaciones de trabajo individuales).

El apartado “Mandatos de configuración de filtros de circuitos IPX” en la página 701 describe con detalle los mandatos utilizados para configurar los filtros IPX de circuitos.

Ajuste de rendimiento de IPX

El direccionador IPX implementa una vía doble para reenviar paquetes, una rápida y otra lenta, para dirigir el tráfico más eficazmente.

La vía rápida reenvía solamente paquetes de datos, y la vía lenta maneja los paquetes de administración, como son los paquetes RIP y SAP. La vía rápida utiliza una antememoria de direcciones que permite que el direccionador reenvíe un paquete rápidamente.

Las búsquedas más lentas en la tabla de direccionamiento se realizan sólo al crear una entrada de la antememoria. La antememoria tiene un mecanismo de verificación de la antigüedad que permite ocuparse inteligentemente de los desbordamientos. Se puede configurar el tamaño de la antememoria mediante el menú de configuración de IPX.

La antememoria de la vía rápida de IPX consta de dos entradas: local y remota. Cada entrada puede manejar las necesidades de cada uno de los tipos de direcciones.

Los mandatos de la antememoria se utilizan para establecer un límite al número máximo de tipos de entradas permitido.

Antememoria local

El tamaño de la antememoria local debe ser igual al número total de clientes de cada red local o cliente del direccionador, más un 10% para prevenir un número excesivo de peticiones de depuración. Utilizando el ejemplo de la Figura 49 en la página 671, el direccionador 5 (Direcc. R5) tiene 9 clientes (C) más el servidor (S), lo que hace un total de 10. Este total:

1. Se multiplica por el 10% (10, en el ejemplo).
2. Se suma este total (1) al total de clientes (para obtener el margen de seguridad).
3. Este nuevo total (11) es el que se utilizará como número de entradas de la antememoria local.

Por ejemplo:

```
IPX config>set local-cache size
New IPX local node cache size [32]? 11
```

Cuando se están utilizando todas las entradas de la antememoria, se eliminarán las entradas menos frecuentemente utilizadas.

Antememoria remota

El tamaño de la antememoria remota debe ser igual al número total de redes remotas utilizadas por el direccionador, más un 10% para prevenir un número excesivo de peticiones de eliminación. En la Figura 49 en la página 671, hay 10 redes IPX que Direcc. R5 puede leer a través de la red IPX 5. Por lo tanto, el número total de clientes de Direcc./R5 es 10. Este total:

1. Se multiplica por el 10% (10, en el ejemplo).
2. Se suma a este total (1) al total de redes remotas (10), para obtener el margen de seguridad.
3. Este nuevo total (11) es el que se utilizará como número de entradas de la antememoria remota.

Por ejemplo:

```
IPX config>set remote-cache size
New IPX remote network cache size [32]? 11
```

Las entradas de la antememoria pueden verse utilizando el mandato se 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
```

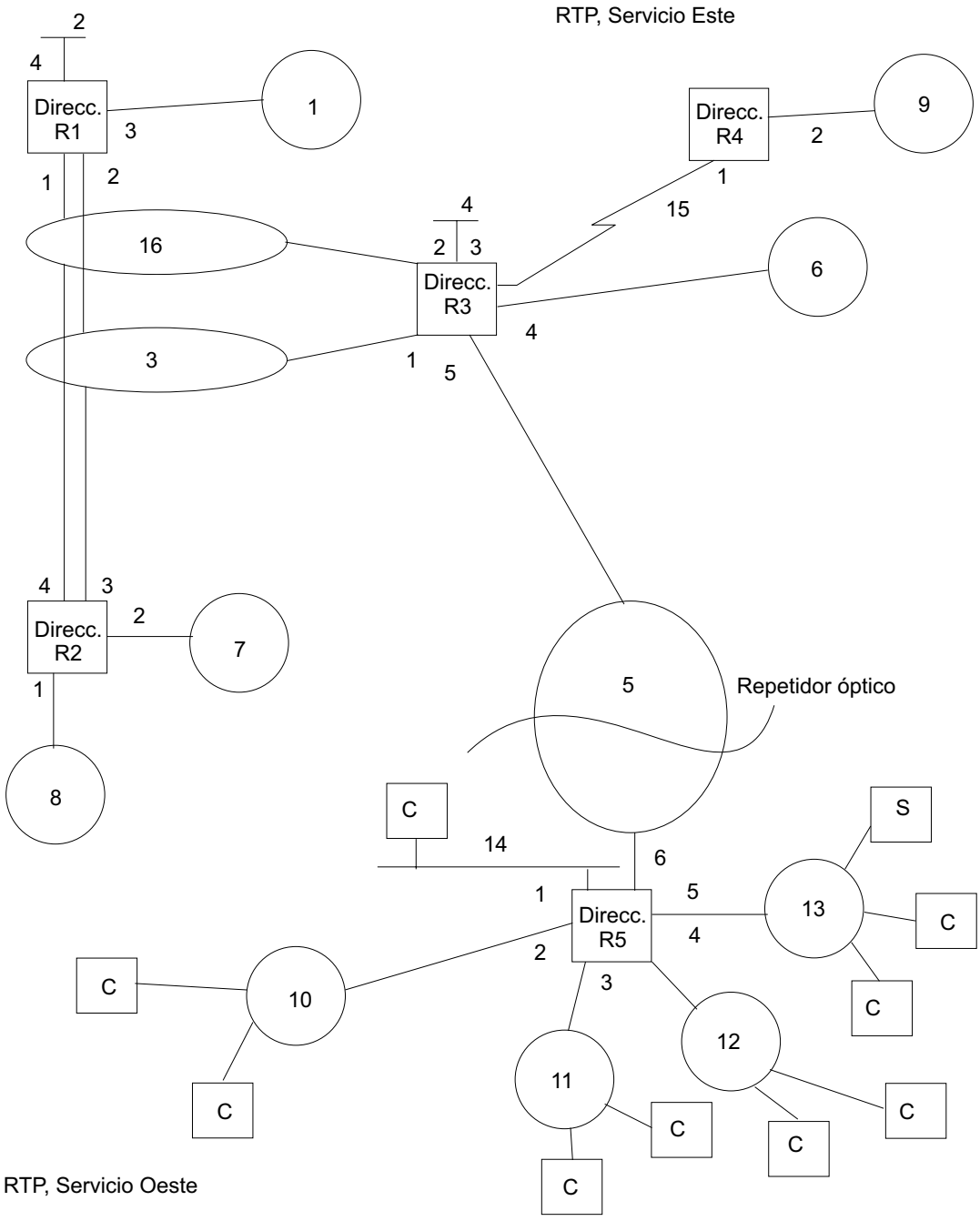


Figura 49. Red IPX de ejemplo

Direccionamiento de horizonte dividido

La función horizonte dividido es un método de direccionamiento que evita la difusión general de actualizaciones RIP y SAP al direccionador del que se averiguaron.

En general, el horizonte dividido debe habilitarse en todos los circuitos para evitar que los paquetes cuenten hasta infinito y los anuncios RIP y SAP innecesarios. Sin embargo, hay algunos casos, en los que puede ser necesario inhabilitar el horizonte dividido, como es el caso de las configuraciones que son parcialmente en malla frame-relay y X.25.

Otro caso en que puede ser necesario inhabilitar el horizonte dividido es la configuración de direccionamiento de IPX parcialmente en malla descrita en el documento RFC 1483.

En una red frame-relay parcialmente en malla, como la que se muestra en la Figura 50, los direccionadores de las ramas no pueden comunicarse unos con otros a menos que el direccionador de las oficinas principales difunda toda la información de direccionamiento a los demás direccionadores. En este caso, el horizonte dividido debe inhabilitarse en el circuito frame-relay de las oficinas principales y habilitarse en cada una de las ramas, para evitar que generen tráfico innecesario.

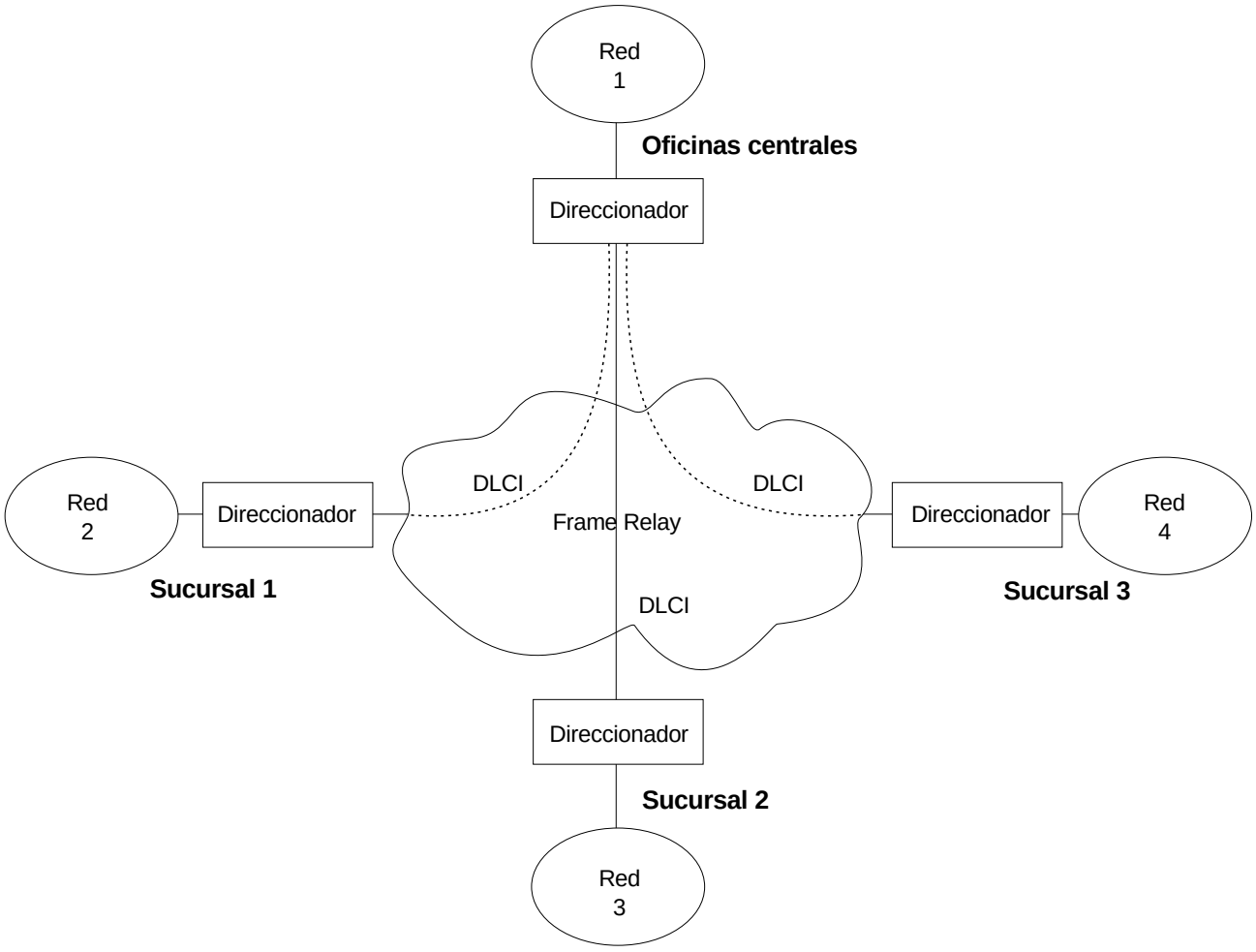


Figura 50. Red Frame-Relay parcialmente en malla

Si tuviera que cambiar el valor del horizonte dividido, utilice el mandato **set split-horizon**:

```
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

En este capítulo se describe cómo configurar el protocolo IPX y cómo utilizar los mandatos de supervisión de IPX. Incluye las secciones siguientes:

Acceso al entorno de configuración de IPX

Para acceder al entorno de configuración de IPX, escriba el mandato siguiente en el indicador `Config>`:

```
Config> protocol IPX
IPX Protocol user configuration
IPX Config>
```

Mandatos de configuración de IPX

En este apartado se trata de los mandatos de configuración de IPX. En la Tabla 39 en la página 674 se listan los mandatos de configuración de IPX. Estos mandatos especifican los parámetros de red para los direccionadores que transmitan paquetes IPX. Los mandatos se entran en el indicador `IPX config>`. Para activar las modificaciones que se realicen en la configuración, reinicie el direccionador.

Tabla 39. 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 de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Add	Añade un circuito IPX de difusión general o IPXWAN punto a punto, añade filtros IPX globales (controles de acceso), filtros SAP globales, y rutas o servicios estáticos.
Delete	Suprime un circuito IPX de difusión general o IPXWAN punto a punto, suprime filtros IPX globales (controles de acceso), filtros SAP globales y rutas o servicios estáticos.
Disable/Enable	Habilita o inhabilita IPX globalmente o, habilita o inhabilita globalmente la utilización de rutas o servicios IPX estáticos para circuitos IPX concretos. Habilita o inhabilita el filtrado de paquetes Keepalive, el avance de difusión RIP-SAP, la respuesta a la petición SAP de obtener el servidor más próximo, las difusiones NetBIOS, y habilita o inhabilita RIP o SAP para circuitos determinados.
Filter-lists	Accede a la configuración de filtros de circuitos IPX. En este entorno es donde se configuran los filtros de circuitos IPX: ROUTER, RIP, SAP e IPX.
Frame	
List	Muestra la configuración actual del protocolo IPX.
Move	Vuelve a ordenar los elementos de filtro IPX globales (controles de acceso), o traslada un circuito IPX de una interfaz a otra.
Set	Establece el número de sistema principal, el nombre e ID de nodo del direccionador IPXWAN, el tipo de direccionamiento IPXWAN, el tiempo de espera de la conexión y el temporizador de reintentos, los números de red IPX, los tamaños máximos de las tablas RIP y SAP, los tamaños de las antememorias local y remota, los estados de los filtros IPX globales (controles de acceso) y de los filtros SAP globales, los tamaños de antememoria, los intervalos de actualización RIP y SAP, el coste del circuito RIP (ciclos RIP), el tamaño de la tabla de filtros Keepalive y la utilización del horizonte dividido.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Add

Utilice el mandato **add** para añadir a la configuración de IPX un filtro IPX global (controles de acceso), un circuito IPX de difusión general, un filtro SAP global, un circuito IPX punto a punto, o una ruta o servicio estáticos.

Sintaxis:

add access-control . . .
broadcast-circuit . . .
filter . . .
ipxwan-circuit . . .
route-static . . .
sap-static . . .

access-control *tipo red-dest sist-pral-dest rango-sockets-dest red-orig sist-pral-orig rango-sockets-orig*

Determina si se debe pasar un paquete al nivel IPX. Los controles de acceso de IPX proporcionan al protocolo IPX una función global de control de acceso en el nivel de paquetes de IPX. La lista de controles de acceso es un conjunto de entradas ordenadas, que el direccionador utiliza para filtrar paquetes. Cada entrada puede ser del tipo Incluyente o Excluyente. Cada entrada consta de números de red de origen y de destino, de direcciones de sistema principal y de un rango de sockets.

Cuando el protocolo IPX recibe un paquete proveniente de una red, y el control de acceso está habilitado, se comprueba con la lista de controles de acceso. Se compara su red, dirección y socket con sus iguales de la lista, hasta que se da una coincidencia. Si se da una coincidencia y la entrada es del tipo Incluyente, se procede a la recepción del paquete (y posiblemente a su reenvío). Si la entrada coincidente es del tipo Excluyente, el paquete se descarta. Si no se da ninguna coincidencia, el paquete también se descarta.

Después de crear una lista de controles de 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 de acceso.

Nota: Los controles de acceso se aplican a todos los paquetes recibidos. Si no se habilita la recepción de paquetes RIP (socket 453, en hexadecimal) o SAP (socket 452, en hexadecimal), el reenviador no estará operativo.

```
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

Muestra si los paquetes se envían o se descartan para una dirección determinada o para un conjunto de direcciones. Entre I para incluirlos. Esto hace que el direccionador reciba el paquete y que lo reenvíe, si cumple los criterios que se especifican en los argumentos restantes. Entre E para excluirlos. Esto hace que el direccionador descarte los paquetes.

Red-dest

Número de red del destino. Escriba el número de red, en hexadecimal.

Valores válidos: de X'00000000' a X'FFFFFFFF'

Un cero (0) especifica todas las redes.

Valor por omisión: 0

Sist-pral-dest

Número del sistema principal de la red de destino. Escriba el número de sistema principal, en hexadecimal.

Valores válidos: de X'000000000000' a X'FFFFFFFFFFFF'

Un cero (0) especifica todos los sistemas principales de la red.

Valor por omisión: Ninguno

Rango-sockets-dest
Dos números que denotan un rango inclusivo de sockets de destino. El valor del socket de destino se utiliza para filtrar paquetes IPX.

Valores válidos: de X'0000' a X'FFFF'

Valor por omisión: 0

Red-orig
Número de red del origen. Escriba el número de red, en hexadecimal.

Este parámetro define el número de la red IPX de origen cuyos paquetes filtra este direccionador.

Si quiere que los filtros se basen *únicamente* en el valor de la red de origen, el filtro se aplicará a todos los sockets de origen, redes de origen, tipos de paquetes y número de saltos.

Valores válidos: de X'00000000' a X'FFFFFFFF'

Un cero (0) especifica todas las redes.

Valor por omisión: 0

Sist-pral-orig
Número de sistema principal de la red de origen. Escriba el número de sistema principal, en hexadecimal.

Valores válidos: de X'000000000000' a X'FFFFFFFFFFFF'

Un cero (0) especifica todos los sistemas principales de la red.

Valor por omisión: Ninguno

Rango-sockets-orig
Dos números que denotan un rango inclusivo de sockets de origen.

Valores válidos: de X'0000' a X'FFFF'

Valor por omisión: 0

Nota: No es necesario utilizar los controles de acceso ni los filtros SAP para que IPX funcione en un entorno NetWare. Utilícelos sólo en caso necesario.

Ejemplo: `add access-control E 201 1 451 451 329 0 0 FFFF`

Este control de acceso impide que 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 IPX de difusión general.

núm-interfaz
Especifica la interfaz de red para la que está configurado el número de circuito IPX.

Valores válidos: cualquier número de interfaz de red válido

Valor por omisión: 0

núm-circuito-ipx
Especifica el número de circuito IPX. Este número debe ser diferente para cada uno de los circuitos IPX configurados en el direccionador y se utiliza en muchos de los mandatos de configuración para hacer referencia a los circuitos IPX.

Valores válidos: de 1 a 65.535

Valor por omisión: el siguiente número de circuito IPX disponible

núm-red
Especifica el número de red IPX que se utilizará para el circuito IPX. El número de red IPX 0 sólo es válido en RIP o circuitos de direccionamiento estático no numerados 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: de 1 a 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*
Evita el desbordamiento de bindery en NetWare para los usuarios de grandes redes, al permitir que el usuario determine cuál es el número de saltos razonable para un servicio dado. Los filtros SAP de IPX permiten configurar el protocolo para que no tenga en cuenta ciertas entradas de los anuncios SAP. Esto se hace para limitar el tamaño de la base de datos SAP. Esto puede ser necesario debido a limitaciones de tamaño en versiones anteriores de los servidores de archivos de NetWare. También puede ser necesario limitar la cantidad de datos SAP enviados a través de enlaces WAN.

Los filtros SAP consisten en una lista global ordenada de entradas de filtros. Cada entrada de filtro consta de una cuenta de saltos máxima, un tipo de servicio y un nombre de servicio opcional. Cuando se recibe un paquete de respuesta SAP, las entradas SAP se comparan con las de la lista de filtro. Si la entrada SAP coincide con una entrada de la lista de filtro y si su número de saltos es mayor que el especificado, no se tiene en cuenta y no se entra en la base de datos SAP. Si la entrada SAP coincide con una entrada de la lista de filtro y si su número de saltos es menor o igual que el especificado, se acepta y se entra en la base de datos SAP. Si no coincide con ninguna entrada, la entrada SAP se acepta. Los argumentos de este mandato son los siguientes:

Saltos
Número máximo de saltos permitidos por el servicio.

Valores válidos: Entero comprendido entre 0 y 16.

Valor por omisión: 1

Tipo-servicio
Valor numérico que representa la clase de servicio.

Valores válidos: Valor hexadecimal comprendido entre X'0000' y X'FFFF'.

Utilice el valor X'0000' para filtrar todos los servicios.

Valor por omisión: 4

Se puede ver una lista de tipos de servicios escribiendo el mandato **slist** en el indicador IPX>.

Nombre-servicio
Identifica el nombre del servidor. Normalmente, este campo no se suele entrar.

Valores válidos: Una serie de 1 a 47 caracteres ASCII (de X'20' a X'7E').

Valor por omisión: ninguno

Ejemplo: `add filter 2 039B NOTES-CHICAGO`

En este ejemplo no se tienen en cuenta los anuncios SAP para el servidor Lotus Notes “NOTES-CHICAGO” con más de 2 saltos.

circuito-ipxwan *núm-interfaz núm-circuito-ipx núm-red [utilizar-PVC] [núm-circ-FR]*
Añade un circuito IPXWAN punto a punto.

núm-interfaz
Especifica una interfaz PPP o Frame Relay ya existente para la que debe configurarse el circuito IPX.

Valores válidos: cualquier número de interfaz de red válido

Valor por omisión: 0

núm-circuito-ipx
Especifica el número de circuito IPX. Este número debe ser diferente para cada uno de los circuitos IPX configurados en el direccionador y se utiliza en muchos de los mandatos de configuración para hacer referencia a los circuitos IPX.

Valores válidos: de 1 a 65.535

Valor por omisión: el siguiente número de circuito IPX disponible

núm-red
Especifica el número de red IPX que se utilizará para el circuito IPX. El número de red IPX 0 sólo es válido en RIP o circuitos de direccionamiento estático no numerados 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: de 0 a FFFFFFFD

Valor por omisión: 1

utilizar-PVC

Este parámetro sólo es necesario si se va a configurar el circuito IPXWAN para una interfaz Frame Relay. Especifica si el circuito IPXWAN va a configurarse para un circuito virtual permanente o conmutado Frame Relay. Si se responde a la solicitud afirmativamente significa que el circuito IPXWAN se configurará para un PVC. 'No' significa que el circuito IPX se configurará para un SVC.

Valores válidos: Yes o No

Valor por omisión: Yes

núm-circ-FR

Este parámetro sólo es necesario si se va a configurar el circuito para Frame Relay. Si el circuito IPXWAN que se va a configurar es un circuito virtual permanente Frame Relay, el parámetro especifica el número de circuito PVC Frame Relay. Si el circuito IPXWAN que se va a configurar es un circuito virtual conmutado 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 válidos

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 ? Cartagena
```

route-static *red-dest núm-circuito-ipx salto-siguiente ciclos saltos*

Añade una ruta estática.

red-dest

Especifica el número de la red IPX de destino.

Valores válidos: de X'1' a X'FFFFFFFE'

Valor por omisión: 1

núm-circuito-ipx

Especifica un circuito IPX ya existente para el que debe configurarse la ruta estática.

Valores válidos: un número de circuito IPX ya existente

Valor por omisión: 1

salto-siguiente

Especifica el número de sistema principal IPX del direccionador de salto siguiente desde el que se puede llegar a la red de destino.

Valores válidos: de X'1' a X'FFFFFFFFFFFE'

Valor por omisión: ninguno

ciclos
Indica el número de ciclos entre la red de destino y su direccionador. El número de ciclos representa el tiempo que se tarda en transmitir un paquete IPX de 576 bytes desde este direccionador hasta la red de destino. Un ciclo son 55 milisegundos.

Valores válidos: de 0 a 30.000

Valor por omisión: 0

saltos
Indica el número de saltos entre la red de destino y su direccionador.

Valores válidos: de 0 a 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 *tipo-servicio nombre-servicio núm-circuito-ipx red-servidor nodo-servidor socket-servidor saltos*
Añade un servicio SAP estático.

tipo-servicio
Especifica la clase de servicio, en hexadecimal.

Valores válidos: de X'0' a X'FFFF'

Valor por omisión: 4

nombre-servicio
Especifica el nombre ASCII del servicio.

Valores válidos: hasta 47 de los caracteres ASCII siguientes: 'A'–'Z', 'a'–'z', '0'–'9', '_', '-', '@'.

Valor por omisión: Ninguno

núm-circuito-ipx
Especifica un circuito IPX ya existente para el que debe configurarse el servicio SAP estático.

Valores válidos: un número de circuito IPX ya existente

Valor por omisión: 1

red-servidor
Especifica el número de red IPX interna o el número de red IPX inicial del servidor.

Valores válidos: de X'1' a X'FFFFFFFE'

Valor por omisión: 1

nodo-servidor
Especifica el nodo IPX del servidor.

Valores válidos: de X'1' a X'FFFFFFFFFFFE'

Valor por omisión: Ninguno

socket-servidor
Especifica el número de socket del servidor.

Valores válidos: de X'0' a X'FFFF'

Valor por omisión: 451

saltos
Indica el número de saltos entre el servidor y este direccionador.

Valores válidos: de 0 a 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 IPX de difusión general o IPXWAN punto a punto, un filtro IPX global (controles de acceso), un filtro SAP global, o una ruta o servicio estáticos.

Sintaxis:

delete access-control . . .
circuit . . .
filter . . .
route-static . . .
sap-static . . .

access-control *núm-línea*
Suprime el control de acceso que coincide con el número de línea entrado. Escriba el mandato **list** para ver los números de línea actuales.

Ejemplo: `delete access-control 2`

circuit *núm-circuito-ipx*
Suprime el circuito IPX de difusión general o el circuito IPXWAN punto a punto. También suprimirá todas las rutas y los servicios estáticos, y los filtros de circuitos asociados 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 SAP especificado. El nombre del filtro SAP debe escribirse exactamente igual a como aparece cuando se ejecuta el mandato list. A continuación se describen los argumentos:

Saltos

Número máximo de saltos permitidos por el servicio.

Valores válidos: de 0 a 16

Valor por omisión: 16

Tipo-servicio

Valor numérico que representa la clase de servicio. Escriba un número hexadecimal de 2 bytes.

Valores válidos: de X'0000' a X'FFFF'

Valor por omisión: Ninguno

Nombre-servicio

Si la entrada que se va a suprimir tiene un nombre, especifique el nombre.

Valores válidos: Una serie de 1 a 47 caracteres ASCII (de X'20' a X'7E').

Valor por omisión: Ninguno

Ejemplo: `delete filter 2 039B NOTES-CHICAGO`

route-static *red-dest núm-circuito-ipx salto-siguiente*

Suprime una ruta estática.

red-dest

Especifica el número de la red IPX de destino.

Valores válidos: de X'1' a X'FFFFFFFE'

Valor por omisión: 1

núm-circuito-ipx

Especifica el circuito IPX para el que se está configurando la ruta estática.

Valores válidos: un número de circuito IPX ya existente

Valor por omisión: 1

salto-siguiente

Especifica el número de sistema principal IPX del direccionador de saltos siguiente desde el que puede accederse a la red de destino.

Valores válidos: de X'1' a 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 *tipo-servicio nombre-servicio núm-circuito-ipx*
Suprime un servicio SAP estático.

tipo-servicio
Especifica la clase de servicio, en hexadecimal.

Valores válidos: de X'0' a X'FFFF'

Valor por omisión: 4

nombre-servicio
Especifica el nombre ASCII del servicio.

Valores válidos: hasta 47 de los caracteres ASCII siguientes: 'A'–'Z', 'a'–'z', '0'–'9', '_', '-', '@'.

Valor por omisión: Ninguno

núm-circuito-ipx
Especifica el circuito IPX para el que se está configurando el servicio SAP estático.

Valores válidos: un número de circuito ipx ya existente

Valor por omisión: 1

Ejemplo:

```
delete sap-static
Sap type: (0-ffff) [4]?
Sap name: (0-ffff) []? srvarch1
IPX circuit number [1]? 2
```

Disable

Utilice el mandato **disable** para inhabilitar IPX globalmente o, para inhabilitar globalmente la utilización de rutas y servicios IPX estáticos para circuitos IPX concretos. También se puede utilizar el mandato **disable** para inhabilitar las respuestas a la petición SAP de obtener el servidor más próximo, el avance de difusión RIP-SAP, o para inhabilitar RIP o SAP para circuitos determinados.

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 IPX de difusión general o el circuito IPXWAN punto a punto especificados por el *núm-circuito-ipx*.

Ejemplo: `disable circuit`

```
IPX circuit number [1]? 2
```

ipx Inhabilita globalmente el protocolo IPX.

Ejemplo: `disable ipx`

keepalive-filtering *núm-circuito-ipx*
Inhabilita el filtrado Keepalive para el circuito IPX de difusión general o IPXWAN punto a punto especificados por el *núm-circuito-ipx*.

Ejemplo: `disable keepalive-filtering`

```
IPX circuit number [1]? 2
```

netbios-broadcast *núm-circuito-ipx*
Inhabilita la recepción y envío de difusiones NetBIOS de Novell (paquetes de tipo 20) para el circuito IPX especificado por el *núm-circuito-ipx*. El valor por omisión es que esté habilitada. La recepción y envío de difusiones NetBIOS de Novell se inhabilita automáticamente para los circuitos IPXWAN de direccionamiento estático, incluso aunque la característica esté habilitada 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 de obtener el servidor más próximo para el circuito IPX de difusión general o IPXWAN punto a punto especificados por el *núm-circuito-ipx*.

Nota: Esta característica debe inhabilitarse con mucha precaución. Este mandato debe utilizarse solamente cuando una red IPX disponga de varios direccionadores (o servidores) y se sepa que el "mejor" servidor no está tras este direccionador.

Ejemplo: `disable reply-to-get-nearest`

```
IPX circuit number [1]? 2
```

rip *núm-circuito-ipx*
Inhabilita RIP para el circuito IPX de difusión general o IPXWAN punto a punto especificados por el *núm-circuito-ipx*. El valor por omisión es que RIP esté habilitado para todos los circuitos. RIP se inhabilitará automáticamente para los circuitos IPXWAN que utilicen el direccionamiento estático, incluso aunque esté habilitado en la configuración.

Ejemplo: `disable rip 1`

rip-sap-pacing *núm-circuito-ipx*
Impide el avance de difusión RIP/SAP para el circuito IPX de difusión general o IPXWAN punto a punto especificados por el *núm-circuito-ipx*. Cuando el avance está inhabilitado, las difusiones RIP y SAP periódicas se transmiten para el circuito con un intervalo entre paquetes de 55 milisegundos (el valor por omisión). Habilite el avance solamente para los circuitos en que las difusiones RIP y SAP pueden causar congestión (por ejemplo, se puede habilitar el avance para circuitos frame-relay o X.25 con muchos circuitos virtuales).

Ejemplo: `disable rip-sap-pacing`

```
IPX circuit number [1]? 2
```

route-static
Inhabilita globalmente la utilización de rutas estáticas.

Ejemplo: `disable route-static`

sap *núm-circuito-ipx*

Inhabilita SAP para el circuito IPX de difusión general o IPXWAN punto a punto especificados por el *núm-circuito-ipx*. El valor por omisión es que SAP esté habilitado para todos los circuitos. SAP se inhabilitará automáticamente para los circuitos RLAN e IPXWAN de direccionamiento estático, incluso aunque esté habilitada en la configuración.

Ejemplo: `disable sap`

```
IPX circuit number [1]? 2
```

sap-static

Inhabilita globalmente la utilización de servicios estáticos.

Ejemplo: `disable sap-static`

Enable

Utilice el mandato **enable** para habilitar IPX globalmente o para circuitos concretos. El mandato enable también puede utilizarse para habilitar globalmente la utilización de rutas o servicios IPX estáticos, o para habilitar el filtrado de paquetes Keepalive, el avance de difusión RIP-SAP, la respuesta a la petición SAP de obtener el servidor más próximo, y RIP o SAP para circuitos determinados.

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 los circuitos IPX de difusión general o IPXWAN punto a punto especificados por el *núm-circuito-ipx* y especifica el número de red IPX para el circuito IPX. El circuito IPX se habilitará si se ha configurado 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 IPX de difusión general o IPXWAN punto a punto que se va a habilitar.

Valores válidos: cualquier número de circuito ipx que sea válido

Valor por omisión: 0

núm-red

Especifica la red IPX que se utilizará para el circuito. El número de red IPX 0 sólo es válido en RIP o circuitos de direccionamiento estático no numerados 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: de X'0' a X'FFFFFFFD'

Valor por omisión: 1

Ejemplo:

ipx Habilita globalmente el protocolo IPX.

Ejemplo: **`enable ipx`**

keepalive-filtering *núm-circuito-ipx*
Habilita el filtrado Keepalive para el circuito IPX de difusión general o IPXWAN punto a punto especificados por el *núm-circuito-ipx*.

Ejemplo: **`enable keepalive-filtering`**

```
IPX circuit number [1]? 2
```

netbios-broadcast *núm-circuito-ipx*
Habilita la recepción y envío de difusiones NetBIOS de Novell (paquetes de tipo 20) para el circuito IPX especificado por el *núm-circuito-ipx*. El valor por omisión es que esté habilitada. La recepción y envío de difusiones NetBIOS de Novell se inhabilita automáticamente para los circuitos IPXWAN de direccionamiento estático, incluso aunque la característica esté habilitada en la configuración.

Ejemplo: **`enable netbios-broadcast`**

```
IPX circuit number [1]? 2
```

reply-to-get-nearest-server *núm-circuito-ipx*
Habilita el direccionador para que responda a las peticiones SAP de obtener el servidor más próximo para el circuito IPX de difusión general o IPXWAN punto a punto especificados por el *núm-circuito-ipx*.

Ejemplo: **`enable reply-to-get-nearest`**

```
IPX circuit number [1]? 2
```

rip *núm-circuito-ipx*
Habilita RIP para el circuito IPX de difusión general o IPXWAN punto a punto especificados por el *núm-circuito-ipx*. El valor por omisión es que RIP esté habilitado para todos los circuitos IPX. RIP se inhabilitará automáticamente para los circuitos RLAN e IPXWAN de direccionamiento estático, incluso si en la configuración está habilitado.

Ejemplo: **`enable rip`**

```
IPX circuit number [1]? 2
```

rip-sap-pacing *núm-circuito-ipx*
Habilita el avance de difusión RIP/SAP para el circuito IPX de difusión general o IPXWAN punto a punto especificados por el *núm-circuito-ipx*.

Nota: El direccionador calcula un intervalo entre paquetes que garantiza que la difusión se lleve a cabo dentro de los intervalos de actualización RIP y SAP configurados. Puede que sea necesario configurar estos intervalos con valores mayores, para que el direccionador calcule un intervalo entre paquetes lo suficientemente grande.

El avance debe habilitarse solamente para los circuitos en que las difusiones RIP y SAP pueden causar congestión (por ejemplo, para circuitos frame-relay o X.25 con muchos circuitos virtuales).

Ejemplo: `enable rip-sap-pacing`

```
IPX circuit number [1]? 2
```

route-static
Habilita globalmente la utilización de rutas estáticas.

Ejemplo: `enable route-static`

sap *núm-circuito-ipx*
Habilita SAP para el circuito IPX de difusión general o IPXWAN punto a punto especificados por el *núm-circuito-ipx*.

Ejemplo: `enable sap`

sap-static
Habilita globalmente la utilización de servicios estáticos.

Ejemplo: `enable sap-static`

Filter-lists

Utilice el mandato **filter-lists** para acceder al indicador `IPX` *`tipo-filtro`*`-List Config>`. Los tipos de listas de filtro válidas son router, rip, sap e ipx.

Para obtener más información sobre los mandatos disponibles desde el indicador `IPX` *`tipo-filtro`*`-List Config>`, consulte “Mandatos de configuración de filtros de circuitos IPX” en la página 701.

Sintaxis:

filter-lists router-lists
rip-lists
sap-lists
ipx-lists

Ejemplo: `filter-lists router-lists`

Frame

Utilice el mandato **frame** para especificar el formato de paquete para los circuitos IPX (también puede establecerse la encapsulación utilizando el mandato **network** de CONFIG).

Nota: Cuando los registros de configuración no son correctos o no son válidos, se utilizarán los valores de trama por omisión.

Sintaxis:

frame ethernet_II . . .
ethernet_8022 . . .
ethernet_8023 . . .
ethernet_SNAP . . .
token-ring MSB . . .
token-ring LSB . . .
token-ring_SNAP MSB . . .
token-ring_SNAP LSB . . .

ethernet_II *núm-circuito-ipx*

Establece el tipo de trama como ethernet_II para el circuito IPX de difusión general especificado por el *núm-circuito-ipx*. La encapsulación ethernet_II utiliza la versión 2.0 de ethernet, con el tipo de protocolo 8137. Este es el valor por omisión a partir de la versión 4.0 de NetWare.

Ejemplo: `frame ethernet_II`

```
IPX circuit number [1]?
```

ethernet_8022 *núm-circuito-ipx*

Establece el tipo de trama como ethernet_8022 para el circuito IPX de difusión general especificado por el *núm-circuito-ipx*. La encapsulación ethernet_8022 utiliza la encapsulación 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 para el circuito IPX de difusión general especificado por el *núm-circuito-ipx*. La encapsulación ethernet_8023 utiliza la encapsulación ethernet 802.3 sin cabecera LLC. Este era el valor por omisión antes de la versión 4.0 de NetWare. También es el 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 para el circuito IPX de difusión general especificado por el *núm-circuito-ipx*. La encapsulación ethernet_SNAP utiliza la encapsulación SNAP con PID 0000008137.

Ejemplo: `frame ethernet_SNAP`

```
IPX circuit number [1]?
```

token-ring MSB *núm-circuito-ipx*

Establece el tipo de trama como token-ring MSB para el circuito IPX de difusión general especificado por el *núm-circuito-ipx*. La encapsulación token-ring MSB utiliza la encapsulación LLC con SAP E0, y utiliza direcciones MAC no canónicas. Este es el valor por omisión de NetWare. También es el 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 token-ring LSB para el circuito IPX de difusión general especificada por el *núm-circuito-ipx*. La encapsulación token-ring LSB utiliza la encapsulación LLC con SAP E0, y utiliza direcciones 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 token-ring_SNAP MSB para el circuito IPX de difusión general especificado por el *núm-circuito-ipx*. La encapsulación token-ring_SNAP MSB utiliza la encapsulación SNAP con PID 0000008137, y utiliza direcciones 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 token-ring LSB para el circuito IPX de difusión general especificada por el *núm-circuito-ipx*. La encapsulación token-ring LSB utiliza la encapsulación SNAP con PID 0000008137 y utiliza direcciones MAC no canónicas.

List

Utilice el mandato **list** para visualizar la configuración de IPX actual.

Sintaxis:

list access-controls
all
circuit
filters
route-static
sap-static
summary

access-controls
Lista los filtros IPX globales (controles de acceso). Este mandato muestra la información que se puede ver en la sección “Access Control Configuration” del ejemplo 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: Cartagena



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    SRVARCH01                       ABC      000000000001 451  3    3      2

SAP Filter Configuration:
-------------------------
IPX SAP Filters:  Enabled
Index Max Hops  Type  Service Name
1     5         4     SRVARCH02

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 IPX de difusión general o IPXWAN punto a punto especificado por el *núm-circuito-ipx*. Este mandato muestra la información que se puede ver en las secciones “IPX Configuration”, “RIP Configuration”, “SAP Configuration” e “IPXWAN Configuration” del ejemplo del mandato **list all**.

filters Lista los filtros SAP globales. Este mandato muestra la información que se puede ver en la sección “SAP Filter Configuration” del ejemplo del mandato **list all**.

route-static

Lista las rutas estáticas. Este mandato muestra la información que puede verse en la sección “Static Route Configuration” del ejemplo del mandato **list all**.

sap-static

Lista los servicios estáticos. Este mandato muestra la información que puede verse en la sección “Static Services Configuration” del ejemplo del mandato **list all**.

summary Lista un resumen de la configuración de IPX, RIP, SAP, IPXWAN, y del filtrado Keepalive, para todos los circuitos para los que está habilitado IPX. Este mandato muestra la información que se puede ver en las secciones “IPX Globals”, “IPX Configuration”, “RIP Configuration”, “SAP Configuration” e “IPXWAN Configuration” del ejemplo del mandato **list all**.

IPX Globals

Se muestra la información global siguiente:

- Si IPX está habilitado o inhabilitado globalmente
- Número de sistema principal IPX
- Número máximo de servicios
- Número máximo de redes
- Número máximo de rutas
- Número máximo de rutas por cada destino
- Número máximo de entradas de la antememoria local
- Número máximo de entradas de la antememoria remota
- Tamaño de la tabla de filtros Keepalive

IPX Configuration

Se muestra la información siguiente para cada circuito para el que esté habilitado IPX:

- Número de circuito IPX
- Número de interfaz de red
- Número de red IPX (Netnum)
- Si IPX está habilitado o inhabilitado para el circuito
- Si la difusión NetBIOS está habilitada o inhabilitada para el circuito
- Si el filtrado Keepalive está habilitado o inhabilitado para el circuito
- Encapsulación

PVC circuit number

Muestra el número del circuito PVC Frame Relay.

SVC circuit name
Muestra el nombre del circuito SVC Frame Relay.

RIP Configuration
Se muestra la información siguiente para cada circuito para el que esté habilitado IPX:

- Número de circuito IPX
- Número de interfaz de red
- Número de red IPX (Netnum)
- Si RIP está habilitado o inhabilitado
- Temporizador del intervalo de actualización RIP
- Si el horizonte dividido está habilitado o inhabilitado
- Si el avance de difusión RIP está habilitado o inhabilitado
- Coste de la ruta IPX (en ciclos)

SAP Configuration
Se muestra la información siguiente para cada circuito para el que esté habilitado IPX:

- Número de circuito IPX
- Número de interfaz de red
- Número de red IPX (Netnum)
- Si SAP está habilitado o inhabilitado
- Temporizador del intervalo de actualización SAP
- Si el horizonte dividido está habilitado o inhabilitado
- Si el avance de difusión SAP está habilitado o inhabilitado
- Si está habilitada la respuesta a la petición SAP de obtener el servidor más próximo.

IPXWAN Configuration
Se muestra la información global siguiente:

- Nombre del direccionador
- ID de nodo del direccionador

Se muestra la siguiente información para cada circuito IPXWAN:

- Número de circuito IPX
- Número de interfaz de red
- Número de red IPX (Netnum)
- Tipo de direccionamiento
- Temporizador de conexión
- Temporizador de reintentos

Static Routes Configuration
Muestra si las rutas estáticas están habilitadas o inhabilitadas globalmente. Además, se muestra la información siguiente para cada ruta estática configurada.

- Número de red IPX de destino
- Saltos
- Ciclos
- Dirección de nodo del salto siguiente
- Número de circuito IPX
- Número de interfaz de red

Static Services Configuration

Muestra si los servicios estáticos están habilitados o inhabilitados globalmente. Además, se muestra la información siguiente para cada servicio estático configurado.

- Tipo de servicio
- Nombre de servicio
- Número de red IPX del servicio
- Dirección de nodo IPX del servicio (sistema principal)
- Socket
- Saltos
- Número de circuito IPX
- Número de interfaz de red

SAP Filter Configuration

Muestra si los filtros SAP globales están habilitados o inhabilitados. Además, se muestra la información siguiente para cada filtro SAP global configurado.

- Índice
- Número máximo de saltos
- Tipo de servicio
- Nombre de servicio

Access Control Configuration

Muestra si los filtros IPX globales (controles de acceso) están habilitados o inhabilitados. Además, se muestra la información siguiente para cada filtro IPX global configurado (control de acceso).

- Índice del control de acceso (#)
- Tipo de filtro (de inclusión o de exclusión)
- Número de red IPX de destino
- Número de nodo IPX de destino (sistema principal)
- Rango de sockets IPX de destino
- Número de red IPX de origen
- Número de nodo IPX de origen (sistema principal)
- Rango de sockets IPX de origen

Move

Utilice el mandato **move** para volver a ordenar los elementos de filtro IPX (controles de acceso) o para trasladar un circuito IPX de una interfaz a otra.

Sintaxis:

m**ove** a**ccess-control** *núm-línea-orig núm-línea-dest*
c**ircuit** *núm-circuito-ipx núm-interfaz [utilizar-PVC]]núm-circ-FR]*

access-control *núm-línea-orig núm-línea-dest*

núm-línea-orig
Especifica el número de línea del control de acceso que se quiere cambiar de orden.

núm-línea-dest
Especifica el número de línea del control de acceso tras la que se colocará la línea de origen.

Las líneas siguientes a la línea a la que se ha movido el control de acceso, se volverán 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 [utilizar-PVC núm-circ-FR]*

Traslada un circuito IPX de una interfaz de red a otra. Este mandato también traslada todas las rutas y servicios estáticas, y los filtros de circuitos IPX asociados con el *núm-circuito-ipx* asociado, al mismo *núm-interfaz*. Si se va a trasladar un circuito IPXWAN a una interfaz Frame Relay, se le solicitará que especifique si el circuito nuevo es un circuito PVC o SVC Frame Relay, y que proporcione el número o el nombre del circuito Frame Relay, según corresponda.

núm-circuito-ipx

Especifica el circuito IPX que se va a trasladar.

Valores válidos: un número de circuito IPX ya existente

Valor por omisión: 1

núm-interfaz

Especifica la interfaz de red a la que se va a trasladar el circuito.

Valores válidos: un número de interfaz de red ya existente.

Valor por omisión: 0

utilizar-PVC

Especifica si el circuito IPXWAN va a trasladarse a un circuito PVC o SVC Frame Relay. Si la solicitud se responde afirmativamente significa que el circuito IPXWAN se va a trasladar a un circuito PVC. 'No' significa que el circuito IPXWAN se va a trasladar a un circuito 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 ya existentes.

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 nombre e ID de nodo del direccionador IPXWAN, el tipo de direccionamiento IPXWAN, el tiempo de espera de la conexión y el temporizador de reintentos, los números de red IPX, los tamaños máximos de las tablas RIP y SAP, los tamaños de las antememorias local y remota, los estados de los filtros IPX globales (control de acceso) y de los filtros SAP globales, los intervalos de actualización RIP y SAP, el coste de la ruta IPX (en ciclos), el tamaño de la tabla de filtros Keepalive y la utilización del horizonte dividido.

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 IPX globales (controles de acceso). Escriba **on** u **off**.

Ejemplo: `set access-control on`

filter *on* **u** *off*

Activa o desactiva los filtros SAP globales. Escriba **on** u **off**.

Ejemplo: `set filter on`

host-number *núm-sist-pral*

Especifica el número de sistema principal utilizado por los circuitos serie que ejecutan IPX. Cada direccionador IPX que opera con circuitos serie debe tener un número diferente de sistema principal. Esto es necesario ya que los circuitos serie no tienen direcciones de nodo hardware a partir de las que crear un número de sistema principal. No puede ser una dirección de multidifusión.

Nota: Si se configura una mezcla de circuitos IPX de difusión general y de circuitos IPXWAN para la misma interfaz, es recomendable que el número de sistema principal se configure como el id de nodo IPXWAN seguido de X'0000'.

Valores válidos: Un número hexadecimal de 12 dígitos comprendido entre X'000000000001' y X'FEFFFFFFFFFF'.

Valor por omisión: ninguno

Este número debe ser diferente para cada direccionador.

Ejemplo: `set host-number 0000000000F4`

Nota: Para poder configurar IPXWAN se necesita el ID de nodo y el nombre del direccionador. Utilice los mandatos **set node-ID** y **set name** para configurar estos parámetros.

ipxwan *núm-circuito-ipx tipo-direccionamiento tiempo-espera temporizador-reintentos*

Establece el tipo de direccionamiento IPXWAN, el tiempo de espera de la conexión y el temporizador de reintentos. Antes de poder invocar el mandato **set ipxwan**, debe añadirse un circuito IPXWAN.

núm-circuito-ipx

Especifica el circuito IPXWAN punto a punto para el que se establecerán los parámetros.

Valores válidos: cualquier número de circuito IPXWAN punto a punto ya existente

Valor por omisión: 1

tipo-direccionamiento

Especifica el tipo de direccionamiento IPXWAN a negociar.

- **u** para RIP no numerado
- **r** para RIP numerado
- **b** para ambos, RIP numerado y no numerado
- **s** para direccionamiento estático

Valores válidos: 'u', 'U', 'r', 'R', 'b', 'B', 's', 'S'

Valor por omisión: 'u'

tiempo-espera

Este valor especifica el límite de tiempo, en segundos, en que la negociación IPXWAN debe realizarse satisfactoriamente. Si no se pudiera realizar satisfactoriamente antes de que venza el tiempo configurado para el temporizador de conexión, IPXWAN inicia un temporizador de reintentos. El dispositivo no volverá a intentar la negociación hasta que venza el tiempo configurado para el temporizador de reintentos.

Valores válidos: Un número entero de segundos, comprendido entre 5 y 300.

Valor por omisión: 60 segundos

temporizador-reintentos

Este parámetro especifica el tiempo que se tardará después de que haya vencido el tiempo de espera para realizar una conexión, antes de volver a intentar establecer la conexión.

Valores validos: Un número entero de segundo, comprendido entre 5 y 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 podrá mantener la tabla de filtros Keepalive. Estas entradas consisten en todas las parejas cliente-servidor y servidor-servidor conectadas actualmente en el enlace WAN.

Valores válidos: de 1 a 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 la antememoria local.

El tamaño de la antememoria local debe ser igual al número total de clientes de cada red local o cliente del direccionador, más un 10% para prevenir un número excesivo de peticiones de depuración.

Valores válidos: Están comprendidos entre 1 y 10.000.

Valor por omisión: 64. Para obtener más información, consulte “Antememoria local” en la página 669 y “Antememoria remota” en la página 670.

Ejemplo: `set local-cache size`

```
New IPX local node cache size [64]? 80
```

maximum routes-per-destination *rutas*

Especifica el número máximo de rutas para cada red de destino que se almacenarán en la tabla de rutas RIP de IPX.

Valores válidos: Un entero comprendido entre 1 y 64.

Valor por omisión: 1. Para obtener información adicional sobre rutas múltiples, consulte “Configuración de varias rutas” en la página 659.

Ejemplo: `set maximum routes-per-destination 8`

maximum networks *tamaño*

Especifica el tamaño de la tabla de redes RIP de IPX. Este valor refleja el número de redes que hay en la interred en que funciona IPX.

Valores válidos: de 1 a 2.048

Las restricciones de memoria del direccionador pueden impedir que se utilice el tamaño máximo de la tabla.

Valor por omisión: 32. Este valor no puede ser mayor que el *tamaño* de maximum total-route-entries.

Ejemplo: `set maximum networks 30`

maximum services *tamaño*
Especifica el tamaño de la tabla de servicios SAP de IPX. Este valor refleja el número de servicios SAP en la interred en que funciona IPX.

Valores válidos: de 1 a 2.048

Las restricciones de memoria del direccionador pueden impedir que se utilice el tamaño máximo de la tabla.

Valor por omisión: 32

Ejemplo: `set maximum services 30`

maximum total-route-entries *tamaño*
Especifica el tamaño de la tabla de rutas RIP de IPX. Este valor refleja el número total de rutas, incluidas las rutas alternativas, que hay en la interred en que funciona IPX.

Valores válidos: de 1 a 4.096

Valor por omisión: 32

Este valor debe ser al menos tan grande como el tamaño de *maximum networks*. Para obtener información adicional sobre las rutas múltiples, consulte “Configuración de varias rutas” en la página 659.

Ejemplo: `set maximum total-route-entries 40`

name *nombre_direccionador*
Le permite asignar un nombre simbólico al direccionador. IPXWAN necesita que los direccionadores tengan id de nodo y nombre.

Valores válidos: Una serie de longitud variable de entre 1 y 47 caracteres.

El nombre del direccionador puede contener los caracteres de la A a la Z, los números del 0 a 9, y los signos subrayado (_), guión (-), y "arroba" (@).

Valor por omisión: ninguno.

Ejemplo: `set name newyork_accounting`

net-number *núm-circuito-ipx núm-red*
Especifica el número de red IPX del circuito IPX de difusión general o del circuito IPXWAN punto a punto.

núm-circuito-ipx
Especifica un circuito IPX de difusión general o IPXWAN punto a punto.

Valores válidos: un número de circuito ya existente

Valor por omisión: 1

núm-red
Especifica el número de red IPX que se utilizará para el circuito IPX. El número de red IPX 0 sólo es válido en RIP o circuitos de direccionamiento estático no numerados 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. Se hará caso omiso del mandato set si no se ha configurado un número de red IPX válido.

Valores válidos: de X'0' a 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 IPXWAN interna. Los valores 0, FFFFFFFF y FFFFFFFE no son válidos como números 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 la antememoria remota.

El tamaño de la antememoria remota debe ser igual al número total de redes remotas utilizadas por el direccionador, más un 10% para prevenir un número excesivo de peticiones de depuración.

Valores válidos: Están comprendidos entre 1 y 10.000.

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 del circuito, en ciclos, asociado con este circuito. El número de ciclos representa el tiempo que se tarda en transmitir un paquete IPX de 576 bytes para este circuito IPX. Un ciclo son 55 milisegundos. El valor 0 indica que el direccionador calculará el valor del ciclo. Si se establece un valor distinto de cero, se alterará temporalmente cualquier otro valor calculado, incluso IPXWAN.

núm-circuito-ipx

Especifica un circuito IPX de difusión general o IPXWAN punto a punto.

Valores válidos: cualquier número de circuito IPX válido

Valor por omisión: 1

valor

Especifica el valor del ciclo

Valores válidos: Están comprendidos entre 1 y 30.000.

Valor por omisión: 0

Ejemplo: `set rip-ticks`

```
IPX circuit number [1]? 2
RIP ticks value (in 55msec ticks) [0]? 3
```

rip-update-interval *núm-circuito-ipx intervalo*

Especifica el intervalo, en minutos, en el que se deben producir las difusiones RIP periódicas para un circuito IPX especificado.

Si se aumenta el intervalo de actualización RIP, se reduce el tráfico de las líneas WAN y de los circuitos de marcación. También se evita que los circuitos de marcación a petición tengan que marcar tan a menudo.

Nota: Aunque los anuncios RIP realizados se controlan mediante este intervalo, el direccionador sigue difundiendo los cambios ocurridos en la topología de la red a medida que los averigua.

núm-circuito-ipx

Especifica un circuito IPX de difusión general o IPXWAN punto a punto.

Valores válidos: cualquier número de circuito IPX válido

Valor por omisión: 1

intervalo

Especifica el intervalo, en minutos

Valores válidos: Están comprendidos entre 1 y 1.440 minutos.

Valor por omisión: 1 minuto. Para obtener información adicional sobre el intervalo de actualización RIP, consulte “Especificación del intervalo de actualización RIP” en la página 657.

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 intervalo, en minutos, en el que se deben emitir las difusiones SAP periódicas para un circuito IPX especificado.

Si se aumenta el intervalo SAP, se reduce el tráfico de las líneas WAN y de los circuitos de marcación. También se evita que los circuitos de marcación a petición tengan que marcar tan a menudo.

Nota: Aunque los anuncios SAP realizados se controlan mediante este intervalo, el direccionador sigue difundiendo los cambios ocurridos en los servicios a medida que los averigua.

núm-circuito-ipx

Especifica un circuito IPX de difusión general o IPXWAN punto a punto.

Valores válidos: cualquier número de IPX válido

Valor por omisión: 1

intervalo

Especifica el intervalo, en minutos.

Valores válidos: Están comprendidos entre 1 y 1.440 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 dividido utilizado para el circuito IPX.

Si existe un solo circuito virtual Frame Relay para el circuito, el horizonte dividido estará habilitado; en caso contrario, estará inhabilitado.

En general, el horizonte dividido debe habilitarse (*enabled*). A veces es necesario inhabilitar el horizonte dividido para circuitos de difusión general que son parcialmente en malla en configuraciones Frame-Relay y X.25. Para obtener información adicional sobre el horizonte dividido, consulte “Direccionamiento de horizonte dividido” en la página 671.

heuristic

Habilita el horizonte dividido para el circuito IPX, excepto para circuitos IPX de difusión general de Frame Relay.

Valores válidos: cualquier número de circuito IPX válido

Valor por omisión: 1

enabled

Habilita el horizonte dividido para el circuito IPX.

Valores válidos: de 1 a 1.440

Valor por omisión: 1

disabled

Inhabilita el horizonte dividido para el circuito IPX.

Valores válidos: de 1 a 1.440

Valor por omisión: 1

Ejemplo: `set split-horizon enabled 0`

```
IPX circuit number [1]? 2
```

Acceso al entorno de configuración de filtros de circuitos IPX

Para acceder al entorno de configuración de filtros IPX, escriba el mandato siguiente en el indicador `IPX config>`:

```
IPX Config> filter-lists tipo
IPX tipo-List Config>
```

Donde *tipo* es el tipo de filtro IPX que se va a configurar. Los tipos válidos son *router-lists, rip-lists, sap-lists* e *ipx-lists*.

Para crear un filtro, es necesario indicar un número de circuito IPX.

Mandatos de configuración de filtros de circuitos IPX

En este apartado se describen los mandatos utilizados para configurar los filtros de circuitos IPX; ROUTER, RIP, SAP e IPX. Para configurar estos filtros, escriba el mandato `filter-lists` *tipo* en el indicador `IPX Config>` y, a continuación, escriba los mandatos de configuración en el indicador `IPX` *tipo*`-List Config>`.

Tabla 40. Resumen de los mandatos de configuración de filtros IPX

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Attach	Conecta una lista de filtro determinada con un filtro concreto.
Create	Crea un filtro o lista de filtro.
Default	Establece la acción por omisión de un filtro a *include* o *exclude*
Delete	Suprime un filtro o una lista de filtro.
Detach	Desconecta una lista de filtro de un filtro.
Disable	Inhabilita los filtros.
Enable	Habilita los filtros.
List	Muestra la configuración actual de los filtros.
Move	Vuelve a ordenar la lista de filtro conectada a un filtro.
Set-cache	Establece el tamaño de la antememoria para un filtro determinado.
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 xxxi.

Attach

Utilice el mandato **attach** para conectar una lista de filtro con un filtro.

Sintaxis:

a**ttach** *nombre-lista núm-filtro*

nombre-lista
Especifica el nombre de la lista de filtro. El mandato **list** puede utilizarse para visualizar una lista de nombres de las listas de filtro configuradas.

Valores válidos: Cualquier serie alfanumérica de hasta 16 caracteres

Valor por omisión: Ninguno

núm-filtro
Especifica el número del filtro. Mediante el mandato list puede obtenerse una lista numerada de filtros configurados.

Ejemplo: `attach lista_de_prueba 1`

Create

Utilice el mandato **create** para crear un filtro o una lista de filtro.

Sintaxis:

create list ...
filter ...

list *nombre-lista*
Crea una lista con el nombre especificado.

Valores válidos: Cualquier serie alfanumérica de hasta 16 caracteres

Valor por omisión: ninguno

También se puede entrar el mandato **create list** sin ningún nombre de lista. En ese caso se le solicitará que entre el nombre de lista.

Ejemplo: `create list lista_de_ejemplo`

filter *sentido núm-circuito-ipx*

Crea un filtro para el sentido especificado en el circuito especificado. Especifique *input* para filtrar los paquetes recibidos en el circuito especificado. Especifique *output* para filtrar los paquetes que se van a enviar por el circuito especificado.

Al crear un filtro, automáticamente se le asignará un número, y a partir de ahora, se utilizará para identificar el filtro, en lugar de tener que teclear el circuito y el sentido (input o bien output) para cada uno de los mandatos siguientes.

Ejemplo: `create filter input 1`

Default

Utilice el mandato **default** para establecer la acción por omisión para un filtro. La acción por omisión se toma cuando no se da ninguna coincidencia para ninguno de los elementos de filtro.

Sintaxis:

def**ault**	*acción núm-filtro*
Ejemplo:	`default exclude 1`

acción

Especifica la acción por omisión. **Include** especifica que si no se da ninguna coincidencia con ningún elemento de filtro, se procesará el paquete. **Exclude** indica que si no se da ninguna coincidencia, el paquete se descartará.

núm-filtro

Especifica el número del filtro. Utilice el mandato **list** para visualizar una lista numerada de filtros configurados.

Delete

Utilice el mandato **delete** para suprimir un filtro o una lista de filtro.

Sintaxis:

del**ete**	list ...
	filter ...

list *nombre-lista*

Suprime la lista especificada. El mandato list puede utilizarse para visualizar los nombres de las listas de filtro configuradas.

Ejemplo: `delete list lista_de_ejemplo`

filter *núm-filtro*

Suprime el filtro especificado. El mandato list puede utilizarse para visualizar una lista numerada de filtros configurados.

Ejemplo: `delete filter 1`

Detach

Utilice el mandato **detach** para desconectar una lista de filtro de un filtro.

Sintaxis:

det**ach** *nombre-lista núm-filtro*

nombre-lista
Especifica el nombre de la lista de filtro. El mandato list puede utilizarse para visualizar una lista de los nombres de filtros configurados.

Valores válidos: Cualquier serie alfanumérica de hasta 16 caracteres

Valor por omisión: Ninguno

núm-filtro
Especifica el número del filtro. El mandato list puede utilizarse para visualizar una lista numerada de filtros configurados.

Ejemplo: `detach lista_de_prueba 1`

Disable

Utilice el mandato **disable** para inhabilitar globalmente los filtros o para inhabilitar un filtro concreto.

Sintaxis:

di**sable** all
filter ...

all Inhabilita todos los filtros del tipo actual (ROUTER, RIP, SAP o IPX).

Ejemplo: disable all

filter *núm-filtro*
Inhabilita el filtro especificado. Utilice el mandato list para visualizar una lista numerada de filtros configurados.

Ejemplo: disable filter 1

Enable

Utilice el mandato **enable** para habilitar globalmente los filtros o para habilitar un filtro concreto.

Sintaxis:

en**able** all
filter ...

all Habilita todos los filtros del tipo actual (ROUTER, RIP, SAP o IPX).

Ejemplo: enable all

filter *núm-filtro*
Habilita el filtro especificado. Utilice el mandato list para visualizar una lista numerada de filtros configurados.

Ejemplo: enable filter 1

List

Utilice el mandato **list** para visualizar globalmente el estado del tipo de filtrado actual, o para visualizar información sobre un filtro determinado.

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 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 de filtro de un filtro. Los paquetes se comparan con las listas de filtro en el orden dado por la lista. La primera coincidencia detiene el proceso de filtrado.

Sintaxis:

move *nomb-lista-orig nomb-lista-dest núm-filtro*

nomb-lista-orig
Especifica la lista que se va a trasladar al filtro.

nomb-lista-dest
Especifica la lista antes de la que se trasladará nomb-lista-orig.

núm-filtro
Especifica el filtro al que pertenecen las listas. El mandato list puede utilizarse para visualizar una lista de los filtros configurados y de sus listas de filtro conectadas.

Ejemplo: `move lista-de-prueba-1 lista-de-prueba-2 2`

Set-cache

Utilice el mandato **set-cache** para establecer el tamaño de la antememoria del filtro. Los filtros de circuitos IPX son los únicos que admiten antememoria; los filtros de circuitos ROUTER, RIP y SAP no la admiten.

Sintaxis:

s**et-cache** *tamaño núm-filtro*

tamaño
Especifica el tamaño de la antememoria de filtros (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. El mandato list puede utilizarse para visualizar una lista numerada de filtros configurados.

Ejemplo: `set-cache 10 1`

Update

El mandato **update** accede al indicador `IPX` *`tipo`*`-List` *`nombre-lista`* `Config>`. Desde este indicador se pueden ejecutar mandatos para añadir, suprimir o trasladar elementos de la lista que se vaya a actualizar. Desde aquí, también se puede establecer la acción de la lista de filtro que se va a actualizar.

Sintaxis:

u**pdate** *nombre-lista*

nombre-lista
Especifica el nombre de la lista de filtro. El mandato list puede utilizarse para visualizar los nombres configurados de la lista de filtro.

Ejemplo: `update lista-de-prueba`

Add (submandato de Update)

Utilice el submandato **add** para añadir elementos a una lista de filtro. Los parámetros de la lista varían dependiendo del tipo de filtro de circuito (ROUTER, RIP, SAP o IPX) que se vaya a configurar. Para todos los tipos de filtros de circuito, el mandato **add** puede escribirse sin parámetros. En ese caso se le solicitará que entre los parámetros necesarios.

Add (ROUTER)

Sintaxis:

a**dd** *núm-nodo máscara*

núm-nodo
Especifica el valor que se comparará con el número de nodo origen del direccionador, enviado por el paquete de respuesta RIP (después de aplicarle una operación lógica AND con la máscara). Si se quiere comparar un solo nodo, asigne al parámetro núm-nodo el valor de la dirección y establezca la

máscara como FFFFFFFFFFFF. Si se quieren comparar todos los nodos, establezca los parámetros núm-nodo y máscara como 000000000000.

Valores válidos: de X'000000000000' a X'FFFFFFFFFFFF'

Valor por omisión: ninguno

máscara
Especifica el valor al que se aplicará una operación lógica AND con la dirección de nodo origen del direccionador, enviada por el paquete de respuesta RIP (antes de compararlo con el parámetro dirección).

Si se quiere comparar una sola dirección, asigne la dirección al parámetro dirección y establezca la máscara como FFFFFFFFFFFF. Si se quieren comparar todas las direcciones, establezca los parámetros dirección y máscara a 000000000000.

Valores válidos: de X'000000000000' a X'FFFFFFFFFFFF'

Valor por omisión: X'FFFFFFFFFFFF'

Ejemplo: `add 400000001000 ffffffff0000`

Add (RIP)

Sintaxis:

a**dd** *valor-inic-rango-redes valor-fin-rango-redes*

valor-inic-rango-redes
Valor inicial del rango de números de red IPX que se van a filtrar. Si se quiere comparar un solo número de red, asigne este número de red a los parámetros valor-inic-rango-redes y valor-fin-rango-redes. Si se quieren comparar todos los números de red, defina el valor-inic-rango-redes como X'00000001' y el valor-fin-rango-redes como X'FFFFFFFE'.

Valores válidos: de X'1' a X'FFFFFFFE'

Valor por omisión: X'1'

valor-fin-rango-redes
Valor final del rango de números de red IPX que se van a filtrar.

Valores válidos: de X'1' a X'FFFFFFFE'

Valor por omisión: X'1'

Ejemplo: `add 00000001 FFFFFFFE`

Add (SAP)

Sintaxis:

a**dd** *operador-comparación saltos tipo-sap nombre*

operador-comparación
Especifica el tipo de operador de comparación de la cuenta de saltos para esta lista.

Valores válidos:

<

<=

=

>=

>

Valor por omisión: <= Los parámetros operador-comparación y saltos no se tienen en cuenta para los filtros de salida.

saltos
Especifica la cuenta de saltos para esta lista. Si no se quiere filtrar basándose en la cuenta de saltos, escriba <= 16 para los parámetros operador-comparación y saltos. Los parámetros operador-comparación y saltos no se tienen en cuenta para los filtros de salida.

Valores válidos: de 0 a 16

Valor por omisión: 16

tipo-sap
Especifica el tipo de servicio que se va a filtrar. Escriba el tipo de servicio o X'0000', para indicar todos los tipos de servicios.

Valores válidos: de X'0' a X'FFFF'

Valor por omisión: 4

nombre
Especifica el nombre del servicio que se va a filtrar.

Valores válidos:

Una serie de 1 a 47 caracteres ASCII (de X'20' a X'7E').

El interrogante (?) y el asterisco (*) se utilizan como comodines. El interrogante puede utilizarse varias veces para representar un único carácter del nombre del servidor. El asterisco puede utilizarse varias veces para representar una parte del nombre del servidor. El interrogante y el asterisco también pueden utilizarse conjuntamente.

Valor por omisión: ninguno

Ejemplo: `add < 6 0004 *`

Add (IPX)

Sintaxis:

a**dd** *operador-comparación saltos tipo-ipx valor-inic-rango-redes-dest valor-fin-rango-redes-dest nodo-dest máscara-dest valor-inic-rango-sockets-dest valor-fin-rango-sockets-dest valor-inic-rango-redes-orig valor-fin-rango-redes-orig nodo-orig máscara-orig valor-inic-rango-sockets-orig valor-fin-rango-sockets-orig*

operador-comparación
Especifica el tipo de operador de comparación de la cuenta de saltos para esta lista. Los parámetros operador-comparación y saltos no se tienen en cuenta para los filtros de salida.

Valores válidos:

- <
- <=

- =
- >=
- >

Valor por omisión: <=

saltos
Especifica la cuenta de saltos para esta lista. Si no se quiere filtrar basándose en la cuenta de saltos, escriba <= 16 para los parámetros operador-comparación y saltos. Los parámetros operador-comparación y saltos no se tienen en cuenta para los filtros de salida.

tipo-ipx
Especifica el tipo de paquete IPX que se va a filtrar. Escriba el tipo de paquete, o 00 para indicar todos los tipos de paquetes.

Valores válidos: de X'0' a X'FF'

Valor por omisión: X' 0'

valor-inic-rango-redes-dest
Valor inicial del rango de números de red IPX de destino que se van a filtrar. Si se quiere comparar un solo número de red, asigne este número de red a los parámetros valor-inic-rango-redes-dest y valor-fin-rango-redes-dest. Si se quieren comparar todos los números de red, defina el valor-inic-rango-redes-dest como X'00000001' y el valor-fin-rango-redes-dest como X'FFFFFFFE'.

Valores válidos: de X'00000000' a X'FFFFFFFF'

Valor por omisión: X'00000000'

valor-fin-rango-redes-dest
Valor final del rango de números de red IPX de destino que se van a filtrar. Si se quiere comparar un solo número de red, asigne este número de red a los parámetros valor-inic-rango-redes-dest y valor-fin-rango-redes-dest. Si se quieren comparar todos los números de red, defina el valor-inic-rango-redes-dest como X'00000001' y el valor-fin-rango-redes-dest como X'FFFFFFFE'.

Valores válidos: de X'00000000' a X'FFFFFFFF'

Valor por omisión: X'00000000'

nodo-dest
Especifica el valor que se comparará con el número del nodo de destino (después de aplicarle una operación lógica AND con la máscara-dest). Si se quiere comparar un solo nodo, asigne el número de nodo al parámetro nodo-dest y establezca la máscara-dest como X'FFFFFFFFFFFF'. Si se quieren comparar todos los nodos, establezca los parámetros nodo-dest y máscara-dest como X'000000000000'.

Valores válidos: de X'000000000000' a X'FFFFFFFFFFFF'

Valor por omisión: X'000000000000'

máscara-dest
Especifica el valor al que se aplicará una operación lógica AND con la dirección de nodo de destino (antes de compararlo con el parámetro dirección-dest). Si se quiere comparar una sola dirección, asigne la dirección al parámetro dirección-dest y establezca la máscara-dest como X'FFFFFFFFFFFF'. Si se quieren comparar todas las direcciones, establezca los parámetros dirección-dest y máscara-dest como X'000000000000'.

Valores válidos: de X'000000000000' a X'FFFFFFFFFFFF'

Valor por omisión: X'000000000000'

valor-inic-rango-sockets-dest
Valor inicial del rango de sockets IPX de destino que se van a filtrar. Si se quiere comparar un solo socket, asigne el socket a los parámetros valor-inic-rango-sockets-dest y valor-fin-rango-sockets-dest. Si se quieren comparar todos los sockets, establezca el parámetro valor-inic-rango-sockets-dest como X'0000' y el parámetro valor-fin-rango-sockets-dest como X'FFFF'.

Valores válidos: de X'0000' a X'FFFF'

Valor por omisión: 0

valor-fin-rango-sockets-dest
Valor final de rango de sockets IPX de destino que se van a filtrar. Si se quiere comparar un solo socket, asigne el socket a los parámetros valor-inic-rango-sockets-dest y valor-fin-rango-sockets-dest. Si se quieren comparar todos los sockets, establezca el parámetro valor-inic-rango-sockets-dest como X'0000' y el parámetro valor-fin-rango-sockets-dest como X'FFFF'.

Valores válidos: de X'0000' a X'FFFF'

Valor por omisión: 0

valor-inic-rango-redes-orig
Valor inicial del rango de números de red IPX de origen que se van a filtrar. Si se quiere comparar un solo número de red, asigne el número de red a los parámetros valor-inic-rango-redes-orig y valor-fin-rango-redes-orig. Si se quieren comparar todos los números de red, establezca el parámetro valor-inic-rango-redes-orig como X'00000001' y el parámetro valor-fin-rango-redes-orig como X'FFFFFFFE'.

Valores válidos: de X'00000000' a X'FFFFFFFE'

Valor por omisión: X'00000000'

valor-fin-rango-redes-orig
Valor final de rango de números de red IPX de origen que se van a filtrar. Si se quiere comparar un solo número de red, asigne el número de red a los parámetros valor-inic-rango-redes-orig y valor-fin-rango-redes-orig. Si se quieren comparar todos los números de red, establezca el parámetro valor-inic-rango-redes-orig como X'00000001' y el parámetro valor-fin-rango-redes-orig como X'FFFFFFFE'.

Valores válidos: de X'00000000' a X'FFFFFFFE'

Valor por omisión: X'00000000'

nodo-orig
Especifica el valor que se comparará con el número de nodo origen (después de aplicarle una operación lógica AND con la máscara-orig). Si se quiere comparar un solo nodo, asigne el número de nodo al parámetro nodo-orig y establezca la máscara-orig como X'FFFFFFFFFFFF'. Si se quieren comparar todos los nodos, establezca los parámetros nodo-orig y máscara-orig como X'000000000000'.

Valores válidos: de X'00000000' a X'FFFFFFFF'

Valor por omisión: X'00000000'

máscara-orig
Especifica el valor al que se aplicará una operación lógica AND con la dirección de nodo origen (antes de compararlo con el parámetro dirección-orig). Si se quiere comparar una sola dirección, asigne la dirección al parámetro dirección-orig y establezca la máscara-orig como X'FFFFFFFFFFFF'. Si se quieren comparar todas las direcciones, establezca los parámetros dirección-orig y máscara-orig como X'000000000000'.

Valores válidos: de X'000000000000' a X'FFFFFFFFFFFF'

Valor por omisión: X'000000000000'

valor-inic-rango-sockets-orig
Valor inicial del rango de sockets IPX de origen que se van a filtrar. Si se quiere comparar un solo socket, asigne el socket a los parámetros valor-inic-rango-sockets-orig y valor-fin-rango-sockets-orig. Si se quieren comparar todos los sockets, establezca el parámetro valor-inic-rango-sockets-orig como X'0000' y el parámetro valor-fin-rango-sockets-orig como X'FFFF'.

Valores válidos: de X'0000' a X'FFFF'

Valor por omisión: X'0000'

valor-inic-rango-sockets-orig
Valor final del rango de sockets IPX de origen que se van a filtrar. Si se quiere comparar un solo socket, asigne el socket a los parámetros valor-inic-rango-sockets-orig y valor-fin-rango-sockets-orig. Si se quieren comparar todos los sockets, establezca el parámetro valor-inic-rango-sockets-orig como 0000 y el parámetro valor-fin-rango-sockets-orig como FFFFF.

Valores válidos: de X'0000' a 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 que se envían desde de las redes IPX 5A a 6A hacia la red IPX 4.

Delete (submandato de Update)

Utilice el submandato **delete** para suprimir un elemento de la lista de filtro actual.

Sintaxis:

d**elete** *núm-elemento*

núm-elemento
Especifica el número del elemento de la lista. Este número puede obtenerse con el mandato list, que permite listar los elementos de la lista de filtro.

Ejemplo: `delete 4`

List (submandato de Update)

Utilice el submandato **list** para mostrar la acción de la lista de 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. Después de cambiar el orden de los elementos de filtro, se vuelven a numerar para que reflejen la nueva ordenación. El mandato list puede utilizarse para visualizar una lista numerada de elementos de filtro configurados.

El parámetro *núm-línea-orig* señala la línea que se va a trasladar. Esta línea se trasladará delante del elemento especificado por el parámetro *núm-línea-dest*.

Sintaxis:

move *núm-línea-orig núm-línea-dest*

Ejemplo: `move 5 2`

Set-action (submandato de Update)

Utilice el submandato **set-action** para indicar la acción que se debe llevar a cabo cuando se dé una coincidencia con una lista de filtro.

Sintaxis:

set-action include
exclude

include Especifica que si se da una coincidencia para el filtro actual, el paquete se procesará (se incluirá) para los filtros ROUTER e IPX. Para los filtros RIP y SAP, **include** especifica que la entrada RIP o SAP se procesará.

Ejemplo: `set-action include`

exclude Especifica que si se da una coincidencia para el filtro actual, el paquete se descartará (se excluirá) para los filtros ROUTER e IPX. Para los filtros RIP y SAP, **exclude** especifica que si se da una coincidencia, la entrada RIP o SAP no se tendrá en cuenta.

Ejemplo: `set-action exclude`

Acceso al entorno de supervisión de IPX

Para obtener información sobre cómo acceder al entorno de supervisión de IPX, consulte “Cómo empezar (introducción a los circuitos de usuario)” del manual *Access Integration Services Guía del usuario de software*

Mandatos de supervisión de IPX

En la Tabla 41 se listan los mandatos de supervisión de IPX. Los mandatos de supervisión de IPX le permiten ver los parámetros y las estadísticas de los circuitos y redes que transmiten paquetes IPX. Los mandatos de supervisión muestran valores de configuración de los niveles físico, de trama y de paquete. También tiene la opción de ver los valores de los tres niveles de protocolo a la vez.

Escriba los mandatos de supervisión de IPX en el indicador `IPX>`. En la Tabla 41 se describen resumidamente los mandatos de supervisión de IPX.

Tabla 41 (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 de mandatos concretos (si se dispone de ellas). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Access-controls	Muestra si están habilitados los filtros IPX globales (controles de acceso), las sentencias de control de acceso de IPX y el número de paquetes que han coincidido con cada sentencia de control de acceso.
Cache	Lista el contenido actual de la antememoria de direccionamiento.
Counters	Muestra el número de errores de direccionamiento y de desbordamiento de paquetes.
Delete keepalive connection	Suprime una entrada de la tabla de filtros Keepalive.
Disable	Inhabilita IPX globalmente o para circuitos IPX específicos.
Dump routing tables	Muestra el contenido de la tabla de direccionamiento.
Enable	Habilita IPX globalmente o para circuitos IPX específicos.
Filters	Muestra si los filtros SAP globales están habilitados, las sentencias de filtros SAP y el número total de anuncios SAP que se han filtrado.
Filter-Lists	Accede a la consola de filtros de circuitos IPX. Es aquí donde pueden supervisarse los filtros de circuitos ROUTER, RIP, SAP e IPX.
IPXWAN	Lista información sobre IPXWAN para los circuitos IPXWAN punto a punto.
Keepalive	Muestra el estado de cada conexión cliente-servidor activa en la tabla de filtros keepalive.
List	Lista la configuración actual o la dirección IPX de cada circuito habilitado.
Ping	Envía paquetes IPXPING a otro sistema principal y espera respuesta. Este mandato puede utilizarse para identificar un problema en un entorno de interred.

Tabla 41 (Página 2 de 2). Resumen de los mandatos de supervisión de IPX

Mandato	Función
Recordroute	Envía paquetes IPXPING de registro de ruta a otro sistema principal y espera respuesta. Utilice este mandato para registrar y mostrar la ruta de ida y vuelta entre este dispositivo y otro sistema principal. Utilice esta información para identificar problemas en un entorno de interred.
Reset	Restablece circuitos IPX específicos, filtros SAP globales, filtros IPX globales (controles de acceso), rutas y servicios estáticos, o filtros de circuitos ROUTER, RIP, SAP o IPX (listas de filtro).
Sizes	Muestra los tamaños configurados de las antememorias del nodo local y de la red remota, y el número de entradas de la antememoria que se están utilizando actualmente.
Slist	Muestra el contenido de la tabla de servidores SAP de IPX.
Traceroute	Envía paquetes IPXPING de rastreo de rutas a otro sistema principal y espera respuesta. Utilice este mandato para rastrear y visualizar cada salto que da un paquete en el camino que recorre desde este dispositivo hasta el sistema principal de destino. Utilice esta información para identificar problemas en un entorno de interred.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Access Controls

Utilice el mandato **access-controls** para listar el estado de los filtros IPX globales (controles de acceso), las sentencias de control de acceso de IPX, y el número de veces que se ha seguido una 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 del control de acceso

Type
Muestra si los paquetes se envían o se descartan para una dirección determinada o para un conjunto de direcciones. I significa incluir. Esto permite enviar los paquetes. E significa excluir. Esto hace que el direccionador descarte los paquetes.

Dest net
Número de red del destino. Un cero (0) significa todas las redes.

Dest host
Número de sistema principal de la red de destino; un cero (0) significa todos los sistemas principales de la red.

Dest sock
Dos números que denotan un rango inclusivo de sockets de destino.

Src net
Número de red del origen. Un cero (0) significa todas las redes.

Src host
Número de sistema principal de la red de origen. Un cero significa todos los sistemas principales de la red.

Src sock
Dos números que denotan un rango inclusivo de sockets de origen.

Count
Especifica el número de paquetes IPX de entrada que han coincidido con cada sentencia de control de acceso, haciendo que se cumpla la acción asociada con su Tipo (Incluir o Excluir).

Cache

Utilice el mandato **cache** para visualizar el contenido de la antememoria de direccionamiento de 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 la red remota 420 puede accederse a través del circuito serie cuyo número de red IPX es 412. La segunda entrada es la red IPX 412. Es una red Ethernet conectada directamente al direccionador. Esta entrada es una entrada de red local general. Aparecerá una entrada de red local general para cada red conectada directamente después de que hayan comenzado a reenviar paquetes IPX. La última entrada es una entrada local de una red Ethernet. Esta entrada de la antememoria IPX se ha utilizado para enviar 1 paquete al número de nodo IPX 0000 0420 0000 del número de red 412.

Counters

Utilice el mandato **counters** para visualizar el número de errores de direccionamiento y de desbordamiento de paquetes que se han producido. En el ejemplo, los contadores muestran que no se ha producido ningún error.

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 llegar a su destino.

Checksum
La suma de comprobación no es correcta, o el paquete ha sufrido alguna inconsistencia grave antes de llegar a su destino.

Destination unreachable
El sistema principal de destino no puede accederse desde aquí.

Hop count expired
El paquete ha pasado a través de 15 direccionadores de interred sin llegar a su destino.

circuit size exceeded
El paquete es demasiado grande para poder ser reenviado a través de alguna red intermedia.

Destination errors

Unknown
Se ha detectado un error no especificado en el destino.

Checksum
La suma de comprobación no es correcta o se ha detectado en el destino que el paquete ha sufrido alguna inconsistencia grave.

Nonexistent socket
El socket especificado no existe en el sistema principal de destino.

Congestion
El destino no puede aceptar el paquete a causa de limitaciones de los recursos.

IPX Input Packet Overflows

Net Especifica el nombre del circuito.

Count
Especifica el número de paquetes que no pueden recibirse a causa de limitaciones de los recursos.

Delete

Utilice el mandato **delete** para eliminar una entrada de la tabla de filtros Keepalive.

Sintaxis:

de**lete** *núm-entrada*

núm-entrada

Especifica la entrada de la tabla que se va a suprimir. Puede utilizarse el mandato **Keepalive** para listar el contenido de la tabla de filtros Keepalive.

Ejemplo: `delete 1`

Disable

Utilice el mandato **disable** para inhabilitar IPX globalmente o para circuitos específicos.

Sintaxis:

di**sable** circuit ...
ipx

circuit *núm-circuito-ipx*

Inhabilita el circuito IPX especificado por el *núm-circuito-ipx*. IPX puede volverse a habilitar mediante el mandato **enable**.

Ejemplo: `disable circuit 2`

ipx Inhabilita IPX globalmente para todos los circuitos IPX. IPX puede volverse a habilitar globalmente ejecutando 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 al direccionador.
- RIP - especifica que el protocolo de direccionamiento de IPX, RIP, es quien ha proporcionado esta ruta.

- Old - especifica que el tiempo de validez de esta ruta ha vencido y que ya no se utiliza. La ruta permanece en la tabla brevemente para informar a otros direccionadores de que la ruta ya no es válida; después de este breve intervalo, ya no se volverá a mostrar.
- Stat - especifica que esta es una ruta estática.

Dest net Especifica el número de la red de destino.

Hops Especifica el número de saltos hasta este destino.

Delay Especifica el tiempo estimado que tardará el direccionador en transmitir el paquete y éste en llegar a su destino. La unidad de retardo es el número de ciclos de reloj del PC IBM que tarda en enviar un paquete de 576 bytes, que es de 18,21 ciclos de reloj por segundo. El retardo mínimo es de 1 unidad.

Age Especifica la antigüedad de la información de direccionamiento en minutos y segundos. Si no se actualiza alguna entrada de la tabla de direccionamiento, el direccionador emprenderá las acciones siguientes:

- Después de que transcurran tres intervalos de actualización RIP, la ruta se marcará como Old (antigua) y el direccionador anunciará que la ruta ya no es válida. El intervalo de actualización RIP puede mostrarse ejecutando el mandato de IPX **config**. Para obtener más información sobre los intervalos RIP, consulte “Especificación del intervalo de actualización RIP” en la página 657.
- 60 segundos después, la dirección se suprime y no vuelve a aparecer en el vuelco a pantalla.

Via router Especifica el salto siguiente para los paquetes dirigidos a redes que no están conectadas directamente. Para las redes conectadas directamente, esta 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 pantalla aparecen las entradas del número de ruta y de red utilizadas y el total disponible. Si se utilizan todas las entradas de red, es probable que el tamaño de la tabla de direccionamiento no sea lo suficientemente grande. Utilice el mandato de configuración de IPX **set maximum networks** para aumentar el tamaño.

Si se utilizan todas las entradas de rutas, es posible que haya rutas hacia redes IPX que no puedan mantenerse en la tabla, incluidas algunas nuevas y las entrantes. Si no quiere aumentar el número de rutas disponibles, reduzca el número máximo de rutas por red.

Enable

Utilice el mandato **enable** para habilitar IPX globalmente o para circuitos concretos.

Sintaxis:

en**able**	circuit ...
	ipx

circuit *núm-circuito-ipx*

Habilita el circuito IPX especificado por el *núm-circuito-ipx*. Antes de que se pueda habilitar IPX, debe haberse configurado un número de red IPX para el circuito.

Ejemplo: `enable circuit 2`

ipx Habilita IPX globalmente para todos los circuitos IPX habilitados.

Ejemplo: `enable ipx`

Filters

Utilice el mandato **filters** para visualizar si se han habilitado los filtros SAP globales, las sentencias de filtros SAP, y el número total de anuncios SAP que se han filtrado.

Sintaxis:

filters

Ejemplo: `filters`

```
IPX SAP Filters:  Enabled
Count  Max Hops  Type  Service Name
0      5         4     SRVARCH01
```

Count Indica el número de anuncios SAP que se han filtrado (descartado).

Max Hops

Indica el número máximo de saltos permitidos para el servicio.

Type Valor numérico de la clase de servicio.

Service name

Nombre del servicio, si lo tuviera.

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 más información sobre los mandatos disponibles desde este indicador, consulte “Mandatos de supervisión de filtros de circuitos IPX” en la página 731.

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 IPXWAN para circuitos IPXWAN punto a punto.

Sintaxis:

ipxwan detailed . . .
summary

detailed *núm-circuito-ipx*

Lista la información IPXWAN para el 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 vecino, tal como se recibe en el paquete de petición de información de RIP/SAP.

Neighbor Node ID

El ID de nodo (también llamado número de red principal) del vecino. Este es un número de red IPX único para toda la interred. Es un valor de 32 bits.

Negotiated Routing Type

El tipo de direccionamiento negociado. Actualmente, los tipos admitidos son: RIP/SAP, RIP no numerado y direccionamiento estático. Si el tipo de direccionamiento negociado es RIP no numerado o direccionamiento estático, no será necesario tener un número de red común para el enlace.

Link Delay

El retardo del enlace en ciclos de 1/18 de segundo calculado por el origen. Es un valor de 16 bits. Siempre es un valor calculado, por lo que no hay un valor por omisión.

Common Net#

El número de red acordado por ambos extremos del enlace. Este número debe ser único para toda la interred. Es un valor de 32 bits. Si el tipo de direccionamiento es RIP no numerado o direccionamiento estático, el valor 0 aparecerá como número de red común para ambos mandatos **IPXWAN detailed** y **IPXWAN summary**. No existe valor por omisión; debe negociarse.

Connection Timeouts

Número de veces que la conexión ha excedido el tiempo de espera. Una conexión excede periódicamente el tiempo de espera si no se intercambian paquetes IPXWAN. Se puede configurar

este tiempo de espera ejecutando el mandato **set ipxwan**. El valor por omisión de este tiempo de espera es de 60 segundos.

Connection Retries
Número de veces que se ha reintentado la conexión después de que se agotara el tiempo de espera. El tiempo que se espera (antes de volver a intentar la conexión) puede configurarse mediante el mandato **set ipxwan**. El valor por omisión es de 60 segundos.

Timer Requests Sent
Número de paquetes de petición de temporizador IPXWAN enviados.

Timer Requests Received
Número de paquetes de petición de temporizador IPXWAN recibidos.

Timer Responses Sent
Número de paquetes de respuesta de temporizador IPXWAN enviados.

Timer Responses Received
Número de paquetes de respuesta de temporizador IPXWAN recibidos.

Info Requests Sent
Número de paquetes de petición de información IPXWAN enviados.

Info Requests Received
Número de paquetes de petición de información IPXWAN recibidos.

Info Responses Sent
Número de paquetes de respuesta de información IPXWAN enviados.

Info Responses Received
Número de paquetes de respuesta de información IPXWAN recibidos.

summary Lista información resumida sobre IPXWAN para todos los circuitos IPXWAN punto a punto.

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 único para toda la interred. El número de red común será 0 si el tipo de direccionamiento negociado es RIP no numerado o direccionamiento estático.

NodeID
ID de nodo (también llamado número de red interna) del vecino.

Neighbor Name
Nombre de direccionador del vecino, tal como se recibe en el paquete de petición de información de RIP/SAP.

Keepalive

Muestra el estado de cada conexión cliente-servidor activa en la tabla de filtros keepalive.

Sintaxis:

keepalive

Ejemplo:

```
Keepalive
Conn #     Net  /   Node     /Sock        Net  /   Node     /Sock
          ------------------------------------------------------------------
0         272727/000000000001/4001         302/0000C911EF1C/4004
                (server conn # 1, conn type: passive, last heard  1:00 ago)
1         272727/000000000001/4001         302/0000C911B0D9/4004
                (server conn # 2, conn type: passive, last heard  1:00 ago)
```

List

Utilice el mandato **list** para listar la configuración actual o la dirección IPX de cada circuito IPX habilitado.

Sintaxis:

list *addresses*
configuration

addresses
Lista las direcciones 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: Cartagena
```

Configuration
Lista la configuración de IPX actual. Este mandato muestra la misma información que el mandato de configuración **list summary**. En “List” en la página 689 hay un ejemplo de lo que puede verse en pantalla y una explicación de la salida del mandato.

Ping

Utilice el mandato **ping** para que el direccionador envíe paquetes IPXPING a un destino determinado (“hacer ping”) y espere respuesta. Este mandato puede utilizarse para identificar problemas en un entorno de interred.

Este proceso se realiza continuamente. Las respuestas recibidas se muestran emparejadas con el número de red IPX y el número de nodo del remitente, el número de saltos y el tiempo de ida y vuelta, en milisegundos.

Para detener el proceso de ping, escriba un carácter cualquiera en el entorno de supervisión. En ese momento, aparecerá un resumen de los paquetes perdidos, el tiempo de ida y de vuelta y el número de destinos a los que no se ha podido acceder.

Cuando se da una dirección de multidifusión como destino, puede haber varias respuestas para cada paquete enviado, una por cada miembro de grupo. Cada respuesta devuelta se muestra con la dirección de origen de quien ha respondido.

Notas:

1. Especificar la dirección de difusión general (FFFFFFFFFFFF) debe hacerse con sumo cuidado, ya que esto puede producir un gran número de paquetes IPXPING de respuesta, lo que degradaría el rendimiento de la red y del software de direccionamiento.
2. Si entra el mandato **ping** sin parámetros, se le solicitará que los escriba todos. Si sólo entra los parámetros ***destination network*** y ***destination node***, se utilizarán los valores por omisión para los parámetros que faltan.

Sintaxis:

p**ing** *red-dest nodo-dest red-orig nodo-orig tamaño cadencia*

red-dest
Especifica el número de la red IPX de destino. Este parámetro es obligatorio.

Valores válidos: de X'1' a X'FFFFFFFD'

Valor por omisión: 1

nodo-dest
Especifica la dirección del nodo IPX de destino. Este parámetro es obligatorio.

Valores válidos: de X'1' a X'FFFFFFFFFFFF'

Valor por omisión: Ninguno

red-orig
Especifica el número de red IPX de origen. Este parámetro es opcional. El valor debe ser un número de red conocido asociado con un circuito IPX conectado directamente. Si no se especifica ninguna red de origen, el número de red del circuito IPX al que se envían los paquetes IPXPING de petición, se utilizará como dirección IPX de origen. Si el circuito IPX es un circuito IPXWAN de direccionamiento RIP no numerado o de direccionamiento estático, la dirección de nodo del circuito IPX que se utiliza como número de red de origen se utilizará como nodo de origen.

Valores válidos: de X'1' a X'FFFFFFFD'

Valor por omisión: 1

nodo-orig
Especifica la dirección de nodo IPX de origen. Este parámetro es opcional. El valor debe ser una dirección de nodo conocida asociada con un circuito IPX conectado directamente. Si no se especifica ningún nodo de origen, la dirección de nodo del circuito IPX al que se envían los paquetes IPXPING de petición, se utilizará como nodo IPX de origen. Si el circuito IPX es un circuito IPXWAN de direccionamiento RIP no numerado o de direccionamiento estático,

la dirección de nodo del circuito IPX que se utiliza como número de red de origen se utilizará como nodo de origen.

Valores válidos: de X'1' a X'FFFFFFFFFFFE'

Valor por omisión: Ninguno

tamaño
Especifica el número de bytes de datos que se añadirán a la petición de ping. Este parámetro es opcional. Los datos incluyen la hora de la primera vez que se envía la petición, por lo que la cantidad especificada no puede menor que 4 bytes. Tampoco puede ser mayor que el tamaño máximo de paquete que admita el direccionador o el circuito de salida. Este valor puede variar dependiendo de la configuración.

Valores válidos: de 4 al máximo admitido por el direccionador

Valor por omisión: 56 bytes

cadencia
Especifica el número de segundos entre peticiones de ping. Este parámetro es opcional.

Valores válidos: de 1 a 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 notificar la ruta hacia el destino y la ruta de regreso a todos los circuitos que reenvían paquetes. Si se invoca el mandato recordroute sin parámetros, se le solicitará que los escriba todos. Solamente son obligatorios el número de red IPX de destino y la dirección de nodo IPX de destino.

Hay dos sucesos que finalizan un mandato recordroute. El primero es pulsar una tecla. El segundo es que se envíe el número máximo de paquetes de petición de registro de ruta.

Sintaxis:

r**ecordroute** *red-dest nodo-dest red-orig nodo-orig cadencia número*

red-dest
Especifica el número de la red IPX de destino. Este parámetro es obligatorio.

Valores válidos: de X'1' a X'FFFFFFFD'

Valor por omisión: 1

nodo-dest
Especifica la dirección del nodo IPX de destino. Este parámetro es obligatorio.

Valores válidos: de X'1' a X'FFFFFFFFFFFE'

Valor por omisión: Ninguno

red-orig
Especifica el número de red IPX de origen. Este parámetro es opcional. El valor debe ser un número de red conocido asociado con un circuito IPX conectado directamente. Si no se especifica ninguna red de origen, el número de red del circuito IPX al que se envían los paquetes de registro de ruta, se utilizará como dirección IPX de origen. Si el circuito IPX es un circuito IPXWAN de direccionamiento RIP no numerado o de direccionamiento estático, se utilizará como dirección de origen el número de red de otro circuito IPX numerado, puesto que los circuitos IPXWAN de direccionamiento no numerado y de direccionamiento estático no tienen asignado un número de red IPX.

Valores válidos: de X'1' a X'FFFFFFFD'

Valor por omisión: 1

nodo-orig
Especifica la dirección de nodo IPX de origen. Este parámetro es opcional. El valor debe ser una dirección de nodo conocida asociada con un circuito IPX conectado directamente. Si no se especifica ningún nodo de origen, la dirección de nodo del circuito IPX al que se envían los paquetes de registro de ruta, se utilizará como nodo IPX de origen. Si el circuito IPX es un circuito IPXWAN de direccionamiento RIP no numerado o de direccionamiento estático, la dirección de nodo del circuito IPX que se utiliza como número de red de origen se utilizará como nodo de origen.

Valores válidos: de X'1' a X'FFFFFFFFFFFE'

Valor por omisión: Ninguno

cadencia
Especifica el número de segundos entre peticiones de registro de ruta. Este parámetro es opcional.

Valores válidos: de 1 a 60

Valor por omisión: 1

número
Especifica el número máximo de peticiones de registro de ruta que se enviarán. Este parámetro es opcional. Un cero hará que el registro de ruta continúe hasta que se pulse una tecla.

Valores válidos: de 0 a 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
```

La ruta completa se notifica solamente en la primera respuesta o cuando la ruta cambia. En el ejemplo anterior, la ruta cambia dos veces.

Reset

Utilice el mandato **reset** para restablecer circuitos IPX específicos, filtros SAP globales, filtros IPX globales (controles de acceso), rutas y servicios estáticos, o filtros de circuito ROUTER, RIP, SAP o IPX (listas de filtro).

Sintaxis:

re**set**	access-controls
	circuit . . .
	filters
	filter-lists
	route-static
	sap-static

access-controls
Restablece los filtros IPX globales (controles de acceso) utilizando los valores de los parámetros de configuración almacenados en la memoria de configuración. Los cambios hechos en la configuración de filtros IPX globales se activarán.

Ejemplo: reset access-controls

circuit *núm-circuito-ipx*
Restablece IPX para el circuito IPX especificado, utilizando los valores de los parámetros de configuración almacenados en la memoria de configuración. Los cambios hechos en la configuración de IPX para el circuito IPX se activarán.

Ejemplo: reset circuit 2

filters
Restablece los filtros SAP globales utilizando los valores de los parámetros de configuración almacenados en la memoria de configuración. Los cambios hechos en la configuración de filtros SAP globales se activarán.

Ejemplo: reset filters

filter-lists *tipo-filtro*
Restablece los filtros de circuitos utilizando los valores de los parámetros de configuración almacenados en la memoria de configuración. Los cambios hechos en la configuración de los filtros de circuitos se activarán. Los ***tipos de filtros*** válidos son: router, rip, sap e ipx.

Ejemplo: reset filter-lists rip

route-static
Restablece las rutas estáticas utilizando los valores de los parámetros de configuración almacenados en la memoria de configuración. Los cambios hechos en la configuración de las rutas estáticas se activarán.

Ejemplo: reset route-static

sap-static
Restablece los servicios estáticos utilizando los valores de los parámetros de configuración almacenados en la memoria de configuración. Los cambios hechos en la configuración de los servicios estáticos se activarán.

Ejemplo: reset sap static

Sizes

Utilice el mandato **sizes** para visualizar los tamaños configurados de las antememorias del nodo local y de la red remota, y el número de entradas de la antememoria que se están utilizando actualmente (este mandato no muestra 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 mostrar 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    DESARR2                        1     0:50       11/0000000000B4/0451
SAP  4    PLANNING                       2     0:50       BB/0000000000B7/0451
SAP  4    DESARR                         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  ARBOLDIR                       2     0: 5 2C29ABE9/000000000001/4005
Stat 26B  ARBOLDIR                       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 ha vencido el tiempo de espera asociado a este servicio y que ya no se va a utilizar. El servicio se mantiene durante un breve período de tiempo en la tabla para informar a los demás direccionadores de que el servicio ya no es válido. Después, se suprime y ya no se vuelve a mostrar.
Stat - indica que este servicio es estático.

Typ Especifica el tipo de servidor, en hexadecimal. Los servidores de archivos son del tipo 0004. Los números de los otros tipos los asigna Novell.

Service name
Especifica el nombre exclusivo del servidor para este tipo de servidor. Para ahorrar espacio, solamente se muestran los primeros 30 caracteres del nombre de 47 caracteres.

Hops
Especifica el número de saltos de direccionador desde este direccionador hasta el servidor.

Age Especifica la antigüedad de la información del servicio. Si no se actualiza una entrada de la tabla SAP, el direccionador emprenderá las acciones siguientes:

- Después de que transcurran tres intervalos de actualización SAP, el servicio se marcará como Del y el direccionador anunciará que el servicio ya no es válido. El intervalo de actualización SAP puede mostrarse ejecutando el mandato de IPX **config**.

- 60 segundos después, el servicio se suprime y no vuelve a aparecer en la información que muestra el mandato **slist**.

Net/Host/Sock
Especifica la dirección del servicio. La dirección consta de los parámetros siguientes:

- Número de red
- Número de sistema principal de red (la dirección del primer circuito de la red)
- Número de socket a través del que se puede acceder al servicio

En la parte inferior de la pantalla aparece el número de entradas utilizadas y el total disponible. Si se utilizan todas las entradas, es probable que el tamaño de 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 notificar cada salto que da una petición de ping en su camino hacia su destino final. Si se invoca el mandato traceroute sin parámetros, se le solicitará que los escriba todos. Solamente son obligatorios el número de red IPX de destino y la dirección de nodo IPX de destino.

Hay tres sucesos que finalizan un mandato traceroute. El primero es pulsar una tecla. El segundo es que se reciba una respuesta de la dirección de destino. El tercero es que se alcance el número máximo de saltos.

Sintaxis:

t**raceroute** *red-dest nodo-dest red-orig nodo-orig tamaño rastreos cadencia saltos*

red-dest
Especifica el número de la red IPX de destino. Este parámetro es obligatorio.

Valores válidos: de X'1' a X'FFFFFFFD'

Valor por omisión: 1

nodo-dest
Especifica la dirección del nodo IPX de destino. Este parámetro es obligatorio.

Valores válidos: de X'1' a X'FFFFFFFFFFFE'

Valor por omisión: Ninguno

red-orig
Especifica el número de red IPX de origen. Este parámetro es opcional. El valor debe ser un número de red conocido asociado con un circuito IPX conectado directamente. Si no se especifica ninguna red de origen, el número de red del circuito IPX al que se envían los paquetes de rastreo de rutas, se utilizará como dirección IPX de origen. Si el circuito IPX es un circuito IPXWAN de direccionamiento RIP no numerado o de direccionamiento estático, se utilizará como dirección de origen el número de red de otro circuito IPX numerado, puesto que los circuitos IPXWAN de direccionamiento no numerado y de direccionamiento estático no tienen asignado un número de red IPX.

Valores válidos: de X'1' a X'FFFFFFFD'

Valor por omisión: 1

nodo-orig
Especifica la dirección de nodo IPX de origen. Este parámetro es opcional. El valor debe ser una dirección de nodo conocida asociada con un circuito IPX conectado directamente. Si no se especifica ningún nodo de origen, la dirección de nodo del circuito IPX al que se envían los paquetes de rastreo de rutas, se utilizará como nodo IPX de origen. Si el circuito IPX es un circuito IPXWAN de direccionamiento RIP no numerado o de direccionamiento estático, la dirección de nodo del circuito IPX que se utiliza como número de red de origen se utilizará como nodo de origen.

Valores válidos: de X'1' a X'FFFFFFFFFFFE'

Valor por omisión: Ninguno

tamaño
Especifica el número de bytes de datos que se añadirán a la petición de rastreo de rutas. Este parámetro es opcional. Los datos incluyen la hora de la primera vez que se envío la petición, por lo que el número especificado no puede ser menor que 4 bytes. Tampoco puede ser mayor que el tamaño máximo de paquete que admita el direccionador o el circuito de salida. Este valor puede variar dependiendo de la configuración.

Valores válidos: de 4 al máximo admitido por el direccionador

Valor por omisión: 56

rastreos
Especifica cuántas peticiones de rastreo de rutas se enviarán por cada salto. Este parámetro es opcional.

Valores válidos: de 1 a 10

Valor por omisión: 3

cadencia
Especifica el número de segundos entre rastreos, cuando no hay respuesta a una petición de rastreo de rutas. Este parámetro es opcional.

Valores válidos: de 1 a 60

Valor por omisión: 1

saltos
Especifica el número máximo de saltos permitidos para enviar peticiones de rastreo de rutas. Este parámetro es opcional. Sin NLSP, un paquete puede atravesar un máximo de 16 nodos (de aquí que el valor por omisión sea 16). Con NLSP o la solución del semidireccionador IBM 6611, el límite ya no es 16.

Valores válidos: de 1 a 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 de rastreo de rutas se notifica solamente una vez mientras no cambie. En el ejemplo anterior, dos direccionadores distintos han respondido a la petición de rastreo de rutas de un salto. Esto sucederá si la ruta hacia el destino cambia entre rastreos.

Una petición de rastreo de rutas notifica otra información, además del tiempo de ida y vuelta de un rastreo:

- '*' - No se ha recibido ningún paquete de respuesta en el tiempo especificado.
- 'H!' - No se puede acceder a la red de destino. Esto se notificará si la ruta hacia el destino se ha perdido después de arrancar el rastreo de rutas.
- 'BF' - No hay almacenamientos intermedios disponibles.

Mandatos de supervisión de filtros de circuitos IPX

La Tabla 42 lista los mandatos disponibles desde el indicador `IPX *tipo*-Lists>`. En este apartado se explica detalladamente cada uno de los mandatos.

Para acceder al indicador `IPX tipo-Lists>`, escriba **`filter-lists`** `tipo` en el indicador `IPX>`. Los tipos válidos son router-lists, rip-lists, sap-lists e ipx-lists.

Tabla 42. Resumen de los mandatos de supervisión de filtros de circuitos IPX

Mandato	Función
Cache	Muestra el contenido de la antememoria de filtros para el circuito especificado. El filtro IPX es el único que admite antememoria de filtros.
Clear	Inicializa los contadores del filtro especificado o inicializa los contadores de todos los filtros del tipo actual (ROUTER, 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 xxxi.

Cache

Utilice el mandato **cache** para visualizar el contenido de la antememoria de filtros. El filtro IPX es el único que admite antememoria. Los filtros ROUTER, RIP y SAP no admiten antememoria de filtros.

Sintaxis:

ca**che filter** *núm-filtro*

núm-filtro

Especifica el número del filtro. El mandato list puede utilizarse para visualizar una lista numerada de 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 inicializar los contadores del filtro especificado o para inicializar los contadores de todos los filtros del tipo actual (ROUTER, RIP, SAP o IPX).

Sintaxis:

c**lear** all
filter ...

all Inicializa los contadores de todos los filtros del tipo actual (ROUTER, RIP, SAP o IPX).

Ejemplo: `clear all`

filter *núm-filtro*
Inicializa los contadores del número de filtro especificado. El mandato list puede utilizarse para visualizar una lista numerada de filtros configurados.

Ejemplo: `clear filter 1`

Disable

Utilice el mandato **disable** para inhabilitar filtros específicos o para inhabilitar todos los filtros del tipo actual (ROUTER, RIP, SAP o IPX).

Sintaxis:

d**isable** all
filter *núm-filtro*

all Inhabilita todos los filtros del tipo actual (ROUTER, RIP, SAP o IPX).

Ejemplo: `disable all`

filter *núm-filtro*
Inhabilita el número de filtro especificado. El mandato list puede utilizarse para visualizar una lista numerada de filtros configurados.

Ejemplo: `disable filter 1`

Enable

Utilice el mandato **enable** para habilitar filtros específicos o para habilitar todos los filtros del tipo actual (ROUTER, RIP, SAP o IPX).

Sintaxis:

en**able** all

filter *núm-filtro*

all Habilita todos los filtros del tipo actual (ROUTER, RIP, SAP o IPX).

Ejemplo: `enable all`

filter *núm-filtro*
Habilita el número de filtro especificado. El mandato list puede utilizarse para visualizar una lista numerada de 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 (ROUTER, RIP, SAP o IPX).

Sintaxis:

list all
filter *núm-filtro*

all Lista la configuración de todos los filtros del tipo actual (ROUTER, 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. El mandato list puede utilizarse para visualizar una lista numerada de 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
```

Soporte de reconfiguración dinámica de IPX

En este apartado se describe el modo en que la reconfiguración dinámica (DR) afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

IPX da soporte al mandato **delete interface** de CONFIG (Talk 6) con la matización siguiente:

> Cuando se suprima la interfaz de red, se suprimirán de la memoria de configuración todos los circuitos IPX, las rutas estáticas, los servicios estáticos y los filtros de circuito (ROUTER RIP, SAP e IPX) configurados en la interfaz de red.

Mandato activate interface de GWCON (Talk 5)

IPX da soporte al mandato **activate interface** de GWCON (Talk 5) con las matizaciones siguientes:

- Para poder activar IPX en una interfaz de red nueva, debe estar habilitado actualmente de manera global.
- Para poder activar IPX en una interfaz de red nueva, debe estar habilitado actualmente al menos en una intefaz de red.
- Para activar rutas estáticas en la interfaz de red, debe utilizarse el mandato GWCON, protocol IPX, reset route-static.
- Para activar servicios estáticos en la interfaz de red, debe utilizarse el mandato GWCON, protocol IPX, reset sap-static.
- Para activar filtros de circuito en la interfaz de red, debe utilizarse el mandato GWCON, protocol IPX, reset filter-lists.

En la tabla siguiente se resumen los cambios de configuración de IPX que se activan cuando se invoca el mandato **activate interface** de GWCON (Talk 5):

Mandatos ejecutados como parte del mandato activate interface de GWCON (Talk 5)
GWCON, protocol IPX, reset circuit
Nota: Cuando se active la interfaz de red, se activarán también todos los circuitos IPX configurados en la interfaz de red.

Mandato reset interface de GWCON (Talk 5)

IPX da soporte al mandato **reset interface** de GWCON (Talk 5) con las matizaciones siguientes:

- Para restablecer rutas estáticas en la interfaz de red, debe utilizarse el mandato GWCON, protocol IPX, reset route-static.
- Para restablecer servicios estáticos en la interfaz de red, debe utilizarse el mandato GWCON, protocol IPX, reset sap-static.
- Para restablecer filtros de circuito en la interfaz de red, debe utilizarse el mandato GWCON, protocol IPX, reset filter-lists.

En la tabla siguiente se resumen los cambios de configuración de IPX que se activan cuando se invoca el mandato **reset interface** de GWCON (Talk 5):

Mandatos ejecutados como parte del mandato reset interface de GWCON (Talk 5)
GWCON, protocol IPX, reset circuit
Nota: Cuando se restablezca la interfaz de red, se restablecerán también todos los circuitos IPX configurados en la interfaz de red.

Mandatos de restablecimiento de componente de GWCON (Talk 5)

IPX da soporte a los mandatos **reset** de GWCON (Talk 5) específicos de IPX siguientes:

Mandato GWCON, protocol IPX, reset circuit

Descripción: Se restablece el circuito IPX especificado.

Efecto en la red: El circuito IPX se suprime y se vuelve a crear utilizando para ello los parámetros de circuito IP de la memoria de configuración. Todas las rutas y los servicios averiguados por medio del circuito IPX se anuncian como desactivados, se suprimen y se averiguan de nuevo al volverse a crear el circuito IPX. Si el número de red IPX del circuito ha cambiado, las sesiones en las que participen los clientes de dicho circuito se perderán y puede que haya que restablecer los clientes.

Limitaciones:

- Para restablecer rutas estáticas en el circuito restablecido, debe utilizarse el mandato **GWCON, protocol IPX, reset route-static**.
- Para restablecer servicios estáticos en el circuito restablecido, debe utilizarse el mandato **GWCON, protocol IPX, reset sap-static**.
- Para restablecer filtros de circuito en el circuito restablecido, debe utilizarse el mandato **GWCON, protocol IPX, reset filter-lists**.

En la tabla siguiente se resumen los cambios de configuración de IPX que se activan cuando se invoca el mandato **GWCON, protocol IPX, reset circuit**:

Mandatos cuyos cambios los activa el mandato GWCON, protocol IPX, reset circuit
CONFIG, protocol IPX, add broadcast-circuit
CONFIG, protocol IPX, add ipxwan-circuit
CONFIG, protocol IPX, delete circuit
CONFIG, protocol IPX, disable circuit
CONFIG, protocol IPX, disable keepalive-filtering
CONFIG, protocol IPX, disable netbios-broadcast
CONFIG, protocol IPX, disable reply-to-get-nearest serve
CONFIG, protocol IPX, disable rip
CONFIG, protocol IPX, disable rip-sap-pacing
CONFIG, protocol IPX, disable sap
CONFIG, protocol IPX, enable circuit
CONFIG, protocol IPX, enable keepalive-filtering
CONFIG, protocol IPX, enable netbios-broadcast
CONFIG, protocol IPX, enable reply-to-get-nearest serve
CONFIG, protocol IPX, enable rip
CONFIG, protocol IPX, enable rip-sap-pacing
CONFIG, protocol IPX, enable sap
CONFIG, protocol IPX, frame
CONFIG, protocol IPX, move circuit
CONFIG, protocol IPX, set ipxwan
CONFIG, protocol IPX, set net-number
CONFIG, protocol IPX, set rip-ticks
CONFIG, protocol IPX, set rip-update-interval
CONFIG, protocol IPX, set sap-update-interval
CONFIG, protocol IPX, set split-horizon

Mandato GWCON, protocol IPX, reset route-static

Descripción: Se restablecen todas las rutas estáticas, incluida la ruta por omisión y si el direccionamiento estático IPX está inhabilitado o habilitado globalmente.

Efecto en la red: No causa trastornos en la red.

Limitaciones: Ninguna.

En la tabla siguiente se resumen los cambios de configuración de IPX que se activan cuando se invoca el mandato **GWCON, protocol IPX, reset route-static**:

Mandatos cuyos cambios los activa el mandato GWCON, protocol IPX, reset route-static
CONFIG, protocol IPX, add route-static
CONFIG, protocol IPX, delete route-static
CONFIG, protocol IPX, disable route-static
CONFIG, protocol IPX, enable route-static

Mandato GWCON, protocol IPX, reset sap-static

Descripción: Se restablecen todos los servicios estáticos, incluido si el uso de los servicios estáticos IPX está inhabilitado o habilitado globalmente.

Efecto en la red: No causa trastornos en la red.

Limitaciones: Ninguna.

En la tabla siguiente se resumen los cambios de configuración de IPX que se activan cuando se invoca el mandato GWCON, protocol IPX, reset sap-static:

Mandatos cuyos cambios los activa el mandato GWCON, protocol IPX, reset sap-static
CONFIG, protocol IPX, add sap-static
CONFIG, protocol IPX, delete sap-static
CONFIG, protocol IPX, disable sap-static
CONFIG, protocol IPX, enable sap-static

Mandato GWCON, protocol IPX, reset filters

Descripción: Se restablecen todos los filtros de SAP, incluido si el uso de los filtros de SAP está inhabilitado o habilitado globalmente.

Efecto en la red: No causa trastornos en la red.

Limitaciones: Ninguna.

En la tabla siguiente se resumen los cambios de configuración de IPX que se activan cuando se invoca el mandato **GWCON, protocol IPX, reset filters**:

Mandatos cuyos cambios los activa el mandato GWCON, protocol IPX, reset filters
CONFIG, protocol IPX, add filter
CONFIG, protocol IPX, delete filter
CONFIG, protocol IPX, set filter

Mandato GWCON, protocol IPX, reset access-controls

Descripción: Se restablecen todos los filtros de IPX (controles de acceso), incluido si el uso de los filtros de IPX está inhabilitado o habilitado globalmente.

Efecto en la red: No causa trastornos en la red.

Limitaciones: Ninguna.

En la tabla siguiente se resumen los cambios de configuración de IPX que se activan cuando se invoca el mandato **GWCON, protocol IPX, reset access-controls**:

Mandatos cuyos cambios los activa el mandato GWCON, protocol IPX, reset access-controls
CONFIG, protocol IPX, add access-control
CONFIG, protocol IPX, delete access-control
CONFIG, protocol IPX, move access-control
CONFIG, protocol IPX, set access-control

Mandato GWCON, protocol IPX, reset filter-lists router

Descripción: Se restablecen todos los filtros de circuito ROUTER, las listas de filtro y los elementos de filtro, incluido si el uso de los filtros de circuito ROUTER está inhabilitado o habilitado globalmente.

Efecto en la red: No causa trastornos en la red.

Limitaciones: Ninguna.

En la tabla siguiente se resumen los cambios de configuración de IPX que se activan cuando se invoca el mandato **GWCON, protocol IPX, reset filter-lists router**:

Mandatos cuyos cambios los activa el mandato GWCON, protocol IPX, reset filter-lists router
CONFIG, protocol IPX, filter-lists router, attach
CONFIG, protocol IPX, filter-lists router, create
CONFIG, protocol IPX, filter-lists router, default
CONFIG, protocol IPX, filter-lists router, delete
CONFIG, protocol IPX, filter-lists router, detach
CONFIG, protocol IPX, filter-lists router, disable
CONFIG, protocol IPX, filter-lists router, enable
CONFIG, protocol IPX, filter-lists router, move
CONFIG, protocol IPX, filter-lists router, update, add
CONFIG, protocol IPX, filter-lists router, update, delete
CONFIG, protocol IPX, filter-lists router, update, move
CONFIG, protocol IPX, filter-lists router, update, set-action

Mandato GWCON, protocol IPX, reset filter-lists rip

Descripción: Se restablecen todos los filtros de circuito RIP, las listas de filtro y los elementos de filtro, incluido si el uso de los filtros de circuito ROUTER está inhabilitado o habilitado globalmente.

Efecto en la red: No causa trastornos en la red.

Limitaciones: Ninguna.

En la tabla siguiente se resumen los cambios de configuración de IPX que se activan cuando se invoca el mandato **GWCON, protocol IPX, reset filter-lists rip**:

Mandatos cuyos cambios los activa el mandato GWCON, protocol IPX, reset filter-lists rip
CONFIG, protocol IPX, filter-lists rip, attach
CONFIG, protocol IPX, filter-lists rip, create
CONFIG, protocol IPX, filter-lists rip, default
CONFIG, protocol IPX, filter-lists rip, delete
CONFIG, protocol IPX, filter-lists rip, detach
CONFIG, protocol IPX, filter-lists rip, disable
CONFIG, protocol IPX, filter-lists rip, enable
CONFIG, protocol IPX, filter-lists rip, move
CONFIG, protocol IPX, filter-lists rip, update, add
CONFIG, protocol IPX, filter-lists rip, update, delete
CONFIG, protocol IPX, filter-lists rip, update, move
CONFIG, protocol IPX, filter-lists rip, update, set-action

Mandato GWCON, protocol IPX, reset filter-lists sap

Descripción: Se restablecen todos los filtros de circuito SAP, las listas de filtro y los elementos de filtro, incluido si el uso de los filtros de circuito SAP está inhabilitado o habilitado globalmente.

Efecto en la red: No causa trastornos en la red.

Limitaciones: Ninguna.

En la tabla siguiente se resumen los cambios de configuración de IPX que se activan cuando se invoca el mandato **GWCON, protocol IPX, reset filter-lists sap**:

Mandatos cuyos cambios los activa el mandato GWCON, protocol IPX, reset filter-lists sap
CONFIG, protocol IPX, filter-lists sap, attach
CONFIG, protocol IPX, filter-lists sap, create
CONFIG, protocol IPX, filter-lists sap, default
CONFIG, protocol IPX, filter-lists sap, delete
CONFIG, protocol IPX, filter-lists sap, detach
CONFIG, protocol IPX, filter-lists sap, disable
CONFIG, protocol IPX, filter-lists sap, enable
CONFIG, protocol IPX, filter-lists sap, move
CONFIG, protocol IPX, filter-lists sap, update, add
CONFIG, protocol IPX, filter-lists sap, update, delete
CONFIG, protocol IPX, filter-lists sap, update, move
CONFIG, protocol IPX, filter-lists sap, update, set-action

Mandato GWCON, protocol IPX, reset filter-lists ipx

Descripción: Se restablecen todos los filtros de circuito IPX, las listas de filtro y los elementos de filtro, incluido si el uso de los filtros de circuito IPX está inhabilitado o habilitado globalmente.

Efecto en la red: No causa trastornos en la red.

Limitaciones: Ninguna.

En la tabla siguiente se resumen los cambios de configuración de IPX que se activan cuando se invoca el mandato **GWCON, protocol IPX, reset filter-lists ipx**:

Mandatos cuyos cambios los activa el mandato GWCON, protocol IPX, reset filter-lists ipx
CONFIG, protocol IPX, filter-lists ipx, attach
CONFIG, protocol IPX, filter-lists ipx, create
CONFIG, protocol IPX, filter-lists ipx, default
CONFIG, protocol IPX, filter-lists ipx, delete
CONFIG, protocol IPX, filter-lists ipx, detach
CONFIG, protocol IPX, filter-lists ipx, disable
CONFIG, protocol IPX, filter-lists ipx, enable
CONFIG, protocol IPX, filter-lists ipx, move
CONFIG, protocol IPX, filter-lists ipx, set-cache
CONFIG, protocol IPX, filter-lists ipx, update, add
CONFIG, protocol IPX, filter-lists ipx, update, delete
CONFIG, protocol IPX, filter-lists ipx, update, move
CONFIG, protocol IPX, filter-lists ipx, update, set-action

Mandatos de cambio temporal de GWCON (Talk 5)

IPX da soporte a los mandatos de GWCON que cambian de forma temporal el estado operativo del dispositivo indicados más abajo. Los cambios se pierden cada vez que se vuelve a cargar o iniciar el dispositivo o que se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
GWCON, protocol IPX, disable circuit
GWCON, protocol IPX, disable ipx
GWCON, protocol IPX, enable circuit
GWCON, protocol IPX, enable ipx

Mandatos no reconfigurables dinámicamente

En la tabla siguiente figuran los mandatos de configuración de IPX que no pueden cambiarse dinámicamente. Para activar estos mandatos, es necesario volver a cargar o a arrancar el dispositivo.

Mandatos
CONFIG, protocol IPX, set keepalive-table-size
CONFIG, protocol IPX, set local-cache size
CONFIG, protocol IPX, set maximum networks
CONFIG, protocol IPX, set maximum routes-per-destination
CONFIG, protocol IPX, set maximum services
CONFIG, protocol IPX, set maximum total-route-entries
CONFIG, protocol IPX, set name
CONFIG, protocol IPX, set node-id
CONFIG, protocol IPX, set remote-cache size

Apéndices

Apéndice A. Funcionamiento conjunto con el direccionador IBM 6611

Hay una serie de cuestiones de configuración que deben tenerse en cuenta para que la implementación de DLSw por IBM Access Integration Services funcione conjuntamente con el direccionador IBM 6611.

Las secciones siguientes proporcionan una visión general de tales cuestiones e indican qué características de la implementación de DLSw por IBM Access Integration Services no pueden funcionar junto a las características del IBM 6611.

Nota: Las cuestiones que se citan aquí se derivan de las pruebas efectuadas con el software MPNP V1.2 del IBM 6611. Es posible que no sean aplicables a otras versiones del software MPNP.

Tales cuestiones se han clasificado según las secciones siguientes:

Cuestiones acerca de la configuración de puente

Las siguientes cuestiones se refieren a la configuración de puente:

- La identificación de LAN (número de segmento) de DLSw debe coincidir en los dos direccionadores, IBM 2212 e IBM 6611. Si se da constantemente una falta de coincidencia, acceda al configurador de IBM Access Integration Services (Talk 6) y seleccione el protocolo DLSw. El mandato **set srb** puede utilizarse entonces para establecer un valor de número de segmento que coincida con el equivalente de IBM 6611.
- El valor máximo de MTU que puede utilizarse para la trama de puente es de 2100 bytes. Éste es el valor mayor que soporta actualmente el IBM 6611. Si se especifican valores de MTU menores que 2100, es importante que los valores configurados coincidan en los direccionadores IBM 2212 e IBM 6611.

Cuestiones relacionadas con DLSw

Las cuestiones de funcionamiento conjunto relacionadas con DLSw son las siguientes:

- La implementación de DLSw por IBM Access Integration Services no da soporte a la generación del mensaje SSP_IAMOKAY (tipo de mensaje SSP X'x1D') mientras la implementación de DLSw del IBM 6611 esté soportada. Este mensaje SSP no figura entre las especificaciones del documento RFC 1434 y es eliminado silenciosamente por la implementación de DLSw por IBM Access Integration Services cuando se recibe.
- La implementación de DLSw del IBM 6611 procesa los mensajes SSP_ENTER_BUSY/EXIT_BUSY que se reciban de la implementación de

DLSw por el IBM Access Integration Services, pero no generará mensajes SSP similares relacionados con el control de flujo.

- La implementación de DLSw por el IBM Access Integration Services da soporte el mensaje definido por el usuario SSP_TEST_CIRCUIT_REQ (tipo de mensaje SSP X'x7A') que genera un direccionador DLSw del IBM 6611 funcionando como nodo de red APPN. Al recibir este mensaje, la implementación de DLSw por IBM Access Integration Services retornará el mensaje definido por el usuario SSP_TEST_CIRCUIT_RSP (tipo de mensaje SSP X'x7B'). Esta respuesta es esperada por la implementación del nodo de red APPN del direccionador DLSw del IBM 6611.

Cuestiones de configuración relacionadas con IP

A continuación se enumeran las cuestiones a tener en cuenta en la configuración de IP:

- La función de grupo de DLSw cliente/servidor e igual/igual que permite que los nodos vecinos de DLSw de IBM Access Integration Services se encuentren el uno al otro de forma dinámica no puede funcionar conjuntamente con la implementación DLSw del IBM 6611. Como resultado, deberá utilizarse el mandato de configuración de DLSw **add tcp neighbor** para definir las direcciones IP estáticas de los nodos adyacentes iguales DLSw del IBM 6611.
- Esta restricción de funcionamiento conjunto acerca de la característica de grupo de DLSw del IBM Access Integration Services posee implicaciones para la selección de RIP/OSPF:
  - Para utilizar grupos de DLSw en un 2212, también debe configurarse OSPF/MOSPF. Sin embargo, puesto que estos grupos de DLSw no funcionan conjuntamente con el 6611, es posible configurar el 2212 habilitando solamente RIP y sin configurar OSPF.
  - Aunque OSPF y RIP pueden estar habilitados por IBM 2212, MOSPF (si se selecciona mediante la configuración de OSPF) no está soportado por el IBM 6611.
- En la configuración de IP del IBM Access Integration Services asegúrese que los patrones de relleno configurados para direcciones de difusión en una interfaz dada coincidan con las definiciones equivalentes en el IBM 6611.
- El sistema de reserva de ancho de banda (BRS) del IBM Access Integration Services, que puede utilizarse para garantizar ancho de banda para el tranporte de tráfico SNA sobre DLSw, no puede funcionar conjuntamente con la implementación de DLSw del IBM 6611.

  Aunque la prioridad que asigna el hardware de IBM 2212 para BRS puede implementarse en el sentido de salida, no se garantizará el orden de prioridad si los direccionadores IP intermedios no dan soporte a BRS. Además, debido a que el 6611 no da soporte a BRS en el extremo final de la línea, BRS sólo puede aplicarse en una sola dirección.

Cuestiones relacionadas con TCP

A continuación se enumeran las cuestiones a tener en cuenta en el funcionamiento conjunto con TCP:

Diferencias en la detección de interrupciones en la conexión TCP
La implementación de DLSw por IBM Access Integration Services detecta cuando se interrumpe una conexión TCP bien cuando no se recibe una respuesta Keepalive (suponiendo que se ha habilitado la opción Keepalive para la conexión) o cuando no pueden entregarse los datos.

Diferencias en el restablecimiento de la conexión TCP
Cuando se interrumpe una conexión TCP, la implementación de DLSw por IBM Access Integration Services restablece la conexión TCP cuando se genera un nuevo mensaje de DLSw SSP_CANUREACH al recibir un mensaje de DLC TEST de una estación final. El IBM 6611 puede que no tenga el mismo comportamiento.

Diferencias respecto a la inhabilitación/habilitación de Keepalive
Tal como se ha indicado previamente, la implementación de DLSw por IBM Access Integration Services permite la habilitación y la inhabilitación de la opción Keepalive cuando se añade (configura) una dirección IP del vecino TCP. Aunque TCP en la implementación DLSw del IBM 6611 responde a mensajes Keepalive recibidos en una sesión TCP, no hay ningún mecanismo para configurar el TCP de 6611 residente para que habilite la generación de mensajes Keepalive de TCP.

Número máximo de conexiones TCP soportadas
En la implementación de DLSw por IBM Access Integration Services, no hay ninguna restricción inalterable sobre el número máximo de conexiones TCP soportadas. Como consecuencia, el número máximo de conexiones TCP soportadas está directamente relacionado con la memoria disponible del IBM 2212. En el caso del IBM 6611, hay una restricción interna inalterable según la cual se da soporte a 100 conexiones TCP en la implementación de DLSw.

Diversas cuestiones de funcionamiento conjunto

Ténganse en cuenta las siguientes cuestiones diversas sobre el funcionamiento conjunto:

- Si se encuentra un problema al tratar de establecer una conexión de DLSw iniciada por el IBM 6611, compruebe la configuración del IBM 6611 para asegurarse que no se haya habilitado involuntariamente el filtrado de direcciones MAC para una dirección MAC asociada de origen o de destino.
- Aunque el documento RFC 1434 no trata específicamente la cuestión de sesiones de DLSw huérfanas (por ejemplo, sesiones DLSw que permanecen en un estado establecido de circuito, sin ninguna actividad posterior), tanto la implementación de DLSw por IBM Access Integration Services como la del IBM 6611 resuelven la cuestión mediante tiempos excedidos de sesión DLSw huérfana. Las sesiones de DLSw que permanecen inactivas en el estado establecido del circuito DLSw durante más de 30 segundos son eliminadas por ambas implementaciones.

Apéndice B. Funcionamiento conjunto con el puente IBM 6611

Antes de implementar el establecimiento de puentes en el IBM 2212, para su funcionamiento conjunto con el establecimiento de puentes en el IBM 6611 deben tenerse en cuenta ciertas cuestiones relativas a la configuración.

Este apéndice proporciona una visión general de tales cuestiones, indicando qué características de la implementación de puentes del IBM 2212 ***no*** funcionan conjuntamente con la implementación de puentes del IBM 6611.

Con el fin de evitar la creación de una red incompatible, deberán tenerse en cuenta los siguientes aspectos relativos a la configuración de puentes al utilizar el IBM 6611 y el IBM 2212, como puentes finales sobre enlaces serie PPP y frame-relay.

Para PPP, el puente de IBM 2212 da soporte a diferentes tipos de MAC (Ethernet y red en anillo), como se describe en el documento RFC 1638, *PPP Bridging Control Protocol*. En el caso de frame-relay, el IBM 2212 da soporte a las especificaciones del documento RFC 1490/2427, *Multiprotocol Interconnect over Frame Relay*.

Actualmente, el puente IBM 6611 admite los tipos de MAC Ethernet y red en anillo a través de PPP y Frame Relay. Sin embargo, el puente IBM 6611 sólo da soporte a tramas MAC de red en anillo cuando el puerto del puente asociado con PPP o frame-relay está configurado como un puerto de direccionamiento en origen. Ello conduce a ciertas restricciones en las topologías de red cuando el IBM 6611 y el IBM 2212 son los dos puentes finales a través de PPP o frame-relay.

En el documento RFC 1638, sección 5.3, se describe cómo un proveedor puede anunciar al puente igual el tipo de MAC que está soportado a través de PPP, de modo que el igual no envía tráfico de tipo MAC no soportado a través de PPP. Actualmente, el puente IBM 2212 no descarta tramas no-Ethernet destinadas a la red PPP. Tampoco intenta convertir todas las tramas a tramas Ethernet antes de enviarlas a través de PPP. Como resultado, el puente IBM 6611 bridge recibe tramas no Ethernet a través de PP y las elimina cuando hay falta de coincidencias en la configuración.

Otras cuestiones de PPP

Debería tenerse en cuenta lo siguiente al configurar un 2212 y un 6611 en una red puenteada:

- Para que el tráfico circule por puente a través de un enlace PPP, la unidad máxima de recepción (MRU) negociada debe ser lo suficientemente grande para contener una trama enviada por puente. Ésta contiene los datos y la cabecera de la capa MAC de la LAN original.

  Por ejemplo, una trama Ethernet puede contener 1500 bytes de datos. Cuando se puentea a través de un enlace WAN, se incluyen 14 bytes adicionales de cabecera MAC de Ethernet en el tráfico que pasa por el puente, haciendo que la medida del paquete sea 1514. Esto significa que la MRU de PPP negociada debe ser al menos de 1514 para que la trama pase el puente.

Debería considerarse utilizar un tamaño de MRU superior al tamaño necesario para contener cualquier trama enviada por puente. Puede utilizarse inicialmente 2000 o 2048 como valor de MRU.

- Asegúrese de que ambos extremos del enlace PPP estén configurados para el mismo tamaño de MRU. Si se utiliza el MRU por omisión para el 2212, asegúrese de que el MRU para el 6611 coincida con el valor de MRU del 2212.

Ejemplos de configuración

Los siguientes ejemplos de topologías de red ***no*** funcionarán. Otras configuraciones posibles alternativas están señaladas con *Alt*. En el caso de WAN, los tipos de LAN pueden ampliarse a tipos MAC.

Ejemplo 1: Token-Ring (SR) - IBM 2212 (SR-TB) - PPP (TB) - IBM 6611 (TB) - Ethernet

Alt: Token Ring (SR) - IBM 2212 (SRB) - PPP (SR) - IBM 6611 (SR-TB) - Ethernet

Ejemplo 2: Token Ring (TB) - IBM 2212 (TB) - PPP (TB) - IBM 6611 (TB) - ETH/TKR

Alt: Token Ring (SR) - IBM 2212 (SRB) - PPP (SR) - IBM 6611 (SR-TB) - ETH

Alt: Token Ring (SR) - IBM 2212 (SRB) - PPP (SR) - IBM 6611 (SRB) - TKR

Alt: Token Ring (TB) - IBM 2212 (SR-TB) - PPP (SR) - IBM 6611 (SRB) - TKR

Alt: Token Ring (TB) - IBM 2212 (SR-TB) - PPP (SR) - 6611 (SR-TB) - ETH

Las tramas de LAN generadas por el nodo de acceso limítrofe (Boundary Access Node, BAN) y DLSw son tramas de red en anillo direccionadas en origen . Según el tipo de medio de transmisión y el comportamiento de la configuración de puentes del puerto de puente de salida asociado, el puente IBM 2212 convierte la trama de red en anillo direccionada en origen del modo siguiente.

1. ETH (TB) en Ethernet
2. PPP / FR / Túnel / en formato TP 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 anilllo

Apéndice C. Lista de Abreviaturas

AARP	AppleTalk Address Resolution Protocol
ABR	Direccionador limítrofe de área
ack	Acuse de recibo
AIX	Advanced Interactive Executive
AMA	Direccionamiento del MAC arbitrario
AMP	Supervisor presente activo
ANSI	Instituto Nacional de Normalización de los Estados Unidos
AP2	AppleTalk Phase 2
APPN	Red de igual a igual
ARE	Trama exploradora de todas las rutas
ARI/FCI	Indicador de dirección reconocida/indicador de trama copiada
ARP	Address Resolution Protocol
AS	Sistema autónomo
ASBR	Direccionador limítrofe 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
ayt	¿Hay alguien ahí?
BAN	Nodo de acceso de límites
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 Configuration Report Server

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

E&M Ear & Mouth

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 para el registro cronológico de sucesos

ELSCon Consola secundaria de ELS

ESI Identificador de sistema final

EST Horario Estándar del Este de los EE.UU

Eth Ethernet

fa-ga Dirección funcional-dirección de grupo

FCS Secuencia de comprobación de trama

FECN Notificación de congestión explícita hacia adelante

FIFO Primero en entrar, primero en salir

FLT Biblioteca de filtros

FR Frame Relay

FRL Frame Relay

FTP File Transfer Protocol

FXO Foreign Exchange Office

FXS Foreign Exchange Station

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 TCP/IP Host Services

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 de Normalización

Kbps Kilobits por segundo

LAN Red de área local

LAPB Protocolo de acceso a enlace equilibrado

LAT Transporte de área local

LCS Estación de canal de LAN

LCP Link Control Protocol

LED Diodo emisor de luz

LF Trama mayor; salto de línea

LIS Subred IP lógica

LLC Control de enlace lógico

LLC2 Control de enlace lógico 2

LMI Interfaz de gestión local

LRM LAN Reporting Mechanism

LS Estado de enlace

LSA Anuncio de estado de enlace

LSA Link Services Architecture

LSB Bit menos significativo

LSI Interfaz de métodos abreviados de LAN

LSreq Petición de estado de enlace

LSrxl Lista de retransmisión de estado de enlace

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

MPC Canal de diversas vías de acceso

MPC+ Canal de diversas vías de acceso de transferencia de datos de alto rendimiento (HPDT)

MSB Bit más significativo

MSDU Unidad de datos de servicio MAC

MRU Unidad máxima de recepción

MTU Unidad máxima de transmisión

nak Sin acuse de recibo

NAS Estación Nways Switch Administration

NBMA Acceso múltiple sin difusión

NBP Name Binding Protocol

NBR Direccionador vecino

NCP Network Control Protocol

NCP Network Core Protocol

NDPS Conmutación de vías de acceso sin interrupciones

NetBIOS Network Basic Input/Output System

NHRP Next Hop Resolution Protocol

NIST National Institute of Standards and Technology

NPDU Unidad de datos de protocolo de red

NRZ No retorno a cero

NRZI No retorno a cero invertido

NSAP Punto de acceso a servicios de red

NSF National Science Foundation

NSFNET National Science Foundation NETwork

NVCNFG Configuración permanente

OOS fuera de servicio

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 Ring Error Monitor

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 Ring Parameter Server

RTMP Routing Table Maintenance Protocol

RTP RouTing update Protocol

RTS Petición de emisión

Rtype Tipo de ruta

rxmits Retransmisiones

rxmt Retransmisión

s Segundo

SAF Filtración de direcciones de origen

SAP Punto de acceso a servicios

SAP Service Advertising Protocol

SCR Velocidad sostenida de célula

SCSP Server Cache Synchronization Protocol

sdel Delimitador de inicio

SDLC Relay de SDLC, control síncrono de enlace de datos

seqno Número de secuencia

SGID Identificación de grupo de servidores

SGMP Simple Gateway Monitoring Protocol

SL Línea serie

SMP Supervisor presente en espera

SMTP Simple Mail Transfer Protocol

SNA Systems Network Architecture

SNAP Subnetwork Access Protocol

SNMP Simple Network Management Protocol

SNPA Punto de conexión de subred

SPF Ruta intraárea OSPF

SPE1 Ruta externa OSPF de tipo 1

SPE2 Ruta externa OSPF de tipo 2

SPIA Tipo de ruta inter-área 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 en origen

SRF Trama específicamente direccionada

SRLY Relay de SDLC

SRT Transparente de direccionamiento en origen

SR-TB Puente transparente-direccionamiento en origen

STA Estático

STB Puente de árbol de extensión

STE Trama exploradora del árbol de extensión

STP Par trenzado y apantallado; protocolo de árbol de extensión

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 extensión transparentes

TTL Período de duración

TTY Teletipo

TX Transmisión

UA Acuse de recibo no numerado

UDP User Datagram Protocol

UI Información no numerada

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

VoFR Voz sobre Frame Relay

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

En este glosario figuran términos y definiciones extraídos de los documentos y publicaciones siguientes:

- *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 propiedad del Instituto Nacional de Normalización de los Estados Unidos (ANSI). Si desea adquirir un ejemplares de esta publicación, diríjase a American National Standards Institute, 11 West 42nd Street, New York, New York 10036, Estados Unidos. Las definiciones se identifican mediante el símbolo (A) que aparece después de la definición.
- ANSI/EIA Standard—440-A, *Fiber Optic Terminology*. Si desea adquirir una copia de este documento, diríjase a Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006, Estados Unidos. Las definiciones se identifican mediante el símbolo (E) que aparece después de la definición.
- *Information Technology Vocabulary* redactado por la Subcomisión 1 (SC1), Comisión Técnica Mixta 1 (JTC1), de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (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.
- *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*
- *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.

Equivale a: 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 de: Es una referencia inversa de un término definido a los demás 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

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 corre-

laciona 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)*.

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 el cometido de agente.

alerta. Mensaje enviado a un punto focal de servicios de gestión de una red para identificar un problema o un problema inminente.

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). Equivale a *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 extensión. 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)

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 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 que indica el tipo de mensaje y el nivel de prioridad del mensaje.

cabecera de transmisión (TH). Información de control, seguida opcionalmente de una unidad básica de información (BIU) o de un segmento de BIU, que crea y utiliza el control de la vía de acceso para direccionar unidades de mensajes y controlar su flujo dentro de la red. Véase también *unidad de información de vía de acceso*.

canal. (1) Vía de acceso por la que pueden enviarse señales, como, por ejemplo, canal de datos, canal de salida. (A) (2) Unidad funcional, controlada por el procesador, que maneja la transferencia de datos entre el almacenamiento del procesador y el equipo de periféricos local.

canal de diversas vías de acceso (MPC). Protocolo de canal que utiliza diversos subcanales unidireccionales para la comunicación bidireccional de VTAM a VTAM.

canal de entrada/salida. En un sistema de proceso de datos, unidad funcional que maneja la transferencia de datos entre el equipo interno y el equipo de periféricos. (I) (A)

canal lógico. En el funcionamiento en modalidad de paquete, canal de emisión y canal de recepción que se utilizan conjuntamente para enviar y recibir datos sobre un enlace de datos al mismo tiempo. Pueden establecerse varios canales lógicos en el mismo enlace de datos si se intercala la transmisión de paquetes.

canalización. Proceso consistente en romper el ancho de banda de una línea de comunicaciones en varios canales, posiblemente de diferentes tamaños. También se denomina ***multiplexación de la división del tiempo*** (TDM).

capa. (1) En una arquitectura de red, grupo de servicios que está completo desde un punto de vista conceptual, que es uno de los grupos de un conjunto de grupos ordenados jerárquicamente y que se extiende por todos los sistemas que se ajustan a la arquitectura de red. (T) (2) En el modelo de referencia interconexión de sistemas abiertos, uno de los siete grupos de servicios, funciones y protocolos ordenados jerárquicamente y completos conceptualmente que se extienden por todos los sistemas abiertos. (T) (3) En SNA, agrupación de funciones relacionadas que están separadas lógicamente de las funciones de otros grupos. La implementación de las funciones de una capa puede cambiar sin que ello afecte a las funciones de otras capas.

capa de control de enlace de datos (DLC). En SNA, capa que está compuesta por las estaciones de enlace que planifican la transferencia de datos sobre un enlace entre dos nodos y realizan un control de errores para el enlace. Ejemplos de control de enlace de datos son: el SDLC para la conexión de enlaces serie por bit y el control de enlace de datos para el canal de System/370.

Nota: Normalmente, la capa de DLC es independiente del mecanismo de transporte físico y asegura la integridad de los datos que alcanzan las capas superiores.

capa de enlace de datos. En el modelo de referencia 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. Equivale a *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 de *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 averigua 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/servidor. En comunicaciones, modelo de interacción en el proceso de datos distribuidos en el que un programa de un sitio envía una petición a un programa de otro sitio y espera una respuesta. El programa

peticionario se denomina cliente; el programa que responde se denomina servidor.

codificar. Convertir datos mediante el uso de un código de manera que sea posible la reconversión al formato original. (T)

colisión. Condición no deseada que deriva de la existencia de transmisiones simultáneas en un canal. (T)

compresión. (1) Proceso consistente en eliminar claros, campos vacíos, redundancias y datos innecesarios para disminuir la longitud de los registros o los bloques. (2) Cualquier codificación destinada a reducir el número de bits utilizados para representar un mensaje o un registro determinado.

comunidad. En el protocolo Simple Network Management Protocol (SNMP), relación administrativa entre las entidades.

concentrador (inteligente). Concentrador de cableado, como, por ejemplo, el IBM 8260, que proporciona funciones de puente y direccionamiento a las LAN con diferentes cables y protocolos.

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 de *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.

Configuration Report Server (CRS). En IBM Token-Ring Network Bridge Program, servidor que acepta mandatos de 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 las estaciones de su anillo. Los informes de configuración son informes de nuevo supervisor activo e informes de vecino ascendente activo más próximo (NAUN).

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. Equivale a *conmutación del circuito*.

conmutación de paquetes. (1) Proceso consistente en direccionar y transferir datos por medio de paquetes dirigidos de manera que un canal esté ocupado durante la transmisión de un paquete solamente. Cuando se completa la transmisión, el canal queda disponible para la transferencia de otros paquetes. (I) (2) Sinónimo de *funcionamiento en modalidad de paquete*. Véase también *conmutación del circuito*.

conmutación del circuito. (1) Proceso que, a petición, conecta dos o más equipos terminales de datos (DTE) y permite el uso exclusivo de un circuito de datos entre ellos hasta que se libera la conexión. (I) (A) (2) Sinónimo de *conmutación de la línea*.

conmutación del enlace de datos (DLSw). Método para transportar protocolos de red que utilizan el tipo 2 de control de enlace lógico (LLC) de IEEE 802.2. SNA y NetBIOS son ejemplos de protocolos que utilizan el tipo 2 de LLC. Véase también *encapsulación* y *simulación*.

consola remota. Estación que ejecuta OS/2, TCP/IP y el programa Nways Switch Resource Control remoto. Puede conectarse con cualquier estación de soporte de red para realizar operaciones en Nways Switch y darle servicio técnico remotamente.

La conexión puede ser mediante:

- Una línea conmutada que utilice un módem

Cualquier estación de soporte de red puede utilizarse como consola remota de otra estación de soporte de red.

control de enlace de datos (DLC). Conjunto de normas utilizado por los nodos de un enlace de datos (como, por ejemplo, un enlace de SDLC o una Red en Anillo) para efectuar un intercambio de información ordenado.

control de enlace de datos de alto nivel (HDLC). En la comunicación de datos, utilización de una serie de bits especificada para controlar enlaces de datos de acuerdo con las normas internacionales respecto al HDLC: la estructura de trama de ISO 3309 y los elementos de procedimientos de ISO 4335.

control de enlace lógico (LLC). Subcapa de LAN de control de enlace de datos (DLC) que proporciona dos tipos de operaciones de DLC para el intercambio ordenado de información. El primer tipo es el servicio sin conexiones, que permite enviar y recibir información sin establecer un enlace. La subcapa de LLC no efectúa recuperación de errores ni control del flujo para el servicio sin conexiones. El segundo tipo es el servicio orientado a las conexiones, que requiere el establecimiento de un enlace antes del intercambio de información. El servicio orientado a las conexiones proporciona transferencia de información en secuencia, control del flujo y recuperación de errores.

control de la vía de acceso (PC). Función que direcciona unidades de mensajes entre las unidades de red accesibles de la red y proporciona las vías de acceso entre éstas. Convierte las unidades básicas de información (BIU) del control de transmisión (posiblemente segmentándolas) en unidades de información de vía de acceso (PIU) e intercambia unidades básicas de transmisión que contienen una o más PIU con el control de enlace de datos. El control de la vía de acceso difiere según el tipo de nodo: algunos nodos (los nodos APPN, por ejemplo) utilizan identificadores de sesión generados localmente para el direccionamiento y otros (los nodos de subárea) utilizan direcciones de red para el direccionamiento.

control del acceso al medio (MAC). En las LAN, subcapa de la capa de control de enlace de datos que da soporte a funciones dependientes del medio y utiliza los servicios de la capa física para proporcionar servicios a la subcapa de control de enlace lógico (LLC). La subcapa del MAC incluye el método para determinar cuándo un dispositivo tiene acceso al medio de transmisión.

control del flujo. (1) En SNA, proceso consistente en gestionar la velocidad a la que pasa el tráfico de datos entre los componentes de la red. La finalidad del control del flujo es optimizar la velocidad del flujo de unidades de mensajes con la congestión mínima de la red; es decir, ni desbordar los almacenamientos intermedios del receptor o de nodos de direccionamiento intermedio ni dejar al receptor esperando más unidades de mensajes. (2) Véase también *ritmo*.

Control síncrono de enlace de datos (SDLC). (1) Disciplina que se ajusta a los subconjuntos de los Advanced Data Communication Control Procedures (ADCCP) del American National Standards Institute (ANSI) y del High-level Data Link Control (HDLC) de la organización internacional para la normalización, y está destinada a la gestión de la transferencia síncrona de información serie por bit de código transparente sobre una conexión de enlace. Los intercambios de transmisiones pueden ser dúplex o semi-dúplex sobre enlaces conmutados o no conmutados. La configuración de la conexión de enlace puede ser de punto a punto, de multipunto o de bucle. (I) (2) Compárese con *comunicación síncrona en binario (BSC)*.

correlación. Proceso consistente en convertir datos que el emisor transmite con un formato 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.

Datagram Delivery Protocol (DDP). En redes AppleTalk, protocolo que proporciona conectividad de red por medio de un servicio de entrega de socket a socket sin conexiones de la capa de internet.

datagrama. (1) En la conmutación de paquetes, paquete individual e independiente de otros paquetes que contiene información suficiente para el direccionamiento desde el equipo terminal de datos (DTE) de origen al DTE de destino sin apoyarse en intercambios anteriores entre los DTE y la red. (I) (2) En TCP/IP, unidad básica de información que pasa a través del entorno de Internet. Un datagrama contiene direcciones de origen y de destino junto con los datos. Un datagrama de Internet Protocol (IP) está compuesto

por una cabecera de IP seguida de los datos de capa de transporte. (3) Véase también *paquete* y *segmento*.

datagrama de IP. En el conjunto de protocolos de Internet, unidad básica de información transmitida a través de una internet. Contiene direcciones de origen y de destino, datos de usuario e información de control, como, por ejemplo, la longitud del datagrama, la suma de comprobación de cabecera y distintivos que indican si el datagrama puede fragmentarse o si se ha fragmentado.

DCE preparado. En la norma EIA 232, señal que indica al equipo terminal de datos (DTE) que el equipo de terminación de circuito de datos (DCE) local está conectado al canal de comunicaciones y se encuentra preparado para enviar datos. Sinónimo de *aparato de datos preparado (DSR)*.

DECnet. Arquitectura de red que define el funcionamiento de una familia de módulos de software, bases de datos y componentes de hardware que se utilizan normalmente con el fin de conectar entre sí sistemas Digital Equipment Corporation para el compartimiento de recursos, cálculo distribuido o configuración de sistemas remotos. Las implementaciones de la red DECnet siguen el modelo Digital Network Architecture (DNA).

detección (de condición de excepción). En Simple Network Management Protocol (SNMP), mensaje enviado por un nodo gestionado (la función de agente) a una estación de gestión para informarle de una condición de excepción.

detección de colisión. En el acceso múltiple con detección de portadora y detección de colisión (CSMA/CD), señal que indica que dos o más estaciones están transmitiendo simultáneamente.

detección de portadora. En una red de área local, actividad continua de una estación de datos para detectar si otra estación está transmitiendo. (T)

detector de portadora. Equivale a *detector de señal de línea recibida (RLSD)*.

detector de portadora de datos (DCD). Equivale a *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 de *detector de portadora* y *detector de portadora de datos (DCD)*.

determinación de problemas. Proceso consistente en determinar el origen de un problema; por ejemplo, un componente de un programa, una anomalía en una máquina, recursos de telecomunicaciones, programas o equipos instalados por el contratista o por el usuario, una anomalía del entorno, como, por ejemplo, pérdida de alimentación, o un error del usuario.

difusión. (1) Transmisión de los mismos datos a todos los destinos. (T) (2) Transmisión simultánea de datos a más de un destino. (3) Compárese con *multidifusión*.

digital. (1) Perteneciente a datos compuestos por dígitos. (T) (2) Perteneciente a datos con formato de dígitos. (A) (3) Compárese con *analógico*.

Digital Network Architecture (DNA). Modelo para todas las implementaciones de hardware y software DECnet.

dirección. En la comunicación de datos, código exclusivo asignado a cada dispositivo, estación de trabajo o usuario conectado a una red.

dirección administrada localmente. En una red de área local, dirección de adaptador que el usuario puede asignar para alterar temporalmente la dirección administrada universalmente. Compárese con *dirección administrada universalmente*.

dirección administrada universalmente. En una red de área local, dirección codificada de forma permanente en un adaptador en el momento de la fabricación. Todas las direcciones administradas universalmente son exclusivas. Compárese con *dirección administrada localmente*.

dirección canónica. En las LAN, formato de IEEE 802.1 de la transmisión de direcciones del control del acceso al medio (MAC) para adaptadores de Red en Anillo y Ethernet. En el formato canónico, el bit menos significativo (situado más a la derecha) de cada byte de dirección se transmite en primer lugar. Compárese con *dirección no canónica*.

dirección de difusión. En comunicaciones, dirección de estación (ocho números 1) reservada como dirección común a todas las estaciones de un enlace. Sinónimo de *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 en el documento RFC 791, que contiene las especificaciones del protocolo IP, estándar 5. 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*.

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 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 generador. 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 generador. El direccionador generador debe configurarse inicialmente por medio de la herramienta configuradora. Compárese con *direccionador no generador*.

direccionador limítrofe. En comunicaciones de Internet, direccionador que está situado en el borde de un sistema autónomo y que se comunica con un direccionador que está situado en el borde de un sistema autónomo diferente.

direccionador no generador. En redes AppleTalk, direccionador que obtiene información del rango de números de red y de la lista de zonas de un direccionador generador conectado a la misma red.

direccionador troncal. (1) Direccionador utilizado para transmitir datos entre áreas. (2) Direccionador de una serie que se utiliza para interconectar redes de manera que formen una internet mayor.

direccionamiento. (1) Asignación de la vía de acceso mediante la cual un mensaje va a alcanzar su destino. (2) En SNA, reenvío de una unidad de mensaje por una vía de acceso determinada a través de una red tal como lo determinan los parámetros contenidos en la unidad de mensaje, como, por ejemplo, la dirección de red de destino de una cabecera de transmisión.

direccionamiento. En la comunicación de datos, manera que tiene una estación de seleccionar la estación a la que va a enviar datos.

direccionamiento de alto rendimiento (HPR). Adición para la arquitectura Advanced Peer-to-Peer Networking (APPN) que mejora el rendimiento y la fiabilidad del direccionamiento de datos, especialmente en la utilización de enlaces de gran velocidad.

direccionamiento de 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 averiguadas en lugar de las rutas configuradas estáticamente durante la inicialización.

direccionamiento en 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 intraárea. En comunicaciones de Internet, direccionamiento de datos dentro de un área.

direcciones MAC arbitrarias (AMA). En la arquitectura DECnet, esquema de direcciones utilizado por DECnet Phase IV-Prime que da soporte a direcciones administradas universalmente y direcciones administradas localmente.

directorio. Tabla de identificadores y referencias para los elementos de datos correspondientes. (I) (A)

dispositivo. Aparato mecánico, eléctrico o electrónico con un fin específico.

dominio. (1) Parte de una red de 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.

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 OSPF (Open Shortest Path First), interfaz punto a punto que conecta direccionadores limítrofes separados por un área de tránsito no troncal. Puesto que los direccionadores de área forman parte de la red troncal OSPF, el enlace virtual conecta la red troncal. Los enlaces virtuales garantizan que la red troncal OSPF no se vuelva discontinua.

equipo de terminación de circuito de datos (DCE). En una estación de datos, equipo que proporciona la conversión de señal y la codificación entre el equipo terminal de datos (DTE) y la línea. (I)

Notas:

1. El DCE puede ser un equipo independiente o parte integral del DTE o del equipo intermedio.
2. Un DCE puede realizar otras funciones que normalmente se llevan a cabo al final de red de la línea.

equipo terminal de datos (DTE). Parte de una estación de datos que funciona como origen y/o destino de datos. (I) (A)

esfera de control (SOC). Conjunto de dominios de punto de control servidos por un solo punto focal de servicios de gestión.

estación. Punto de entrada o salida de un sistema que utiliza recursos de telecomunicaciones; por ejemplo, uno o más sistemas, terminales, dispositivos y programas asociados de una ubicación determinada que pueden enviar o recibir datos sobre una línea de telecomunicaciones.

estación de configuración Nways Switch. Estación de OS/2 dedicada que ejecuta una versión autónoma de la herramienta Nways Switch Configuration Tool (NCT). Se utiliza para generar una base de datos de configuración de red y debe instalarse como consola remota.

estación de enlace. (1) Componentes de hardware y software de un nodo que representan una conexión con un nodo adyacente sobre un enlace específico. Por ejemplo, si el nodo A es el extremo primario de una línea multipunto que se conecta con tres nodos adyacentes, el nodo A tendrá tres estaciones de enlace que representarán las conexiones con los nodos adyacentes. (2) Véase también *estación de enlace adyacente (ALS)*.

estación de gestión. En comunicaciones de Internet, sistema responsable de la gestión de toda una red o de parte de la misma. La estación de gestión se comunica con agentes de gestión de red que residen en el nodo gestionado por medio de un protocolo de gestión de red, como, por ejemplo, Simple Network Management Protocol (SNMP).

estación de gestión de red. En el protocolo Simple Network Management Protocol (SNMP), estación que ejecuta programas de aplicación de gestión que supervisan y controlan elementos de red.

estación de soporte de red. Procesador utilizado para realizar operaciones en Nways Switch y darle servicio técnico localmente. Lo utilizan el administrador o el personal de servicio encargados de Nways Switch.

estado de los enlaces. En los protocolos de direccionamiento, información anunciada sobre las interfaces utilizables y los vecinos a los que se puede llegar de un direccionador o una red. 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 de ***telecopia.***

File Transfer Protocol (FTP). En el conjunto de protocolos de Internet, protocolo de capa de aplicación que utiliza servicios de TCP y Telnet para transferir archivos de datos generales entre máquinas o sistemas principales.

fluctuación. (1) Variaciones no acumulativas a corto plazo de los instantes significativos de una señal digital respecto a sus posiciones ideales en el tiempo. (2) Variaciones no deseadas de una señal digital transmitida. (3) Variaciones en el retardo de la red.

formato decimal con puntos. Representación sintáctica de un entero de 32 bits que consta de cuatro números de 8 bits escritos en base 10 con puntos que los separan. Se utiliza para representar direcciones IP.

fragmentación. (1) Proceso consistente en dividir un datagrama en partes más pequeñas, o fragmentos, para que se ajuste a las posibilidades del medio físico por el que se va a transmitir. (2) Véase también *segmentación*.

fragmento. Véase *fragmentación*.

Frame Relay. (1) Norma de interfaz que describe el límite entre el equipo de un usuario y una red de paquetes rápidos. En los sistemas Frame-Relay, se eliminan las tramas defectuosas; la recuperación se produce de extremo a extremo en lugar de efectuarse salto a salto. (2) Técnica derivada de la norma de canal D de red digital de servicios integrados (RDSI). Supone que las conexiones son fiables y prescinde de la actividad general de control y detección de errores en la red.

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 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.

funcionamiento en modalidad de paquete. Equivale a *conmutación de paquetes*.

G

gestión de red. Proceso consistente en planificar, organizar y controlar un proceso de datos o sistema de información orientado a las comunicaciones.

gestor de red. Programa o grupo de programas que se utiliza para supervisar y gestionar una red así como para diagnosticar los problemas de la misma.

grupo de transmisión (TG). (1) Conexión entre nodos adyacentes que se identifica mediante un número de grupo de transmisión. (2) En una red de subárea, enlace o grupo de enlaces entre nodos adyacentes. Cuando un grupo de transmisión está compuesto por un grupo de enlaces, los enlaces se ven como un solo enlace lógico y el grupo de transmisión se denomina *grupo de transmisión multienlace (MLTG)*. Un *grupo de transmisión multienlace de mezcla de medios (MMMLTG)* contiene enlaces de diferentes tipos de medios (por ejemplo, Red en Anillo, SDLC conmutado, SDLC no conmutado y enlaces Frame-Relay). (3) En una red APPN, enlace entre nodos adyacentes. (4) Véase también *grupos de transmisión paralelo*.

grupos de transmisión paralelo. Diversos grupos de transmisión entre nodos adyacentes, teniendo cada grupo un número de grupo de transmisión distinto.

H

Hello. Protocolo utilizado por un grupo de direccionadores que cooperan y se apoyan entre sí para poder descubrir rutas de retardo mínimo.

heurístico. Perteneciente a métodos exploratorios para la resolución de problemas en los que se descubren soluciones mediante una evaluación del progreso realizada respecto al resultado final.

histéresis. Cantidad que indica cuánto debe cambiar la temperatura una vez pasado el umbral del establecimiento de alerta y antes de que se elimine la condición de alerta.

horizonte dividido. Técnica destinada a minimizar el tiempo para conseguir la convergencia en la red. Un direccionador registra la interfaz sobre la que ha recibido una ruta en particular y no propaga su información sobre la ruta otra vez sobre la misma interfaz.

I

identificación de intercambio (XID). Tipo específico de unidad básica de enlace que se utiliza para la comunicación de características de nodo y enlace entre nodos adyacentes. Los XID se intercambian entre estaciones de enlace antes de la activación del enlace y durante la misma para establecer y negociar las características de enlace y nodo, y después de la activación del enlace para comunicar los cambios de estas características.

identificador de conexión de enlace de datos (DLCI). Identificador numérico de un subpuerto Frame-Relay o segmento de PVC en una red Frame-Relay. Cada subpuerto de un puerto Frame-Relay individual tiene un DLCI exclusivo. La tabla siguiente, extraída de la norma T1.618 del American National Standards Institute (ANSI) y la norma Q.922 de la Comisión Consultiva de la telefonía y telegrafía internacionales (ITU-T/CCITT), indica las funciones asociadas con determinados valores de DLCI:

Valores de DLCI	Función
0	Señalización de canal de entrada
1–15	Se reserva
16–991	Se asigna utilizando procedimientos de conexión de Frame-Relay
992–1007	Gestión de capa 2 de servicio portador de Frame-Relay
1008–1022	Se reserva
1023	Gestión de capa de canal de entrada

identificador de puente. Campo de 8 bytes que se utiliza en un protocolo de árbol de extensión 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.

Instituto Nacional de Normalización de los Estados Unidos (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)

Integrated Digital Network Exchange (IDNX). Procesador que integra aplicaciones a base de voz, datos e imágenes. También gestiona los recursos de transmisión y se conecta a multiplexores y sistemas de soporte de gestión de redes. Permite la integración de equipos de diferentes proveedores.

intercalación. (1) Alternancia de dos o más operaciones o funciones por medio del uso superpuesto de un programa de utilidad informático. (2) En transmisión de datos, alternancia de los paquetes de una corriente de datos con los de otra.

intercambio de conmutaciones de datos (DSE). Equipo instalado en una ubicación individual para proporcionar funciones de conmutación, como, por ejemplo, conmutación del circuito, conmutación de mensajes y conmutación de paquetes. (I)

interconexión de sistemas abiertos (OSI). (1) Interconexión de sistemas abiertos que sigue las normas de la organización internacional para la 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.

línea tronco. Línea de gran velocidad que conecta dos Nways Switch. Puede ser un cable coaxial, un cable de fibra u ondas de radio, por ejemplo, y puede alquilarse en empresas de telecomunicación.

local. (1) Perteneciente a un dispositivo al que se accede directamente sin utilizar una línea de telecomunicaciones. (2) Compárese con *remoto*. (3) Equivale a *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 de *máscara de subred* y *máscara de subred (grupo de nodos)*.

máscara de subred. Equivale a *máscara de dirección*.

máscara de subred (grupo de nodos). Equivale a *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.

modulación en código de pulsaciones (PCM). Norma adoptada para la digitalización de una señal de voz analógica. En la PCM, se realiza un muestreo de la voz a una velocidad de ocho kHz y cada muestra se codifica en una trama de 8 bits.

módulo. (1) Perteneciente a un módulo matemático; por ejemplo, 9 equivale a 4 módulo 5. (2) Véase también *módulo (diferencia)*.

módulo. En Nways Switch, unidad de hardware funcional empaquetada que contiene tarjetas lógicas, conectores y luces. Los módulos se utilizan para empaquetar adaptadores, acopladores de interfaz de línea, extensiones de servidor de voz y otros componentes. Todos los módulos pueden ***conectarse en caliente*** en los subbastidores lógicos.

módulo (diferencia). Número, como por ejemplo un entero positivo, de una relación que divide la diferencia entre dos números relacionados sin dejar un resto; por ejemplo, 9 y 4 tienen un módulo de 5 (9 - 4 = 5; 4 - 9 = -5; y 5 divide tanto 5 como -5 sin dejar un resto).

multiplexación de la división del tiempo (TDM). Véase ***canalización***.

N

Name Binding Protocol (NBP). En redes AppleTalk, protocolo que proporciona la función de conversión de nombre a partir del nombre (serie) de 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 de *nivel de enlace de datos*. Véase *nivel de enlace*.

nodo. (1) En una red, punto donde una o más unidades funcionales conectan canales o circuitos de datos. (I) (2) Cualquier dispositivo conectado a una red que transmite y recibe datos.

nodo Advanced Peer-to-Peer Networking (APPN). Nodo de red APPN o nodo final APPN.

nodo de destino. Nodo al que se envían datos o una petición.

nodo de esfera de control (SOC). Nodo que está incluido directamente en la esfera de control de un punto focal. Un nodo de SOC ha intercambiado elementos de habilitación de los servicios de gestión con su punto focal. Un nodo final APPN puede ser un nodo de SOC si da soporte a la función de intercambio de elementos de habilitación de los servicios de gestión.

nodo de red (NN). Véase *nodo de red Advanced Peer-to-Peer Networking (APPN)*.

nodo de red Advanced Peer-to-Peer Networking (APPN). Nodo que ofrece un amplio rango de servicios de usuario final y que puede proporcionar lo siguiente:

- servicios de directorios distribuidos, incluido el registro de los recursos del dominio con un servidor de directorios central
- Intercambios de bases de datos de topología con otros nodos de red APPN, lo que permite que los nodos de red de la red seleccionen las rutas óptimas para sesiones de LU-LU basándose en las clases de servicio solicitadas
- Servicios de sesiones para los nodos finales clientes y las LU locales
- Servicios de direccionamiento intermedio de una red APPN

nodo de red APPN. Véase *nodo de red Advanced Peer-to-Peer Networking (APPN)*.

nodo de red de entrada baja (LEN). Nodo que proporciona un rango de servicios de usuario final, se conecta directamente con otros nodos utilizando protocolos de igual a igual y hace derivar servicios de red de un nodo de red APPN adyacente implícitamente, es decir, sin el uso directo de sesiones de CP-CP.

nodo final (EN). (1) Véase *nodo final Advanced Peer-to-Peer Networking (APPN)* y *nodo final de red de entrada baja (LEN)*. (2) En comunicaciones, nodo que se conecta frecuentemente a un solo enlace de datos y no puede realizar funciones de direccionamiento intermedio.

nodo final Advanced Peer-to-Peer Networking (APPN). Nodo que proporciona un amplio rango de servicios de usuario final y da soporte a las sesiones entre su punto de control (CP) local y el CP de un nodo de red adyacente. Utiliza estas sesiones con el fin de registrar dinámicamente sus recursos con el CP adyacente (su servidor de nodos de red) para enviar y recibir peticiones de búsqueda en directorios y obtener servicios de gestión. Un nodo final APPN también puede conectarse a una red de subárea como nodo periférico o a otros nodos finales.

nodo final de red de entrada baja (LEN). Nodo LEN que recibe servicios de red de un nodo de red APPN adyacente.

nodo intermedio. Nodo que está al final de más de una rama. (T)

nodos adyacentes. Dos nodos conectados conjuntamente por una vía de acceso, como mínimo, que no conecta ningún otro nodo. (T)

nombre de comunidad. En el protocolo Simple Network Management Protocol (SNMP), serie de octetos que identifica a una comunidad.

nombre de dominio. En el conjunto de protocolos de Internet, nombre de un sistema principal. Un nombre de dominio está compuesto por una secuencia de subnombres separados por un carácter delimitador. Por ejemplo, si el nombre de dominio calificado al completo (FQDN) de un sistema principal es `ralvm7.vnet.ibm.com`, cada uno de los siguientes es un nombre de dominio:

- `ralvm7.vnet.ibm.com`
- `vnet.ibm.com`
- `ibm.com`

notación de sintaxis de abstracción 1 (ASN.1). Método de Interconexión de Sistemas Abiertos (OSI) para la sintaxis de abstracción que se especifica en las normas siguientes:

- ITU-T recomendación X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T recomendación X.680 (1994) | ISO/IEC 8824-1: 1994

Véase también *normas básicas de codificación (BER)*.

número de puerto. En comunicaciones de Internet, identificación de una entidad de aplicación para el servicio de transporte.

número de secuencia. En comunicaciones, número asignado a una trama o paquete en particular para controlar el flujo de la transmisión y la recepción de datos.

número de sistema autónomo. En TCP/IP, número asignado a un sistema autónomo por la misma autorización central que también asigna direcciones IP. El número de sistema autónomo hace posible que los algoritmos de direccionamiento automatizado distingan los sistemas autónomos.

Nways Switch. Sinónimo de IBM 2220 Nways BroadBand Switch.

O

objeto de la MIB. Equivale a *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 de 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 en 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.

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 oel 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, signifi-

cados 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 de *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 direccionamiento en 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.

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 extensión 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 extensión. 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 de *socket*.

puerto de destino. Adaptador asíncrono de 8 puertos que sirve de punto de conexión con un servicio serie.

punto de acceso a servicios (SAP). (1) En la arquitectura interconexión de sistemas abiertos (OSI), punto en el que una entidad de una capa proporciona los servicios de esta capa a una entidad de la capa superior más próxima. (T) (2) Punto lógico que queda disponible mediante un adaptador y donde puede recibirse y

transmitirse información. Muchos enlaces pueden terminar en un solo punto de acceso a servicios.

punto de acceso a servicios de destino (DSAP). En SNA y TCP/IP, dirección lógica que permite que un sistema direccione datos desde un dispositivo remoto al soporte de comunicaciones correspondiente. Compárese con *punto de acceso a servicios de origen (SSAP)*.

punto de acceso a servicios de origen (SSAP). En SNA y TCP/IP, dirección lógica que permite que un sistema envíe datos a un dispositivo remoto desde el soporte de comunicaciones correspondiente. Compárese con *punto de acceso a servicios de destino (DSAP)*.

punto de control (CP). (1) Componente de un nodo APPN o LEN que gestiona los recursos de dicho nodo. En un nodo APPN, el CP puede dedicarse a establecer sesiones de CP-CP con otros nodos APPN. En un nodo de red APPN, el CP también proporciona servicios a nodos finales adyacentes de la red APPN. (2) Componente de un nodo que gestiona los recursos de dicho nodo y, opcionalmente, proporciona servicios a otros nodos de la red. Pueden citarse como ejemplos el punto de control de servicios del sistema (SSCP) de un nodo de subárea de tipo 5, el punto de control de nodo de red (NNCP) de un nodo de red APPN y el punto de control de nodo final (ENCP) de un nodo final APPN o LEN. Un SSCP y un NNCP pueden proporcionar servicios a otros nodos.

punto de control de servicios del sistema (SSCP). Componente de una red de subárea destinado a gestionar la configuración, coordinar las peticiones del operador de red y las de determinación de problemas y proporcionar servicios de directorios además de otros servicios de sesiones para los usuarios de la red. Diversos SSCP, cooperando como iguales entre sí, pueden dividir la red en dominios de control y tener, cada uno de los SSCP, una relación de control jerárquica con las unidades físicas y las unidades lógicas de su propio dominio.

punto de entrada (EP). En SNA, nodo de tipo 2.0, tipo 2.1, tipo 4 otipo 5 que proporciona soporte de gestión de redes distribuidas. Envía datos de gestión de redes sobre sí mismo y los recursos que controla a un punto focal para el proceso centralizado, y recibe y ejecuta los mandatos iniciados por el punto focal para gestionar y controlar sus recursos.

R

rastreo. (1) Registro de la ejecución de un programa de sistema. Muestra las secuencias en que se han ejecutado las instrucciones. (A) (2) Para los enlaces de datos, registro de las tramas y bytes transmitidos o recibidos.

recepción no preparada (RNR). En comunicaciones, mandato o respuesta de enlace de datos que indica una condición temporal de incapacidad para aceptar tramas de entrada.

reconfiguración dinámica (DR). Proceso consistente en cambiar la configuración de una red (las PU y LU periféricas) sin regenerar las tablas de configuración al completo ni desactivar el nodo principal afectado.

recurso. En Nways Switch, elemento de hardware o entidad lógica creados por Control Program. Por ejemplo, los adaptadores, LIC y líneas son recursos físicos. Los puntos de control y conexiones son recursos lógicos.

red. (1) Configuración de software y dispositivos de proceso de datos conectados para el intercambio de información. (2) Grupo de nodos y los enlaces que los interconectan.

red Advanced Peer-to-Peer Networking (APPN). Conjunto de nodos de red interconectados y sus nodos finales clientes.

red APPN. Véase *red Advanced Peer-to-Peer Networking (APPN)*.

red de área amplia (WAN). (1) Red que proporciona servicios de comunicación a un área geográfica mayor que la servida por una red de área local o una red de área metropolitana, y que puede utilizar o proporcionar recursos públicos de comunicación. (T) (2) Red de comunicación de datos diseñada para servir a un área de cientos o miles de kilómetros; por ejemplo, las redes públicas y privadas de conmutación de paquetes y las redes telefónicas nacionales. (3) Compárese con *red de área local (LAN)* y *red de área metropolitana (MAN)*.

red de área local (LAN). (1) Red de sistema ubicada en el lugar de un usuario dentro de un área geográfica limitada. La comunicación dentro de una red de área local no está sujeta a reglamentos externos; no obstante, la comunicación más allá del límite de una LAN puede estar sujeta a alguna forma de reglamento. (T) (2) Red en la que un conjunto de dispositivos están conectados entre sí para la comunicación y que puede conectarse a una red mayor. (3) Véase también *Ethernet* y *Red en Anillo*. (4) Compárese con *red de área metropolitana (MAN)* y *red de área amplia (WAN)*.

red de área metropolitana (MAN). Red formada por la interconexión de dos o más redes que puede funcionar a una velocidad mayor que éstas, puede atravesar límites administrativos y puede utilizar diversos métodos de acceso. (T) Compárese con *red de área local (LAN)* y *red de área amplia (WAN)*.

red de clase A. En comunicaciones de Internet, red en la que el bit situado más a la izquierda (más significativo) de la dirección IP está establecido en 0 y el 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 igual a igual (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.

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) Red 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 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 óptica síncrona (SONET). Norma de los EE.UU. para la transmisión de información digital sobre interfaces ópticas. Está estrechamente relacionada con la recomendación sobre la jerarquía digital síncrona (SDH).

red 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 de no retorno 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 ***no retorno 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) Equivale a *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 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 de *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). LBS envía estas estadísticas a los gestores de LAN correspondientes mediante LAN Reporting Mechanism (LRM).

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.

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) Equivale a *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 de *subred*.

subsistema. Sistema secundario o subordinado que a menudo puede funcionar de manera independiente o asíncrona respecto a un sistema de control. (T)

suma de comprobación. (1) Suma de un grupo de datos que se asocia con el grupo y se utiliza con fines de comprobación. (T) (2) En la detección de errores, función de todos los bits de un bloque. Si las sumas grabadas y las calculadas no coinciden, se indica que hay un error. (3) En un disquete, datos grabados en un sector con fines de detección de errores; una suma de comprobación calculada que no coincide con la suma de comprobación de los datos grabados en el sector indica que hay un sector anómalo. Los datos son numéricos u otras series de caracteres consideradas numéricas con el fin de calcular la suma de comprobación.

supervisor. (1) Dispositivo que observa y registra actividades seleccionadas en un sistema de proceso de datos para el análisis. Sus usos posibles son para indicar cualquier desviación significativa de la norma o para determinar los niveles de utilización de unidades funcionales en particular. (T) (2) Software o hardware que observa, supervisa, controla o verifica operaciones de un sistema. (A) (3) Función necesaria para iniciar la transmisión de una señal del anillo y para proporcionar recuperación de errores de software en el caso de que se pierdan señales, tramas en circulación u otras dificultades. La posibilidad está presente en todas las estaciones de anillo.

supervisor activo. En una Red en Anillo, función realizada en cualquier momento por una estación de anillo que inicia la transmisión de señales y proporciona recursos de recuperación de errores de señales. Cualquier adaptador activo del anillo tiene la posibilidad de proporcionar la función de supervisor activo si falla el supervisor activo actual.

SYNTAX. En el protocolo Simple Network Management Protocol (SNMP), cláusula del módulo de la MIB que define la estructura de datos abstracta correspondiente a un objeto gestionado.

Systems Network Architecture (SNA). Descripción de la estructura lógica, formatos, protocolos y secuencias operativas para la transmisión de unidades de información a través de las redes y para el control de la configuración y del funcionamiento de las mismas. La estructura de capas de SNA permite que los orígenes y destinos finales de la información, es decir, los usuarios, sean independientes de los servicios y recursos de red SNA específicos utilizados para el intercambio de información y que no se vean afectados por dichos servicios y recursos.

T

T1. En los Estados Unidos, línea de acceso público de 1,544 Mbps. Está disponible en veinticuatro canales de 64 Kbps. La versión europea (E1) transmite a 2,048 Mbps.

tabla de correlación de direcciones (AMT). Tabla mantenida en el direccionador AppleTalk que proporciona la correlación actual de las direcciones de nodo con las direcciones de hardware.

tabla de direccionamiento. Conjunto de rutas utilizadas para dirigir el reenvío de datagramas o para establecer una conexión. La información pasa entre direccionadores para identificar la topología de red y la factibilidad de los destinos.

tabla de información de zonas (ZIT). Listado de números de red y sus correlaciones con los nombres de zonas asociadas de internet. Cada direccionador de internet mantiene este listado en una internet AppleTalk.

TCP/IP. (1) Transmission Control Protocol/Internet Protocol. (2) Protocolo de interconexión de sistemas basado en Ethernet/de tipo UNIX que desarrolló originalmente el Departamento de Defensa de los EE.UU. TCP/IP facilitó ARPANET (Advanced Research Projects

Agency Network), una red de paquetes conmutados para la investigación en que la capa 4 era TCP y la capa 3, IP.

Telnet. En el conjunto de protocolos de Internet, protocolo que proporciona un servicio de conexión de terminales remotos. Permite que los usuarios de un sistema principal se conecten con un sistema principal remoto e interactúen como usuarios de terminal conectado directamente de este sistema principal.

terminal de datos preparado (DTR). Señal para el módem que se utiliza con el protocolo EIA 232.

tiempo de espera excedido. (1) Suceso que se produce al final de un período predeterminado de tiempo que ha empezado al aparecer otro suceso especificado. (I) (2) Intervalo de tiempo asignado para que tengan lugar determinadas operaciones; por ejemplo, la respuesta a un sondeo o direccionamiento antes de que se interrumpa el funcionamiento del sistema y deba reiniciarse.

topología. En comunicaciones, ordenación física o lógica de los nodos de una red, especialmente las relaciones de un nodo con otro nodo y los enlaces entre los mismos.

trama. (1) En la arquitectura interconexión de sistemas abiertos, estructura de datos perteneciente a un área particular de información y compuesta por ranuras que pueden aceptar los valores de atributos específicos y de las que pueden deducirse inferencias mediante conexiones apropiadas de procedimiento. (T) (2) Unidad de transmisión en algunas redes de área local, incluida la Red en Anillo de IBM. Incluye delimitadores, caracteres de control, información y caracteres de comprobación. (3) En SDLC, vehículo para cada mandato, cada respuesta y toda información transmitida con procedimientos de SDLC.

trama de información (I). Trama de formato I que se utiliza para la transferencia de información numerada.

trama exploradora. Véase *paquete explorador*.

trama I. Trama de información.

transceptor (transmisor-receptor). En las LAN, dispositivo físico que conecta una interfaz de sistema principal a una red de área local, como, por ejemplo, Ethernet. Los transceptores de Ethernet contienen elementos electrónicos que aplican señales al cable y que detectan colisiones.

Transmission Control Protocol (TCP). Protocolo de comunicaciones utilizado en Internet y en cualquier red que siga las normas del Departamento de Defensa de los EE.UU. para el protocolo interredes. TCP proporciona un protocolo fiable de sistema principal a sistema principal entre sistemas principales en redes de comunicaciones de paquetes conmutados y en los sistemas interconectados de dichas redes. Utiliza Internet Protocol (IP) como protocolo subyacente.

Transmission Control Protocol/Internet Protocol (TCP/IP). Conjunto de protocolos de comunicaciones que dan soporte a funciones de conectividad de igual a igual para redes de área local y amplia.

transporte de vector de gestión de red (NMVT). Unidad de petición/respuesta (RU) de servicios de gestión que fluye sobre una sesión activa entre servicios de gestión de unidad física y servicios de gestión de punto de control (sesión de SSCP-PU).

troncal. (1) En una configuración de anillo de diversos puentes de una red de área local, enlace de gran velocidad al que se conectan los anillos por medio de puentes o direccionadores. Un troncal puede configurarse como bus o como anillo. (2) En una red de área amplia, enlace de gran velocidad al que se conectan nodos o intercambios de conmutaciones de datos (DSE).

U

umbral. (1) En programas de puente de IBM, valor asignado al número máximo de tramas que no se reenvían por un puente debido a errores antes de que se cuente una aparición de “umbral sobrepasado” y se indique en los programas de gestión de red. (2) Valor inicial a partir del cual un contador disminuye hasta 0 o valor hasta el que aumenta o disminuye un contador a partir de un valor inicial.

unidad básica de transmisión (BTU). En SNA, unidad de datos e información de control que pasa entre los componentes del control de la vía de acceso. Una BTU puede constar de una o más unidades de información de vía de acceso (PIU).

unidad de datos de protocolo (PDU). Unidad de datos especificada en un protocolo de una capa determinada y compuesta por información de control de protocolo de esta capa además de, posiblemente, datos de usuario de esta capa. (T)

unidad de datos de protocolo de control de enlace lógico (LLC). Unidad de información intercambiada entre estaciones de enlace de diferentes nodos. La unidad de datos de protocolo de LLC contiene un punto de acceso a servicios de destino (DSAP), un punto de acceso a servicios de origen (SSAP), un campo de control y datos de usuario.

unidad de información de vía de acceso (PIU). Unidad de mensaje compuesta por una sola cabecera de transmisión (TH) o por una TH seguida de una unidad básica de información (BIU) o un segmento de BIU.

unidad de mensaje de soporte de diversos dominios (MDS-MU). Unidad de mensaje utilizada en el soporte de diversos dominios que contiene datos de servicios de gestión y fluye entre conjuntos de funciones de servicios de gestión sobre las sesiones de LU-LU y CP-CP. Esta unidad de mensaje, así como los datos reales de servicios de gestión que contiene, tiene el formato de corriente de datos general (GDS). Véase también *unidad de servicios de gestión de punto de control (CP-MSU)*, *unidad de servicios de gestión (MSU)* y *transporte de vector de gestión de red (NMVT)*.

unidad de red accesible (NAU). Unidad lógica (LU), unidad física (PU), punto de control (CP) o punto de control de servicios del sistema (SSCP). Es el origen o el destino de la información transmitida por la red de control de la vía de acceso. Sinónimo de *unidad de red direccionable*.

unidad de red direccionable (NAU). Equivale a *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

V.24. En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito de datos (DCE).

V.25. En la comunicación de datos, especificación de la CCITT que define el equipo de respuesta automática y el equipo de llamada automática paralelo de la red telefónica general conmutada, incluidos los procedimientos de inhabilitación de dispositivos controlados con eco para las llamadas establecidas de manera manual y automática.

V.34. Recomendación del ITU-T para la comunicación por módem sobre canales estándares de transmisión de voz de 33,6 Kbps (y más lentos) disponibles comercialmente.

V.35. En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito de datos (DCE) con varias velocidades de datos.

V.36. En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito

de datos (DCE) con las velocidades de 48, 56, 64 ó 72 kilobits por segundo.

valor por omisión. Perteneciente a un atributo, condición, valor u opción que se supone cuando no se especifica nada de forma explícita. (I)

variable de corriente de datos general (GDS). Tipo de subestructura de RU que va precedida de un identificador y un campo de longitud e incluye datos de aplicación, datos de control de usuario o datos de control definidos según SNA.

variable de la MIB. En el protocolo Simple Network Management Protocol (SNMP), instancia específica de datos definida en un módulo de la MIB. Sinónimo de *objeto de la MIB*.

vecino. Direccionador de una subred común designado por un administrador de red para recibir información de direccionamiento.

vecino ascendente activo más próximo (NAUN). En la Red en Anillo de IBM, estación que envía datos directamente a una estación determinada del anillo.

vector de control de selección de ruta (RSCV). Vector de control que describe una ruta de una red APPN. El RSCV consta de una secuencia ordenada de vectores de control que identifican los TG y nodos que componen la vía de acceso de un nodo de origen a un nodo de destino.

velocidad de información comprometida. Cantidad máxima de datos en bits que la red acepta entregar.

velocidad de transferencia de datos. Promedio de los bits, caracteres o bloques por unidad de tiempo que pasan entre los miembros del equipo correspondiente en un sistema de transmisión de datos. (I)

Notas:

1. La velocidad se expresa en bits, caracteres o bloques por segundo, minuto u hora.
2. Debe indicarse el equipo correspondiente; por ejemplo, módems, equipo intermedio u origen y destino.

versión. Programa bajo licencia independiente que a menudo tiene un nuevo código o una nueva función significativos.

vertimiento múltiple. (1) Transmisión de los mismos datos a un grupo seleccionado de destinos. (T) (2) Forma especial de difusión en que se entregan copias de un paquete a un subconjunto de todos los destinos posibles solamente.

vía de acceso. (1) En una red, cualquier ruta entre dos nodos cualesquiera. Una vía de acceso puede incluir más de una rama. (T) (2) Serie de componentes de red de transporte (control de la vía de acceso y control de enlace de datos) por los que pasa la información intercambiada entre dos unidades de red accesibles. Véase también *ruta explícita (ER)*, *extensión de ruta* y *ruta virtual (VR)*.

VINES. VIrtual NEtworking System.

VIrtual NEtworking System (VINES). Sistema operativo de red y software de red de Banyan Systems, Inc. En una red VINES, la función de enlace virtual permite que todos los dispositivos y servicios aparenten estar conectados directamente entre sí cuando en realidad pueden encontrarse a miles de kilómetros de distancia. Véase también *StreetTalk*.

vista de la MIB. En el protocolo Simple Network Management Protocol (SNMP), conjunto de objetos gestionados, conocidos por el agente, que es visible en una comunidad en particular.

vuelco. (1) Datos que se han volcado. (T) (2) Copiar el contenido de la totalidad o de parte del almacenamiento virtual con el fin de reunir información de errores.

X

X.21. recomendación de la comisión consultiva de la telefonía y telegrafía internacionales (CCITT) relativa a una interfaz de fines generales entre un equipo terminal de datos y un equipo de terminación de circuito de datos para las operaciones síncronas en una red pública de datos.

X.25. (1) recomendación de la comisión consultiva de la telefonía y telegrafía internacionales (CCITT) relativa a la interfaz entre un equipo terminal de datos y las redes de datos de paquetes conmutados. (2) Véase también *conmutación de paquetes*.

Xerox Network Systems (XNS). Conjunto de protocolos de internet desarrollados por Xerox Corporation. Aunque es similar a los protocolos TCP/IP, XNS utiliza unos formatos de paquete y una terminología diferentes. Véase también *Internetwork Packet Exchange (IPX)*.

Z

zona. En redes AppleTalk, subconjunto de nodos dentro de una internet.

Zone Information Protocol (ZIP). En redes AppleTalk, protocolo que proporciona un servicio de gestión de zonas manteniendo una correlación de los nombres de zonas y los números de red de la internet en la capa de sesión.

Índice

A

B

C

CH

D

E

F

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

Hoja de Comentarios

Access Integration Services
Configuración y supervisión de protocolos
Manual de consulta, volumen 1
Versión 3.4

Número de Publicación SC10-3438-01

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
SC10-3438-01

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

SC10-3438-01

Corte o Doble
Por la Línea

SC10-3438-01