Nways Multiprotocol Routing Services

Utilización y configuración de las características Versión 3.4

SC10-3429-01

Nways Multiprotocol Routing Services

Utilización y configuración de las características Versión 3.4

SC10-3429-01

Nota

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

Segunda edición (octubre de 1999)

Este manual es la traducción del original inglés *Nways Multiprotocol Routing Services Using and Configuring Features Version 3.4 (SC30-3992-02)*

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

Puede solicitar las publicaciones a través del representante de IBM o la sucursal de IBM de su localidad. No hay stock de publicaciones en la dirección que se indica más abajo.

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

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

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

http://www.networking.ibm.com

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

Contenido

Figuras

Tablas

Avisos

IBM puede no ofrecer en otros países los productos, los servicios o las características que se describen en este documento. Consulte con su representante local de IBM para obtener información sobre los productos y servicios disponibles actualmente en su área. Las referencias a programas, productos o servicios de IBM no pretenden establecer o implicar que sólo puedan utilizarse los productos, programas o servicios de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual IBM. Sin embargo, la evaluación y verificación del funcionamiento de cualquier producto, programa o servicio no IBM son responsabilidad del usuario.

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

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
EE.UU.

Para realizar consultas sobre licencias relacionadas con información de doble byte (DBCS), póngase en contacto con el Departamento de propiedad intelectual de IBM de su país o envíe las consultas por escrito a:

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

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país donde tales disposiciones sean incoherentes con la legislación local: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN “TAL CUAL” SIN GARANTÍAS DE NINGUNA CLASE, YA SEAN EXPRESAS O IMPLÍCITAS, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UN PROPÓSITO DETERMINADO. Algunos países no permiten la renuncia de las garantías expresas o implícitas en determinadas transacciones, por consiguiente, puede que esta declaración no se aplique a su caso.

Marcas registradas

Los términos siguientes son marcas registradas de International Business Machines Corporation en EE.UU. y/o en otros países:

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

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

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

NetView es una marca registrada de Tivoli Systems, Inc. en EE.UU. y/o en otros países.

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

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

Prefacio

Este manual contiene la información que necesitará para utilizar la interfaz de usuario del direccionador para la configuración y utilización de las características instaladas en el dispositivo Nways. Un dispositivo Nways específico puede no dar soporte a todas las características que se describen en este manual. Si una característica es específica del dispositivo, se le informa de ello con:

- Una nota en el capítulo o sección pertinente
- Una sección en el prefacio que lista las características y los dispositivos que las soportan

Este manual soporta el IBM 2210 y hace referencia al mismo como “direccionador” o “dispositivo.” Los ejemplos del manual representan la configuración de un IBM 2210, pero la salida real que se ve puede variar. Utilice los ejemplos como directriz sobre lo que puede ver mientras configura el dispositivo.

Quién debe leer este manual

Este manual está dirigido a las personas que instalan o gestionan redes de sistemas. A pesar de que la experiencia en hardware y software de redes de sistemas es útil, no es necesario tener experiencia en programación para utilizar el software de protocolos.

Obtención de información adicional

Puede que se efectúen cambios en la documentación después de que se impriman los manuales. Si hay información adicional disponible o si es necesario efectuar cambios después de que se hayan impreso los manuales, encontrará los cambios en un archivo (llamado README) en el CD-ROM. Podrá visualizar el archivo con un editor de texto de código ASCII.

Acerca del software

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

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

  El código base viene instalado de fábrica en el 2210.
- El Programa de configuración Programa de configuración para IBM Nways Multiprotocol Routing Services (denominado en este manual: *Programa de con-*

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

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

También puede obtener el Programa de configuración para IBM Nways Multiprotocol Routing Services en la página de presentación del soporte técnico de red de IBM. Consulte el manual *Guía del usuario del Programa de configuración para Nways Multiprotocol and Access Services,*, GC10-3430, para conocer los directorios y la dirección del 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 soporte de almacenamiento toma por omisión el valor de UTP a menos que se especifique STP.

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

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

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

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

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

   Nombre de archivo: *nombarchivo.ext*

Publicaciones de IBM 2210 Nways Multiprotocol Router

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

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

Actualizaciones y correcciones de la información: Para mantenerse informado de los cambios técnicos, las aclaraciones y los arreglos implementados después de que se imprimieran los manuales, consulte la página de presentación de redes de IBM en:

`http://www.networking.ibm.com`

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

Gestión de red y operaciones

SC10-3427 *Guía del usuario de software*

En este manual se explica cómo:

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

SC10-3429 *Utilización y configuración de las características*

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

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

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

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

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

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

Configuración

Ayuda en línea

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

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

Este manual describe cómo utilizar el Programa de configuración.

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

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

Seguridad

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

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

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

Planificación e instalación

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

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

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

Diagnósticos y mantenimiento

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

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

Resumen de cambios para la biblioteca de software de IBM 2210

La lista siguiente se aplica a los cambios efectuados en el software en la Versión 3 Release 4:

- Mejoras de Frame Relay:
  - Soporte de Frame Handler (FH) nuevo
  - Regulación de PU para manejar ráfagas de tráfico para dar soporte a los controladores 3745

  - Nuevo tipo de interfaz (subinterfaz de Frame Relay) para permitir interfaces virtuales en la misma interfaz física
  - Soporte IP innumerable

- Mejoras de VPN:
  - Mejoras de CPE:
    - La información de política de los servidores LDAP se almacena localmente.
    - Configuración rápida de política.
    - Comprobación de coherencia de política.
    - Ahora la información de política puede recuperarse de los servidores LDAP dentro de un dominio administrativo.
    - Ping de túnel IPSec.
  - Mejoras de IP:
    - Mejoras de direccionamiento de voz:
      - Compresión de cabeceras IP en PPP (RFC 2507, 2508, 2509)
      - Interposición de tráfico de voz entre paquetes de datos fragmentados en PPP multienlace
      - Interposición de tráfico de voz entre paquetes de datos fragmentados en Frame Relay
      - Desviación del cifrado y de la compresión de paquetes PPP o Frame Relay para el tráfico de voz
    - Dirección de bucle de retorno IP

      Este soporte permite a los usuarios definir direcciones IP en una interfaz especial para soportar requisitos de TN3270 Gateway, Network Dispatcher e IPSec.
    - IPv6
      - Se proporciona una función de direccionamiento entre dominios (BGP4+) para IPv6 que soporta información de direccionamiento y direcciones IPv6 y utiliza TCP6 para transporte.
      - Se soporta el tráfico IPv6 a través de la emulación de LAN ethernet ATM sin encapsulación o túneles.
    - Múltiples vías de acceso de reenvío

      El direccionamiento IP puede utilizar hasta cuatro rutas estáticas de coste igual para soportar múltiples enlaces paralelos en una dirección y máscara determinadas.
    - Agregación de rutas IP
    - Mejoras de multidistribución:
      - Modalidad PIM-DM (Protocol Independent Multicast-Dense Mode) para IPv4.
      - Ahora los administradores de red pueden controlar el flujo de datos de multidistribución IP que entran y salen de las redes utilizando filtros de tráfico de entrada y salida.
    - NSSA (Not-so-stubby area) (Área no tan llena)

      OSPF soporta NSSA (not-so-stubby area) según se define en RFC 1587 y ahora se soporta el último borrador de Internet.
    - RED (Random Early Detection) (Detección temprana aleatoria)

- Mejoras de políticas de servicios diferenciales
- Mejoras de VRRP:
  - Se puede utilizar la dirección MAC de hardware en lugar de una dirección MAC virtual para identificar una pasarela redundante; esto puede proporcionar una mejora del rendimiento.
  - Cuando hay más de un candidato de reserva disponible, se pueden configurar opciones de apropiación.
  - Para seleccionar el direccionador IP maestro, se pueden utilizar criterios adicionales, por ejemplo la interfaz de red o la ruta disponible, para soportar funciones que no son IP.

- Interfaz alternativa de marcación a petición para redireccionamiento WAN
- Mejoras en TN3270
  - Selección de LU
  - Equilibrado de carga de agrupación de LU
  - Desconexión de Talk 5 de sesiones TN3270
  - Información de informes adicional
  - Soporte de direcciones 1 y 255
- Mejoras de Network Dispatcher
  - Anuncio de direcciones de cluster de Network Dispatcher mediante protocolos de direccionamiento
  - Un nuevo SSL Advisor
- Soporte de DLSw SDLC PU1
- Soporte de encapsulación de Ethernet para ambas ethernet tipo II (valor por omisión) y 802.3 simultáneamente en la misma interfaz
- Mejoras de DHCP:
  - Copia de seguridad de disco fijo para información de alquiler
  - Soporte de múltiples direcciones IP para interfaces DHCP
  - Soporte de alquiler corto
- Mejoras de RADIUS
  - Escalabilidad de Radius
  - Inicio de sesión de último recurso
- Escalabilidad de L2TP
- Mejora de Thin Server

  Conexión a un servidor alternativo o un servidor maestro de reserva
- Mejoras de recuperación de archivo de servicio

Cómo obtener ayuda

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

Cómo salir de un entorno de nivel inferior

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

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

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

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

Utilización de las características Reserva de ancho de banda y Puesta en cola según prioridad

Este capítulo describe las características Sistema de reserva de ancho de banda y Puesta en cola según prioridad, que están actualmente disponibles para las interfaces Frame Relay y PPP. El capítulo incluye las secciones siguientes:

Sistema de reserva de ancho de banda

El Sistema de reserva de ancho de banda (BRS) le permite decidir qué paquetes deben excluirse cuando la demanda (tráfico) excede al suministro (productividad) en una conexión de red. Cuando la utilización de ancho de banda alcanza el 100%, el BRS determina el tráfico que debe desactivarse en la configuración.

La reserva de ancho de banda "reserva" el ancho de banda de transmisión para las clases de tráfico especificadas. Cada clase tiene asignado un porcentaje mínimo de ancho de banda de la conexión. Vea la Figura 1 en la página 2 y la Figura 2 en la página 2.

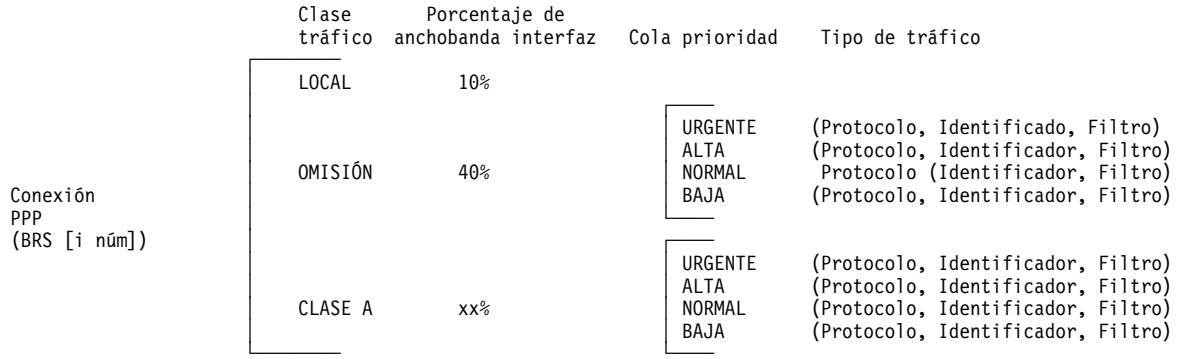
En interfaces PPP, el usuario define las clases de tráfico (clases t) y se asigna a cada clase de tráfico un porcentaje de ancho de banda de la interfaz PPP. Existen como mínimo dos clases de tráfico:

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

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

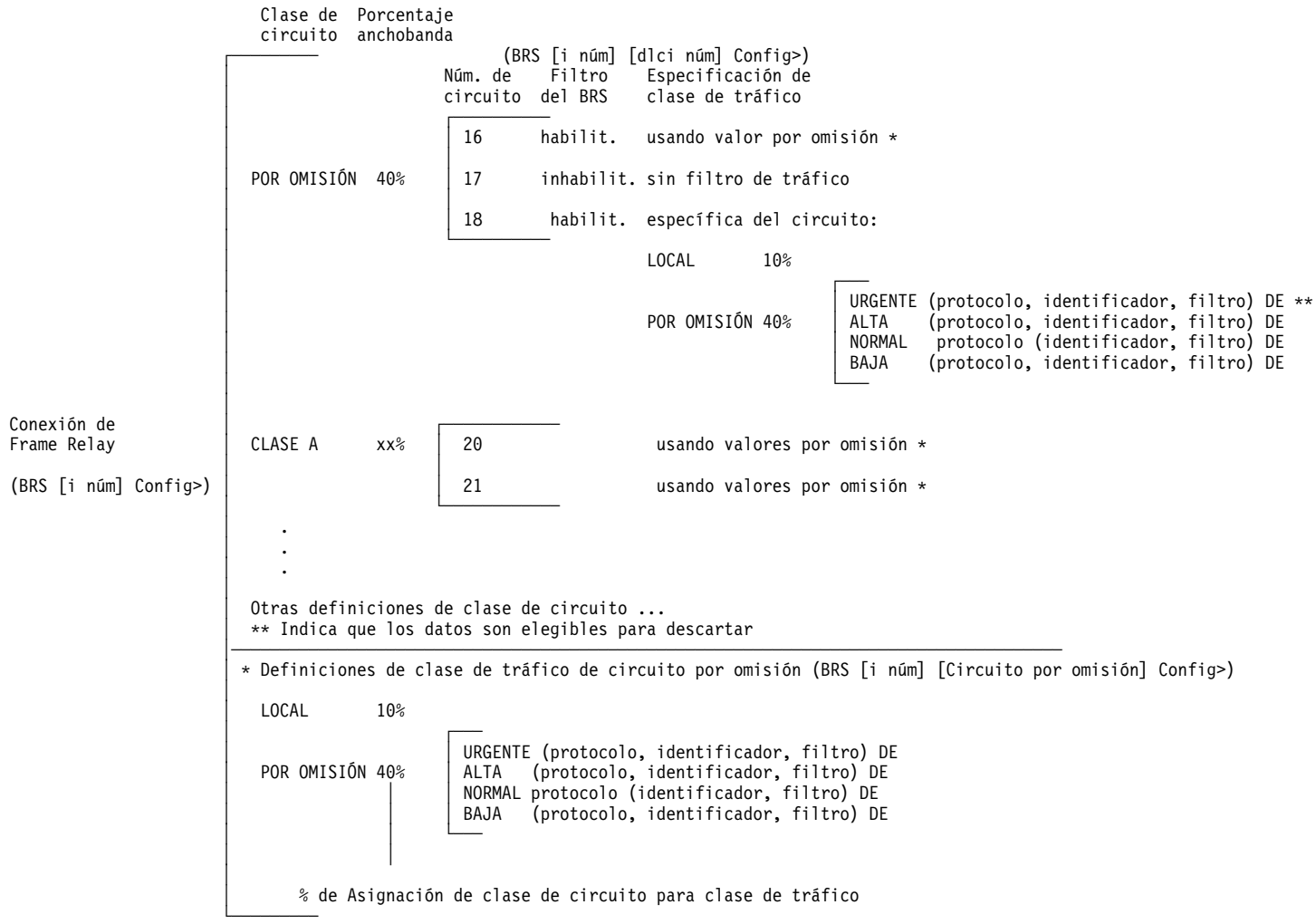
En interfaces Frame Relay, el usuario define las clases de circuito (clases c) y se asigna a cada clase de circuito un porcentaje de ancho de banda de la interfaz Frame Relay. Existe cómo mínimo una clase de circuito: la clase de circuito DEFAULT a la que se asignan inicialmente todos los circuitos. Se pueden crear clases de circuito adicionales y asignar circuitos a estas clases c. En cada circuito de Frame Relay, el usuario puede definir clases de tráfico (clases t) y a cada clase de tráfico se le asigna un porcentaje de ancho banda del circuito de Frame Relay. El soporte de clase de tráfico para los circuitos de Frame Relay es similar al soporte de clase de tráfico para interfaces PPP. Vea la Figura 2 en la página 2 para obtener información sobre las Relaciones entre la clase de circuito y la clase de tráfico de Frame Relay.

Utilización de BRS y Puesta en cola según prioridad



Nota: Inicialmente todos los protocolos se asignan a la cola de prioridad NORMAL de la clase de tráfico DEFAULT. El usuario puede asignar un protocolo, filtro o identificador a una cola de prioridad dentro de una clase de tráfico.

Figura 1. Relación entre la clase de tráfico y la cola de prioridad de clase de tráfico BRS de PPP



Nota: Inicialmente todos los protocolos se asignan a la cola de prioridad NORMAL de la clase de tráfico DEFAULT. El usuario puede asignar un protocolo, filtro o identificador a una cola de prioridad dentro de una clase de tráfico.

Figura 2. Relación entre la clase de circuito y la clase de tráfico BRS de Frame Relay

Estos porcentajes reservados son una *porción* mínima del ancho de banda para la conexión de la red. Si una red funciona al máximo, los mensajes de cada clase

sólo se pueden transmitir cuando utilizan el ancho de banda configurado para la clase. En este caso, las transmisiones adicionales se retienen hasta que efectúan las transmisiones del ancho de banda. En el caso de una ruta de tráfico ligera, una corriente de paquetes puede utilizar un ancho de banda que supere el mínimo permitido hasta el 100% si no hay más tráfico.

La reserva de ancho de banda es realmente una *protección*. En general, un dispositivo no debe intentar utilizar más del 100% de su velocidad de línea. Si lo hace, probablemente necesitará una línea de más velocidad. Sin embargo, el carácter "inesperadamente denso" del tráfico puede hacer que la velocidad de transmisión solicitada exceda el 100% durante un período breve de tiempo. En estos casos, se habilita la reserva de ancho de banda y, de este modo, se asegura la entrega del tráfico con la prioridad más alta (es decir, no se descarta).

La reserva de ancho de banda se ejecuta con los tipos de conexión siguientes:

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

Reserva de ancho de banda en Frame Relay

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

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

Cuando el BRS recibe un paquete desde Frame Relay, se utilizan las clases c y las clases t configuradas para determinar cuándo se va a transmitir dicho paquete. El BRS pone en cola el paquete de acuerdo con los siguientes criterios: clase c, circuito, clase t y prioridad dentro de la clase t. La clase c a la que se ha asignado el circuito se pone en una cola de clases c y la cola de clases c se clasifica según un algoritmo de cola asignado adecuado. Dentro de una clase c, los circuitos que tienen paquetes para transmitir son atendidos en modalidad rotatoria. Las clases t dentro de cada clase c también se clasifican de acuerdo con un algoritmo de cola asignado adecuado. Dentro de la clase t, los paquetes todavía se ponen en cola según su prioridad (urgente, alta, normal o baja).

Un paquete se elimina de la cola y se transmite cuando cumple todos los criterios siguientes:

1. Es el paquete siguiente en la clase c siguiente
2. Es el paquete siguiente en el circuito siguiente dentro de la clase c
3. Es uno de los paquetes de la clase c siguiente para dicha clase c
4. Es el paquete siguiente en el grupo de prioridad siguiente para dicha clase t

Cuando se habilita la interfaz y uno o más circuitos para el BRS y no se configura ninguna clase c ni clase t, todos los circuitos se asignan a una clase c llamada *por omisión*. Con esta configuración, tan solo existirá la clase c por omisión en la cola

de clases c y cada uno de los circuitos de la clase c con paquetes para transmitir se manejará siguiendo un orden rotatorio. Si desea que el BRS haga esto, deje todos los circuitos en la clase c por omisión y no cree ninguna otra clase de circuito.

Los circuitos huérfanos y los circuitos que no tengan el BRS explícitamente habilitado utilizan este entorno de cola BRS por omisión en todas las situaciones. El BRS los asigna a la clase c por omisión.

Para configurar el BRS, debe seguir este orden:

1. Habilitar el BRS en la interfaz.
2. Habilitar los BRS en los circuitos y añadir las clases c.
3. Asignar los circuitos a las clases c.
4. Si lo desea, definir clases t para cada una de las clases c.

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

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

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

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

Soporte de puesta en cola

Con la reserva de banda en Frame Relay, cada circuito puede poner en cola las tramas mientras están en estado de congestión, incluso para interfaces y circuitos que no están habilitados para reserva de banda.

Elegibilidad de descartar

La red de Frame Relay puede descartar la transmisión de los datos que exceden la CIR en un PVC. El bit DE lo puede establecer el direccionador para indicar que parte del tráfico debe considerarse como elegible para descartar. Si es apropiado, la red Frame Relay descartará las tramas marcadas como elegibles para descartar, lo cual hace posible que las tramas que no están marcadas como elegibles para descartar puedan transmitirse en la red. Cuando se asigna un protocolo, filtro o identificador a una clase de tráfico, puede especificar si el tráfico del protocolo, el filtro o el identificador es elegible para descartar. Consulte el apartado “Assign” en la página 33 para obtener más información sobre cómo configurar el tráfico como elegible para descartar. El tráfico de voz (identificado mediante el protocolo VOFR) debe configurarse siempre como **no** elegible para descartar.

Definiciones de circuito por omisión para el manejo de clases de tráfico

Las interfaces de Frame Relay pueden tener definidos varios circuitos. En lugar de tener que configurar completamente definiciones de clase de tráfico para cada circuito, el BRS le permite definir un conjunto por omisión de clases de tráfico y asignaciones de protocolo, filtro e identificadores llamado definiciones de circuito por omisión que puede ser utilizado por cualquier circuito en la interfaz. Cuando el BRS está inicialmente habilitado en un circuito, el circuito está inicializado para utilizar definiciones de circuito por omisión. Si un circuito no puede utilizar las definiciones de circuito por omisión para el manejo de clases de tráfico, puede crear definiciones específicas del circuito utilizando los mandatos **add-class**, **change-class**, **assign**, **deassign**, **tag** y **untag**.

Si un circuito utiliza definiciones específicas del circuito y desea que en lugar de ello utilice las definiciones de circuito por omisión, puede utilizar el mandato **use-circuit-defaults** en el indicador de mandatos del BRS del circuito.

Las definiciones de circuito por omisión para el manejo de clases de tráfico se definen utilizando el mandato **set-circuit-defaults** en el indicador de mandatos del BRS de la interfaz Frame Relay. Este mandato le lleva a un indicador de mandatos por omisión BRS circuit donde puede añadir, cambiar y suprimir clases de tráfico, asignar y desasignar protocolos, filtros e identificadores y crear identificadores BRS. Los cambios en las definiciones de circuito por omisión para las clases de tráfico dan como resultado actualizaciones dinámicas en el manejo de clases de tráfico para todos los circuitos que utilizan definiciones de circuito por omisión.

Configuración del BRS para voz a través de Frame Relay

Las tramas de voz se pueden transportar a través de circuitos dedicados. En esta situación, habilite el BRS en la interfaz y en los circuitos y acepte los valores por omisión en los circuitos asociados con la voz. Puede que desee crear múltiples clases c y asignar los circuitos dedicados a voz a una clase c que esté asociada con un porcentaje de ancho de banda grande y asignar los circuitos asociados con datos a una clase de circuito asociada con un porcentaje menor de ancho de banda.

Si la voz y otro tipo de tráfico se transporta a través de los mismos circuitos, habilite el BRS en la interfaz y los circuitos. Si desea que todos los circuitos sean atendidos en modalidad rotatoria sin favorecer uno o más circuitos puede decidir no crear clases c adicionales aparte de la clase c por omisión. A continuación, para cada circuito a través del cual se van a transportar voz y datos, es recomendable crear una clase t con el mandato **create-super-class** y asignar el tráfico VOFR a esta clase. Además cree tantas clases t como sea necesario y asigne otros tipos de tráfico a estas clases t. Esta configuración le ayudará a asegurarse de que el tráfico de voz tenga prioridad sobre cualquier otro tráfico y que las tramas de voz no segmentadas se puedan intercalar entre segmentos de datos fragmentados si la fragmentación está habilitada. Se recomienda habilitar la fragmentación en la interfaz Frame Relay si va a enviar voz y datos a través de la misma interfaz. La fragmentación dará como resultado tramas más pequeñas y, de este modo, existirá un retardo menor entre tramas de voz consecutivas.

Consulte el mandato **enable fragmentation** en el capítulo “Configuración y supervisión de las interfaces de Frame Relay” en la publicación *Guía del usuario de software* para obtener más información sobre cómo habilitar la fragmentación.

Puesta en cola según prioridad

La reserva de ancho de banda asigna porcentajes de ancho de banda de conexión total para *clases* o *clases t* de tráfico especificadas, definidas por el usuario. Salvo para una clase t creada mediante el mandato **create-super-class**pubs que tiene prioridad sobre todas las demás clases t, las clases t de BRS están asociadas con un porcentaje de ancho de banda. Se pueden asignar protocolos y filtros a clases t y a colas de prioridad específicas dentro de una clase t. Con la puesta en cola según prioridad, se puede asignar un protocolo o filtro a una cola específica dentro de una clase de tráfico con valores: Una clase t de BRS es un grupo de paquetes identificado por el mismo nombre; por ejemplo, una clase llamada “ipx” para designar a todos los paquetes IPX.

Con la puesta en cola según prioridad, se puede asignar a cada clase t de ancho de banda uno de los siguientes valores de nivel de prioridad:

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

para clases de tráfico especificadas o clases t, definidas por el usuario.

Además, puede establecer el número de paquetes que esperan en la cola para cada nivel de prioridad en cada clase t de ancho de banda. El mandato **queue-length** de BRS establece el número máximo de almacenamientos intermedios de salida que pueden ponerse en cola en cada cola de prioridad de BRS y el número máximo de almacenamientos intermedios de salida que pueden ponerse en cola en cada cola de prioridad de BRS cuando los almacenamientos intermedios de entrada del direccionador son insuficientes. Puede establecer longitudes de cola de prioridad tanto para PPP como para Frame Relay.

Atención: Si establece valores de longitud de cola demasiado altos, puede reducir gravemente el rendimiento del direccionador.

Para el BRS, puede establecer longitudes de cola de prioridad para conexiones de la WAN PPP y Frame Relay. Consulte el apartado “Queue-length” en la página 47 para obtener una descripción del mandato **queue-length**.

Los valores de prioridad en una clase t de ancho de banda no tienen efecto sobre otras clases de ancho de banda. Ninguna clase de ancho de banda tiene prioridad sobre las otras.

Puesta en cola según prioridad sin reserva de ancho de banda

Cuando se configura la puesta en cola según prioridad sin reserva de ancho de banda, el tráfico con la prioridad más alta se transmite primero. En casos de tráfico denso con prioridad alta, los niveles de prioridad más baja se pueden pasar por alto. Sin embargo, combinando la puesta en cola según prioridad con reserva de ancho de banda, la transmisión de paquetes se puede asignar a todos los tipos de tráfico.

Configuración de clases de tráfico

Cree una clase de tráfico utilizando el mandato **add-class** y, a continuación, asignando tipos de tráfico a la clase utilizando el mandato **assign**. El tráfico se asigna a una clase de tráfico basándose en su *tipo de protocolo* o basándose en un filtro que identifica adicionalmente a un tipo específico de *tráfico de protocolo* (por ejemplo, paquetes IP SNMP).

Los tipos de protocolo soportados son:

- IP
- ARP
- DNA
- VINES
- IPX
- OSI
- VOFR
- AP2
- ASRT
- SNA/APPN-ISR
- APPN-HPR®
- HPR/IP

Filtros del BRS

Utilizando la reserva de ancho de banda, puede tratar el tráfico de un protocolo específico de modo diferente a otro tráfico que utilice el mismo tipo de protocolo. Por ejemplo, puede asignar tráfico IP SNMP a una clase de tráfico y prioridad distintas de las de otro tráfico IP. En este ejemplo, SNMP es un filtro del BRS dado que *filtra* (es decir, identifica exclusivamente) tráfico de un protocolo específico. El tráfico de protocolo IP, ASRT (puente) y APPN-HPR se puede filtrar mediante la reserva de ancho de banda. Están soportados los filtros siguientes:

- Túnel IP
- Túnel SDLC a través de IP (Retransmisión SDLC)
- Túnel BSC a través de IP (Retransmisión BSC)
- Rlogin
- Telnet
- SNA/APPN-ISR
- APPN-HPR
- SNMP
- Multidifusión IP
- DLSw
- Filtro MAC
- NetBIOS
- HPR-Red
- HPR-Alta
- HPR-Media
- HPR-Baja
- XTP
- Números de puerto o sockets TCP/UDP
- Byte de TOS
- Bit de prioridad

BRS y filtrado

En las siguientes secciones se describe cómo utilizar el BRS con varios tipos de filtrado.

Filtrado e identificadores de dirección MAC

El filtrado de Dirección de MAC se maneja mediante la acción conjunta entre la reserva de ancho de banda y el filtrado de MAC (MCF) utilizando *identificadores*. Por ejemplo, un usuario con reserva de ancho de banda puede categorizar el tráfico de puente asignándole un identificador.

El proceso de identificación se realiza creando un elemento de filtro en la consola de configuración de filtrado de MAC y, a continuación, asignando un número de identificador al mismo. Este número de identificador se utiliza para configurar clases de tráfico para todos los paquetes asociados con este identificador. Actualmente los valores de identificador deben estar dentro del rango de 1 a 64. Consulte el apartado “Utilización de filtrado de MAC” en la página 57 para obtener información adicional sobre el filtrado de MAC.

Nota: Los identificadores ***sólo*** se pueden aplicar a los paquetes puenteados. En una conexión PPP o Frame Relay, se puede asignar un máximo de cinco filtros de MAC con identificador como filtros de reserva de ancho de banda y se designan como TAG1 a TAG5. Primero se busca TAG1, después TAG2 y así sucesivamente hasta TAG5. Un único identificador de filtro MAC puede constar de cualquier número de Direcciones de MAC establecidas en la MCF.

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

Los identificadores también pueden hacer referencia a “grupos,” como en el ejemplo de Túnel IP. Los puntos finales del Túnel IP pueden pertenecer a cualquier número de grupos. Los paquetes se asignan a un grupo particular mediante la característica de identificación del filtrado de Dirección de MAC. Para obtener información adicional sobre el filtrado de MAC, consulte el apartado “Utilización de filtrado de MAC” en la página 57 y el apartado “Configuración y supervisión de Filtrado de MAC” en la página 61.

Para aplicar la reserva de ancho de banda y la puesta en cola según prioridad a paquetes con identificador:

1. Utilice los mandatos de configuración de filtrado de MAC en el indicador de mandatos `filter config>` para configurar identificadores para los paquetes que pasan a través del puente. Consulte el apartado “Utilización de filtrado de MAC” en la página 57 para obtener más información.
2. Utilice el mandato **tag** de reserva de ancho de banda para hacer referencia a un identificador para la reserva de ancho de banda.
3. Con el mandato **assign** de reserva de banda, asigne el identificador del BRS a una clase t. El mandato **assign** también le solicita una prioridad de cola dentro de dicha clase t del BRS.

Filtrado de número de puerto TCP/UDP

Puede asignar paquetes TCP/IP desde un rango de puertos TCP o UDP a una clase t y prioridad del BRS basándose en el número de puerto UDP o TCP del paquete y, opcionalmente, basándose en un socket. Puede especificar un máximo de 5 filtros de número de puerto UDP/TCP, donde los filtros especifican un número de puerto TCP o UDP individual, un rango de números de puerto TCP o UDP, o un identificador de socket. A continuación, puede asignar dicho filtro a una clase y prioridad de tráfico de BRS dentro de la clase.

Si está habilitado el filtrado de puerto UDP/TCP, el BRS busca en cada paquete TCP o UDP para ver si el número de puerto de destino o de origen coincide con uno de los números de puerto especificados para el filtrado. Además, si define una dirección IP como parte del filtro UDP/TCP del BRS y la dirección IP de destino o de origen coincide con la dirección de filtro que ha definido, el BRS asigna el paquete a la clase y prioridad de tráfico para dicho filtro de número de puerto.

Por ejemplo, puede configurar un filtro de número de puerto UDP para números de puerto UDP dentro del rango de 25 a 29 y asignar el filtro a la clase de tráfico 'A' con una prioridad 'normal'. El BRS pone en cola cualquier paquete UDP con un número de puerto de origen o de destino dentro del rango de 25 a 29 en la cola de prioridad normal para la clase de tráfico 'A'.

También puede configurar un filtro de número de puerto TCP para el número de puerto TCP 50 para la dirección IP 5.5.5.25 y asignar el filtro a la clase de tráfico 'B' con una prioridad 'urgente'. El BRS pone en cola cualquier paquete TCP cuyo número de puerto de origen o de destino sea 50 y cuya dirección IP de destino o de origen sea 5.5.5.25 en la cola de prioridad urgente para la clase de tráfico 'B'.

Filtrado de bit del TOS IPv4

Puede crear filtros que distingan entre tipos diferentes de tráfico de IP según los valores de los bits del Tipo de Servicio (TOS). Estos filtros del TOS se pueden utilizar para asignar tráfico IPv4 con valores particulares de los bits del TOS a una clase y prioridad diferentes de los otros tipos de tráfico IP. Cada filtro permite tráfico IPv4 cuyo valor de byte de TOS coincida con la definición de un filtro de TOS configurado al cual debe asignarse una clase y prioridad de tráfico exclusivas. La configuración de un filtro de TOS incluye una especificación de valor de máscara para definir qué bits dentro del byte de TOS deben coincidir, así como la especificación de valores de rango bajo y alto para los bits que entran dentro de la máscara. El mecanismo de filtrado se basa exclusivamente en valores de TOS IPv4; por lo tanto, no se basa en la identificación del tipo de protocolo IPv4 o de información de número de puerto como en la mayoría de otros filtros de IP.

Este filtro es más extensivo en su aplicación que el filtrado de prioridad de IPv4 del BRS, que solamente está relacionado con los 3 bytes más a la izquierda del byte del TOS. Cuando se combina con el soporte de control de acceso de IP para establecer los bits del TOS, el soporte de filtro de bits del TOS del BRS le permiten efectuar el filtrado para el tráfico que se envía a través de un túnel de seguridad, es decir fragmentado, o que no se puede identificar utilizando el soporte de filtro de número de puerto UDP y TCP del BRS. Además, el soporte de control de acceso de IP le permite establecer los bits del TOS para un valor definido por el usuario en lugar de tener que utilizar los valores de bits de prioridad de codificación dura para APPN y DLSw asociados con el filtrado de bits de prioridad de IPv4 del BRS.

Por lo tanto, se recomienda utilizar el soporte de control de acceso de IP y de filtro de TOS del BRS en lugar del filtrado de bits de prioridad IPv4 del BRS.

Tal como se indica en el apartado “Orden de prioridad de filtrado” en la página 12, las coincidencias de filtro de TOS se comprueban antes que los filtros de bits de prioridad IPv4 y que otros filtros específicos de IP. Las comprobaciones para las coincidencias de filtro de TOS1 a TOS5 se realizan secuencialmente, empezando por el filtro TOS1. Se puede definir un máximo de 5 filtros de TOS.

Importante: Tenga en cuenta que un paquete con un valor de TOS determinado se maneja de acuerdo con la primera definición de filtro de TOS con la que coincide el valor. Tenga cuidado al configurar los filtros para que el filtro indicado filtre un byte de TOS particular, y que no lo filtre accidentalmente un filtro con un número bajo. Consulte “Using IP” en *Utilización y configuración de las características* para obtener más información.

Utilización del proceso de bits de prioridad de IP Versión 4 para el tráfico SNA en túneles seguros y fragmentos secundarios de IP

El BRS normalmente distingue entre el tráfico TCP y UDP de IP, según sus números de puerto. Sin embargo, el BRS no puede identificar los puertos cuando el tráfico se ha encapsulado por segunda vez, como por ejemplo el tráfico de IP transportado a través de un túnel de seguridad de IP o en un fragmento UDP o TCP secundario. El proceso de bits de prioridad de IP versión 4 se ha añadido al BRS para permitir que el BRS filtre paquetes de túnel de seguridad de IP o paquetes de fragmento secundario TCP y UDP.

Nota: Se recomienda utilizar el filtrado de bits del TOS de IPv4 del BRS en lugar del proceso de bits de prioridad de IPv4. Consulte el apartado “Filtrado de bit del TOS IPv4” en la página 9 para obtener más detalles.

Cuando se direcciona tráfico APPN/HPR a través de IP, cada prioridad de transmisión de APPN-HPR (red, alta, media y baja) se correlaciona con un valor particular de los tres bits de prioridad de IP versión 4.

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

Cuando el filtrado de prioridad de IPv4 está habilitada para el BRS y los bits de prioridad en un paquete de IP coinciden con uno de los valores utilizados para el tráfico APPN/HPR, el paquete se pone en cola en la cola de prioridad de la clase t del BRS a la que se asigna la prioridad de transmisión de HPR correspondiente. Por ejemplo, si un paquete de IP tiene un valor de prioridad de `'110'b` y el filtro HPR-Red del BRS se asigna a la clase t A y al nivel de prioridad normal, el paquete se pone en cola en la cola de prioridad normal de clase t A. Si un filtro de prioridad de transmisión de HPR del BRS no está configurado, pero está configurado el filtro APPN-HPR, el paquete se pone en cola en la cola de prioridad y la clase t a la que está asignado el filtro APPN-HPR.

Los tres tipos siguientes de tráfico se correlacionan con el valor de prioridad de IPv4 '011'b:

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

Dado que varios tipos de tráfico se correlacionan con un valor, el BRS no puede distinguir entre ellos cuando está habilitado para filtrar basándose en los bits de prioridad de IPv4. Por lo tanto, cuando el BRS encuentra un paquete de IP con un valor de prioridad de '011'b, evalúa los filtros del BRS en el orden siguiente para determinar si el filtro está habilitado o no. Cuando encuentra un filtro del BRS que está configurado, el paquete se pone en la cola en la cola de prioridad y clase t a la que está asignado el filtro del BRS:

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

Si un paquete tiene uno de los valores de prioridad que filtra el BRS, pero no está configurado ninguno de los tipos de filtro del BRS aplicables, el paquete se pone en cola en la cola de prioridad y clase t del BRS a la cual se ha asignado el protocolo IP.

Cuando un cliente envía tráfico TN3270 al 2210 a través de una red de área amplia en la que está habilitado el BRS, el BRS no puede dar prioridad al tráfico desde el cliente a menos que el cliente establezca los bits de prioridad en '011'b.

Debe configurar el manejo de bits de prioridad de IPv4 en varios lugares:

1. En BRS se configura si el BRS debe filtrar o no basándose en los bits de prioridad de IPv4. Sólo efectúa este tipo de filtrado para paquetes de túnel IP seguro o paquetes de fragmento secundario TCP y UDP.
2. Cuando se configura DLSw, HPR a través de IP, y TN3270, se especifica si el 2210 debe establecer los bits de prioridad de IPv4 para los paquetes que origina para cada uno de estos tipos de protocolo.

Efectúe los tres pasos siguientes para utilizar el filtrado de bits de prioridad de IPv4:

1. Active el filtrado de prioridad de IPv4 en el BRS.
2. Configure clases t de BRS y asigne protocolos y filtros para varias categorías de tráfico SNA, del mismo modo que debe hacerse para tráfico SNA que no se transporte en un túnel IP seguro o que no esté fragmentado.
3. Habilite el valor de los bits de prioridad de IPv4 cuando configure los protocolos DLSw, HPR a través de IP, y TN3270.
4. Configure IPSec para crear un túnel de seguridad a través del cual circulará el tráfico DLSw, HPR a través de IP y TN3270.

Filtrado de SNA y APPN para tráfico puenteado

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

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

Los filtros APPN-HPR le permiten asignar tráfico de HPR que se puentea a una clase t del BRS. El tráfico de HPR se identifica como cualquier paquete puenteado con un SAP de destino o de origen de `X'04'`, `X'08'`, `X'0C'` o `X'C8'` y cuyo campo de control LLC (802.2) indica que es una trama de información no numerada (UI).

Los filtros HPR-Red, HPR-Alta, HPR-Media y HPR-Baja permiten filtrar adicionalmente el tráfico puenteado de HPR de acuerdo con la prioridad de transmisión de HPR. Por ejemplo, si desea asignar tráfico de HPR que utiliza la prioridad de transmisión de red a una clase t y prioridad y que todo el otro tráfico puenteado de HPR a una clase t o prioridad diferentes, debe asignar el filtro HPR-Red a la clase t y prioridad adecuados y utilizar el filtro APPN-HPR para asignar el resto del tráfico HPR a una clase t o prioridad diferentes.

El tráfico APPN-HPR que se direcciona a través de IP se filtra utilizando el número de puerto UDP asignado para prioridades de transmisión de HPR de red, alta, media y baja. Se utiliza un número de puerto UDP adicional para los intercambios XID. Todos los números de puerto UDP utilizados para soportar APPN-HPR a través de IP son configurables.

Si no está habilitado el APPN en un direccionador intermedio en la red IP, puede configurar números de puerto UDP para HPR a través de IP desde el indicador de mandatos `BRS Config>`. Si está habilitado el APPN en el dispositivo, el BRS utilizará los valores configurados en el indicador de mandatos `APPN Config>`.

Otros filtros pueden ayudarle a asignar tráfico. Por ejemplo, el filtro DLSw le permite asignar tráfico SNA-DLSw que se envíe a través de una conexión TCP a una clase t del BRS.

Para los filtros SNA/APPN-ISR y APPN-HPR, si desea comprobar los SAP que no sean los anteriores, cree un filtro de ventana deslizante utilizando el filtro de MAC e identifique dicho filtro. A continuación, asigne el filtro de MAC identificado a una clase t del BRS.

Orden de prioridad de filtrado

Es posible que un paquete coincida con más de un tipo de filtro del BRS. Por ejemplo, un paquete puenteado de túnel IP que contiene datos SNA puede coincidir con el filtro de túnel IP y con el filtro SNA/APPN-ISR. El orden con el que se evalúan los filtros determinan si un paquete coincide o no con un tipo de filtro del BRS es el siguiente:

1. Filtros del TOS (IP)
2. Manejo de prioridad de IPv4
3. Coincidencia de identificador de filtro de MAC para paquetes puenteados (IP/ASRT)

4. NetBIOS para puenteado (IP/ASRT)
5. SNA/APPN-ISR para puenteado (IP/ASRT)
6. HPR-Red (IP/ASRT/APPN-HPR)
7. HPR-Alta (IP/ASRT/APPN-HPR)
8. HPR-Media (IP/ASRT/APPN-HPR)
9. HPR-Baja (IP/ASRT/APPN-HPR)
10. APPN-HPR (IP/ASRT)
11. Filtros de número de puerto UDP/TCP (IP)
12. Túnel IP (IP)
13. Retransmisión SDLC/BSC (IP)
14. DLSw (IP)
15. Multidifusión (IP)
16. SNMP (IP)
17. Rlogin (IP)
18. Telnet (IP)
19. XTP (IP)

Nota: Los protocolos a los que se aplica un filtro aparecen entre paréntesis.

Configuraciones de ejemplo

Utilización de definiciones de circuito por omisión para el manejo de clases de tráfico de circuitos Frame Relay

Notas:

1 Configurar la característica BRS.
2 Habilitar el BRS en la interfaz 1.
3 Habilitar el BRS en los circuitos 16, 17, 18. Las definiciones de circuito por omisión para el manejo de clases de tráfico se utilizan para estos circuitos.
4 Acceder al menú set-circuit-defaults para definir las definiciones de circuito por omisión para el manejo de clases de tráfico.
5 Añadir clases de tráfico y asignación de protocolos y filtros a las clases de tráfico.
6 Listar y mostrar las definiciones del BRS para el circuito 16. Dado que el circuito 16 utiliza definiciones de circuito por omisión, se visualizan las clases de tráfico y asignaciones de protocolo y filtro definidas por las definiciones de circuito por omisión.
7 Cambiar circuito 17 de utilizar definiciones de circuito por omisión a utilizar definiciones específicas del circuito para el manejo de clases de tráfico creando una clase exclusiva, CIRC171. Esta clase puede tener asignados protocolos, filtros o identificadores.
8 Cambiar las definiciones de circuito por omisión de modo que cada una de las clases de tráfico DEF1 y DEF2 reserven el 10% del ancho de banda y, a continuación, mostrar que estos cambios han afectado al circuito 16 pero no al circuito 17, ya que el circuito 17 ahora utiliza definiciones específicas del circuito.
9 Modificar el circuito 17 para utilizar definiciones de circuito por omisión para el manejo de clases de tráfico en lugar de definiciones específicas del circuito.

```
t 6
 Gateway user configuration
 Config>feature brs      1
 Bandwidth Reservation User Configuration
 BRS Config>interface 1     2
 BRS [i 1]Config>enable
 Please restart router for this command to take effect.
 BRS [i 1] Config>circuit 16    3
 BRS [i 1][dlci 16] Config>enable
 Defaults are in effect for this circuit.
 Please restart router for this command to take effect.
 BRS [i 1][dlci 16] Config>exit
 BRS [i 1]Config>circuit 17
 BRS [i 1][dlci 17] Config>enable
 Defaults are in effect for this circuit.
 Please restart router for this command to take effect.
 BRS [i 1][dlci 17] Config>exit
 BRS [i 1]Config>circuit 18
 BRS [i 1][dlci 18] Config>enable
 Defaults are in effect for this circuit.
 Please restart router for this command to take effect.
 BRS [i 1][dlci 18] Config>
 *restart
 Are you sure you want to restart the gateway? (Yes or [No]): yes



 *t 6
 Gateway user configuration
 Config>feature brs
 Bandwidth Reservation User Configuration
 BRS Config>interface 1
 BRS[i 1] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 1
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 10%
 total circuit classes defined (counting one default) 1


 class DEFAULT has 10% bandwidth allocated
   the following circuits are assigned:
       16  using defaults.
       17  using defaults.
       18  using defaults.

 default class is DEFAULT
```

```
BRS [i 1] Config>?
 ENABLE
 DISABLE
 SET-CIRCUIT-DEFAULTS
 CIRCUIT
 ADD-CIRCUIT-CLASS
 DEL-CIRCUIT-CLASS
 CHANGE-CIRCUIT-CLASS
 DEFAULT-CIRCUIT-CLASS
 ASSIGN-CIRCUIT
 DEASSIGN-CIRCUIT
 QUEUE-LENGTH
 LIST
 SHOW
 CLEAR-BLOCK
 EXIT
 BRS [i 1] Config>set-circuit-defaults     4
 BRS [i 1] [circuit defaults] Config>?
 ADD-CLASS
 DEL-CLASS
 CHANGE-CLASS
 DEFAULT-CLASS
 TAG
 UNTAG
 ASSIGN
 DEASSIGN
 LIST
 EXIT
 BRS [i 1] [circuit defaults] Config>add    5
 Class name [DEFAULT]?DEF1
 Percent bandwidth to reserve [10]? 5
 BRS [i 1] [circuit defaults] Config>add
 Class name [DEFAULT]?DEF2
 Percent bandwidth to reserve [10]?5
 BRS [i 1] [circuit defaults] Config>assign ip
 Class name [DEFAULT]?DEF1
 Priority <URGENT/HIGH/NORMAL/LOW> [NORMAL]?
 Frame Relay Discard Eligible <NO/YES> [NO]?
 BRS [i 1] [circuit defaults] Config>assign asrt
 Class name [DEFAULT]? DEF2
 Priority <URGENT/HIGH/NORMAL/LOW> [NORMAL]?
 Frame Relay Discard Eligible <NO/YES> [NO]?
 BRS[i 1] [circuit defaults] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 1, default circuit
 total bandwidth allocated 60%
 total classes defined (counting one local and one default) 4


 class LOCAL has 10% bandwidth allocated
   protocols and filters cannot be assigned to this class.
```

```
class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol VOFR with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible

class DEF1 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority NORMAL is not discard eligible


class DEF2 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority NORMAL is not discard eligible

assigned tags:

default class is DEFAULT with priority NORMAL

BRS  [i 1] [circuit defaults] Config>exit
BRS  [i 1] Config>circuit 16     6
BRS  [i 1][dlci 161] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, circuit number 16 using defaults.
maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 4


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.


class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol VOFR with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible

class DEF1 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority NORMAL is not discard eligible


class DEF2 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority NORMAL is not discard eligible

assigned tags:

default class is DEFAULT with priority NORMAL
```

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

 BANDWIDTH RESERVATION currently in RAM
 interface number 1, circuit number 16 using defaults.
 maximum queue length 10, minimum queue length 3
 4 current defined classes:
   class LOCAL has 10% bandwidth allocated
   class DEFAULT has 40% bandwidth allocated
   class DEF1 has 5% bandwidth allocated
   class DEF2 has 5% bandwidth allocated

 protocol and filter assignments:

 Protocol/Filter      Class              Priority    Discard Eligible
 ---------------      -----              --------    ----------------
 IP                   DEF1                 NORMAL            NO
 ARP                  DEFAULT              NORMAL            NO
 DNA                  DEFAULT              NORMAL            NO
 VINES                DEFAULT              NORMAL            NO
 IPX                  DEFAULT              NORMAL            NO
 OSI                  DEFAULT              NORMAL            NO
 VOFR                 DEFAULT              NORMAL            NO
 AP2                  DEFAULT              NORMAL            NO
 ASRT                 DEF2                 NORMAL            NO

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

```
BRS [i 1] Config>circuit 17
 BRS [i 1] [dlci 17] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 1, circuit number 17 using defaults.
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 60%
 total classes defined (counting one local and one default) 4


 class LOCAL has 10% bandwidth allocated
   protocols and filters cannot be assigned to this class.


 class DEFAULT has 40% bandwidth allocated
   the following protocols and filters are assigned:
     protocol ARP with default priority is not discard eligible
     protocol DNA with default priority is not discard eligible
     protocol VINES with default priority is not discard eligible
     protocol IPX with default priority is not discard eligible
     protocol OSI with default priority is not discard eligible
     protocol VOFR with default priority is not discard eligible
     protocol AP2 with default priority is not discard eligible

 class DEF1 has 5% bandwidth allocated
   the following protocols and filters are assigned:
     protocol IP with priority NORMAL is not discard eligible


 class DEF2 has 5% bandwidth allocated
   the following protocols and filters are assigned:
     protocol ASRT with priority NORMAL is not discard eligible

 assigned tags:

 default class is DEFAULT with priority NORMAL

 BRS [i 1] [dlci 17] Config>add-class    7
 This circuit is currently using circuit defaults...
 Are you sure you want to override the defaults ?(Yes or [No]): yes
 Class name [DEFAULT]? CIRC171
 Percent bandwidth to reserve [10]? 5
 BRS[i 1] [dlci 17] Config>assign vines
 Class name [DEFAULT]? CIRC171
 Priority <URGENT/HIGH/NORMAL/LOW> [NORMAL]?
 Frame Relay Discard Eligible <NO/YES>[NO]?
```

```
BRS [i 1] [dlci 17] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 1, circuit number 17
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 65%
 total classes defined (counting one local and one default) 5


 class LOCAL has 10% bandwidth allocated
   protocols and filters cannot be assigned to this class.


 class DEFAULT has 40% bandwidth allocated
   the following protocols and filters are assigned:
     protocol ARP with default priority is not discard eligible
     protocol DNA with default priority is not discard eligible
     protocol IPX with default priority is not discard eligible
     protocol OSI with default priority is not discard eligible
     protocol VOFR with default priority is not discard eligible
     protocol AP2 with default priority is not discard eligible


 class DEF1 has 5% bandwidth allocated
   the following protocols and filters assigned:
     protocol IP with priority NORMAL is not discard eligible


 class DEF2 has 5% bandwidth allocated
   the following protocols and filters are assigned:
     protocol ASRT with priority NORMAL is not discard eligible


 class CIRC171 has 5% bandwidth allocated
   the following protocols and filters are assigned:
     protocol VINES with priority NORMAL is not discard eligible

 assigned tags:

 default class is DEFAULT with priority NORMAL

 BRS [i 1] [dlci 17] Config>show

 BANDWIDTH RESERVATION currently in RAM
 interface number 1, circuit number 17
 maximum queue length 10, minimum queue length 3
 5 current defined classes:
   class LOCAL has 10% bandwidth allocated
   class DEFAULT has 40% bandwidth allocated
   class DEF1 has 5% bandwidth allocated
   class DEF2 has 5% bandwidth allocated
   class CIRC171 has 5% bandwidth allocated
```

```
protocol and filter assignments:

Protocol/Filter      Class              Priority    Discard Eligible
---------------      -----              --------    ----------------
IP                   DEF1                 NORMAL             NO
ARP                  DEFAULT              NORMAL             NO
DNA                  DEFAULT              NORMAL             NO
VINES                CIRC171              NORMAL             NO
IPX                  DEFAULT              NORMAL             NO
OSI                  DEFAULT              NORMAL             NO
VOFR                 DEFAULT              NORMAL             NO
AP2                  DEFAULT              NORMAL             NO
ASRT                 DEF2                 NORMAL             NO

BRS [i 1] [dlci 17] Config>exit
BRS [i 1] Config>set-circuit-defaults
BRS [i 1] [circuit defaults] Config>change DEF1     8
Percent bandwidth to reserve [ 5]? 10
BRS [i 1] [circuit defaults] Config>change DEF2
Percent bandwidth to reserve [5]? 10
BRS [i 1] [circuit defaults] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, default circuit
total bandwidth allocated 70%
total classes defined (counting one local and one default) 4


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.


class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol VOFR with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible

class DEF1 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority NORMAL is not discard eligible


class DEF2 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority NORMAL is not discard eligible

assigned tags:

default class is DEFAULT with priority NORMAL

BRS [i 1] [circuit defaults] Config>exit
```

```
BRS [i 1] Config>circuit 16
  BRS [i 1] [dlci 16] Config>list

  BANDWIDTH RESERVATION listing from SRAM
  bandwidth reservation is enabled
  interface number 1, circuit number 16 using defaults.
  maximum queue length 10, minimum queue length 3
  total bandwidth allocated 70%
  total classes defined (counting one local and one default) 4


  class LOCAL has 10% bandwidth allocated
    protocols and filters cannot be assigned to this class.


  class DEFAULT has 40% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ARP with default priority is not discard eligible
      protocol DNA with default priority is not discard eligible
      protocol VINES with default priority is not discard eligible
      protocol IPX with default priority is not discard eligible
      protocol OSI with default priority is not discard eligible
      protocol VOFR with default priority is not discard eligible
      protocol AP2 with default priority is not discard eligible

  class DEF1 has 10% bandwidth allocated
    the following protocols and filters are assigned:
      protocol IP with priority NORMAL is not discard eligible


  class DEF2 has 10% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ASRT with priority NORMAL is not discard eligible

  assigned tags:

  default class is DEFAULT with priority NORMAL

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

```
BRS [i 1] Config>circuit 17
  BRS [i 1[ [dlci 17] Config>list

  BANDWIDTH RESERVATION listing from SRAM
  bandwidth reservation is enabled
  interface number 1, circuit number 17
  maximum queue length 10, minimum queue length 3
  total bandwidth allocated 65%
  total classes defined (counting one local and one default) 5


  class LOCAL has 10% bandwidth allocated
    protocols and filters cannot be assigned to this class.


  class DEFAULT has 40% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ARP with default priority is not discard eligible
      protocol DNA with default priority is not discard eligible
      protocol IPX with default priority is not discard eligible
      protocol OSI with default priority is not discard eligible
      protocol VOFR with default priority is not discard eligible
      protocol AP2 with default priority is not discard eligible


  class DEF1 has 5% bandwidth allocated
    the following protocols and filters are assigned:
      protocol IP with priority NORMAL is not discard eligible


  class DEF2 has 5% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ASRT with priority NORMAL is not discard eligible


  class CIRC171 has 5% bandwidth allocated
    the following protocols and filters are assigned:
      protocol VINES with priority NORMAL is not discard eligible

  assigned tags:

  default class is DEFAULT with priority NORMAL

  BRS [i 1] [dlci 17] Config>use-circuit-defaults     9
  This circuit is currently NOT using circuit defaults...
  Are you sure you want to delete current definitions and use defaults ? (Yes or
  [No]): yes
  Defaults are in effect for this circuit.
  Please restart router for this command to take effect.
  BRS [i 1] [dlci 17] Config>
  *restart
  Are you sure you want to restart the gateway? (Yes or [No] ):yes
```

```
*t 6
Gateway user configuration
Config>feature brs
Bandwidth Reservation User Configuration
BRS Config>interface 1
BRS [i 1] Config>circuit 17
BRS [i 1] [dlci 17] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, circuit number 17 using defaults.
maximum queue length 10, minimum queue length 3
total bandwidth allocated 70%
total classes defined (counting one local and one default) 4


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.


 class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol VOFR with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible

class DEF1 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority NORMAL is not discard eligible


class DEF2 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority NORMAL is not discard eligible

assigned tags:

default class is DEFAULT with priority NORMAL


BRS [i 1] [dlci 17] Config>show

BANDWIDTH RESERVATION currently in RAM
interface number 1, circuit number 17 using defaults.
maximum queue length 10, minimum queue length 3
4 current defined classes:
  class LOCAL has 10% bandwidth allocated
  class DEFAULT has 40% bandwidth allocated
  class DEF1 has 10% bandwidth allocated
  class DEF2 has 10% bandwidth allocated

protocol and filter assignments:

Protocol/Filter      Class              Priority    Discard Eligible
---------------      -----              --------    ----------------
IP                   DEF1                 NORMAL            NO
ARP                  DEFAULT              NORMAL            NO
DNA                  DEFAULT              NORMAL            NO
VINES                DEFAULT              NORMAL            NO
IPX                  DEFAULT              NORMAL            NO
OSI                  DEFAULT              NORMAL            NO
VOFR                 DEFAULT              NORMAL            NO
AP2                  DEFAULT              NORMAL            NO
ASRT                 DEF2                 NORMAL            NO

BRS [i 1] [dlci 17] Config>exit
```

Configuración y supervisión de Reserva de ancho de banda

Este capítulo describe la configuración del Sistema de reserva de ancho de banda (BRS) y de los mandatos operativos.

Este capítulo incluye las secciones siguientes:

Visión general de configuración de la Reserva de ancho de banda

Para acceder a los mandatos de configuración de reserva de ancho de banda y configurar la reserva de ancho de banda en el direccionador:

1. En el indicador de mandatos `OPCON (*)`, entre **talk 6**.
2. En el indicador de mandatos `Config>`, entre **feature brs**.
3. En el indicador de mandatos `BRS Config>`, entre **interface *número***. La interfaz debe ser una interfaz de punto a punto o Frame Relay. BRS no se puede configurar en subinterfaces Frame Relay. Consulte "Using Frame Relay Interfaces" en la publicación *Guía del usuario de software* para obtener más información.
4. En el indicador de mandatos `BRS [i 0] Config>`, entre **enable**.

   Es el nivel del indicador de mandatos de interfaz y el número de interfaz es cero en este caso. Debe repetir el paso 3 y el paso 4 para cada interfaz que configure.

   Si configura el BRS en una interfaz Frame Relay, continúe en el paso 4a:

   Si configura el BRS en cualquier otra interfaz, vaya directamente al paso 5.

   a. En el indicador de mandatos `BRS [i 0] Config>`, entre **circuit** *número*, donde *número* es el número del circuito que desea configurar.

   b. En el indicador de mandatos `BRS [i 0] [dlci 16] Config>`, entre **enable**. Es el nivel de indicador de mandatos del circuito y el número de circuito (DLCI) es 16 en este caso.

   c. En el indicador de mandatos `BRS [i 0] [dlci 16] Config>`, entre **exit** para volver al indicador de mandatos del nivel de interfaz.

   d. Repita los pasos desde el 4a hasta el 4c para cada circuito para el cual desee definir clases t del BRS.
5. Reinicie el direccionador.
6. Repita los pasos del 1 al 3 para configurar la reserva de ancho de banda para la interfaz particular que ha habilitado.
7. Si configura el BRS en una interfaz PPP, en el indicador de mandatos `BRS[i 0]Config>`, configure las clases de tráfico y asigne protocolos, filtros e identifi-

cadores a las clases de tráfico utilizando los mandatos de configuración que se listan en la Tabla 3 en la página 29. Si configura el BRS en una interfaz FR, siga los pasos del 8 al 10.

8. Si configura el BRS en una interfaz FR, puede configurar clases de circuito y asignar circuitos a clases de circuito utilizando los mandatos que se listan en la Tabla 2 en la página 28.
9. Si desea utilizar las definiciones de circuito por omisión, entre el mandato **set-circuit-defaults** en el indicador de mandatos `BRS[i 0]Config>`. Esto le conduce al indicador de mandatos `BRS[i 0][circuit defaults]` en el que puede utilizar los mandatos apropiados de la Tabla 3 en la página 29 para configurar clases de tráfico y asignar protocolos, filtros e identificadores a las clases de tráfico. Cuando acabe de definir las definiciones de circuito por omisión para el manejo de clases de tráfico, entre "exit" para volver al indicador de mandatos `BRS[i 0] Config>`.
10. Si tiene circuitos FR que no pueden utilizar definiciones de circuito por omisión para el manejo de clases de tráfico, entre **circuit** *circuito-virtual-permanente número_circuito*. Con esto se accede al indicador de mandatos de circuito donde puede utilizar los mandatos que se listan en la Tabla 3 en la página 29 para crear definiciones específicas del circuito para el manejo de clases de tráfico.

Nota: No es necesario reiniciar el direccionador para que entren en vigor los cambios efectuados en la configuración de clase t y clase c.

El mandato **talk 6 (t 6)** le permite acceder al proceso de configuración.

El mandato **feature brs** le permite acceder al proceso de configuración del BRS. Puede entrar este mandato utilizando el nombre de característica (brs) o el número (1).

El mandato **interface número** selecciona la interfaz determinada que desea configurar para la reserva de ancho de banda. Para configurar una clase del BRS primero debe utilizar el mandato **enable** para habilitar el BRS en la interfaz. En el paso 4 en la página 25, el indicador de mandatos indica que el número de interfaz seleccionado es cero.

El mandato **circuit número** selecciona el circuito en la interfaz FR en la que desea configurar las clases de tráfico de BRS. Para configurar una clase t de BRS para el circuito primero debe utilizar el mandato **enable** para habilitar el BRS en el circuito. En el paso 4b en la página 25, el indicador de mandatos indica que se ha seleccionado el circuito 16 de la interfaz 0.

Debe habilitar la reserva de ancho de banda para la interfaz y el circuito seleccionados y, a continuación, reiniciar el direccionador antes de configurar clases de circuito (sólo Frame Relay) y clases de tráfico.

Para volver al indicador de mandatos `Config>` en cualquier momento, entre el mandato **exit** en los distintos niveles de los indicadores de mandatos del BRS hasta que se encuentre en el indicador de mandatos `Config>`.

Mandatos de configuración de la Reserva de ancho de banda

Esta sección describe los mandatos de configuración de la Reserva de ancho de banda. Los mandatos que se pueden utilizar difieren según el indicador de mandatos de configuración del BRS que se visualice (`BRS Config>`, `BRS [i x] Config>` o `BRS [i x] [dlci y] Config>` o `BRS [i x] [circuit defaults] Config>`).

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

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Activate-IP-precedence-filtering	Activa el filtrado de prioridad de IPv4 del BRS de paquetes APPN y SNA que se envían a través de un túnel IP seguro o que están en fragmentos TCP o UDP secundarios. También puede configurar el valor de los bits de prioridad de IPv4 cuando configure DLSw, HPR a través de IP o TN3270.
Deactivate-IP-precedence-filtering	Desactiva el proceso de filtrado de prioridad de IPv4.
Enable-hpr-over-ip-port-numbers	Habilita la utilización del filtrado del BRS para tráfico APPN-HPR a través de IP y permite la configuración de los números de puerto UDP utilizados para identificar paquetes HPR a través de IP. **Nota:** Si el APPN está en la imagen de carga, este mandato no está soportado dado que el BRS sabe mediante APPN si se ha configurado HPR a través de IP y, si se ha configurado, conoce los números de puerto UDP que se utilizarán para los paquetes de HPR a través de IP a partir del soporte APPN.
Disable-hpr-over-ip-port-numbers	Inhabilita el filtrado del BRS del tráfico APPN-HPR a través de IP. **Nota:** Si el APPN está en la imagen de carga, este mandato no está soportado dado que el BRS conoce mediante APPN si se ha configurado o no HPR a través de IP.

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

Mandato	Función
Interface	Selecciona una interfaz en la que configurar la reserva de ancho de banda. **Nota:** Este mandato debe entrarse antes de utilizar cualquier otro mandato de configuración. Vea la Tabla 2 en la página 28 y la Tabla 3 en la página 29.
List	Lista las interfaces que pueden soportar la reserva de ancho de banda y, para cada interfaz, indica si la reserva de ancho de banda está habilitada o inhabilitada.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Tabla 2 (Página 1 de 2). Mandatos de configuración de interfaz del BRS disponibles desde el indicador de mandatos BRS [i número] Config> para interfaces Frame Relay

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Add-circuit-class	Establece el nombre de una clase c de ancho de banda y su porcentaje de ancho de banda.
Assign-circuit	Asigna un circuito especificado a la clase c de ancho de banda especificado.
Change-circuit-class	Cambia la cantidad de ancho de banda configurada para una clase c de ancho de banda.
Circuit	Accede al indicador de mandatos de nivel de circuito de BRS (`BRS [i x][dlci y] Config>`) donde se pueden utilizar los mandatos que se listan en Tabla 3 en la página 29 para configurar la Reserva de ancho de banda en el circuito de Frame Relay.
Clear-block	Borra de la SRAM los datos de configuración asociados con la interfaz actual. Se borran los datos de configuración de clase de circuito y las definiciones de circuito por omisión para el manejo de clases de tráfico.
Deassign-circuit	Restaura el circuito especificado a la clase c por omisión.
Default-circuit-class	Asigna el nombre de una clase c de ancho de banda por omisión y su porcentaje de ancho de banda de la interfaz.
Del-circuit-class	Suprime la clase c de ancho de banda especificada.
Disable	Inhabilita la reserva de ancho de banda en la interfaz.
Enable	Habilita la reserva de ancho de banda en la interfaz.
List	Visualiza las clases c y las definiciones de circuito asignadas de la SRAM.

Tabla 2 (Página 2 de 2). Mandatos de configuración de interfaz del BRS disponibles desde el indicador de mandatos BRS [i número] Config> para interfaces Frame Relay

Mandato	Función
Queue-length	Establece los valores máximo y mínimo para el número de paquetes en una cola de prioridad.
Set-circuit-defaults	Accede al indicador de mandatos `BRS [i x] [circuit defaults] Config>` de modo que se pueden utilizar los mandatos apropiados de la Tabla 3 en la página 29 para crear las definiciones de circuito por omisión para el manejo de clases de tráfico.
Show	Visualiza las clases c definidas y los circuitos asignados que existen actualmente en la SRAM.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxi.

La tabla siguiente lista los mandatos de circuito del BRS disponibles desde el indicador de mandatos `BRS [i x] Config>` para interfaces PPP, el indicador de mandatos `BRS [i x] dlci [y] Config>` para circuitos Frame Relay y desde el indicador de mandatos `BRS [i x] [circuit defaults] Config>`.

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

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxx.
Add-class	Asigna una cantidad designada de ancho de banda a una clase de tráfico definida por el usuario.
Create-super-class	Define la clase t llamada *superclase*.
Assign	Asigna un protocolo o filtro a una clase de tráfico configurada.
Change-class	Cambia la cantidad de ancho de banda configurada para una clase t de ancho de banda.
Clear-block	Borra la clase de tráfico y protocolo, el filtro y los datos de configuración de asignación de identificador de la SRAM para la interfaz PPP o el circuito Frame Relay. **Nota:** Este mandato no se puede utilizar desde el indicador de mandatos `BRS [i x] [circuit defaults] Config>`.
Deassign	Restaura la cola del paquete o filtro especificado a la clase t y prioridad por omisión.
Default-class	Establece la clase t y prioridad por omisión al valor deseado y asigna todos los protocolos no asignados a la nueva clase t por omisión.
Del-class	Suprime una clase t de ancho de banda previamente configurada.
Disable	Inhabilita la reserva de ancho de banda en la interfaz PPP o circuito Frame Relay. **Nota:** El BRS no se puede habilitar o inhabilitar desde el indicador de mandatos `BRS [i x] [circuit defaults] Config>`.

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

Mandato	Función
Enable	Habilita la reserva de ancho de banda en la interfaz PPP o circuito Frame Relay. **Nota:** El BRS no se puede habilitar o inhabilitar desde el indicador de mandatos `BRS [i x] [circuit defaults] Config>`.
List	Lista las clases t, protocolo, filtro y asignaciones de identificador configurados que se almacenan en la SRAM.
Queue-length	Establece los valores máximo y mínimo para el número de paquetes en una cola de prioridad. **Nota:** Este mandato no está soportado en el indicador de mandatos `BRS [i x] [circuit defaults] Config>`.
Show	Visualiza las clases t y protocolo, filtro y asignaciones de identificador definidas actualmente que se almacenan en la RAM. **Nota:** Este mandato no está soportado en el indicador de mandatos `BRS [i x] [circuit defaults] Config>`.
Tag	Asigna un nombre de identificador de BRS (TAG1 - TAG5) a un filtro de MAC que se ha identificado durante la configuración de la característica de Filtrado de MAC.
Untag	Elimina la relación entre un nombre de identificador del BRS (TAG1 - TAG5) y un filtro de MAC que se ha identificado durante la configuración de la característica de filtrado de MAC.
Use-circuit-defaults	Permite al usuario suprimir las definiciones específicas del circuito y utilizar las definiciones de valores por omisión para el circuito para el manejo de clases de tráfico. Este mandato solamente es válido en el indicador de mandatos `BRS [i x] dlci [y] Config>` para Frame Relay. **Nota:** Se debe reiniciar el direccionador para que los valores por omisión entren en vigor.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Utilice los mandatos apropiados para configurar la reserva de ancho de banda para el Point-to-Point protocol (PPP) y Frame Relay. Para Frame Relay, debe configurar el circuito y la interfaz de red. Para PPP, sólo debe configurar la interfaz de red.

Notas:

1. Cuando los mandatos **clear-block, disable**, **enable**, **list** y **show** se emiten desde el menú BRS interface (Interfaz del BRS), afectan o listan la información de reserva de ancho de banda configurada para la interfaz seleccionada. Cuando estos mandatos se emiten desde el menú BRS circuit (Circuito del BRS), tan solo se ve afectada o se lista la información de reserva de ancho de banda de Frame Relay configurada para el circuito virtual permanente (PVC).
2. Antes de utilizar los mandatos de reserva de ancho de banda, tenga en cuenta lo siguiente:
   - Debe utilizar el mandato **interface** para seleccionar una interfaz antes de utilizar cualquier otro mandato de configuración. (La configuración del BRS lo impone.)

- El parámetro *Class-name* es sensible a las mayúsculas y minúsculas.
- Para ver los *nombres de clase* actuales, utilice el mandato **list** o **show**.
- Una vez habilitada la reserva de ancho de banda o una interfaz o circuito, puede añadir/suprimir/cambiar las clases de circuito y tráfico y asignar circuitos o protocolos dinámicamente. Los únicos mandatos para los que es necesario reiniciar un direccionador antes de que entren en vigor son los mandatos **enable**, **disable**, **use-circuit-defaults** y **clear-block**.

3. No es necesario reiniciar el direccionador para que entren en vigor los cambios efectuados en la configuración de clase t y clase c.

Activate-IP-precedence-filtering

Utilice el mandato **activate-ip-precedence-filtering** para activar el filtrado de prioridad de IPv4 del BRS de paquetes APPN y SNA que se envían a través de un túnel IP seguro o que están en fragmentos TCP o UDP secundarios. También puede configurar el valor de los bits de prioridad de IPv4 cuando configure DLSw, HPR a través de IP o TN3270. Consulte el apartado “Utilización del proceso de bits de prioridad de IP Versión 4 para el tráfico SNA en túneles seguros y fragmentos secundarios de IP” en la página 10 para obtener información.

Sintaxis:

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

Add-circuit-class

Nota: Tan solo se utiliza cuando se configura Frame Relay.

Utilice el mandato **add-circuit-class** en el nivel de interfaz para asignar una cantidad designada de ancho de banda que deberá utilizar el grupo de circuitos asignado a la clase c de ancho de banda definida por el usuario.

Sintaxis:

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

Add-class

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

Nota: Si este mandato se utiliza para un circuito Frame Relay que utilice actualmente definiciones de circuito por omisión para el manejo de clases de tráfico, se le preguntará si desea o no alterar temporalmente las definiciones de circuito por omisión. Si responde “Sí”, se modificará el circuito para que utilice definiciones específicas del circuito para el manejo de clases de tráfico y se permitirá el mandato. Si responde “No”, se cancelará anormalmente el mandato y se seguirán utilizando definiciones de circuito por omisión para el circuito. Si desea cambiar las definiciones de circuito por omisión, debe ir al indicador de mandatos `BRS [i x][circuit defaults]Config>`.

Sintaxis:

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

Ejemplo 1: Añadir una clase llamada CIRC17 en un circuito Frame Relay

```
  BRS [i 1] [dlci 17] Config>add-class
This circuit is currently using circuit defaults...
 Are you sure you want to override the defaults ?(Yes or [No]):y
 Class name [DEFAULT]? CIRC17
 Percent bandwidth to reserve [10]?5
BRS [i 1] [dlci 17] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 1, circuit number 17
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 65%
 total classes defined (counting one local and one default) 5


 class LOCAL has 10% bandwidth allocated
   protocols and filters cannot be assigned to this class.


 class DEFAULT has 40% bandwidth allocated
   the following protocols and filters are assigned:
     protocol DNA with default priority is not discard eligible
     protocol VINES with default priority is not discard eligible
     protocol IPX with default priority is not discard eligible
     protocol OSI with default priority is not discard eligible
     protocol VOFR with default priority is not discard eligible
     protocol AP2 with default priority is not discard eligible
     protocol ASRT with default priority is not discard eligible


 class DEF1 has 5% bandwidth allocated
   protocol IP with priority NORMAL is not discard eligible.


 class DEF2 has 5% bandwidth allocated
  protocol ARP with priority NORMAL is not discard eligible.


 class CIRC171 has 5% bandwidth allocated
  no protocols or filters are assigned to this class.

 assigned tags:

 default class is DEFAULT with priority NORMAL
```

Ejemplo 2: Añadir una clase llamada class1 en un circuito Frame Relay

```
BRS [i 2] [dlci 128]>add
This circuit is currently using circuit defaults...
Are you sure you want to override the defaults ?(Yes or [No]): y
Class name [DEFAULT]?
Class is already allocated.
BRS [i 2] [dlci 128]>add class1
Percent bandwidth to reserve [10]?
BRS [i 2] [dlci 128]>

BRS [i 2] [dlci 128]> list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
interface number 2, circuit number 128
 maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 3


 class LOCAL has 10% bandwidth allocated
   protocols and filters cannot be assigned to this class.


 class DEFAULT has 40% bandwidth allocated
   the following protocols and filters are assigned:
    protocol IP with default priority is not discard eligible
    protocol ARP with default priority is not discard eligible
     protocol DNA with default priority is not discard eligible
     protocol VINES with default priority is not discard eligible
     protocol IPX with default priority is not discard eligible
     protocol OSI with default priority is not discard eligible
     protocol VOFR with default priority is not discard eligible
     protocol AP2 with default priority is not discard eligible
     protocol ASRT with default priority is not discard eligible

  class class1 has 10% bandwidth allocated
  no protocols or filters are assigned to this class.

 assigned tags:

 default class is DEFAULT with priority NORMAL

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

Assign

Utilice el mandato **assign** para asignar identificadores especificados, paquetes de protocolos o filtros a una clase t determinada y prioridad dentro de dicha clase. Los cuatro tipos de prioridad incluyen:

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

Nota: El protocolo Voz a través de Frame Relay (VOFR) se utiliza cuando se envían paquetes de voz a través de una interfaz Frame Relay. Si un circuito tan solo va a transportar paquetes de voz, asigne sólo una clase t en el circuito y especifique el protocolo como VOFR. Sólo se permite una clase t puesto que una clase t no tiene prioridad sobre otra clase t. Si existe más de una clase t, una clase t que no transporte voz puede obtener el control del ancho de banda e interferir en la transmisión de tráfico de voz. Para asegurarse de que el tráfico de voz recibirá inmediatamente transmisión, tan solo debe proporcionarse al tráfico VOFR el tipo de prioridad *Urgente*.

Debe configurarse Fragmentación a través de Frame Relay en el circuito tal como se describe en el mandato **enable fragmentation** en el capítulo "Configuración y supervisión de las interfaces de Frame Relay" de la publicación *Guía del usuario de software* si dicho circuito va a transportar tráfico de datos y de voz. Es necesario para que los paquetes de datos grandes no agoten el ancho de banda y para evitar que los paquetes de voz se transmitan con demasiada rapidez.

Sintaxis:

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

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

Nota: Si este mandato se utiliza para un circuito Frame Relay que utilice actualmente definiciones de circuito por omisión para el manejo de clases de tráfico, se le preguntará si desea o no alterar temporalmente las definiciones de circuito por omisión. Si responde "Sí", se modificará el circuito para que utilice definiciones específicas del circuito para el manejo de clases de tráfico y se permitirá el mandato. Si responde "No", se cancelará anormalmente el mandato y se seguirán utilizando definiciones de circuito por omisión para el circuito. Si desea cambiar las definiciones de circuito por omisión, debe ir al indicador de mandatos `BRS [i x][circuit defaults]Config>`.

Ejemplo 1:

```
assign IPX test
priority <URGENT/HIGH/NORMAL/LOW>: [NORMAL]? low
protocol IPX maps to class test with priority LOW Discard eligible <yes/no> [N]?
```

Ejemplo 2: Asignar un filtro de TOS a la clase1; la clase1 se ha añadido previamente a la configuración utilizando el mandato *add class*.

```
BRS [i 2] [dlci 128]>assign ?
IP
ARP
DNA
VINES
IPX
OSI
VOFR
AP2
ASRT
TUNNELING-IP
SDLC/BSC-IP
RLOGIN-IP
TELNET-IP
NETBIOS
SNA/APPN-ISR
SNMP-IP
MULTICAST-IP
DLSW-IP
TAG1
TAG2
TAG3
TAG4
TAG5
APPN-HPR
NETWORK-HPR
HIGH-HPR
MEDIUM-HPR
LOW-HPR
XTP-IP
UDP_TCP1
UDP_TCP2
UDP_TCP3
UDP_TCP4
UDP_TCP5
TOS1
TOS2
TOS3
TOS4
TOS5
Protocol or filter name [IP]? TOS1  1
Class name [DEFAULT]? class1  2
Priority  [NORMAL]?
Frame Relay Discard Eligible  [NO]?
TOS Mask [1-FF] [FF]?
TOS Range (Low) [0-FF] [0]? 1
TOS Range (High) [1]? 3
BRS [i 2] [dlci 128]> list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
interface number 2, circuit number 128
 maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 3


 class LOCAL has 10% bandwidth allocated
   protocols and filters cannot be assigned to this class.
```

```
 class DEFAULT has 40% bandwidth allocated
   the following protocols and filters are assigned:
    protocol IP with default priority is not discard eligible
    protocol ARP with default priority is not discard eligible
     protocol DNA with default priority is not discard eligible
     protocol VINES with default priority is not discard eligible
     protocol IPX with default priority is not discard eligible
     protocol OSI with default priority is not discard eligible
     protocol VOFR with default priority is not discard eligible
     protocol AP2 with default priority is not discard eligible
     protocol ASRT with default priority is not discard eligible


  class class1 has 10% bandwidth allocated
   the following protocols and filters are assigned:
    filter TOS1 with priority NORMAL is not discard eligible
       with TOS range x1 - x3 and TOS mask xFF

 assigned tags:

 default class is DEFAULT with priority NORMAL

BRS [i 2] [dlci 128]>show

BANDWIDTH RESERVATION currently in RAM
interface number 2, circuit number 128
 maximum queue length 10, minimum queue length 3
3 current defined classes:
 class LOCAL has 10% bandwidth allocated
 class DEFAULT has 40% bandwidth allocated
  class class1 has 10% bandwidth allocated

protocol and filter assignments:

Protocol/Filter      Class              Priority    Discard Eligible
---------------      -----              --------    ----------------
IP                   DEFAULT              NORMAL            NO
ARP                  DEFAULT              NORMAL            NO
DNA                  DEFAULT              NORMAL            NO
VINES                DEFAULT              NORMAL            NO
IPX                  DEFAULT              NORMAL            NO
OSI                  DEFAULT              NORMAL            NO
VOFR                 DEFAULT              NORMAL            NO
AP2                  DEFAULT              NORMAL            NO
ASRT                 DEFAULT              NORMAL            NO
TOS1                 class1               NORMAL            NO
   with TOS range x1 - x3
    and TOS mask xFF

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

1 Para utilizar el filtro de TOS es necesario entrar tres parámetros: Máscara de TOS, Rango-bajo de TOS y Rango-alto de TOS. Consulte el mandato “Add” en el capítulo “Configuración y supervisión de IP” de la publicación *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener una descripción de estos parámetros.

Assign-circuit

Nota: Tan solo se utiliza cuando se configura Frame Relay.

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

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

Sintaxis:

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

Change-circuit-class

Nota: Tan solo se utiliza cuando se configura Frame Relay.

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

Sintaxis:

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

Change-class

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

Nota: Si este mandato se utiliza para un circuito Frame Relay que utilice actualmente definiciones de circuito por omisión para el manejo de clases de tráfico, se le preguntará si desea o no alterar temporalmente las definiciones de circuito por omisión. Si responde “Sí”, se modificará el circuito para que utilice definiciones específicas del circuito para el manejo de clases de tráfico y se permitirá el mandato. Si responde “No”, se cancelará anormalmente el mandato y se seguirán utilizando definiciones de circuito por omisión para el circuito. Si desea cambiar las definiciones de circuito por omisión, debe ir al indicador de mandatos `BRS [i x][circuit defaults]Config>`.

Sintaxis:

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

Circuit

Nota: Tan solo se utiliza cuando se configura Frame Relay.

Utilice el mandato **circuit** para configurar un circuito virtual permanente (PVC) o un circuito virtual conmutado (SVC) de Frame Relay. Este mandato sólo de puede emitir desde el indicador de mandatos de configuración de interfaz de BRS (`BRS [i número] Config>`).

Sintaxis:

c**ircuit**

Para utilizar los mandatos **add-class**, **assign**, **default-class**, **del-class**, **deassign** o **change-class**, debe habilitar el BRS en el circuito y reiniciar o volver a cargar el direccionador.

Ejemplo para PVC:

```
BRS [i 1] Config> circuit
Circuit (PVC number or SVC name) to reserve bandwidth:  [16]

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

Ejemplo para SVC:

```
BRS [i 1] Config> circuit
Circuit (PVC number or SVC name) to reserve bandwidth:  [16] svc01

BRS [i 1 ] [svc svc01] Config> enable
```

Después de emitir el mandato **enable** para el circuito Frame Relay y de reiniciar o volver a cargar el direccionador, están disponibles los mandatos de configuración siguientes para el circuito:

add-class	deassign	enable	tag
assign	default-class	exit	untag
change-class	del-class	list	clear-block
disable	show	use-circuit-defaults	

Clear-block

Utilice el mandato **clear-block** para borrar de la SRAM los datos de configuración de reserva de ancho de banda actuales.

Sintaxis:

cl**ear-block**

- Si entra este mandato desde el indicador de mandatos de interfaz para PPP, se borran todos los datos de configuración del BRS para la interfaz.
- Si entra este mandato desde el indicador de mandatos de interfaz para Frame Relay, el BRS deja de estar habilitado en la interfaz o en cualquier circuito de la interfaz y se borran todos los datos de configuración de clase de circuito y las definiciones de circuito por omisión para el manejo de clases de tráfico. Sin embargo, los datos de configuración de clase de tráfico para cada circuito individual no se borran y están disponibles si se vuelve a habilitar el BRS en la interfaz.
- Para borrar los datos de configuración de clase de tráfico de un circuito, primero entre el mandato **circuit** desde el indicador de mandatos de nivel de interfaz y, a continuación, el mandato **clear-block** desde el indicador de mandatos de nivel de circuito. Después de borrar los datos de configuración de clase de tráfico para cada circuito, entre el mandato **clear-block** desde el indicador de mandatos de nivel de interfaz para borrar los datos de configuración de clase de circuito. Los cambios no entran en vigor hasta que el direccionador se reinicia o se vuelve a cargar.

Ejemplo:

```
clear-block
You are about to clear BRS configuration information for this interface
Are you sure you want to do this (Yes or No): y
BRS [i 1] Config>
```

Create-super-class

Utilice el mandato **create-super-class** para configurar una clase t llamada *super-clase* en la interfaz PPP o circuito Frame Relay. Tan solo se puede configurar una super-clase para cada interfaz PPP o circuito Frame Relay. No hay ningún porcentaje de ancho de banda asociado con la super-clase. Los datos de protocolo o filtro asignados a una superclase se transmitirán antes que los datos de protocolo o filtro asignados a cualquier otra clase t en la interfaz PPP o el circuito Frame Relay. Debe configurarse una superclase para el protocolo Voice over Frame Relay (VOFR) para un circuito que transporta paquetes de voz y de datos. En este entorno, la configuración de la superclase para transportar voz ayuda a asegurar que los paquetes de voz tengan prioridad.

Sintaxis:

cr**eate-super-class**

Deactivate-IP-precedence-filtering

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

Sintaxis:

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

Deassign

Utilice el mandato **deassign** para restaurar el proceso de poner en cola del paquete de protocolos o filtro especificado a la clase t y prioridad por omisión.

Nota: Si este mandato se utiliza para un circuito Frame Relay que utilice actualmente definiciones de circuito por omisión para el manejo de clases de tráfico, se le preguntará si desea o no alterar temporalmente las definiciones de circuito por omisión. Si responde “Sí”, se modificará el circuito para que utilice definiciones específicas del circuito para el manejo de clases de tráfico y se permitirá el mandato. Si responde “No”, se cancelará anormalmente el mandato y se seguirán utilizando definiciones de circuito por omisión para el circuito. Si desea cambiar las definiciones de circuito por omisión, debe ir al indicador de mandatos `BRS [i x][circuit defaults]Config>`.

Sintaxis:

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

Deassign-circuit

Nota: Tan solo se utiliza cuando se configura Frame Relay.

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

Sintaxis:

deassign-c #

Default-circuit-class

Nota: Tan solo se utiliza cuando se configura Frame Relay.

Utilice el mandato **default-circuit-class** en el nivel de interfaz para establecer el nombre definido por el usuario de la clase c de ancho de banda por omisión y el porcentaje de ancho de banda asignado a dicha clase de circuitos, incluyendo los huérfanos, que no están asignados a una clase c de ancho de banda.

Sintaxis:

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

Del-circuit-class

Nota: Tan solo se utiliza cuando se configura Frame Relay.

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

Sintaxis:

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

Default-class

Utilice el mandato **default-class** para establecer la clase t y prioridad por omisión en el valor que desee. Si no se ha asignado previamente ningún valor, se utilizan los valores por omisión del sistema. De lo contrario, se utiliza el último valor asignado anteriormente.

Nota: Si este mandato se utiliza para un circuito Frame Relay que utilice actualmente definiciones de circuito por omisión para el manejo de clases de tráfico, se le preguntará si desea o no alterar temporalmente las definiciones de circuito por omisión. Si responde “Sí”, se modificará el circuito para que utilice definiciones específicas del circuito para el manejo de clases de tráfico y se permitirá el mandato. Si responde “No”, se cancelará anormalmente el mandato y se seguirán utilizando definiciones de circuito por omisión para el circuito. Si desea cambiar las definiciones de circuito por omisión, debe ir al indicador de mandatos `BRS [i x][circuit defaults]Config>`.

Sintaxis:

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

Del-class

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

Nota: Si este mandato se utiliza para un circuito Frame Relay que utilice actualmente definiciones de circuito por omisión para el manejo de clases de tráfico, se le preguntará si desea o no alterar temporalmente las definiciones de circuito por omisión. Si responde “Sí”, se modificará el circuito para que utilice definiciones específicas del circuito para el manejo de clases de tráfico y se permitirá el mandato. Si responde “No”, se cancelará anormalmente el mandato y se seguirán utilizando definiciones de circuito por omisión para el circuito. Si desea cambiar las definiciones de circuito

por omisión, debe ir al indicador de mandatos `BRS [i x][circuit defaults]Config>`.

Sintaxis:

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

Disable

Utilice el mandato **disable** para inhabilitar la reserva de ancho de banda en la interfaz (si se ha entrado desde el indicador de mandatos de la interfaz) o en el circuito (si se ha entrado desde el indicador de mandatos del circuito). Los cambios no entran en vigor hasta que el direccionador se reinicia o se vuelve a cargar.

Para verificar si está inhabilitada la reserva de ancho de banda, entre el mandato **list**.

Sintaxis:

disable

Disable-hpr-over-ip-port-numbers

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

Sintaxis:

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

Para verificar que el filtrado de BRS de tráfico HPR a través de IP está inhabilitada, entre el mandato **list**.

Nota: Si se incluye APPN en la imagen de carga, se configura si va a utilizarse o no tráfico de HPR a través de IP en el indicador de mandatos `APPN Config>`.

Enable

Utilice el mandato **enable** para habilitar la reserva de ancho de banda en la interfaz (si se ha entrado desde el indicador de mandatos de interfaz) o en el circuito (si se ha entrado desde el indicador de mandatos de circuito). Los cambios no entran en vigor hasta que el direccionador se reinicia o se vuelve a cargar.

Sintaxis:

enable

Notas:

1. Cuando configure el BRS en una interfaz PPP, emita el mandato **enable** en el indicador de mandatos de interfaz y, a continuación, reinicie o vuelva a cargar el direccionador antes de configurar las clases de tráfico y de asignar protocolos y filtros a clases de tráfico.
2. Cuando el BRS está inicialmente habilitado en un circuito Frame Relay, el circuito está inicializado para utilizar definiciones de circuito por omisión para el manejo de clases de tráfico. Emita el mandato **enable** en el indicador de mandatos de interfaz y en el indicador de mandatos de circuito de cada circuito para el que desee definir clases de tráfico. A continuación, reinicie o vuelva a

cargar el direccionador antes de configurar clases de circuito para la interfaz y clases de tráfico para cada circuito. Por ejemplo:

```
 t 6
Gateway user configuration
Config>f brs
Bandwidth Reservation User Configuration
BRS Config>interface 1
BRS [i 1] Config>enable
Please restart router for this command to take effect
BRS [i 1] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1
maximum queue length 10, minimum queue length 3
total bandwidth allocated 10%
total circuit classes defined (counting one default) 1


class DEFAULT has 10% bandwidth allocated
  no circuits are assigned to this class.

default class is DEFAULT

BRS [i 1] Config>circ 16
BRS [i 1] [dlci 16] Config>enable
Defaults are in effect for this circuit.
Please restart router for this command to take effect.
BRS [i 1] [dlci 16] Config>ex
Please restart router for this command to take effect.
BRS [i 1] [dlci 16] Config>
*restore
Are you sure you want to restart the gateway? (Yes or [No]): y
```

Enable-hpr-over-ip-port-numbers

Utilice el mandato **enable-hpr-over-ip-port-numbers** para habilitar el filtrado de BRS de tráfico APPN-HPR a través de IP y para configurar los números de puerto UDP que se utilizan para identificar paquetes HPR a través de IP.

Nota: Si se incluye APPN en la imagen de carga, se habilita HPR a través de IP y se especifican los números de puerto UDP utilizados para tráfico HPR a través de IP en el indicador de mandatos `APPN Config>`.

Sintaxis:

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

Ejemplo:

```
BRS Config> enable-hpr-over-ip-port-numbers
XID exchange port number [12000]?
HPR net  trans prio port number [12001]?
HPR high trans prio port number [12002]?
HPR medium trans prio port number [12003]?
HPR low    trans prio port number [12004]?
```

número de puerto de intercambio XID

Este parámetro especifica el número de puerto UDP que debe utilizarse para el intercambio XID. Este número de puerto debe ser igual que el que se define en otros dispositivos de la red.

Valores válidos: 1024 - 65535

Valor por omisión: 12000

Número de puerto de prioridad de red

Este parámetro especifica el número de puerto UDP que debe utilizarse para el tráfico de prioridad de la red. Este número de puerto debe ser igual que el que se define en otros dispositivos de la red.

Valores válidos: 1024 - 65535

Valor por omisión:12001

Número de puerto de intercambio de prioridad alta

Este parámetro especifica el número de puerto UDP que debe utilizarse para el tráfico de prioridad alta. Este número de puerto debe ser igual que el que se define en otros dispositivos de la red.

Valores válidos: 1024 - 65535

Valor por omisión:12002

Número de puerto de intercambio de prioridad media

Este parámetro especifica el número de puerto UDP que debe utilizarse para el tráfico de prioridad media. Este número de puerto debe ser igual que el que se define en otros dispositivos de la red.

Valores válidos: 1024 - 65535

Valor por omisión:12003

Número de puerto de intercambio de prioridad baja

Este parámetro especifica el número de puerto UDP que debe utilizarse para el tráfico de prioridad baja. Este número de puerto debe ser igual que el que se define en otros dispositivos de la red.

Valores válidos: 1024 - 65535

Valor por omisión:12004

Interface

Utilice el mandato **interface** para seleccionar la interfaz serie a la que se aplicarán mandatos de configuración de reserva de ancho de banda. *La reserva de ancho de banda se soporta en direccionadores que ejecutan interfaces PPP (Point-to-Point Protocol) y Frame Relay.*

Nota: No se soporta la Reserva de ancho de banda a través de subinterfaces Frame Relay. Consulte Using Frame Relay Interfaces en la publicación *Guía del usuario de software* para obtener más información.

Sintaxis:

interface *número-interfaz*

Notas:

1. Para entrar mandatos de reserva de ancho de banda para una nueva interfaz, este mandato debe entrarse ***antes*** de utilizar otros mandatos de configuración de reserva de ancho de banda. Si ha salido del indicador de mandatos de reserva de ancho de banda y desea volver a efectuar cambios de reserva de ancho de banda en una interfaz previamente configurada, primero debe volverse a entrar este mandato.
2. Si se utiliza Restauración de la WAN y el BRS está configurado en una interfaz primaria, el BRS también debe configurarse en una interfaz secundaria. Generalmente cuando se utiliza Restauración de la WAN, la interfaz secundaria

toma la identidad de la interfaz primaria. Para el BRS esto no es así; por lo tanto, es necesario configurar el BRS en la interfaz primaria y la interfaz secundaria.

Para habilitar la Reserva de ancho de banda en una interfaz particular, en el indicador de mandatos `BRS Config>`, entre el número de la interfaz que soporta el protocolo o característica particular. Entonces puede utilizar el mandato **enable** de BRS Talk 6 tal como se describe en este capítulo. Después de habilitar el número de interfaz, deberá reiniciar o volver a cargar el 2210 para que el mandato entre en vigor antes de efectuar otros cambios de configuración en la interfaz.

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

List

Utilice el mandato **list** para visualizar las clases de ancho de banda actualmente definidas y su porcentaje garantizado.

El mandato **list** y el mandato **show** son similares. El mandato **list** visualiza las definiciones actuales de la SRAM y el mandato **show** visualiza las definiciones actuales de la RAM.

Sintaxis:

list *número-interfaz*

Según el indicador de mandatos en el que emita el mandato **list**, se visualizan distintas salidas. Puede emitir el mandato **list** desde los siguientes indicadores de mandatos:

- `BRS [i 1] [dlci 16] Config>`
- `BRS [i 1] Config>`
- `BRS Config>`
- `BRS [i 1] [circuit defaults] Config>`

Nota: Cuando se emite este mandato desde un indicador de mandatos de circuito Frame Relay (`BRS [i x] [dlci y] Config>`) indica si el circuito utiliza definiciones de circuito por omisión o definiciones específicas del circuito para el manejo de clases de tráfico. Si el circuito utiliza definiciones de circuito por omisión, se visualiza la clase de tráfico, el protocolo, el filtro y las asignaciones de identificador actualmente definidos para las definiciones de circuito por omisión. Sin embargo, si desea modificar las definiciones de circuito por omisión, debe ir al indicador de mandatos `BRS[i x] [circuit defaults] Config>` para efectuar los cambios.

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

En el indicador de mandatos de nivel de interfaz de BRS para Frame Relay, el mandato **list** lista las clases de circuito, sus porcentajes de ancho de banda configurados y los circuitos asignados.

Ejemplo 1

```
BRS Config>list
 Bandwidth Reservation is available for 2 interfaces.

 Interface   Type            State
 ---------   ----            -----
         1   FR              Enabled
         2   PPP             Enabled

 The use of HPR over IP port numbers is disabled

 BRS Config>interface 1
 BRS [i 1] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
interface number 1
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 10%
 total circuit classes defined (counting one default) 1


 class DEFAULT has 10% bandwidth allocated
   the following circuits are assigned:
       17
       16  using defaults.
       18  using defaults.

 default class is DEFAULT

 BRS [i 2] Config>exit
 BRS Config>interface 2
 BRS [i 2] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 2
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 50%
 total classes defined (counting one local and one default) 2


 class LOCAL has 10% bandwidth allocated
   protocols and filters cannot be assigned to this class.


 class DEFAULT has 40% bandwidth allocated
   the following protocols and filters are assigned:
     protocol IP with default priority
     protocol ARP with default priority
     protocol DNA with default priority
     protocol VINES with default priority
     protocol IPX with default priority
     protocol OSI with default priority
     protocol VOFR with default priority
     protocol AP2 with default priority
     protocol ASRT with default priority

 assigned tags:

 default class is DEFAULT with priority NORMAL

 BRS [i 2] Config>
```

Ejemplo 2

```
 BRS [i 1] [dlci 17] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 3


 class LOCAL has 10% bandwidth allocated
   protocols and filters cannot be assigned to this class.


 class DEFAULT has 40% bandwidth allocated
   the following protocols and filters are assigned:
   protocol ASRT with priority NORMAL is not discard eligible
   filter NETBIOS with priority NORMAL is not discard eligible


class CLASS1 has 10% bandwidth allocated
   the following protocols and filters are assigned:
   protocol IP with priority NORMAL is not discard eligible
   protocol ARP with priority NORMAL is not discard eligible
   protocol DNA with priority NORMAL is not discard eligible
   protocol VINES with priority NORMAL is not discard eligible
   protocol IPX with priority NORMAL is discard eligible
   protocol OSI with priority NORMAL is not discard eligible
   protocol VOFR with priority NORMAL is not discard eligible
   protocol AP2 with priority NORMAL is not discard eligible
```

Ejemplo 3

```
 BRS [i 1] [circuit defaults] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 1, default circuit
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 70%
 total classes defined (counting one local and one default) 4


 class LOCAL has 10% bandwidth allocated
   protocols and filters cannot be assigned to this class.



 class DEFAULT has 40% bandwidth allocated
   the following protocols and filters are assigned:
     protocol DNA with default priority is not discard eligible
     protocol VINES with default priority is not discard eligible
     protocol IPX with default priority is not discard eligible
     protocol OSI with default priority is not discard eligible
     protocol VOFR with default priority is not discard eligible
     protocol AP2 with default priority is not discard eligible
     protocol ASRT with default priority is not discard eligible


 class DEF1 has 10% bandwidth allocated
   protocol IP with priority NORMAL is not discard eligible.


 class DEF2 has 10% bandwidth allocated
  protocol ARP with priority NORMAL is not discard eligible.

 assigned tags:

 default class is DEFAULT with priority NORMAL

  BRS [i 1] [circuit defaults] Config>
```

Ejemplo 4

```
BRS Config>list
 Bandwidth Reservation is available for 2 interfaces.

 Interface   Type            State
 ---------   ----            -----
         1   FR              Enabled
         2   PPP             Enabled

 The use of HPR over IP port numbers is enabled.

    Transmission Type   Port Number
    -----------------   -----------
        XID exchange        12000
        HPR network         12001
        HPR high            12002
        HPR medium          12003
        HPR low             12004
```

Queue-length

Utilice el mandato **queue-length** para establecer el número de paquetes que se pueden poner en cola en cada cola de prioridad del BRS. Cada clase de BRS tiene un valor de prioridad asignado a sus protocolos, filtros e identificadores y cada cola de prioridad puede almacenar el número de paquetes que se especifican con este mandato.

Sintaxis:

g**ueue-length** *longitud-máxima longitud-mínima*

Este mandato establece el número máximo de almacenamientos intermedios que se pueden poner en cola en cada cola de prioridad del BRS así como el número máximo que se puede poner en cola en cada cola de prioridad del BRS cuando existe una escasez de almacenamientos intermedios de entrada del direccionador.

Si emite **queue-length** para una interfaz PPP, el mandato establece los valores de longitud de cola para cada cola de prioridad de cada clase t de BRS definida para la interfaz.

Si emite **queue-length** para una interfaz Frame Relay (en el indicador de mandatos: `BRS [i 0] Config>`), el mandato establece los valores de longitud de cola por omisión para cada cola de prioridad de cada clase t de BRS definida para cada circuito virtual permanente de la interfaz.

Si emite **queue-length** para un PVC Frame-Relay (en un indicador de mandatos similar al siguiente: `BRS [i 0] [dlci 16] Config>`) el mandato establece los valores de longitud de cola para cada cola de prioridad de cada clase t del BRS definida para el PVC. Estos valores alteran temporalmente los valores de longitud de cola por omisión establecidos para la interfaz Frame Relay.

Atención: No utilice este mandato a menos que sea indispensable. Para la mayoría de usuarios los valores recomendados son los valores por omisión para la longitud de cola. Si establece valores de longitud de cola demasiado altos, puede reducir gravemente el rendimiento del direccionador.

Set-circuit-defaults

Utilice el mandato **set-circuit-defaults** para acceder a los mandatos utilizados para definir las definiciones de circuito por omisión para el manejo de clases de tráfico. A continuación, estas definiciones de circuito por omisión las puede utilizar cualquier circuito Frame Relay en la interfaz que puede utilizar las mismas clases de tráfico, protocolo, filtro y asignaciones de identificadores.

Sintaxis:

se**t-circuit-defaults**

Show

Utilice el mandato **show** para visualizar las clases de ancho de banda actualmente definidas que se almacenan en la RAM.

Sintaxis:

sh**ow** *número-interfaz*

Según el indicador de mandatos en el que se emita el mandato **show**, se visualizan distintas salidas. Puede emitir el mandato **show** desde los siguientes indicadores de mandatos:

- `BRS [i x] Config>` - indicador de mandatos de nivel de interfaz para el número de interfaz *x*.
- `BRS [i x] [dlci y] Config>` - indicador de mandatos de nivel de circuito para el circuito *y* en el número de interfaz Frame Relay *x*. En el ejemplo siguiente se muestra la salida del mandato show desde el indicador de mandatos de nivel de circuito.

```
BRS [i 1] [dlci 17] Config>show

Protocol/Filter      Class              Priority    Discard Eligible
---------------      -----              --------    ----------------
IP                   CLASS1               NORMAL              NO
ARP                  CLASS1               NORMAL              NO
DNA                  CLASS1               NORMAL              NO
VINES                CLASS1               NORMAL              NO
IPX                  CLASS1               NORMAL              YES
OSI                  CLASS1               NORMAL              NO
VOFR                 CLASS1               NORMAL              NO
AP2                  CLASS1               NORMAL              NO
ASRT                 DEFAULT              NORMAL              NO
NETBIOS              DEFAULT              NORMAL              NO
```

En el indicador de mandatos para PPP y el indicador de mandatos de circuito para Frame Relay, se visualiza información de clase de tráfico. En el indicador de mandatos de interfaz para Frame Relay, se visualiza información de clase de circuito.

Notas:

1. Cuando se emite este mandato desde un indicador de mandatos de circuito Frame Relay (`BRS [i x] [dlci y] Config>`) indica si el circuito utiliza definiciones de circuito por omisión o definiciones específicas del circuito para el manejo de clases de tráfico. Si el circuito utiliza definiciones de circuito por omisión, se visualiza la clase de tráfico, el protocolo, el filtro y las asignaciones de identificador actualmente definidos para las definiciones de circuito por omisión. Sin embargo, si desea modificar las definiciones de circuito por

omisión, debe ir al indicador de mandatos `BRS[i x] [circuit defaults] Config>` para efectuar los cambios.

2. Este mandato no se puede utilizar desde el indicador de mandatos `BRS [i x] [circuit defaults] Config>`.

Tag

Utilice el mandato **tag** para asignar un elemento de filtro de MAC que se ha identificado durante la configuración de la característica de filtrado de MAC al siguiente nombre de identificador de BRS disponible. Los nombres de identificador de BRS son TAG1, TAG2, TAG3, TAG4 y TAG5. Utilice el nombre de identificador del BRS en el mandato assign para asignar el identificador a una clase de tráfico del BRS.

Sintaxis:

tag *número-identificador_filtro_mac*

Utilice el mandato **list** para listar los identificadores de filtro de MAC que se han asignado a un nombre de identificador de BRS y los nombres de identificador del BRS que se han asignado a una clase de tráfico de ancho de banda.

Nota: Si este mandato se utiliza para un circuito Frame Relay que utilice actualmente definiciones de circuito por omisión para el manejo de clases de tráfico, se le preguntará si desea o no alterar temporalmente las definiciones de circuito por omisión. Si responde “Sí”, se modificará el circuito para que utilice definiciones específicas del circuito para el manejo de clases de tráfico y se permitirá el mandato. Si responde “No”, se cancelará anormalmente el mandato y se seguirán utilizando definiciones de circuito por omisión para el circuito. Si desea cambiar las definiciones de circuito por omisión, debe ir al indicador de mandatos `BRS [i x][circuit defaults]Config>`.

Untag

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

Sintaxis:

untag *número-identificador_filtro_mac*

Utilice el mandato **list** para mostrar los identificadores de filtro de MAC que están asignados a un nombre de identificador del BRS y los nombres de identificador del BRS que están asignados a una clase de tráfico.

Nota: Si este mandato se utiliza para un circuito Frame Relay que utilice actualmente definiciones de circuito por omisión para el manejo de clases de tráfico, se le preguntará si desea o no alterar temporalmente las definiciones de circuito por omisión. Si responde “Sí”, se modificará el circuito para que utilice definiciones específicas del circuito para el manejo de clases de tráfico y se permitirá el mandato. Si responde “No”, se cancelará anormalmente el mandato y se seguirán utilizando definiciones de circuito por omisión para el circuito. Si desea cambiar las definiciones de circuito

por omisión, debe ir al indicador de mandatos `BRS [i x][circuit defaults]Config>`.

Use-circuit-defaults

Utilice el mandato **use-circuit-defaults** en el nivel de circuito para suprimir las definiciones específicas del circuito y utilizar las definiciones de circuito por omisión para el manejo de clases de tráfico. Se le solicitará que confirme que desea utilizar los valores por omisión de circuito.

Sintaxis:

us**e-circuit-defaults**

Notas:

1. Este mandato sólo se utiliza cuando se configura Frame Relay
2. Se debe reiniciar o volver a cargar el direccionador para que los valores por omisión entren en vigor.

Ejemplo:

```
BRS [i 1] [dlci 17] Config>use-circuit-defaults
This circuit is currently NOT using circuit defaults...
 Are you sure you want to delete current definitions and use defaults ? (Yes or
 [No]): y
 Defaults are in effect for this circuit.
 Please restart router for this command to take effect.
 BRS [i 1] [dlci 17] Config>
 *restart
 Are you sure you want to restart the gateway? (Yes or [No]): y
```

Acceso al indicador de mandatos de supervisión de reserva de ancho de banda

Para acceder a los mandatos de supervisión de reserva de ancho de banda y supervisar la reserva de ancho de banda en el direccionador, haga lo siguiente:

1. En el indicador de mandatos OPCON (*), escriba **talk 5**.
2. En el indicador de mandatos GWCON (+), escriba **feature brs.**
3. En el indicador de mandatos `BRS>`, escriba **interface *número***, donde *número* es el número de la interfaz que desea supervisar. Llegará al indicador de mandatos de nivel de interfaz del BRS, `BRS [i x]>`, donde `x` es el número de interfaz.
4. Para Frame Relay solamente, escriba **circuit *número*** en el indicador de mandatos de interfaz para especificar el circuito en esta interfaz que desea supervisar.

   Llegará al indicador de mandatos de nivel de circuito `BRS [i x] [dlci y]>`, donde `x` es el número de interfaz e `y` es el número de circuito.
5. En el indicador de mandatos, escriba el mandato de supervisión apropiado. (Consulte el apartado “Mandatos de supervisión de la Reserva de ancho de banda” en la página 51.)

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

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

El mandato **interface *número*** selecciona la interfaz determinada que desea supervisar para la reserva de ancho de banda.

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

Para volver al indicador de mandatos GWCON en cualquier momento, escriba el mandato **exit** en el indicador de mandatos `BRS>`.

Después de acceder al indicador de mandatos de supervisión de reserva de ancho de banda (`BRS>`), puede entrar cualquiera de los mandatos de supervisión específicos que se describen en la Tabla 4.

Mandatos de supervisión de la Reserva de ancho de banda

Esta sección resume y explica los mandatos de la Reserva de ancho de banda. La 4 muestra los mandatos de supervisión de la Reserva de ancho de banda. Los mandatos que se pueden utilizar difieren según el indicador de mandatos de supervisión del BRS (`BRS>`, `BRS [i x]>` o `BRS [i x] [dlci y]>`).

Tabla 4 (Página 1 de 2). Resumen de mandatos de supervisión de la Reserva de ancho de banda

Mandato	Usado sólo con FR	Función
? (Help)		Visualiza todos los mandatos disponibles para este nivel de mandato o lista las opciones para mandatos específicos (si está disponible). Consulte el apartado “Cómo obtener ayuda” en la página xxx
Circuit	sí	Selecciona el DLCI de un circuito virtual permanente (PVC) de Frame Relay. Para supervisar el tráfico de reserva de ancho de banda de Frame Relay, debe estar en el nivel de indicador de mandatos de circuito.
Clear		Borra los contadores de clase t actuales y los almacena como contadores de clase t de **last**. Los contadores se listan según la clase.
Clear-circuit-class	sí	Borra los contadores de clase c actuales y los almacena como contadores de clase c de **last**. Los contadores se listan según la clase.
Counters		Visualiza los contadores de clase t actuales.
Counters-circuit-class	sí	Visualiza los contadores de clase c actuales.
Interface		Selecciona la interfaz que debe supervisarse. **Nota:** Este mandato debe entrarse antes de utilizar cualquier otro mandato de supervisión de reserva de ancho de banda.
Last		Visualiza los últimos contadores de clase t que se han guardado.

Tabla 4 (Página 2 de 2). Resumen de mandatos de supervisión de la Reserva de ancho de banda

Mandato	Usado sólo con FR	Función
Last-circuit-class	sí	Visualiza los últimos contadores de clase c que se han guardado.
Exit		Le devuelve al nivel de mandato anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi

Circuit

Nota: Sólo se utiliza cuando se supervisa Frame Relay.

Utilice el mandato **circuit** para seleccionar el DLCI de un PVC de Frame Relay para supervisarlo. Este mandato sólo se puede emitir desde el indicador de mandatos de supervisión de interfaz del BRS (`BRS [i número]>`).

Sintaxis:

ci**rcuit** *número-circuito-virtual-permanente*

Después de seleccionar el circuito de Frame Relay, se pueden utilizar los mandatos siguientes en el indicador de mandatos de circuito:

```
CLEAR
COUNTERS
LAST
EXIT
```

Clear

Utilice el mandato **clear** para guardar los contadores de clase t de reserva de ancho de banda actuales de modo que se puedan recuperar utilizando el mandato **last** y borrar los valores. Los contadores se guardan según la clase de tráfico de ancho de banda.

Sintaxis:

clear

Clear-Circuit-Class

Nota: Sólo se utiliza cuando se supervisa Frame Relay.

Utilice el mandato **clear-circuit-class** para guardar los contadores de clase c de reserva de ancho de banda actuales de modo que se puedan recuperar utilizando el mandato **last-circuit-class** y borrar los valores. Los contadores se guardan según la clase de circuito.

Sintaxis:

clear-c**ircuit-class**

Counters

Utilice el mandato **counters** para visualizar estadísticas que describan el tráfico de reserva de ancho de banda para las clases de tráfico configuradas para una interfaz PPP o circuito Frame Relay.

Sintaxis:

counters

Ejemplo: **`counters`**

```
Bandwidth Reservation Counters
interface number 1
Class            Pkt Xmit     Bytes Xmit     Bytes Ovfl     Pkt Ovfl    Q_len

LOCAL               10            914             0            0
   LOW               0              0             0            0        0
   NORMAL           10            914             0            0        0
   HIGH              0              0             0            0        0
   URGENT            0              0             0            0        0
DEFAULT             55           5555             0            0
   LOW               0              0             0            0        0
   NORMAL           20           5020             0            0        0
   HIGH              0              0             0            0        0
   URGENT           35            535             0            0        0
CLASS_1              5            910             0            0
   LOW               0              0             0            0        0
   NORMAL            5            910             0            0        0
   HIGH              0              0             0            0        0
   URGENT            0              0             0            0        0
CLASS_2             70           4123             0            0
   LOW              10            617             0            0        0
   NORMAL           55           3117             0            0        0
   HIGH              0              0             0            0        0
   URGENT            5            389             0            0        0

TOTAL              140          11502             0            0
```

Bytes Ovfl

Lista el número de bytes para los paquetes que no se han podido transmitir debido a que se ha alcanzado la longitud máxima de cola para una cola de prioridad o a que no se ha podido poner en cola el paquete porque la cola de prioridad estaba en el umbral mínimo de longitud de cola y el paquete procedía de una interfaz con escasez de almacenamientos intermedios de recepción.

Pkt Ovfl Lista el número de paquetes que no se han podido transmitir debido a que se ha alcanzado la longitud máxima de cola para una cola de prioridad o a que el paquete no se ha podido poner en cola porque la cola de prioridad estaba en el umbral mínimo de longitud de cola y el paquete procedía de una interfaz con escasez de almacenamientos intermedios de recepción.

Q_len El número actual de paquetes que esperan para ser transmitidos en cada una de las colas dentro de cada clase de tráfico.

Counters-circuit-class

Nota: Sólo se utiliza cuando se supervisa Frame Relay.

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

Sintaxis:

counters-c**ircuit-class**

Ejemplo: **`counters-circuit-class`**

```
Bandwidth Reservation Circuit Class Counters
Interface 1


Class         Pkt Xmit     Bytes Xmit     Bytes Ovfl
DEFAULT             25           3402             26
CIRCLASS1            1             56              0
CIRCLASS2            0              0              0

TOTAL               26           3458             26
```

Interface

Utilice el mandato **interface** para seleccionar la interfaz serie a la que se aplicarán mandatos de supervisión de reserva de ancho de banda. *La reserva de ancho de banda se soporta en direccionadores que ejecutan interfaces PPP (Point-to-Point Protocol) y Frame Relay.*

Sintaxis:

i**nterface** *número-interfaz*

Nota: Para entrar mandatos de reserva de ancho de banda para una nueva interfaz, debe entrarse este mandato antes de utilizar cualquier otro mandato de supervisión de reserva de ancho de banda. Si ha salido del indicador de mandatos de supervisión de reserva de ancho de banda (BRS>) y desea volver a supervisar la reserva de ancho de banda, primero debe volver a entrar este mandato.

Para supervisar la Reserva de ancho de banda en una interfaz determinada, en el indicador de mandatos de supervisión BRS>, escriba el número de la interfaz. A continuación, puede utilizar mandatos de supervisión de reserva de ancho de banda tal como se describe en este capítulo.

Last

Utilice el mandato **last** para visualizar las últimas estadísticas de clase t que se han guardado. Las estadísticas de clase t se visualizan en el mismo formato que para el mandato **counters**.

Sintaxis:

last

Last-circuit-class

Nota: Sólo se utiliza cuando se supervisa Frame Relay.

Utilice el mandato **last-circuit-class** para visualizar las últimas estadísticas de clase de circuito que se han guardado. Las estadísticas de clase c se visualizan en el mismo formato que para el mandato **counters-circuit-class**.

Sintaxis:

last-c**ircuit-class**

Soporte de reconfiguración dinámica de la Reserva de ancho de banda

Esta sección describe la reconfiguración dinámica (DR) en lo que afecta a los mandatos de Talk 6 y Talk 5.

Delete interface de CONFIG (Talk 6)

La Reserva de ancho de banda soporta el mandato de CONFIG (Talk 6) **delete interface** sin restricciones.

Activate interface de GWCON (Talk 5)

La Reserva de ancho de banda soporta el mandato de GWCON (Talk 5) **activate interface** sin restricciones.

El mandato de GWCON (Talk 5) **activate interface** soporta todos los mandatos específicos de interfaz de Reserva de ancho de banda.

Reset interface de GWCON (Talk 5)

La Reserva de ancho de banda soporta el mandato de GWCON (Talk 5) **reset interface** sin restricciones.

El mandato de GWCON (Talk 5) **reset interface** soporta todos los mandatos específicos de interfaz de Reserva de ancho de banda.

Mandatos de cambio inmediato de CONFIG (Talk 6)

La Reserva de ancho de banda soporta los mandatos de CONFIG siguientes que cambian inmediatamente el estado operativo del dispositivo. Estos cambios se guardan y se conservan si se vuelve a cargar o se reinicia el dispositivo o si se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
GWCON, feature brs, activate-ip-precedence-filtering
GWCON, feature brs, deactivate-ip-precedence-filtering
GWCON, feature brs, enable-hpr-over-ip-port-numbers
GWCON, feature brs, disable-hpr-over-ip-port-numbers
GWCON, feature brs, interface, add-circuit-class
GWCON, feature brs, interface, assign-circuit
GWCON, feature brs, interface, change-circuit-class
GWCON, feature brs, interface, deassign-circuit
GWCON, feature brs, interface, default-circuit-class
GWCON, feature brs, interface, del-circuit-class
GWCON, feature brs, interface, disable
GWCON, feature brs, interface, enable
GWCON, feature brs, interface, queue-length
GWCON, feature brs, interface, add-class **Nota:** Este mandato también se puede utilizar a nivel de circuito para interfaces Frame Relay.
GWCON, feature brs, interface, assign **Nota:** Este mandato también se puede utilizar a nivel de circuito para interfaces Frame Relay.
GWCON, feature brs, interface, change-class **Nota:** Este mandato también se puede utilizar a nivel de circuito para interfaces Frame Relay.
GWCON, feature brs, interface, create-super-class **Nota:** Este mandato también se puede utilizar a nivel de circuito para interfaces Frame Relay.
GWCON, feature brs, interface, deassign **Nota:** Este mandato también se puede utilizar a nivel de circuito para interfaces Frame Relay.
GWCON, feature brs, interface, default-class **Nota:** Este mandato también se puede utilizar a nivel de circuito para interfaces Frame Relay.
GWCON, feature brs, interface, del-class **Nota:** Este mandato también se puede utilizar a nivel de circuito para interfaces Frame Relay.
GWCON, feature brs, interface, disable **Nota:** Este mandato también se puede utilizar a nivel de circuito para interfaces Frame Relay.
GWCON, feature brs, interface, enable **Nota:** Este mandato también se puede utilizar a nivel de circuito para interfaces Frame Relay.
GWCON, feature brs, interface, tag **Nota:** Este mandato también se puede utilizar a nivel de circuito para interfaces Frame Relay.
GWCON, feature brs, interface, untag **Nota:** Este mandato también se puede utilizar a nivel de circuito para interfaces Frame Relay.

Utilización de filtrado de MAC

Este capítulo describe cómo utilizar el control de acceso al medio (MAC) para especificar filtros de paquete para aplicarlos a los paquetes durante el proceso. El capítulo incluye las secciones siguientes:

Los filtros son un conjunto de normas que se aplican a un paquete para determinar cómo debe manejarse el paquete durante el puenteado. El filtrado de MAC sólo afecta al tráfico puenteado.

Nota: El filtrado de MAC se permite en tráfico de túnel.

Durante el proceso de filtrado, los paquetes se procesan, filtran, o se identifican durante el puenteado. Las acciones son:

- **Procesado** – Se permite que pasen los paquetes a través del puente sin verse afectados.
- **Filtrado** – No se permite que los paquetes pasen a través del puente.
- **Identificado** – Se permite que pasen los paquetes a través del puente, pero están marcados con un número dentro del rango de 1 a 64 basándose en un parámetro configurable.

Un filtro de MAC consta de los objetos siguientes:

1. Elemento-filtro – que es una única norma que se aplica al campo de dirección o a una ventana arbitraria de datos dentro de un paquete. El resultado de aplicar esta norma es una condición de true (coincidencia satisfactoria) o false (ninguna coincidencia).
2. Lista-filtro – que contiene una lista de uno o más elementos-filtro.
3. Filtro – que contiene un conjunto de listas-filtro.

Filtrado de MAC y tráfico DLSw

Puede filtrar el tráfico LLC de entrada para la red DLSw implantando el Filtrado de MAC.

Para establecer un filtro para LLC, utilice el número de *Red puente* como el número de interfaz para el filtro. Determine el número de Red puente añadiendo dos al número de interfaces configuradas para el direccionador. Entre el mandato **list devices** en el indicador de mandatos `Config>` o entre **configuration** en el indicador de mandatos `+` para ver una lista de interfaces.

En el ejemplo siguiente, el número de Red puente es 7.

```
Ifc 0 Ethernet                    CSR  81600, CSR2  80C00, vector 94
Ifc 1 WAN X.25                    CSR  81620, CSR2  80D00, vector 93
Ifc 2 WAN X.25                    CSR  81640, CSR2  80E00, vector 92
Ifc 3 WAN PPP                     CSR 381620, CSR2 380D00, vector 125
Ifc 4 WAN Frame Relay             CSR 381640, CSR2 380E00, vector 124
Ifc 5 Token Ring                  CSR 600000, vector 95
```

Cuando configura un filtro para la Red puente, por ejemplo, el direccionador no elimina las tramas que coinciden con filtros exclusivos. En lugar de ello, reenvía dichas tramas al puente.

Parámetros de filtrado de MAC

Puede especificar algunos de los parámetros siguientes o todos para crear un filtro:

- Dirección de MAC de origen o dirección de MAC de destino
- Datos que deben coincidir dentro del paquete
- Máscara a aplicar a los campos del paquete que deben filtrarse
- Número de interfaz
- Designación de Entrada/Salida
- Designación Incluir/Excluir/Identificar
- Valor de identificador (si se proporciona la designación de identificador)

Parámetros de elemento de filtro

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

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

Cada elemento de filtro especifica un tipo de dirección (SOURCE o DESTINATION) para coincidir con el tipo en el paquete.

La máscara de dirección es una serie de números entrados en hexadecimal, que se utiliza para la comparación con las direcciones del paquete. La máscara se aplica a la dirección MAC SOURCE o DESTINATION MAC del paquete antes de compararla con la dirección MAC especificada.

La máscara de dirección debe tener la misma longitud que la dirección MAC y especifica los bytes a los que se debe aplicar AND lógicamente con los bytes de la dirección MAC antes de realizar la comparación de igualdad con la dirección MAC especificada. Si no se especifica ninguna máscara, se supone que todo son 1.

Parámetros de lista de filtros

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

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

Una lista de filtros se crea a partir de uno o más elementos de filtro. A cada lista de filtros se le proporciona un nombre exclusivo.

La aplicación de una lista de filtros a un paquete consiste en comparar cada elemento de filtro en el orden con que se han añadido los elementos de filtro a la lista. Si cualquier elemento de filtro de la lista devuelve una condición TRUE, la lista de filtros devolverá su acción designada.

Parámetros de filtro

Los parámetros siguientes se utilizan para crear un filtro:

- Nombres de lista de filtros: *serie-ASCII 1* . . . *serie-ASCII n*
- Número de interfaz: un *número-IFC*
- Dirección de puerto: INPUT o OUTPUT
- Acción por omisión: INCLUDE, EXCLUDE o TAG
- Identificador por omisión: un *valor-identificador*

Un filtro se crea asociando un grupo de nombres de lista de filtros con un número de interfaz y asignar una designación INPUT o OUTPUT. La aplicación de un filtro a un paquete significa que cada una de las listas de filtros asociadas debe aplicarse a los paquetes que se reciben (INPUT) o envían (OUTPUT) en la interfaz numerada especificada.

Cuando un filtro evalúa un paquete en una condición INCLUDE, se reenvía el paquete. Cuando un filtro evalúa un paquete en una condición EXCLUDE, el paquete se excluye. Cuando un filtro evalúa una condición TAG, el paquete que se considera se reenvía con un identificador.

La acción por omisión es un parámetro adicional de cada filtro, que es el resultado de una no coincidencia para todas sus listas de filtros. Esta acción por omisión es INCLUDE. Se puede establecer en INCLUDE, EXCLUDE o TAG. Además, si la acción por omisión es TAG, también se proporciona un valor de identificador.

Utilización de identificadores de filtrado de MAC

La lista siguiente incluye algunas de las utilizaciones de los identificadores de filtrado de MAC

- El filtrado de Dirección de MAC se maneja mediante la acción conjunta entre la reserva de ancho de banda y la característica de Filtrado de MAC (MCF) utilizando identificadores. Un usuario con reserva de ancho de banda puede categorizar el tráfico de puente, por ejemplo, asignándole un identificador.
- El proceso de identificación se lleva a cabo creando un elemento-filtro en la consola de configuración de Filtrado de MAC y, a continuación, asignándole un identificador. A continuación, este identificador se utiliza para configurar un clase de ancho de banda para todos los paquetes asociados con este identificador. Los valores de identificador deben estar actualmente dentro del rango de 1 a 64.
- Una vez creado un filtro con identificador en el proceso de configuración de Filtrado de MAC, se utiliza el mandato de configuración **tag** de Reserva de ancho de banda (BRS) para asignar un nombre de identificador del BRS (TAG1, TAG2, TAG3, TAG4 o TAG5) al número de identificador de filtro de MAC. A continuación, el nombre de identificador del BRS se utiliza en el mandato de configuración **assign** del BRS para asignar el filtro de MAC correspondiente a una clase de tráfico y prioridad de ancho de banda.
- Se pueden establecer un máximo de 5 direcciones de MAC con identificador de 1 a 5. Primero se buscará TAG1, después TAG2 y así sucesivamente hasta TAG5.

En el Túnel IP también se puede hacer referencia a los identificadores como “grupos”. Los puntos finales del túnel IP pueden pertenecer a cualquier número de grupos, con paquetes asignados a un grupo particular mediante la característica de identificación del filtrado de dirección de MAC.

Configuración y supervisión de Filtrado de MAC

Este capítulo describe cómo acceder a los indicadores de mandatos de configuración y supervisión de filtrado de MAC y cómo utilizar los mandatos disponibles. El capítulo incluye las secciones siguientes:

Acceso al indicador de mandatos de configuración de filtrado de MAC

Utilice el mandato **feature** del proceso CONFIG para acceder a los mandatos de configuración de filtrado de MAC. El mandato **feature** le permite acceder a los mandatos de configuración para características específicas fuera de los procesos de configuración de protocolo e interfaz de red.

Entre un interrogante de cierre después del mandato **feature** para obtener un listado de las características disponibles para el release de software. Por ejemplo:

```
Config> feature ?
WRS
BRS
MCF
Feature name or number [MCF]?
```

Para acceder al indicador de mandatos de configuración de filtrado de MAC, entre el mandato **feature** seguido del *número de característica* (3) o del *nombre abreviado* (MCF). Por ejemplo:

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

Cuando haya accedido al indicador de mandatos de configuración de filtrado de MAC, puede empezar a entrar mandatos de configuración específicos. Para volver al indicador de mandatos CONFIG en cualquier momento, entre el mandato **exit** en el indicador de mandatos de configuración de filtrado de MAC.

Mandatos de configuración de filtrado de MAC

Esta sección resume los mandatos de configuración de filtrado de MAC. Entre estos mandatos en el indicador de mandatos `Filter config>`.

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

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

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxx.
Attach	Añade una lista de filtros a un filtro.
Create	Crea una lista de filtros o un filtro INPUT o OUTPUT.

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

Mandato	Función
Default	Establece la acción por omisión para el filtro especificado en EXCLUDE, INCLUDE o TAG.
Delete	Elimina toda la información asociada con una lista de filtros. También suprime un filtro creado utilizando el mandato create filter.
Detach	Elimina una lista de filtros de un filtro.
Disable	Inhabilita totalmente el Filtrado de MAC o inhabilita un filtro determinado.
Enable	Habilita totalmente el Filtrado de MAC o habilita un filtro determinado.
List	Lista un resumen de todas las listas de filtros y filtros configurados por el usuario. También genera una lista de listas de filtros conectadas para este filtro y toda la información subsiguiente para el filtro.
Move	Reorganiza las listas de filtros conectadas con un filtro especificado.
Reinit	Reinicia todo el sistema de Filtrado de MAC desde una configuración actualizada, sin afectar el resto del direccionador.
Set-Cache	Cambia el tamaño de antememoria para un filtro.
Update	Añade información a una lista de filtros específica o la suprime de la misma. Le conduce a un menú de submandatos apropiados.
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 añadir una lista de filtros a un filtro.

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

Sintaxis:

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

Create

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

Sintaxis:

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

filter [input or output] *número-interfaz*

list *nombre-lista-filtros*
Crea una lista de filtros. Las listas se denominan mediante una serie exclusiva (Nombre-lista-filtros) de un máximo de 16 caracteres elegidos por el usuario. Este nombre se utiliza para identificar a la lista de filtros que se está creando. Este nombre también se utiliza con otros mandatos asociados con la lista de filtros.

filter [input o output] *número-interfaz*
Crea un filtro y lo sitúa en la red asociada con la dirección INPUT o OUTPUT en la interfaz proporcionada mediante un número de interfaz.

Por omisión, este filtro se crea sin ninguna lista de filtros conectada, con una acción por omisión INCLUDE y está ENABLED.

Default

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

Sintaxis:

def**ault** exclude *número-filtro*

include *número-filtro*

tag *número-identificador número-filtro*

exclude *número-filtro*
Establece la acción por omisión para el filtro con un número de filtro especificado en exclude (excluir).

include *número-filtro*
Establece la acción por omisión para el filtro con un número de filtro especificado en include (incluir).

tag *número-identificador número-filtro*
Establece la acción por omisión para el filtro con el número de filtro especificado en TAG y establece el valor de identificador asociado en un número de identificador.

Delete

Utilice el mandato **delete** para eliminar toda la información asociada con una lista de filtros y para liberar una serie asignada como un nombre para una nueva lista de filtros. Si una lista de filtros está conectada a un filtro que ya ha creado el usuario, este mandato visualizará un mensaje de error en la consola sin suprimir nada. Además también se suprimen todos los elementos de filtro que pertenecen a esta lista.

Este mandato también suprime un filtro creado utilizando el mandato **create filter**.

Sintaxis:

del**ete** list *lista-filtros*

filter *número-filtro*

list *lista-filtros*
Elimina toda la información asociada con una lista de filtros y libera una serie asignada como un nombre para una nueva lista de filtros. La lista de filtros debe ser una serie entrada mediante un mandato **create list** previo.

Si la lista de filtros está conectada a un filtro creado anteriormente por el usuario, este mandato visualizará un mensaje de error en la consola sin suprimir nada. Todos los elementos de filtro que pertenecen a esta lista también se suprimen cuando se utiliza este mandato.

filter *número-filtro*
Suprime un filtro que se ha creado utilizando el mandato **create filter**.

Detach

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

Sintaxis:

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

Disable

Utilice el mandato **disable** para inhabilitar totalmente el Filtrado de MAC o para inhabilitar un filtro determinado.

Sintaxis:

di**sable** all

filter *número-filtro*

all Inhabilita totalmente el Filtrado de MAC. Sin embargo, los filtros todavía están establecidos como ENABLED, si se han habilitado previamente.

filter *número-filtro*
Inhabilita un filtro determinado. El parámetro número-filtro corresponde a los números visualizados en el mandato **list filters**.

Enable

Utilice el mandato **enable** para habilitar totalmente el Filtrado de MAC o para habilitar un filtro determinado.

Sintaxis:

en**able** all

filter *número-filtro*

all Habilita totalmente el Filtrado de MAC, aunque los mismos filtros pueden estar todavía establecidos en DISABLED.

filter *número-filtro*
Habilita un filtro determinado. El parámetro número-filtro corresponde a los números visualizados en el mandato **list filters**.

List

Utilice el mandato **list** para listar un resumen de todas las listas de filtros y filtros configurados por el usuario. No se proporciona una lista de todas las listas de filtros conectadas a un filtro. Entre otra información visualizada por el mandato se incluye:

- Una lista que contiene el estado del sistema de filtrado (ENABLE, DISABLE)
- El conjunto de registros de lista de filtros configurados
- Cada uno de los registros de filtro configurados.

Además, se visualiza la información siguiente para cada filtro:

- Número de filtro
- Número de interfaz
- Dirección de filtro (INPUT, OUTPUT)
- Estado de filtro (ENABLE, DISABLE)

- Acción por omisión de filtro (TAG, INCLUDE, EXCLUDE).

Este mandato también genera una lista de las listas de filtros conectadas para este filtro y toda la información subsiguiente para el filtro.

Sintaxis:

l**ist** all

filter *número-filtro*

all Visualiza un resumen de todas las listas de filtros y filtros configurados.

filter *número-filtro*
Genera una lista de las listas de filtros conectadas para el filtro especificado y toda la información subsiguiente para el filtro.

Move

Utilice el mandato **move** para reorganizar las listas de filtros conectadas con un filtro especificado (proporcionado por el parámetro número-filtro). La lista proporcionada por Nombre1-lista-filtros se mueve inmediatamente antes de la lista proporcionada por Nombre2-lista-filtros.

Sintaxis:

m**ove** *nombre1-lista-filtros nombre2-lista-filtros número-filtro*

Reinit

Utilice el mandato **reinit** para reinicializar todo el sistema de Filtrado de MAC desde una configuración actualizada, sin afectar el resto del direccionador.

Sintaxis:

r**einit**

Set-Cache

Utilice el mandato **set-cache** para cambiar el tamaño de antememoria por omisión (16) por un número dentro del rango de 4 a 32768.

Sintaxis:

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

Update

Utilice el mandato **update** para añadir información a una lista de filtros específica o para suprimir información de la misma. La utilización de este mandato con el nombre de lista de filtros deseado le conduce al indicador de mandatos `Filter filter-list-name Config>` para la lista de filtros específica. A continuación, desde este nuevo indicador de mandatos puede cambiar la información de la lista especificada.

El nuevo nivel de indicador de mandatos se utiliza para añadir elementos de filtro a listas de filtros o para suprimirlos de éstas. El orden con el que se especifican los elementos de filtro para una lista de filtros es importante puesto que determina el orden con el que se aplican los elementos de filtro a un paquete.

Sintaxis:

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

Submandatos de actualización

Esta sección resume los submandatos de configuración de filtrado de MAC. Entre estos submandatos en el indicador de mandatos `Filter filter-list-name config>`.

Tabla 6. Resumen de submandatos de actualización

Submandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Add	Añade filtros de dirección MAC de origen o de destino o un filtro de ventana. Añade elementos de filtro a una lista de filtros.
Delete	Elimina elementos de filtro de una lista de filtros.
List	Lista un resumen de todas las listas de filtros y filtros configurados por el usuario. Además genera una lista de listas de filtros conectadas para este filtro y toda la información subsiguiente para el filtro.
Move	Reorganiza las listas de filtros conectadas con un filtro especificado.
Set-Action	Establece un elemento de filtro para evaluar la condición INCLUDE, EXCLUDE o TAG (con una opción tag-number).
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Utilice los submandatos siguientes para actualizar una lista de filtros.

Add

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

El orden con el que se añaden los elementos de filtro a una lista de filtros determinada es importante porque determina el orden con el que se aplican los elementos de filtro a un paquete.

Cada utilización del submandato **add** crea un elemento de filtro dentro de la lista de filtros. Al primer elemento de filtro creado se le asigna el número de elemento de filtro 1, al siguiente se le asigna el número 2 y así sucesivamente. Después de entrar un submandato **add** satisfactorio, el direccionador visualiza el número de elemento de filtro que se acaba de añadir.

La primera coincidencia que se produce detiene la aplicación de elementos de filtro y la lista de filtros evalúa en INCLUDE, EXCLUDE o TAG, según la acción designada de la lista de filtros. Si ninguno de los elementos de filtro de una lista de filtros produce una coincidencia, se devuelve la acción por omisión (INCLUDE, EXCLUDE o TAG) del filtro.

Sintaxis: a**dd** source *direc-MAC-hex Másc-hex*

destination *direc-MAC-hex Másc-hex*

window MAC *valor-despl datos-hex másc-hex*

window INFO *valor-despl datos-hex másc-hex*

source *direc-MAC-hex Másc-hex*

Añade un número hexadecimal que debe compararse con la dirección MAC de origen. ***direc-MAC-hex*** debe ser un número par de dígitos hexadecimales con un máximo de 16 dígitos y debe entrarse sin 0x delante.

El parámetro másc-hex debe tener la misma longitud que direc-MAC-hex y se aplica un AND lógico entre éste y la dirección MAC designada en el paquete. El argumento másc-hex por omisión debe ser todo 1 binarios.

El parámetro direc-MAC-hex se puede especificar en orden de bits canónicos o no canónicos. Un orden de bits canónicos se especifica igual que un número hexadecimal (por ejemplo, 000003001234). También se puede representar como una serie de dígitos hexadecimales con un guión (-) entre cada dos dígitos (por ejemplo, 00-00-03-00-12-34).

Un orden de bits no canónicos se especifica como una serie de dígitos hexadecimales con dos puntos (:) entre cada dos dígitos (por ejemplo, 00:00:C9:09:66:49). Las direcciones MAC de elementos de filtro siempre se visualizan utilizando un guión (-) o dos puntos (:) para diferenciar entre las representaciones canónicas y las no canónicas.

destination *direc-MAC-hex Másc-hex*

Actúa de igual modo que el submandato add source, con la excepción de que la comparación se realiza con el destino en lugar de la dirección MAC de origen del paquete.

window MAC *valor-despl datos-hex másc-hex*

Añade un elemento de filtro de ventana deslizante utilizando el desplazamiento especificado (calculado desde el principio de la trama) que efectúa una comparación entre los datos hexadecimales con la máscara y los datos del paquete.

window INFO *valor-despl datos-hex másc-hex*

Similar al mandato **add window mac**, salvo que el desplazamiento se calcula con respecto al principio del campo de información.

Delete

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

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

Sintaxis:

de**lete** *número-elemento-filtro*

List

Utilice el submandato **list** para imprimir una lista de todos los registros de elemento de filtro. Se visualiza la información siguiente sobre cada elemento de filtro de dirección MAC:

- La dirección MAC y la máscara de dirección en formato canónico o no canónico.
- números de elemento de filtro
- tipo de dirección (origen o destino)
- acción de lista de filtros

Sintaxis:

list canonical

noncanonical

mac-address canonical

mac-address noncanonical

window

canonical
Imprime un listado de todos los registros de elemento de filtro dentro de una lista de filtros, proporcionando los números de elemento, el tipo de dirección (SRC, DST), la dirección MAC en formato canónico y la máscara de dirección en formato canónico. También proporciona la acción de lista de filtros.

mac-address canonical
Imprime un listado de todos los registros de elemento de filtro dentro de una lista de filtros, proporcionando los números de elemento, el tipo de dirección (SRC, DST), la dirección MAC en formato canónico y la máscara de dirección en formato canónico. Además también se proporciona la acción de lista de filtros.

noncanonical
Imprime un listado de todos los registros de elemento de filtro dentro de una lista de filtros, proporcionando los números de elemento, el tipo de dirección (SRC, DST), la dirección MAC en formato no canónico y la máscara de dirección en formato no canónico. También proporciona la acción de lista de filtros.

mac-address noncanonical
Imprime un listado de todos los registros de elemento de filtro dentro de una lista de filtros, proporcionando los números de elemento, el tipo de dirección (SRC, DST), la dirección MAC en formato no canónico y la máscara de dirección en formato no canónico. También proporciona la acción de lista de filtros.

window Imprime un listado de todos los registros de elemento de filtro de ventana deslizante, proporcionando los números de elemento, la base, el desplazamiento, los datos y la máscara. También proporciona la acción de lista de filtros.

Move

El submandato **move** reorganiza los elementos de filtro dentro de la lista de filtros. El elemento de filtro cuyo número se especifica mediante *nombre1-elemento-filtro* se mueve y se renumera para que quede justo delante de *nombre2-elemento-filtro*.

Sintaxis:

m**ove** *nombre1-elemento-filtro nombre2-elemento-filtro*

Set-Action

El submandato **set-action** le permite establecer un elemento de filtro para evaluar la condición INCLUDE, EXCLUDE o TAG (con una opción tag-number). Si uno de los elementos de filtro de la lista de filtros coincide con el contenido del paquete que se considera para el filtrado, la lista de filtros evaluará a la condición especificada. El valor por omisión es INCLUDE.

Sintaxis:

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

Acceso al indicador de mandatos de supervisión de Filtrado de MAC

Utilice el mandato **feature** desde el proceso GWCON para acceder a los mandatos de supervisión de filtrado de MAC. El mandato **feature** le permite acceder a los mandatos de supervisión para características específicas del direccionador fuera de los procesos de configuración de protocolo e interfaz de red.

Entre un interrogante de cierre después del mandato **feature** para obtener un listado de las características disponibles para el release de software. Por ejemplo:

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

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

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

Cuando haya accedido al indicador de mandatos de supervisión de filtrado de MAC, puede empezar a entrar mandatos de configuración específicos. Para volver al indicador de mandatos GWCON en cualquier momento, entre el mandato **exit** en el indicador de mandatos de supervisión de filtrado de MAC.

Mandatos de supervisión de Filtrado de MAC

Esta sección resume los mandatos de supervisión de filtrado de MAC. Entre estos mandatos en el indicador de mandatos `Filter>`.

Tabla 7. Resumen de mandatos de supervisión de filtrado de MAC

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Clear	Borra las estadísticas "por filtro" listadas en el mandato list filter.
Disable	Inhabilita el Filtrado de MAC globalmente o "por filtro".
Enable	Habilita el Filtrado de MAC globalmente o "por filtro".
List	Lista un resumen de las estadísticas y valores para cada filtro que se ejecuta actualmente en el direccionador.
Reinit	Reinicia todo el sistema de Filtrado de MAC desde una configuración actualizada, sin afectar el resto 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.

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

Clear

Utilice el mandato **clear** para borrar estadísticas de filtro.

Sintaxis:

c**lear** all

filter *número-filtro*

all Borra las estadísticas listadas por el mandato **list all**.

filter *número-filtro*
Borra las estadísticas listadas por el mandato **list filter**.

Disable

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

El mandato también inhabilita el filtro especificado por el número de filtro. Este filtro se inhabilita sin modificar los registros de configuración. Si no se proporciona ningún argumento, el filtrado de MAC se inhabilita globalmente.

Sintaxis:

d**isable** all

filter *número-filtro*

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

filter *número-filtro*
Inhabilita el filtro especificado por el número de filtro. Este filtro se inhabilita sin modificar los registros de configuración. Si no se proporciona ningún número de filtro, el filtrado de MAC se inhabilita globalmente.

Enable

Utilice el mandato **enable** para habilitar el filtrado de MAC globalmente. Este mandato no habilita individualmente cada filtro.

El mandato también habilita el filtro especificado mediante el número de filtro. Este filtro se habilita sin modificar los registros de configuración. Si no se proporciona ningún argumento, el filtrado de MAC se habilita globalmente.

Sintaxis:

e**nable** all

filter *número-filtro*

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

filter *número-filtro*
Habilita el filtro especificado por el número de filtro. Este filtro se habilita sin modificar los registros de configuración. Si no se proporciona ningún número de filtro, el filtrado de MAC se habilita globalmente.

List

Utilice el mandato **list** para listar un resumen de estadísticas y valores para cada filtro que se ejecuta actualmente en el direccionador. Cuando se utiliza el mandato **list all** se visualiza la información siguiente:

- Acción por omisión
- Tamaño de antememoria
- Identificador por omisión
- Estado (habilitado/inhabilitado)
- Número de paquetes que se han filtrado como INCLUDE, EXCLUDE o TAG.

Además, el mandato **list filter** también visualiza la información siguiente para un filtro especificado:

- Toda la información visualizada por el mandato list all
- Todas las listas de filtros que se ejecutan actualmente en este filtro, que incluyen:
  - Nombre de lista
  - Acción de lista
  - Identificador de lista
  - Número de paquetes filtrados por cada lista de filtros.

Sintaxis:

list all

filter *número-filtro*

all lista estadísticas y valores para cada filtro que se ejecuta actualmente en el direccionador.

filter *número-filtro*
Genera estadísticas y valores para cada filtro además de todas las listas de filtros que se ejecutan actualmente en este filtro.

Reinit

Utilice el mandato **reinit** para reinicializar todo el sistema de Filtrado de MAC desde una configuración actualizada, sin afectar el resto del direccionador.

Sintaxis:

reinit

Soporte de reconfiguración dinámica de Filtrado de MAC

Esta sección describe la reconfiguración dinámica (DR) en lo que afecta a los mandatos de Talk 6 y Talk 5.

Delete interface de CONFIG (Talk 6)

El Filtrado de MAC soporta el mandato de CONFIG (Talk 6) **delete interface** sin restricciones.

Activate interface de GWCON (Talk 5)

El Filtrado de MAC soporta el mandato de GWCON (Talk 5) **activate interface** con la consideración siguiente:

> Si hay filtros MAC definidos para la interfaz recién activada, se reinicializarán todos los filtros MAC para cada interfaz.

El mandato de GWCON (Talk 5) **activate interface** soporta todos los mandatos específicos de interfaz de filtrado de MAC.

Reset interface de GWCON (Talk 5)

El Filtrado de MAC soporta el mandato de GWCON (Talk 5) **reset interface** con la consideración siguiente:

> Si hay filtros MAC definidos para la interfaz recién restablecida, se reinicializarán todos los filtros MAC para cada interfaz.

El mandato de GWCON (Talk 5) **reset interface** soporta todos los mandatos específicos de interfaz de Filtrado de MAC.

Mandato reset de componente GWCON (Talk 5)

El Filtrado de MAC soporta el siguiente mandato de GWCON (Talk 5) **reset** específico de Filtrado de MAC:

Mandato GWCON, feature MCF, reinit

Descripción: Reinicializa dinámicamente todos los filtros MAC configurados.

Efecto en la red: Ninguno.

Limitaciones: Ninguna.

El mandato **GWCON, feature mcf, reinit** soporta todos los mandatos de Filtrado de MAC.

Mandato activate de CONFIG (Talk 6)

El Filtrado de MAC soporta el mandato de CONFIG (Talk 6) **activate** siguiente:

Mandato CONFIG, feature MCF, reinit

Descripción: Reinicializa dinámicamente todos los filtros MAC configurados.

Efecto en la red: Ninguno.

Limitaciones: Ninguna.

El mandato **CONFIG, feature mcf, reinit** soporta todos los mandatos de Filtrado de MAC.

Utilización de Restauración de WAN

Este capítulo incluye las secciones siguientes:

Visión general para Restauración de WAN, Redireccionamiento de WAN y Desbordamiento de marcación

Las características Restauración de WAN, Redireccionamiento de WAN y Desbordamiento de marcación tienen funciones similares y pueden confundirse. Esta visión general pretende ayudarle a decidir cuál de estas funciones le será más útil y a encontrar la información necesaria para configurarlas.

Los mandatos de configuración para las tres características se incluyen en el capítulo "Configuración de Restauración de WAN". Para obtener información adicional sobre Redireccionamiento de WAN y Desbordamiento de marcación, consulte el apartado "Característica de Redireccionamiento de WAN" en la página 103.

Restauración de WAN

La Restauración de WAN es la función más básica. Cuando utilice Restauración de WAN, debe configurar un enlace primario y un enlace secundario. En caso de que falle el enlace primario, se inicia el enlace secundario y asume las características del primario. No es necesario configurar ninguna definición de protocolo en el enlace secundario porque utiliza las definiciones de protocolo desde el enlace primario.

Para la Restauración de WAN:

- Existe un emparejamiento entre un enlace primario y un enlace secundario.
- Sólo puede configurar un enlace primario para utilizar un enlace secundario específico.
- No deben configurarse definiciones de protocolo (por ejemplo: direcciones de protocolo) en el enlace secundario.
- El enlace primario puede ser una interfaz serie PPP o una interfaz PPP de múltiples enlaces. No puede ser una interfaz de circuito de marcación PPP.
- El enlace secundario debe ser un circuito de marcación PPP o una interfaz PPP de múltiples enlaces.
- Debe habilitar la característica WRS utilizando el mandato **enable wrs**.
- Debe habilitar el par primario/secundario utilizando el mandato **enable secondary-circuit**.

Nota: Cuando se configura el BRS en un enlace primario y el enlace primario forma parte de un par primario-secundario para Restauración de WAN, debe configurar el BRS en el enlace secundario. Generalmente cuando se configura Restauración de WAN, el enlace secundario adopta la identidad

del enlace primario. Sin embargo, esto no es así para el BRS; por lo tanto, debe configurarse el BRS tanto en el enlace primario como en el enlace secundario.

Redireccionamiento de WAN

El Redireccionamiento de WAN es una función más avanzada. Cuando utilice Redireccionamiento de WAN, debe configurar un enlace primario y un enlace alternativo. En caso de que falle el enlace primario, se inicia el enlace alternativo. Los protocolos de direccionamiento (por ejemplo, RIP o OSPF) detectan el enlace que está disponible y ajustan las rutas que se utilizan para reenviar paquetes.

Para el Redireccionamiento de WAN:

- Existe un emparejamiento entre un enlace primario y un enlace alternativo.
- Puede configurar múltiples enlaces primarios para que utilicen el mismo enlace alternativo.
- Debe configurar definiciones de protocolo en el enlace alternativo.
- El enlace primario puede ser cualquier enlace en el que pueda configurar protocolos direccionables (por ej. IP, IPX). Por ejemplo, el enlace primario puede ser una interfaz de la LAN una interfaz serie PPP, Frame Relay o X.25, o un circuito de marcación PPP o Frame Relay. A continuación se proporcionan ejemplos de tipos de interfaces que no pueden ser enlaces primarios: interfaces serie SDLC, interfaces serie SRLY y redes base como por ejemplo V.25bis e RDSI.
- El enlace alternativo puede ser cualquier enlace en el que puede configurar protocolos direccionables (por ej. IP, IPX) y el tipo de enlace de datos para el enlace alternativo no es necesario que coincida con el tipo de enlace de datos del enlace primario. Por ejemplo, el enlace alternativo puede ser una interfaz de la LAN, una interfaz serie PPP, Frame Relay o X.25, o un circuito de marcación PPP o Frame Relay. A continuación se proporcionan ejemplos de tipos de interfaz que no pueden ser enlaces alternativos: interfaces serie SDLC, interfaces serie SRLY y redes base como por ejemplo V.25bis e RDSI.
- Si el enlace primario es un circuito de marcación, no puede ser un circuito de marcación dial-on-demand. Para configurar el circuito de marcación para que no sea un circuito de marcación dial-on-demand debe configurarlo con **set idle 0** en el indicador de mandatos `Circuit Config>` de marcación. Consulte el apartado “Configuración y supervisión de circuitos de marcación” en la publicación *Guía del usuario de software* para obtener más información.

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

  Nota: Los circuitos de marcación I.430/I.431 y Channelized T1/E1 se pueden utilizar como primarios de WRS sin ninguna configuración explícita.
- Debe habilitar la característica WRS utilizando el mandato **enable wrs**.
- Debe habilitar el par primario/alternativo utilizando el mandato **enable alternate-circuit**.
- Puede configurar opcionalmente horas de estabilización, horas de estabilización de direccionamiento, horas de inicio y detención de reversión para controlar la conmutación de nuevo al enlace primario.

- Si el enlace alternativo es X.25, debe utilizar el mandato **national-personality set disconnect-procedure active** cuando configure la interfaz X.25 del direccionador que tiene habilitado Redireccionamiento de WAN y debe utilizar el mandato **national-personality set disconnect-procedure passive** cuando configure la interfaz X.25 del otro direccionador.

Desbordamiento de marcación

Desbordamiento de marcación es similar a Redireccionamiento de WAN, pero no es necesario que falle el enlace primario para que se inicie el enlace alternativo. En lugar de ello, se supervisa la utilización del enlace primario y, si se excede un umbral, se inicia el enlace alternativo. Además, no se utilizan todos los protocolos en el enlace alternativo. El protocolo IP sólo se activa en el enlace alternativo y los demás protocolos siguen utilizando el enlace primario a menos que éste se desactive.

Si el enlace primario se desactiva, Redireccionamiento de WAN asume el control y cualquier protocolo configurado en la interfaz alternativa puede empezar a detectar y utilizar rutas en la interfaz alternativa.

Para Desbordamiento de marcación:

- Desbordamiento de marcación utiliza el emparejamiento primario/alternativo de un par de Redireccionamiento de WAN.
- Debe configurar un par de redireccionamiento de la WAN para utilizar Desbordamiento de marcación y se aplican todas las restricciones de la configuración de Redireccionamiento de WAN.
- El enlace primario de un par de Redireccionamiento de WAN que se va a utilizar para Desbordamiento de marcación debe ser Frame Relay.
- Debe utilizar el protocolo de direccionamiento OSPF para utilizar Desbordamiento de marcación.
- Debe utilizar el mandato **enable dial-on-overflow** para configurar el umbral de add (añadir) y el umbral de drop (excluir), el intervalo de supervisión de ancho de banda y el tiempo mínimo de alternativo activo.
- Las horas de estabilización, las horas de estabilización de direccionamiento y las horas de inicio de reversión y de detención de reversión no afectan a la operación del desbordamiento de marcación.

Para obtener más información sobre Redireccionamiento de WAN, consulte el apartado “Característica de Redireccionamiento de WAN” en la página 103.

Antes de empezar

Antes de configurar Restauración de WAN, debe tener lo siguiente:

1. Una interfaz serie primaria (línea alquilada) configurada para PPP. Puede utilizar cualquier interfaz serie en el direccionador.
2. Una interfaz con los circuitos de marcación asociados configurados en el direccionador. Puede utilizar una interfaz RDSI, una interfaz V.25bis o una interfaz V.34 como red base.
3. Un circuito de marcación secundario para la marcación cuando se desactive la interfaz primaria. Para configurar un circuito de marcación para ello, establezca

el temporizador de desocupado en cero utilizando el mandato **set idle** en el indicador de mandatos `Circuit Config>` de dicha marcación. Este mandato impide que el circuito de marcación sea Dial-on-Demand.

4. Un circuito de marcación secundario a un extremo del enlace configurado solamente para enviar llamadas. Utilice el mandato **set calls outbound** en el indicador de mandatos `Circuit Config>`.

   Nota: No configure ninguna dirección de protocolo en la interfaz secundaria. Las asignaciones de protocolo para la interfaz primaria se utilizan en el enlace secundario (circuito de marcación) cuando está activo.

5. Un circuito de marcación secundario al otro extremo del enlace configurado solamente para recibir llamadas. Utilice el mandato **set calls inbound** en el indicador de mandatos `Circuit Config>`.

Procedimiento de configuración para Restauración de WAN

Esta sección describe los pasos necesarios para configurar Restauración de WAN. Antes de empezar, utilice el mandato **list device** en el indicador de mandatos `Config>` para listar los números de interfaz de distintos dispositivos.

Siga estos pasos para configurar Restauración de WAN en el direccionador:

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

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

2. Asigne un circuito de marcación secundario a la interfaz primaria. Este circuito de marcación efectuará una copia de seguridad de la interfaz primaria. Por ejemplo:

```
WRS Config>add secondary-circuit
Secondary interface number  [0]? 3
Primary interface number  [0]? 1
```

3. Habilite la Restauración de WAN en el circuito de marcación secundario que ha añadido. Por ejemplo:

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

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

```
WRS Config>enable wrs
```

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

Configuración de circuito de marcación secundario

Para configurar un circuito de marcación:

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

```
Config> list device
```

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

```
Config> add device dial-circuit

Adding device as interface 3
Defaulting Data-link protocol to PPP
Use "net 3" command to configure circuit parameters
```

2. Configure la interfaz secundaria (circuito de marcación) para que tenga el mismo tipo de enlace que la interfaz primaria (PPP) desde el indicador de mandatos `Config>` tal como se muestra a continuación:

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

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

   ```
   Config> network 3
   ```

4. Seleccione la interfaz de red base para el circuito de marcación. La red base puede ser V.25bis, RDSI o V.34.

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

5. Establezca el temporizador de desocupado de circuito de marcación en 0 (0=fijo) como se indica a continuación:

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

6. Establezca un extremo de la conexión de copia de seguridad para recibir llamadas (por ejemplo, direccionador A) como se muestra a continuación:

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

7. Establezca el otro extremo de la conexión de reserva para iniciar llamadas (por ejemplo, direccionador B) como se indica a continuación:

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

Notas:

1. No utilice el mandato **set calls both**. El establecimiento individual de las llamadas ayuda a evitar las colisiones entre los intentos de conexión de entrada y de salida.
2. No configure ninguna dirección de reenvío (por ejemplo, IP, IPX, etc.) en el circuito de marcación. Las asignaciones de protocolo para la interfaz primaria se utilizan en la interfaz secundaria (circuito de marcación) cuando está activa.
3. Para obtener instrucciones para la configuración de RDSI, consulte “Utilización de la interfaz RDSI” en la publicación *Guía del usuario de software*.
4. Para obtener instrucciones para la configuración de V.25bis, consulte “Utilización de la interfaz V.25bis” en la publicación *Guía del usuario de software*.
5. Para obtener instrucciones para la configuración de V.34, consulte “Utilización de la interfaz V.34” en la publicación *Guía del usuario de software*.

Configuración y supervisión de Restauración de WAN

Este capítulo describe la configuración de Restauración de WAN y los mandatos operativos. El capítulo incluye las secciones siguientes:

Nota: Consulte el apartado "Configuración y supervisión de circuitos de marcación" en la publicación *Guía del usuario de software* para obtener información sobre cómo configurar circuitos de marcación. Un circuito de marcación se puede utilizar como interfaz cuando se configura Redireccionamiento de WAN.

Mandatos de configuración de Restauración de WAN, Redireccionamiento de WAN y Desbordamiento de marcación

Los mandatos de configuración de Restauración de WAN le permiten crear o modificar la configuración de interfaz de Restauración de WAN. Esta sección resume y explica los mandatos de configuración de Restauración de WAN.

La Tabla 8 lista los mandatos de configuración de Restauración de WAN y su función. Entre estos mandatos en el indicador de mandatos `WRS Config>`. Para acceder a `WRS Config>`, entre **feature wrs** en el indicador de mandatos `Config>`.

Tabla 8. Resumen de los mandatos de configuración de Restauración de WAN

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxx.
Add	Añade una correlación de primario-secundario (para Restauración de WAN) o primario-alternativo (para Redireccionamiento de WAN).
Disable	Inhabilita el WRS, una correlación de circuito secundario individual o correlación de circuito alternativo.
Enable	Habilita el WRS, una correlación de circuito secundario individual o correlación de circuito alternativo.
List	Visualiza la configuración actual de Restauración.
Remove	Elimina una correlación entre primario y secundario o una correlación entre primario y alternativo creada con add.
Set	Establece los valores para la estabilización, estabilización de direccionamiento y temporizadores de reversión de hora.
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 identificar un circuito de marcación secundario o alternativo o una interfaz de enlace alquilado para un enlace serie primario.

Sintaxis:

add alternate-circuit

secondary-circuit

alternate-circuit

El mandato **add alternate-circuit** enlaza una interfaz alternativa con una interfaz primaria para finalidades de Redireccionamiento de WAN. Puede asignar varias interfaces primarias a una sola interfaz alternativa. No es necesario que el tipo de enlace alternativo sea igual que el tipo de enlace primario (por ejemplo, el tipo de enlace alternativo puede ser un circuito de marcación PPP y el tipo de enlace primario puede ser una línea alquilada de Frame Relay).

Ejemplo:

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

Alternate interface number

Es el número que se ha asignado previamente a la interfaz alternativa. Cualquier interfaz de la LAN, interfaz serie PPP, Frame Relay o X.25, o circuito de marcación PPP o Frame Relay es una interfaz alternativa elegible. El valor por omisión es 0.

Primary interface number

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

secondary-circuit

El mandato **add secondary-circuit** enlaza una interfaz secundaria con una interfaz primaria para finalidades de Restauración de WAN. Deben haberse configurado previamente ambas interfaces. Sólo puede asignar una interfaz secundaria a una primaria y viceversa.

Ejemplo:

```
WRS Config>add secondary-circuit
Secondary interface number  [0]? 4
Primary interface number  [0]? 1
```

Secondary interface number

Es el número de interfaz de circuito de marcación previamente asignado a la interfaz secundaria cuando se añadió el dispositivo. Cualquier circuito de marcación PPP o interfaz PPP de múltiples enlaces puede ser una interfaz secundaria. El valor por omisión es 0.

Primary interface number

Es el número de interfaz de la interfaz primaria que se ha asignado previamente al añadir el dispositivo. Una interfaz

primaria puede ser cualquier línea alquilada previamente definida que ejecute PPP. El valor por omisión es 0.

Disable

Utilice el mandato **disable** para inhabilitar la función Restauración de WAN o para inhabilitar un emparejamiento primario/secundario para Restauración de WAN o para inhabilitar un emparejamiento primario/alternativo para Redireccionamiento de WAN o para inhabilitar Desbordamiento de marcación para un emparejamiento primario/alternativo.

Sintaxis:

disable alternate-circuit

dial-on-overflow

secondary-circuit

wrs

alternate-circuit *número-interfaz*

Inhabilita el emparejamiento primario/alternativo para Redireccionamiento de WAN.

Ejemplo:

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

Alternate interface number

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

dial-on-overflow *número-interfaz-alt*

Inhabilita el desbordamiento de marcación para todos los emparejamientos primario/alternativo utilizando una interfaz alternativa especificada.

Ejemplo:

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

Alternate interface number

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

secondary-circuit *número-interfaz*

Inhabilita la restauración de una interfaz primaria determinada mediante su interfaz secundaria asociada hasta el siguiente mandato **enable secondary-circuit** en la consola el WRS. Ambas interfaces deben haberse configurado previamente y enlazarse en la configuración del WRS.

Ejemplo:

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

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

wrs Inhabilita globalmente la característica Restauración de WAN en el direccionador. Esto significa que las características Redireccionamiento de WAN y Desbordamiento de marcación también están inhabilitadas.

Enable

Utilice el mandato **enable** para habilitar la función Restauración de WAN, para habilitar un emparejamiento primario/secundario para Restauración de WAN, para habilitar un emparejamiento primario/alternativo para Redireccionamiento de WAN o para habilitar el desbordamiento de marcación para un emparejamiento primario/alternativo.

Sintaxis:

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

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

Ejemplo:

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

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

dial-on-overflow
Habilita el desbordamiento de marcación y le permite establecer parámetros para controlar el funcionamiento del desbordamiento de marcación.

Ejemplo:

```
WRS>enable dial-on-overflow

Para el desbordamiento de marcación, sólo el tráfico IP puede desbordarse a la
interfaz alternativa.
Primary interface number  ]0]? 1
add-threshold (1-100% utilization) [90]?
drop-threshold(0-99% utilization) [60]?
bandwidth test interval(10-200 seconds) [15]?
minimum time to keep the alternate up (20-21600 sec.) [300]?
Dial-on overflow is enabled.
Remember to configure the primary interface's line speed!
```

Primary interface number
Es el número de interfaz de la interfaz primaria para la que está habilitando el desbordamiento de marcación. El valor por omisión es 0.

add-threshold
Determina cuándo una interfaz alternativa se activará para ancho de banda adicional. Este valor debe expresarse como

un porcentaje de la velocidad de línea configurada de la interfaz primaria. El valor por omisión es 90%.

drop-threshold
Determina cuándo una interfaz alternativa ya no es necesaria para ancho de banda adicional. Este valor debe expresarse como un porcentaje de la velocidad de línea configurada de la interfaz primaria. El valor por omisión es 60%.

bandwidth monitoring interval
Determina con qué frecuencia se supervisa el ancho de banda de la interfaz primaria para *umbral-add* y *umbral-drop.* El valor por omisión es 15 segundos.

Minimum time to keep alternate up
Este período de tiempo debe incluir tiempo suficiente para que los direccionadores establezcan la nueva ruta cuando el tráfico de IP en el direccionador local se redirecciona a la interfaz alternativa. El valor por omisión es 5 minutos.

secondary-circuit *número-interfaz*
Habilita la restauración de un enlace primario por parte del enlace secundario indicado.

Ejemplo:

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

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

wrs Habilita la función de la característica Restauración de WAN en el direccionador. Esto significa que si las características Redireccionamiento de WAN y Desbordamiento de marcación están configuradas, también se habilitan.

List

Utilice el mandato **list** para visualizar información de configuración global para la característica y para visualizar información de configuración para pares primario-secundario de Restauración de WAN, pares primario-alternativo de Redireccionamiento de WAN y Desbordamiento de marcación.

Sintaxis:

list

Ejemplo:

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

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

  1 - WAN Frame Re   2 - WAN Frame Relay      Yes    dflt  dflt  Not Set  Not Set 15


 Dial-on-overflow is enabled.
 Primary    add-       drop-      test       minimum
 Interface  threshold  threshold  interval   alt up time
 ---------  ---------  ---------  ---------  -----------
      1         29%        20%      15 sec.   300 sec.
```

Remove

Utilice el mandato **remove** para suprimir la correlación entre una interfaz alternativa o secundaria (de seguridad) y la interfaz primaria.

Sintaxis:

remove alternate-circuit

secondary-circuit

alternate-circuit *número-interfaz-alternativa número-interfaz-primaria*
Elimina la correlación entre una interfaz alternativa (de seguridad) y la interfaz primaria para Redireccionamiento de WAN. Ambas interfaces deben haberse asignado y enlazado previamente utilizando el mandato **add alternate-circuit**.

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

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

Ejemplo:

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

secondary-circuit *número-interfaz-secundaria número-interfaz-primaria*
Elimina la correlación entre una interfaz secundaria (de seguridad) y la interfaz primaria para Restauración de WAN. Ambas interfaces deben haberse asignado y enlazado previamente utilizando el mandato **add secondary-circuit**.

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

Número-interfaz-primaria

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

Ejemplo:

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

Set

Utilice el mandato **set** para establecer los parámetros para Redireccionamiento de WAN.

Sintaxis:

set **?**

default

first-stabilization

routing-stabilization

stabilization

start-time-of-day-revert-back

stop-time-of-day-revert-back

default Utilice el mandato **set default** para establecer los valores por omisión que deben utilizar los enlaces que no tienen configuradas horas de estabilización ni de primera estabilización.

first-stabilization

Establece el valor de primera estabilización por omisión que deben utilizar los enlaces para los que no se ha configurado hora de primera estabilización.

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

stabilization

Establece el valor de estabilización por omisión que deben utilizar los enlaces para los que no se ha configurado hora de estabilización.

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

first-stabilization

Establece el número de segundos de inicialización de direccionador antes de que el direccionamiento para este enlace primario se conmute al enlace alternativo si no está activo el enlace primario.

Ejemplo:

```
WRS Config>set first Primary interface number [0]? 1
First primary stabilization time (0 - 3600 seconds -1 = default)  [-1]?
```

Primary interface number

Es el número de interfaz primaria para la que está estableciendo la primera-estabilización. El valor por omisión es 0.

First primary stabilization time

La hora de estabilización para esta interfaz primaria. El valor por omisión es 1.

routing-stabilization

Establece el valor de estabilización-direccionamiento. Este parámetro define el número de segundos que el enlace primario y el enlace alternativo permanecen activos después de haber detectado que el enlace primario está activo y que el temporizador de estabilización, si existe alguno, ha caducado. El tiempo de estabilización-direccionamiento se proporciona de modo que los protocolos de direccionamiento, como por ejemplo, OSPF o RIP tengan suficiente tiempo para reconocer la disponibilidad de la nueva ruta. Sin el temporizador de estabilización de direccionamiento, el tráfico puede interrumpirse durante unos segundos mientras la ruta alternativa se ha inhabilitado y la ruta primaria todavía no se ha encontrado.

Si el enlace alternativo estaba activo antes del redireccionamiento, dicho enlace permanece activo y se ignora el temporizador de estabilización de direccionamiento. Si el enlace alternativo se había desactivado antes del redireccionamiento, o durante el redireccionamiento, dicho enlace permanece desactivado y se ignoran el temporizador de estabilización de direccionamiento y el temporizador de estabilización.

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

Primary interface number

Valores válidos: de 0 al número de interfaces configurado en el direccionador

Valor por omisión: 0

Routing-stabilization timer

Valores válidos: de 1 a 3600 segundos

Valor por omisión: 0

stabilization

Establece el número de segundos necesarios después de detectar por primera vez el enlace primario como activo antes de que empiece el proceso de reinicialización del direccionamiento en el enlace primario. Cuando caduca el temporizador de estabilización, se desactiva el enlace alternativo a menos que se haya configurado el temporizador de estabilización de direccionamiento. El temporizador de estabilización de direccionamiento se iniciará tan pronto como caduque el temporizador de estabilización y mantendrá los enlaces primario y alternativo el tiempo suficiente para mantener el tráfico en el enlace alternativo mientras los protocolos de direccionamiento, como por ejemplo OSPF y RIP, restablecen la ruta a través del enlace primario.

Ejemplo:

```
WRS Config>set first Primary interface number [0]? 1
Primary stabilization time (0 - 3600 seconds -1 = default)  [-1]?
```

Primary interface number

Es el número de interfaz primaria de la interfaz primaria para la que está estableciendo la estabilización. El valor por omisión es 0.

Primary stabilization time

El tiempo de estabilización para la interfaz primaria. El valor por omisión es 1.

start-time-of-day-revert-back

La hora más temprana del día en que el direccionador puede conmutar de nuevo a la ruta primaria. El direccionador puede revertir a la primaria cualquier hora entre la hora del día inicial de reversión y la hora del día final de reversión. La reversión a la primaria sólo se produce si la primaria está activa y se cumplen los parámetros de estabilización. El valor por omisión es 0.

Ejemplo:

```
WRS Config>set start
Primary interface number  [0]? 1
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0] 3
Start time-of-day revert back configured. Remember to configure stop time-of-day
```

Primary interface number

Es el número de interfaz primaria para la que está estableciendo la primera-estabilización. El valor por omisión es 0.

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

Esta hora marca la hora inicial para la ventana de reversión. El direccionador puede revertir a la interfaz primaria en cualquier momento entre la hora del día inicial de reversión y la hora del día final de reversión. La reversión a la interfaz primaria sólo se produce si la interfaz primaria está activa y se cumplen los parámetros de estabilización. El valor por omisión es 1.

stop-time-of-day-revert-back

Esta hora marca la hora final para la ventana de reversión. El direccionador puede revertir a la interfaz primaria en cualquier momento entre la hora del día inicial de reversión y la hora del día final de reversión. La reversión a la interfaz primaria sólo se produce si la interfaz primaria está activa y se cumplen los parámetros de estabilización. El valor por omisión es 1.

Ejemplo:

```
WRS Config>set stop Primary interface number  [0]? 1
Time-of-Day revert back window stop (1 - 24 hours, 0 = not configured) [0]?5
```

Primary interface number

Es el número de interfaz primaria para la que está estableciendo la primera-estabilización. El valor por omisión es 0.

Time-of-day-revert-back-window stop

Esta hora marca la hora final para la ventana de reversión. El direccionador puede revertir a la interfaz primaria en cualquier momento entre la hora del día inicial de reversión y la hora del día final de reversión. La reversión a la interfaz primaria sólo se produce si la interfaz primaria está activa y se cumplen los parámetros de estabilización. El valor por omisión es 1.

Acceso al proceso de supervisión de interfaz de Restauración de WAN

Para acceder al proceso de supervisión de interfaz de Restauración de WAN, entre el mandato siguiente en el indicador de mandatos GWCON (+):

```
+ feature wrs
```

Mandatos de supervisión de Restauración de WAN

Los mandatos de supervisión de Restauración de WAN (WRS) le permiten supervisar el estado de los pares primario-secundario de Restauración de WAN, pares primario-alternativo de Redireccionamiento de WAN y Desbordamiento de marcación. Las modificaciones efectuadas en el estado operativo de Restauración de WAN, Redireccionamiento de WAN y Desbordamiento de marcación mediante la interfaz de supervisión no se mantienen en los reinicios del direccionador.

Acceda al indicador de mandatos WRS entrando **feature wrs** en el indicador de mandatos de GWCON (+). La Tabla 9 lista los mandatos del WRS y sus funciones, y las secciones siguientes explican los mandatos.

Tabla 9. Mandatos de supervisión de Restauración de WAN

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Clear	Borra las estadísticas de supervisión visualizadas utilizando el mandato **list**.
Disable	Inhabilita el WRS, o un circuito secundario, o alternativo, individual, o el desbordamiento de marcación.
Enable	Habilita el WRS, o un circuito secundario, o alternativo, individual, o el desbordamiento de marcación.
List	Visualiza la información de supervisión para uno o todos los circuitos alternativos o secundarios.
Set	Establece los valores para la estabilización, estabilización de direccionamiento y temporizadores de hora del día de reversión.
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 borrar estadísticas de Restauración de WAN, Redireccionamiento de WAN y desbordamiento de marcación que se visualizan utilizando el mandato **list**.

Sintaxis:

c**lear**

Nota: Este mandato borra *Período de restauración más largo*, pero no borra *Período de restauración más reciente*. Para la visualización de la pantalla, consulte el ejemplo del mandato **list**.

Disable

Utilice el mandato **disable** para inhabilitar completamente la característica Restauración de WAN, inhabilitar la restauración de una interfaz primaria determinada mediante su interfaz secundaria asociada, inhabilitar una interfaz alternativa o inhabilitar el desbordamiento de marcación.

Sintaxis:

disable alternate-circuit

dial-on-overflow

secondary-circuit

wrs

alternate-circuit

Inhabilita un par primario/secundario para Redireccionamiento de WAN. Puede ser que varios emparejamientos utilicen el mismo circuito alternativo. Este mandato inhabilita todos los emparejamientos que utilicen el circuito alternativo especificado.

Ejemplo:

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

Alternate circuit number

Es el número del circuito alternativo. El valor por omisión es 0.

dial-on-overflow

Inhabilita el desbordamiento de marcación para el emparejamiento primario/alternativo especificado sin cambiar el estado habilitado/inhabilitado del Redireccionamiento de WAN para dicho emparejamiento. Si el desbordamiento de marcación direcciona activamente, acaba cuando finaliza el siguiente intervalo de supervisión.

secondary-circuit

Inhabilita la restauración de una interfaz primaria determinada mediante su interfaz secundaria asociada hasta el siguiente mandato **restart**, **reload** o **enable secondary-circuit**. Ambas interfaces deben haberse configurado previamente y enlazarse en la configuración del WRS.

Normalmente, en **talk 5** (GWCON), el mandato **disable** hace que la interfaz quede inactiva y permanezca inactiva. Sin embargo, para la interfaz secundaria de Restauración de WAN, éste no es el caso. El mandato **disable** aplicado a la interfaz secundaria no inhabilita la interfaz. Sólo inhabilita la llamada actual (es decir, hace que se desconecte cualquier llamada activa.) Para inhabilitar la utilización del circuito secundario, debe entrar **disable secondary-circuit** en el indicador de mandatos de supervisión de Restauración de WAN e inhabilitar la interfaz secundaria en el indicador de mandatos GWCON de nivel superior. **Ejemplo:**

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

Secondary interface number

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

wrs La inhabilitación del WRS inhabilita Restauración de WAN, Redireccionamiento de WAN y Desbordamiento de marcación en el direccionador hasta el siguiente mandato **restart**, **reload** o **enable WRS**.

Enable

Utilice el mandato **enable** para habilitar la interfaz de Restauración de WAN, habilitar la restauración de un enlace primario mediante un circuito secundario, habilitar un circuito alternativo o habilitar el desbordamiento de marcación.

Sintaxis:

en**able** alternate-circuit

dial-on-overflow

secondary-circuit

wrs

alternate-circuit

Habilita los emparejamientos primario/alternativo para Redireccionamiento de WAN para todos los emparejamientos utilizando el alternativo especificado.

Ejemplo:

```
WRS> enable alternate-circuit
Alternate circuit number  [0]? 3
```

Alternate circuit number

Es el número de interfaz del circuito alternativo. El valor por omisión es 0.

dial-on-overflow

Habilita el desbordamiento de marcación y le permite establecer los parámetros que controlan el desbordamiento de marcación. Opcionalmente, le permite hacer que el protocolo IP se conmute inmediatamente al alternativo, si se ha sobrepasado el umbral de add.

Ejemplo:

```
WRS> dial-on-overflow

For dial-on-overflow, only IP traffic can overflow to the alternate interface.
Primary interface number [0]? 1
add-threshold (1-100% utilization) [90]?
drop-threshold(0-99% utilization) [60]?
bandwidth test interval(10-200 seconds) [15]?
minimum time to keep the alternate up (20-21600 sec.) [300]?
Dial-on overflow is enabled.
Remember to configure the primary interface's line speed!

Do you want to switch IP traffic to the alternate now?(Yes or [No]):
WRS>
```

secondary-circuit

Habilita la restauración de un enlace primario por parte del enlace secundario indicado.

Ejemplo:

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

Secondary interface number

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

wrs Habilita la función de la característica Restauración de WAN en el direccionador. Esta característica debe habilitarse para utilizar Restauración de WAN, Redireccionamiento de WAN o Desbordamiento de marcación.

Set

Utilice el mandato **set** para establecer los parámetros para Redireccionamiento de WAN.

Sintaxis:

set **?** default

first-stabilization

routing-stabilization

stabilization

start-time-of-day-revert-back

stop-time-of-day-revert-back

default Utilice el mandato **set default** para establecer los valores por omisión que deben utilizar los enlaces que no tienen configuradas horas de estabilización ni de primera estabilización.

Ejemplo:

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

first-stabilization

Establece el valor de primera estabilización por omisión que deben utilizar los enlaces para los que no se ha configurado hora de primera estabilización.

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

stabilization

Establece el valor de estabilización por omisión que deben utilizar los enlaces para los que no se ha configurado hora de estabilización.

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

first-stabilization

Establece el número de segundos de inicialización de direccionador antes de que el direccionamiento para este enlace primario se conmute al enlace alternativo si no está activo el enlace primario.

Ejemplo:

```
WRS Config>set first Primary interface number [0]? 1
First primary stabilization time (0 - 3600 seconds -1 = default)  [-1]?
```

Primary interface number

Es el número de interfaz primaria para la que está estableciendo la primera-estabilización. El valor por omisión es 0.

First primary stabilization time

La hora de estabilización para esta interfaz primaria. El valor por omisión es 1.

routing-stabilization

Establece el valor de estabilización-direccionamiento. Este parámetro define el número de segundos que el enlace primario y el enlace alternativo permanecen activos después de haber detectado que el enlace primario está activo y que el temporizador de estabilización, si existe alguno, ha caducado. El tiempo de estabilización-direccionamiento se proporciona de modo que los protocolos de direccionamiento, como por ejemplo, OSPF o RIP tengan suficiente tiempo para reconocer la disponibilidad de la nueva ruta. Sin el temporizador de estabilización de direccionamiento, el tráfico puede interrumpirse durante unos segundos mientras la ruta alternativa se ha inhabilitado y la ruta primaria todavía no se ha encontrado.

Si el enlace alternativo estaba activo antes del redireccionamiento, dicho enlace permanece activo y se ignora el temporizador de estabilización de direccionamiento. Si el enlace alternativo se había desactivado antes del redireccionamiento, o durante el redireccionamiento, dicho enlace permanece desactivado y se ignoran el temporizador de estabilización de direccionamiento y el temporizador de estabilización.

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

Primary interface number

Valores válidos: de 0 al número de interfaces configurado en el direccionador

Valor por omisión: 0

Routing-stabilization timer

Valores válidos: de 1 a 3600 segundos

Valor por omisión: 0

stabilization

Establece el número de segundos necesarios después de detectar por primera vez el enlace primario como activo antes de que empiece el proceso de reinicialización del direccionamiento en el enlace primario. Cuando caduca el temporizador de estabilización, se desactiva el enlace alternativo a menos que se haya configurado el temporizador de estabilización de direccionamiento. El temporizador de estabilización de direccionamiento se iniciará tan pronto como caduque el temporizador de estabilización y mantendrá los enlaces primario y alternativo el tiempo suficiente para mantener el tráfico en el enlace alternativo mientras los protocolos de direccionamiento, como por ejemplo OSPF y RIP, restablecen la ruta a través del enlace primario.

Ejemplo:

```
WRS Config>set first Primary interface number [0]? 1
Primary stabilization time (0 - 3600 seconds -1 = default)  [-1]?
```

Primary interface number

Es el número de interfaz primaria de la interfaz primaria para la que está estableciendo la estabilización. El valor por omisión es 0.

Primary stabilization time

El tiempo de estabilización para la interfaz primaria. El valor por omisión es 1.

start-time-of-day-revert-back

La hora más temprana del día en que el direccionador puede conmutar de nuevo a la ruta primaria. El direccionador puede revertir a la primaria cualquier hora entre la hora del día inicial de reversión y la hora del día final de reversión. La reversión a la primaria sólo se produce si la primaria está activa y se cumplen los parámetros de estabilización. El valor por omisión es 0.

Ejemplo:

```
WRS Config>set start
Primary interface number [0]? 1
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0] 3
Start time-of-day revert back configured. Remember to configure stop time-of-day
```

Primary interface number

Es el número de interfaz primaria para la que está estableciendo la primera-estabilización. El valor por omisión es 0.

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

Esta hora marca la hora inicial para la ventana de reversión. El direccionador puede revertir a la interfaz primaria en cualquier momento entre la hora del día inicial de reversión y la hora del día final de reversión. La reversión a la interfaz primaria sólo se produce si la interfaz primaria está activa y se cumplen los parámetros de estabilización. El valor por omisión es 1.

stop-time-of-day-revert-back

Esta hora marca la hora final para la ventana de reversión. El direccionador puede revertir a la interfaz primaria en cualquier momento entre la hora del día inicial de reversión y la hora del día final de reversión. La reversión a la interfaz primaria sólo se produce si la interfaz primaria está activa y se cumplen los parámetros de estabilización. El valor por omisión es 1.

Ejemplo:

```
WRS Config>set stop Primary interface number  [0]? 1
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0]?
5
```

Primary interface number

Es el número de interfaz primaria para la que está estableciendo la primera-estabilización. El valor por omisión es 0.

Time-of-day-revert-back-window stop

Esta hora marca la hora final para la ventana de reversión. El direccionador puede revertir a la interfaz primaria en cualquier momento entre la hora del día inicial de reversión y la hora del día final de reversión. La reversión a la interfaz primaria sólo se produce si la interfaz primaria está activa y se

cumplen los parámetros de estabilización. El valor por omisión es 1.

List

Utilice el mandato **list** para visualizar información de supervisión sobre uno o todos los pares primario-secundario de Restauración de WAN o sobre uno o todos los pares primario-alternativo de Redireccionamiento de WAN.

Sintaxis:

list all

alternate-circuit

secondary-circuit

summary

all Proporciona información de resumen, seguida de la información específica, para cada interfaz secundaria.

Ejemplo:

```
list all
WAN Restoral/Re-route is enabled with 2 circuits configured
    Total restoral attempts =          7 completions   =          7
    Total packets forwarded =         39
    Longest completed restoral period in hrs:min:sec     0:03:27

    Total overflow attempts =         20 completions   =         19
    Longest completed overflow period in hrs:min:sec     0:05:00

   Primary       Secondary    Restoral  Restoral   Current/Longest
Net Interface  Net Interface  Enabled    Active          Duration
-------------  -------------  --------  --------   --------------------
  4  PPP/0       7  PPP/1       No         No       00:03:27/ 00.06.00

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

Total restoral attempts
El número de veces que ha fallado el enlace primario y que ha hecho que el redireccionador intentara activar un enlace secundario.

Completions
El número de intentos de restauración satisfactorios cuando el enlace secundario se activo y se utilizó.

Total packets forwarded
El número total de paquetes reenviados a través de la interfaz secundaria. Es la suma de ambas direcciones y es acumulativa para todas las restauraciones satisfactorias, hasta que se emita el mandato restart o clear restoral-statistics.

Longest Completed Restoral Period
Este campo visualiza en horas, minutos y segundos el período más largo de tiempo en que una restauración ha estado en operación, sin contar ninguna utilización actual.

Total Overflow Attempts
El número de intentos debido a un desbordamiento.

Completions
El número de intentos de desbordamiento satisfactorios cuando el enlace secundario se activó y se utilizó.

Longest Completed Overflow Period
Visualiza en horas, minutos y segundos el período más largo de tiempo que un desbordamiento ha estado en operación, sin contar ninguna utilización actual.

Primary Net Interface
La interfaz que está siendo sustituida por su interfaz secundaria asociada.

Secondary Net Interface
El circuito de marcación que se utiliza para sustituir la interfaz primaria asociada.

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

Restoral Active
Indica si la restauración está activa (Sí o No).

Current/Longest Duration
Indica en horas, minutos y segundos la duración actual y más larga en que la interfaz de red secundaria ha estado activa.

Primary Net Interface
La interfaz que está siendo sustituida por su interfaz alternativa asociada.

Alternate Net Interface
La interfaz que se utiliza como alternativa para sustituir la interfaz primaria asociada.

Re-route/Overflow Enabled
Indica si el redireccionamiento y el desbordamiento están habilitados (Sí o No).

Re-route/Overflow Active
Indica si el redireccionamiento y el desbordamiento están activos (Sí o No).

Recent Re-route Overflow Duration
Indica en horas, minutos y segundos la duración de redireccionamiento y desbordamiento reciente de la interfaz de red alternativa.

Alternate-circuit
Proporciona totales para un circuito alternativo. Permite que el operador de supervisión recupere el estado de Redireccionamiento de WAN y las estadísticas asociadas para cada interfaz alternativa y su correlación primaria asociada.

Ejemplo:

```
WRS>li alt 7
Primary    1:FR/0 Frame Relay SCC Serial Line
Alternate  7:PPP/1 Point to Point V.25bis Dial Circuit
reroute Enabled, currently inactive
overflow Enabled, currently inactive
Primary first stabilization time: default (0 seconds)
Primary stabilization time: default (0 seconds)
Routing-stabilization time: 15 seconds
Time-of-day revert back not configured: start = 0, stop = 0
Restored 0 times (0 attempts)
Overflow 0 times (0 attempts)
```

Primary Interface
La interfaz que está siendo sustituida por su interfaz alternativa asociada.

Alternate Interface
El circuito de marcación que se utiliza para sustituir la interfaz primaria asociada.

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

Overflow Enabled
Indica si el desbordamiento de esta interfaz primaria está habilitada actualmente.

Primary first stabilization
El número de segundos en la inicialización del direccionador antes de que el direccionamiento para este enlace primario se conmute al enlace alternativo si el enlace primario no está activo.

First stabilization
El número de segundos necesarios después de detectar por primera vez que el enlace primario está activo antes de conmutar el direccionamiento del enlace alternativo de nuevo al enlace primario. El direccionamiento a través del enlace alternativo continúa hasta que el enlace primario permanece activo durante este número de segundos.

Routing stabilization
El número de segundos necesarios después de conmutar el direccionamiento de nuevo al enlace primario antes de que el enlace alternativo se desactive. Durante este tiempo tanto el enlace primario como el enlace alternativo permanecen activos. El intervalo se proporciona para que los protocolos de direccionamiento, como por ejemplo OSPF y RIP, tengan tiempo para reconocer la disponibilidad del direccionador a través de la interfaz primaria.

Time-of-day revert back
La hora del día en la que el direccionador puede conmutar de nuevo a la ruta primaria. El direccionador puede revertir a la primaria cualquier hora entre la hora del día inicial de reversión y la hora del día final de reversión. La reversión a la primaria sólo se produce si la primaria está activa y se cumplen los parámetros de estabilización. El valor por omisión es 0.

Restored times
El número de intentos para redireccionar la interfaz primaria.

Overflow times
El número de intentos de desbordamiento de marcación.

secondary-circuit
Proporciona totales para cada circuito secundario. Permite que el operador de supervisión recupere el estado de Restauración de WAN y las estadísticas asociadas para cada interfaz secundaria y su correlación primaria asociada.

Ejemplo:

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

                                                  Secondary
Primary Interface          Secondary Interface    Enabled
-------------------        -------------------    ---------
1  PPP/0  Point to Poi     3  PPP/1  Point to Poi    Yes

Router primary interface state = Up
Router secondary interface state = Available
Restoral Statistics:

  Primary restoral attempts =       6   completions =    5
  Restoral packets forwarded =    346
    Most recent restoral period in hrs:min:sec          00:08:20
```

Primary Interface
La interfaz que está siendo sustituida por su interfaz secundaria asociada.

Secondary Interface
El circuito de marcación que se utiliza para sustituir la interfaz primaria asociada.

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

Router Primary Interface State
Indica que el estado de la interfaz primaria es uno de los siguientes:

Activo - Indica que el enlace está activo.

Inactivo - Indica que el enlace está inactivo.

Inhabilitado - Indica que el operador ha inhabilitado el enlace.

No presente - Indica que el enlace está configurado pero que existe un problema de hardware.

Router Secondary Interface State
Indica que el estado de interfaz secundaria asociada es uno de los siguientes:

Activo - Indica que el enlace está activo.

Inactivo - Indica que el enlace está inactivo. Esto también ocurre cuando la red base para la interfaz secundaria se inhabilita en el indicador de mandatos `Config>` o en la consola del operador.

Disponible - Indica que el enlace está en la modalidad de espera.

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

Restoral Statistics:

Primary Restoral Attempts
El número de veces que ha fallado el enlace primario y que ha hecho que el direccionador intentara activar un enlace secundario.

Restoral Packets forwarded
Este campo indica el número total de paquetes reenviados.

Most Recent Restoral Period
Indica cuánto tiempo ha estado activo el enlace secundario, la última vez que se utilizó durante la utilización de restauración actual.

summary Proporciona totales para cada circuito secundario.

Ejemplo:

```
list summary
WAN Restoral is enabled with 3 circuit(s) configured

  Total restoral attempts =      3 completions =      2
  Total packets forwarded =    346
  Longest restoral period in hrs:min:sec   00:08:20

Primary Interface and State      Secondary Interface and State
---------------------------   ----------------------------------
 1  PPP/0  - Up                 3  PPP/1  - Available
```

Total restoral attempts
El número de veces que ha fallado el enlace primario y que ha hecho que el direccionador intentara activar un enlace secundario.

Completions
El número de intentos de restauración satisfactorios cuando el enlace secundario se activó y se utilizó.

Total packets forwarded
El número total de paquetes reenviados a través de la interfaz secundaria. Es la suma de ambas direcciones y es acumulativa para todos los períodos de restauración hasta que se utilizó el mandato restart o clear restoral-statistics.

Longest restoral period
Este campo visualiza en horas, minutos, segundos el período más largo de tiempo en que se ha utilizado la restauración, sin contar la actualización actual.

Primary Interface and State
La interfaz que está siendo sustituida por su interfaz secundaria asociada. Los estados válidos son:

Activo - Indica que el enlace está activo.

Inactivo - Indica que el enlace está inactivo.

Inhabilitado - Indica que el operador ha inhabilitado el enlace.

No presente - Indica que el enlace está configurado pero que existe un problema de hardware.

Secondary Interface and State

El circuito de marcación que se utiliza para sustituir al primario asociado. Los estados válidos son:

Activo - Indica que el enlace está activo.

Inactivo - Indica que el enlace está inactivo. Esto también ocurre cuando la red base para la interfaz secundaria se inhabilita en el indicador de mandatos `Config>` o en la consola del operador.

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

Disponible - Indica que el enlace está en la modalidad de espera.

Soporte de reconfiguración dinámica de Restauración de WAN y Redireccionamiento de WAN

Esta sección describe la reconfiguración dinámica (DR) en lo que afecta a los mandatos de Talk 6 y Talk 5.

Delete interface de CONFIG (Talk 6)

La Restauración de WAN y el Redireccionamiento de WAN soportan el mandato de CONFIG (Talk 6) **delete interface** sin restricciones.

Activate interface de GWCON (Talk 5)

La Restauración de WAN y el Redireccionamiento de WAN soportan el mandato de GWCON (Talk 5) **activate interface** con las consideraciones siguientes:

- No se puede activar una interfaz primaria de Restauración de WAN si la interfaz secundaria está restaurando activamente otra interfaz primaria.
- No se puede activar una interfaz primaria de Restauración de WAN si la interfaz secundaria era una interfaz primaria de Restauración de WAN, una interfaz primaria de Redireccionamiento de WAN o una interfaz alternativa de Redireccionamiento de WAN antes del mandato **activate interface**.
- No se puede activar una interfaz secundaria de Restauración de WAN si otra interfaz secundaria está restaurando activamente la interfaz primaria.
- No se puede activar una interfaz secundaria de Restauración de WAN si la interfaz primaria era una interfaz secundaria de Restauración de WAN, una interfaz primaria de Redireccionamiento de WAN o una interfaz alternativa de Redireccionamiento de WAN antes del mandato **activate interface**.
- No se puede activar una interfaz primaria de Redireccionamiento de WAN si la interfaz alternativa se ha utilizado como interfaz primaria de Redireccionamiento de WAN, interfaz primaria de Restauración de WAN o

interfaz alternativa de Restauración de WAN antes del mandato **activate interface**.

- No se puede activar una interfaz alternativa de Redireccionamiento de WAN si la interfaz primaria era la interfaz primaria de otra interfaz alternativa, era una interfaz alternativa de Redireccionamiento de WAN, una interfaz primaria de Restauración de WAN o una interfaz secundaria de Restauración de WAN.

El mandato de GWCON (Talk 5) **activate interface** soporta todos los mandatos específicos de interfaz de Restauración de WAN y Redireccionamiento de WAN.

Reset interface de GWCON (Talk 5)

La Restauración de WAN y el Redireccionamiento de WAN no soportan el mandato de GWCON (Talk 5) **reset interface**.

Mandatos de cambio temporal de GWCON (Talk 5)

La Restauración de WAN y el Redireccionamiento de WAN soportan los mandatos de GWCON siguientes que cambian temporalmente el estado operativo del dispositivo. Estos cambios se pierden siempre que se vuelve a cargar o se reinicia el dispositivo o se ejecuta cualquier mandato reconfigurable dinámicamente.

Mandatos
GWCON, feature wan, disable alternate-circuit
GWCON, feature wan, disable dial-on-overflow
GWCON, feature wan, disable secondary-circuit
GWCON, feature wan, disable wrs
GWCON, feature wan, enable alternate-circuit
GWCON, feature wan, enable dial-on-overflow
GWCON, feature wan, enable secondary-circuit
GWCON, feature wan, set default
GWCON, feature wan, first-stabilization
GWCON, feature wan, stabilization
GWCON, feature wan, routing-stabilization
GWCON, feature wan, start-time-of-day-revert-back
GWCON, feature wan, stop-time-of-day-revert-back

Característica de Redireccionamiento de WAN

Este capítulo describe la característica de redireccionamiento de WAN. El capítulo incluye las secciones siguientes:

Importante

Para los modelos 1Sx y 1Ux, el Redireccionamiento de WAN sólo está disponible si el direccionador tiene un puerto de WAN y un canal-B RDSI activo.

Visión general de Redireccionamiento de WAN

Redireccionamiento de WAN le permite configurar una ruta alternativa de modo que si un enlace primario falla, el direccionador inicia automáticamente una nueva conexión con el destino a través de la ruta alternativa. Consulte el apartado "Visión general para Restauración de WAN, Redireccionamiento de WAN y Desbordamiento de marcación" en la página 75 para obtener una explicación de Restauración de WAN y cómo funcionan conjuntamente Redireccionamiento de WAN y el Desbordamiento de marcación.

El proceso de Redireccionamiento de WAN incluye:

1. La detección de una anomalía del enlace primario
2. La conmutación al enlace alternativo
3. La detección de la recuperación del enlace primario
4. La conmutación de nuevo al enlace primario

El enlace alternativo puede ser cualquier enlace en el que pueden configurarse protocolos direccionables (por ejemplo, IP, IPX) y el tipo de enlace de datos del enlace alternativo no es necesario que coincida con el tipo del enlace primario. Por ejemplo, el enlace alternativo puede ser una interfaz LAN, una interfaz serie PPP, Frame Relay o X.25, o un circuito de marcación PPP o Frame Relay. A continuación se proporcionan ejemplos de tipos de interfaz que no pueden ser enlaces alternativos: interfaces serie SDLC, interfaces serie SRLY y redes base como V.25 bis e ISDN.

Nota: Si el enlace primario o el enlace secundario no son un circuito de marcación, dicho circuito de marcación no se puede configurar para marcación a petición. Utilice el mandato **set idle 0** en el indicador de mandatos `Circuit Config>` para configurar el circuito de marcación de modo que no pueda efectuar marcación a petición. Consulte el apartado "Configuración y supervisión de circuitos de marcación" en la publicación *Guía del usuario de software* para obtener más información.

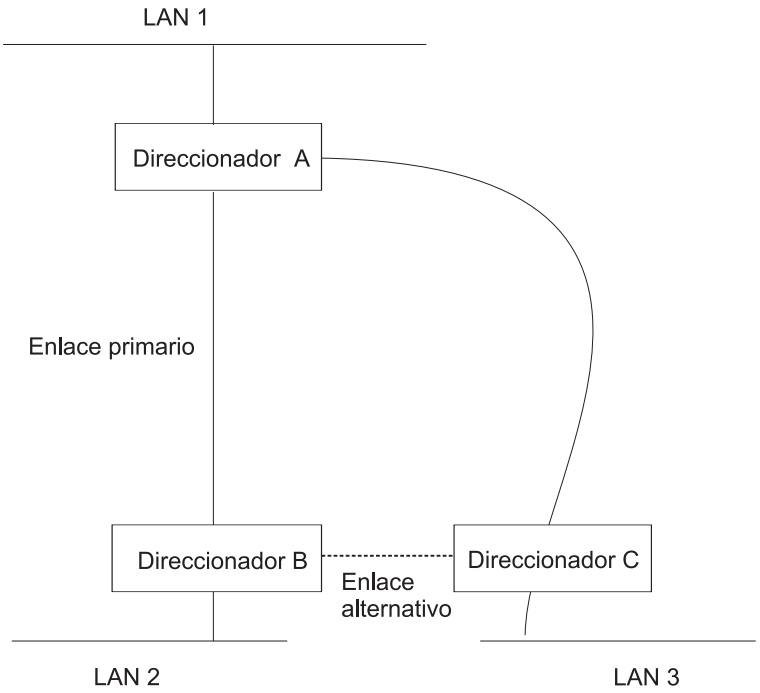


Figura 3. Redireccionamiento de WAN. Normalmente, existe una conexión entre los Direccionadores A y B y los Direccionadores A y C. Si el enlace primario entre los direccionadores A y B falla, el redireccionamiento de WAN establece un enlace alternativo entre los direccionadores B y C. A continuación, los direccionadores A y B se pueden comunicar a través del direccionador C.

Desbordamiento de marcación

El desbordamiento de marcación le permite utilizar una interfaz alternativa para el tráfico IP cuando la velocidad del tráfico en el enlace primario alcanza un umbral especificado. Esto significa que no es necesario desactivar la interfaz primaria antes de activar el enlace alternativo. Cuando el tráfico de la interfaz primaria alcanza el umbral especificado, el direccionador activa el enlace alternativo. Para utilizar el desbordamiento de marcación, debe estar configurado el Redireccionamiento de WAN y la interfaz primaria debe ser Frame Relay. IP es el único protocolo al cual se puede conmutar para la interfaz alternativa mediante desbordamiento de marcación. Además, OSPF debe utilizarse como protocolo de direccionamiento IP en lugar de RIP cuando se utiliza el desbordamiento de marcación.

Para obtener información sobre cómo configurar el desbordamiento de marcación, consulte el apartado “Mandatos de configuración de Restauración de WAN, Redireccionamiento de WAN y Desbordamiento de marcación” en la página 81.

Supervisión de ancho de banda

El intervalo para la supervisión de ancho de banda puede especificarse para el desbordamiento de marcación durante la configuración de Redireccionamiento de WAN. Se supervisa la utilización de ancho de banda de la recepción y transmisión de la interfaz primaria. Cuando el ancho de banda de la interfaz primaria alcanza el umbral *add*, se genera una petición de Redireccionamiento de WAN para activar la interfaz alternativa. Si Redireccionamiento de WAN activa satisfactoriamente la

interfaz alternativa, IP detiene el direccionamiento a través de la interfaz primaria e inicia el direccionamiento a través de la interfaz alternativa.

Si Redireccionamiento de WAN no activa satisfactoriamente la ruta alternativa, intenta periódicamente activar la interfaz alternativa hasta que la utilización del ancho de banda de la interfaz primaria está por debajo del umbral de *drop*.

Cuando la utilización del ancho de banda de recepción y transmisión de la interfaz primaria alcanza el umbral de *drop* y finaliza el tiempo mínimo de activo configurado se desactiva la interfaz alternativa. Esto hace que IP detenga el direccionamiento a través de la interfaz alternativa e inicie la utilización de la interfaz primaria.

El umbral de add y el umbral de drop se especifican como un porcentaje de la velocidad de línea configurada para el enlace primario. La velocidad de línea configurada no siempre coincide con la velocidad real del enlace. La cantidad de tráfico en el enlace en cada dirección se calcula por separado. El umbral se excede si el tráfico en alguna de las dos direcciones es mayor que el porcentaje especificado.

Configuración de Redireccionamiento de WAN

A continuación se describen los pasos necesarios para configurar el redireccionamiento de WAN. La sección siguiente contiene un ejemplo sobre cómo llevar a cabo estas tareas.

Para configurar Redireccionamiento de WAN, es necesario:

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

   Puede especificar una hora del día para reversión al enlace primario que se producirá cuando finalice el período de estabilización (si se ha configurado). Esto permite que el enlace secundario esté activo hasta la hora elegida por el usuario y revertir al enlace primario durante las horas de menos carga.

   Nota: Los enlaces primario y alternativo pueden ser de tipos de enlace de datos diferentes. Los enlaces primario y alternativo pueden ser:

   - Una interfaz LAN.
   - Una interfaz serie PPP.
   - Una interfaz serie Frame Relay.
   - Una interfaz serie X.25.
   - Un circuito de marcación PPP.
   - Un circuito de marcación Frame Relay.

Ejemplo de configuración de Redireccionamiento de WAN

La Figura 4 muestra un redireccionamiento de WAN utilizando un circuito de marcación Frame Relay a través de RDSI como enlace alternativo. Si la DLCI Frame Relay entre el direccionador A y el direccionador C falla, el redireccionamiento de WAN utiliza el circuito de marcación para establecer una conexión alternativa a través del direccionador D. Si uno de los enlaces primarios desde una sucursal a la oficina central falla, el redireccionamiento de WAN establece una ruta alternativa a la oficina central a través de otra sucursal.

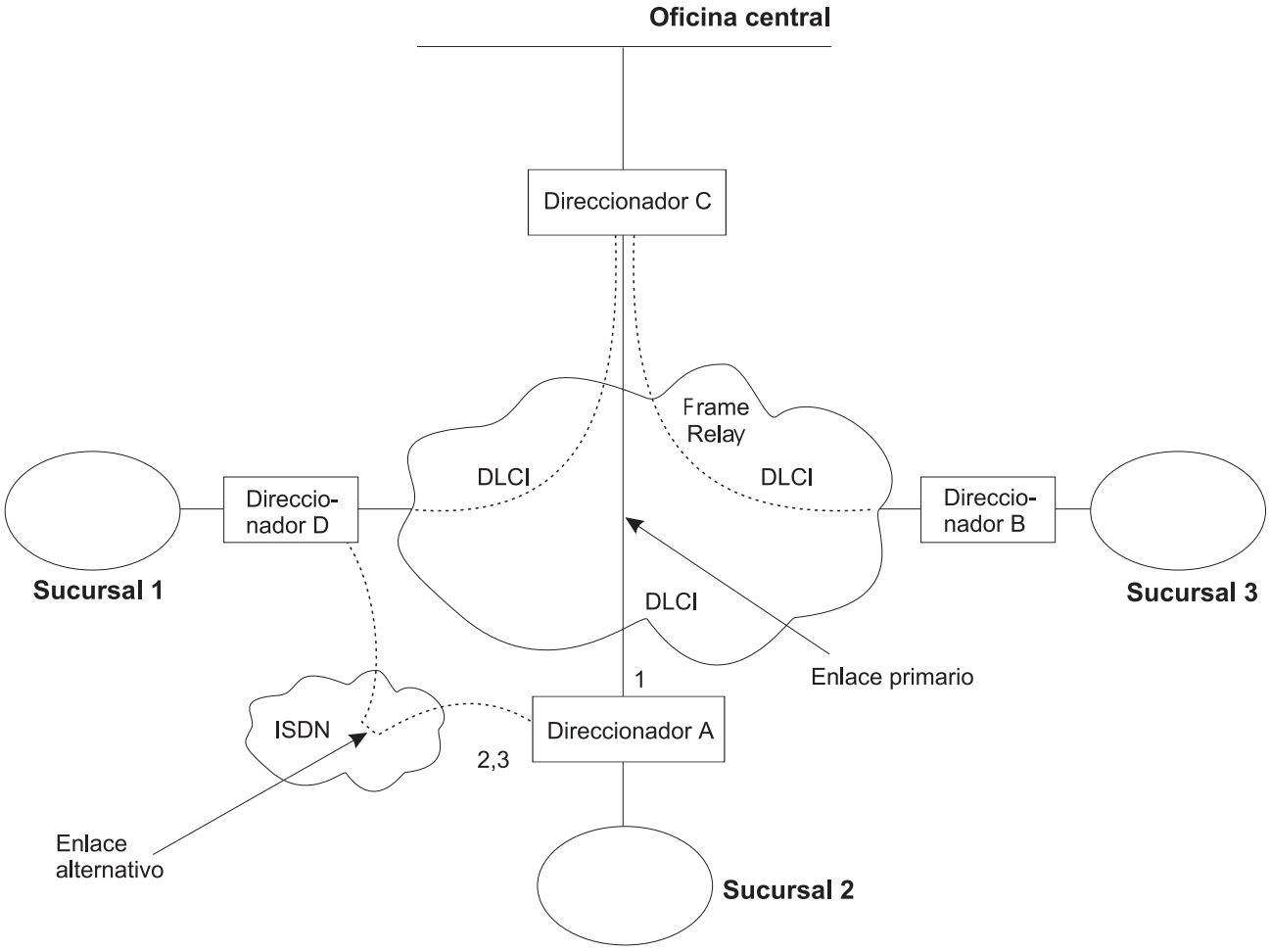


Figura 4. Ejemplo de configuración de Redireccionamiento de WAN. Las sucursales utilizan frame relay para conectarse a la oficina central.

En las secciones siguientes se describe cómo configurar el redireccionamiento de WAN en el Direccionador A en la Figura 4. Deberá:

- Configurar la interfaz frame relay primaria (1) para que tenga un PVC Necesario un Grupo PVC Necesario o habilitar la característica No-PVC en la interfaz frame relay.
- Configurar la interfaz RDSI (2) y su circuito de marcación frame relay (3).
- Asignar el circuito de marcación para que sea el enlace alternativo para la interfaz frame relay primaria y emitir el mandato **set idle 0** en el indicador de mandatos `Circuit Config>` de marcación para inhabilitar la marcación a petición para este circuito.

- Opcionalmente, puede asignar:
  - El período de estabilización para el enlace primario,
  - La ventana de hora del día para reversión para el enlace primario.

A continuación, estas tareas se describen detalladamente.

Configuración de la interfaz Frame Relay

Para configurar la interfaz frame relay para el redireccionamiento de WAN, en el Direccionador A, añada un PVC entre los Direccionadores A y C en la interfaz Frame Relay primaria.

Para hacer que la interfaz FR primaria se declare a sí misma inactiva cuando la conexión con otro(s) direccionador(es) se pierda, tiene tres opciones:

1. Habilitar la característica No-PVC. Cuando esta característica está habilitada, la interfaz FR se desactiva cuando no existe ningún PVC activo.
2. Configurar un PVC según convenga pero sin incluir el PVC en un grupo de PVC necesarios. En este caso, la interfaz FR se desactiva cuando el PVC queda inactivo.
3. Configurar un conjunto de PVC según convenga y como parte de un grupo de PVC necesario. En este caso, la interfaz FR se desactiva cuando todos los PVC de un grupo de PVC necesarios quedan inactivos.

Siga estos pasos para configurar la interfaz Frame Relay primaria:

1. Si todavía no lo ha hecho, establezca el enlace de datos en la interfaz RDSI para que sea Frame Relay.

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

2. Inicie el proceso de configuración de Frame Relay.

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

   Nota: Complete solamente *uno* de los dos pasos restantes para configurar la interfaz frame relay primaria.

3. Añada un PVC utilizando el mandato **add permanent-virtual-circuit**.

   Para configurar el PVC según convenga:

   Entre **y** como respuesta a la pregunta “Is circuit required for interface operation ?”.

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

   a. Entre **y** como respuesta a la pregunta “Does circuit belong to a Required PVC group ?”.

   b. Entre un nombre de grupo como respuesta a la pregunta “What is the group name ?”.

   Si ya ha añadido los PVC, utilice el mandato **change permanent-virtual-circuit** para configurar el PVC según convenga y para asignarlo a un Grupo de PVC necesarios, del modo más apropiado. Consulte Using Frame Relay Interfaces en la publicación *Guía del usuario de software* para obtener más información.

```
FR Config>add permanent-virtual-circuit
Circuit number [16]?
Committed Information Rate (CIR) in bps [64000]?
Committed Burst Size (Bc) in bits [64000]?
Excess Burst Size (Be) in bits [0]?
Assign circuit name []?
Is circuit required for interface operation [N]?y
Does the circuit belong to a required PVC group [N]? y
What is the group name []?group1
```

4. Si lo desea, habilite la característica No-PVC.

   Nota: Complete este paso *solamente* si ha pasado por alto el paso anterior.

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

Se pueden establecer parámetros adicionales para frame relay. Para obtener más información, consulte 'Using Frame Relay' en la publicación *Guía del usuario de software*.

Configuración de la interfaz RDSI y del circuito de marcación

Configure la interfaz RDSI y el circuito de marcación entre el Direccionador A y el Direccionador D. Consulte 'Utilización de la interfaz RDSI' en la publicación *Guía del usuario de software* para obtener información sobre cómo configurar interfaces RDSI y circuitos de marcación.

A diferencia de en la Restauración de WAN, debe configurar protocolos direccionables en el circuito de marcación que se utilizarán como enlace alternativo. Si no se puede impedir que dichos protocolos direccionables envíen paquetes de mantenimiento, el enlace alternativo establecerá una conexión incluso si no es necesario un redireccionamiento. En este caso, si desea utilizar el enlace alternativo sólo para redireccionamiento, inhabilite el circuito de marcación. Para inhabilitar el circuito de marcación, entre el mandato **disable interface** en el indicador de mandatos `Config>`.

Si ha asignado varios circuitos de marcación a la interfaz RDSI, puede establecer una prioridad para los circuitos de marcación. Si todos los canales B tienen circuitos de marcación activos en la interfaz física y un circuito con una prioridad más alta recibe un paquete, la conexión de prioridad más baja se finaliza y el circuito de prioridad más alta establece una conexión.

Puede establecer la prioridad entre 0 y 15, donde 15 es el circuito de prioridad más alta y 0 es el circuito de prioridad más baja. La prioridad por omisión para los circuitos de marcación nuevos es 8. Entre **set priority** en el indicador de mandatos `Circuit Config>` para cambiar la prioridad.

Asignación y configuración del enlace alternativo

Inicie el proceso de configuración de redireccionamiento de WAN para asignar el circuito de marcación como enlace alternativo para una interfaz LAN, una interfaz serie PPP, Frame Relay o X.25, o un circuito de marcación PPP o Frame Relay y, si es necesario, para especificar, los períodos de estabilización y/o la ventana de hora del día para reversión.

Existen tres tipos de períodos de estabilización:

- *Primer período de estabilización* es el período de tiempo que el direccionador espera para que la interfaz primaria se active cuando el direccionador intenta activarla por primera vez. Si, después del primer período de estabilización, el primario no se activa, el redireccionamiento de WAN activa el enlace alternativo.

- *Período de estabilización* es el período de tiempo que el direccionador espera para asegurarse de que el enlace primario sea fiable antes de que conmute del enlace alternativo de nuevo al enlace primario.
- *Período de estabilización de direccionamiento* es el período de tiempo que el direccionador mantiene activo tanto el enlace primario como el enlace alternativo después de haber conmutado del enlace alternativo de nuevo al enlace primario. Este tiempo lo utilizan los protocolos de direccionamiento, como por ejemplo OSPF o RIP, para reconocer la disponibilidad de la nueva ruta a través del enlace primario antes de que el enlace alternativo se desactive.

La ventana de hora del día para reversión es la hora específica del día en la que el usuario desea revertir al enlace primario después de haberlo activado y de que haya pasado el tiempo de estabilidad configurado.

Si se utiliza un reloj de 24 horas, el usuario especifica las horas de inicio y detención de la ventana de reversión. El enlace secundario permanece activo y no se desactiva hasta que se llega a la hora de inicio. Si la hora del día en la que el enlace primario se activa está entre las horas de inicio y de detención (en la ventana), la conmutación al enlace primario se produce inmediatamente después de finalizar el tiempo de estabilidad.

Siga estos pasos para asignar y configurar el enlace alternativo:

1. Inicie el proceso de configuración de Restauración de WAN.

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

2. Asigne el circuito de marcación como enlace alternativo para la interfaz frame relay primaria.

```
WRS Config>add alternate-circuit
Alternate interface number  [0]? 4
Primary interface number  [0]? 1
```

3. Habilite el circuito alternativo.

```
WRS Config>enable alternate-circuit
Alternate interface number  [0]? 4
```

4. Opcionalmente, especifique un primer período de estabilización.

   Para establecer el primer período de estabilización para una interfaz primaria específica, utilice el mandato **set first-stabilization-period**. Para establecer el primer período de estabilización por omisión para todas las interfaces que no tienen períodos específicos, utilice el mandato **set default first-stabilization-period**.

```
WRS Config>set first-stabilization-period
Primary interface number [0]?
First primary stabilization time (0 - 3600 seconds -1=default) [-1]?

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

5. Opcionalmente, especifique un período de estabilización. Para establecer un período de estabilización para interfaces específicas, utilice el mandato **set stabilization-period**. Para establecer un período de estabilización por omisión para todas las interfaces que no tienen establecido ningún período específico, utilice el mandato **set default stabilization-period**.

```
WRS Config>set stabilization-period
Primary interface number [0]?
First primary stabilization time (0 - 3600 seconds -1=default) [-1]?
WRS Config>set default stabilization-period
Default first primary stabilization time (0 - 3600 seconds) [0]?
```

6. Opcionalmente, especifique un período de estabilización de direccionamiento. Para establecer un período de estabilización de direccionamiento para interfaces específicas, utilice el mandato **set routing-stabilization**.

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

7. Opcionalmente, especifique una ventana de hora del día para reversión.

   Para establecer las horas de inicio y detención para ventanas de interfaz específicas, utilice los mandatos start-time-of-day-revert-back y stop-time-of-day-revert-back. El valor por omisión de cero indica que no hay ninguna ventana configurada. El reloj de 24 horas empieza a la 1 a.m. y finaliza a las 24, o medianoche. Si las horas de inicio y detención son iguales (pero no cero), la reversión se producirá exactamente a dicha hora.

   A continuación se proporcionan dos ejemplos sobre cómo establecer la ventana de reversión:

   a. Una hora de inicio que sea 23 y una hora de detención que sea 3 dará como resultado una ventana de reversión desde las 11 p.m. hasta las 3 a.m.

   b. Una hora de inicio que sea 1 y una hora de detención que sea 5 dará como resultado una ventana de reversión desde la 1 a.m. a las 5 a.m.

```
WRS Config> set start-time-of-day-revert-back
Primary interface number [0]?
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0]?
WRS Config> set stop-time-of-day-revert-back
Primary interface number [0]?
Time-of-Day revert back window stop (1 - 24 hours, 0 = not configured) [0]?
```

Utilización de la característica Network Dispatcher

Este capítulo describe cómo utilizar la característica Network Dispatcher y contiene las secciones siguientes:

Network Dispatcher utiliza la tecnología de equilibrado de carga de IBM para determinar el servidor más apropiado para recibir cada conexión nueva. Ésta es la misma tecnología utilizada en el producto SecureWay ® Network Dispatcher de IBM para Solaris, Windows NT® y AIX®.

Visión general del Network Dispatcher

El Network Dispatcher es una característica que aumenta el rendimiento de los servidores reenviando peticiones de sesión TCP/IP a diferentes servidores dentro de un grupo de servidores, equilibrando de este modo las peticiones entre todos los servidores. El reenvío es transparente para los usuarios y las aplicaciones. El Network Dispatcher es útil para aplicaciones de servidor como por ejemplo e-mail, servidores de la World Wide Web, consultas de bases de datos paralelas distribuidas y otras aplicaciones TCP/IP.

El Network Dispatcher también se puede utilizar para el equilibrado de carga del tráfico de aplicaciones UDP sin estado en un grupo de servidores.

El Network Dispatcher puede ayudar a maximizar el potencial de la oficina proporcionando una solución eficaz, flexible y adaptable para problemas de máxima demanda. Durante los períodos de máxima demanda, el Network Dispatcher puede encontrar automáticamente el servidor óptimo para manejar peticiones de entrada.

La función Network Dispatcher no utiliza un servidor de nombres de dominio para el equilibrado de carga. Equilibra el tráfico entre los servidores mediante una combinación exclusiva de equilibrado de carga y gestión de software. El Network Dispatcher también puede detectar un servidor anómalo y reenviar el tráfico a otros servidores disponibles.

Todas las peticiones de cliente que se envían a la máquina Network Dispatcher se reenvían al servidor seleccionado por el Network Dispatcher como servidor óptimo de acuerdo con ciertos pesos establecidos dinámicamente. Network Dispatcher calcula estos pesos basándose en diversos factores que incluyen el número total de conexiones, la carga del servidor y la disponibilidad del servidor.

El servidor envía una respuesta al cliente sin la intervención del Network Dispatcher. No es necesario software adicional en los servidores para comunicarse con el Network Dispatcher.

La función Network Dispatcher es la clave para una gestión estable y eficiente de una red extensa y escalable de servidores. Con el Network Dispatcher puede enlazar muchos servidores individuales para que formen lo que parece ser un único servidor virtual. El sitio aparece como una única dirección IP en el mundo. El Network Dispatcher funciona independientemente de un servidor de nombres de dominio; todas las peticiones se envían a la dirección IP de la máquina del Network Dispatcher.

El Network Dispatcher permite que una aplicación de gestión basada en SNMP supervise el estado del Network Dispatcher recibiendo estadísticas y situaciones de alerta potenciales. Consulte “Gestión de SNMP” en la publicación *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener más información.

El Network Dispatcher proporciona varias ventajas en el equilibrado de carga del tráfico para servidores agrupados, dando como resultado una gestión estable y eficaz de la oficina.

Equilibrado del tráfico TCP y UDP utilizando el Network Dispatcher

Existen muchos métodos diferentes para el equilibrado de carga. Algunos de estos métodos permiten que los usuarios elijan un servidor diferente al azar si el primer servidor es lento o no responde. Otro método es la modalidad rotatoria, en la cual el servidor de nombres de dominio selecciona un servidor para manejar las peticiones. Este método es mejor, pero no tiene en cuenta la carga actual en el servidor de destino ni si el servidor de destino está disponible.

El Network Dispatcher puede equilibrar la carga para diferentes servidores basándose en el tipo de petición, un análisis de la carga en los servidores o un conjunto configurable de pesos asignados por el usuario. Para gestionar cada tipo diferente de equilibrado, el Network Dispatcher tiene los componentes siguientes:

Ejecutor Equilibra la carga de conexiones basadas en el tipo de petición recibida. Los tipos de petición típicos son HTTP, FTP y Telnet. Este componente se ejecuta siempre.

Asesores Consulta los servidores y analiza los resultados por protocolo para cada servidor. El asesor pasa esta información al ***gestor*** para establecer el valor adecuado. El asesor es un componente opcional. No obstante, si no utiliza un asesor, Network Dispatcher no podrá detectar cuándo ha fallado un servidor y continuará enviando conexiones nuevas a un servidor de bajada.

Network Dispatcher soporta asesores para FTP, HTTP, SMTP, NNTP, POP3 y Telnet así como un asesor TN3270 que funciona con servidores TN3270 en los IBM 2210, IBM 2212 e IBM 2216, y un asesor MVS™ que funciona con Workload Manager (WLM) en sistemas MVS. WLM gestiona la cantidad de carga de trabajo en un ID de MVS individual. Network Dispatcher puede utilizar WLM para ayudar a equilibrar la carga de peticiones en servidores MVS que ejecutan OS/390® V1R3 o un release posterior.

No existen asesores de protocolo específicamente para protocolos UDP. Si tiene servidores MVS, puede utilizar el asesor del sistema MVS para proporcionar información de carga del servidor. Además, si el puerto maneja tráfico TCP y UDP, se puede utilizar el asesor de protocolo TCP adecuado para proporcionar entrada de asesor para el puerto. El Network Dispatcher utilizará esta entrada en el equilibrado de carga del tráfico TCP y UDP en dicho puerto.

Gestor Establece pesos para un servidor basándose en:

- Contadores internos en el ejecutor
- Información de retorno desde los servidores proporcionada por los asesores de protocolo
- Información de retorno desde un supervisor del sistema (asesor de MVS).

El gestor es un componente opcional. No obstante, si no utiliza el gestor, Network Dispatcher equilibrará la carga utilizando un método de planificación rotatoria basado en los pesos de servidor que ha configurado para cada servidor.

Cuando utilice el Network Dispatcher para equilibrar la carga de tráfico UDP sin estado, tan solo debe utilizar servidores que respondan al cliente utilizando la dirección IP de destino desde la petición. Consulte el apartado “Configuración de un servidor para el Network Dispatcher” en la página 121 para obtener una explicación más completa.

Alta disponibilidad para el Network Dispatcher

La función Network Dispatcher base tiene las características siguientes que lo convierten en un punto particular de anomalía desde varias perspectivas:

- Examina todo el tráfico en la entrada. Si alguno de los paquetes para una conexión existente utiliza una vía diferente a través de un Network Dispatcher diferente para llegar a un servidor, el servidor restablece inmediatamente la conexión.
- Efectúa un seguimiento de todas las conexiones establecidas y aunque no las finaliza, las entradas que se pierden desde la tabla de conexiones del Network Dispatcher harán que se restablezca una conexión.
- Aparece para cualquier direccionador de saltos anterior como el último salto y la terminación de la conexión.

Todas estas características hacen que las siguientes anomalías sean críticas para todo el cluster:

- Si el Network Dispatcher falla por algún motivo, se pierden todas las tablas de conexiones y, por lo tanto, también se pierden todas las conexiones existentes desde el cliente al servidor. En el supósito de que existe un segundo Network Dispatcher que puede dirigir un cliente a los servidores, las conexiones nuevas sólo podrán pasar después del retardo de protocolo de direccionamiento usual que puede ser de varios minutos.
- Si falla la interfaz del Network Dispatcher configurada para el direccionador IP anterior, debe existir otra interfaz para obtener el mismo Network Dispatcher, en cuyo caso la recuperación se realiza mediante el direccionador IP (utili-

zando el mecanismo de tiempo de ARP con retardos del orden de varios minutos) o se perderán todas las conexiones.

- Si la interfaz del Network Dispatcher con los servidores falla, el direccionador de saltos anterior supone que el Network Dispatcher es el último salto y, por lo tanto, no redireccionará las conexiones nuevas. Las conexiones existentes se perderán y no se establecerán conexiones nuevas.

En todos estos casos de anomalía, que no son únicamente anomalías del Network Dispatcher sino que también son anomalías del entorno del Network Dispatcher, se pierden todas las conexiones existentes. Incluso con un Network Dispatcher de reserva que ejecute mecanismos de recuperación IP estándar, en el mejor de los casos, la recuperación es lenta y sólo se aplica a las conexiones nuevas. En el peor de los casos, no existe recuperación de las conexiones.

Para mejorar la disponibilidad del Network Dispatcher, la función Alta disponibilidad del Network Dispatcher utiliza los mecanismos siguientes:

- Dos Network Dispatcher con conectividad con los mismos clientes y el mismo cluster de servidores, así como la conectividad entre los Network Dispatcher.
- Un mecanismo de “Pulso” entre los dos Network Dispatcher para detectar una anomalía del Network Dispatcher.
- Un criterio de asequibilidad, para identificar qué sistemas principales IP son accesibles o no desde cada Network Dispatcher.
- La sincronización de las bases de datos del Network Dispatcher (es decir, las tablas de conexiones, las tablas de asequibilidad y otras bases de datos).
- Un lógica para elegir el Network Dispatcher activo, que está a cargo de un cluster de servidores determinado, y el Network Dispatcher de espera, que se sincroniza continuamente para dicho cluster de servidores.
- Un mecanismo para realizar entrada en función rápida de IP, cuando la lógica o un operador decide conmutar entre el Network Dispatcher activo y en espera.

Detección de anomalías

Aparte de los criterios básicos de la detección de anomalías, (la pérdida de conectividad entre los Network Dispatcher activo y de espera, que se detecta a través de mensajes de "Pulso") existe otro mecanismo de detección de anomalías denominado “criterio de asequibilidad.” Cuando se configura el Network Dispatcher, se proporciona una lista de sistemas principales a los que cada uno de los Network Dispatcher debe poder llegar para funcionar correctamente. Los sistemas principales pueden ser direccionadores, servidores de IP u otros tipos de sistemas principales. La asequibilidad de sistema principal se obtiene aplicando "ping" al sistema principal.

La conmutación tiene lugar tanto si no se pueden examinar los mensajes de "Pulso" como si el Network Dispatcher activo ya no cumple el criterio de asequibilidad y el Network Dispatcher de espera es asequible. Para tomar la decisión basándose en toda la información disponible, el Network Dispatcher activo envía regularmente sus posibilidades de asequibilidad al Network Dispatcher de espera. A continuación, el Network Dispatcher de espera compara las posibilidades con las suyas y decide si debe conmutar o no.

Sincronización de bases de datos

Los Network Dispatcher primario y de reserva mantienen sus bases de datos sincronizadas mediante el mecanismo de "Pulso". La base de datos del Network Dispatcher incluye tablas de conexiones, tablas de asequibilidad y otra información. La función Alta disponibilidad del Network Dispatcher utiliza un protocolo de sincronización de bases de datos que asegura que ambos Network Dispatcher contengan las mismas entradas de tabla de conexiones. Esta sincronización tiene en cuenta un margen de errores conocidos para los retardos de transmisión. El protocolo realiza una sincronización inicial de bases de datos y, a continuación, mantiene la sincronización de bases de datos mediante actualizaciones periódicas.

Estrategia de recuperación

En el caso de una anomalía de la interfaz o de la máquina del Network Dispatcher, el mecanismo de entrada en función de IP dirigirá rápidamente todo el tráfico hacia el Network Dispatcher de espera. El mecanismo de Sincronización de bases de datos asegura que el Network Dispatcher de espera tenga las mismas entradas que el Network Dispatcher activo, de modo que se mantengan las conexiones existentes de cliente y servidor.

Entrada en función de IP

Nota: Se supone que las Direcciones IP de cluster están en la misma subred lógica que el direccionador de saltos anterior (direccionador IP) a no ser que se esté utilizando el anuncio de direcciones de cluster.

El Direccionador IP resolverá la dirección de cluster mediante el protocolo ARP. Para llevar a cabo la entrada en función de IP, el Network Dispatcher (de espera que se convierte en activo) emitirá una petición de ARP a sí mismo, que se difunde a todas las redes conectadas directamente que pertenecen a la subred lógica del cluster. El direccionador IP de los saltos anteriores actualizará sus tablas ARP (de acuerdo con RFC826) para enviar todo el tráfico para dicho cluster al nuevo Network Dispatcher activo (previamente de espera).

Configuración del Network Dispatcher

Existen varias maneras de configurar el Network Dispatcher para dar soporte al sitio. Si sólo tiene un nombre de sistema principal para su local al cual se conectarán todos los clientes, puede definir un único cluster y los puertos en los que desee recibir conexiones. Esta configuración se muestra en la Figura 5 en la página 116.

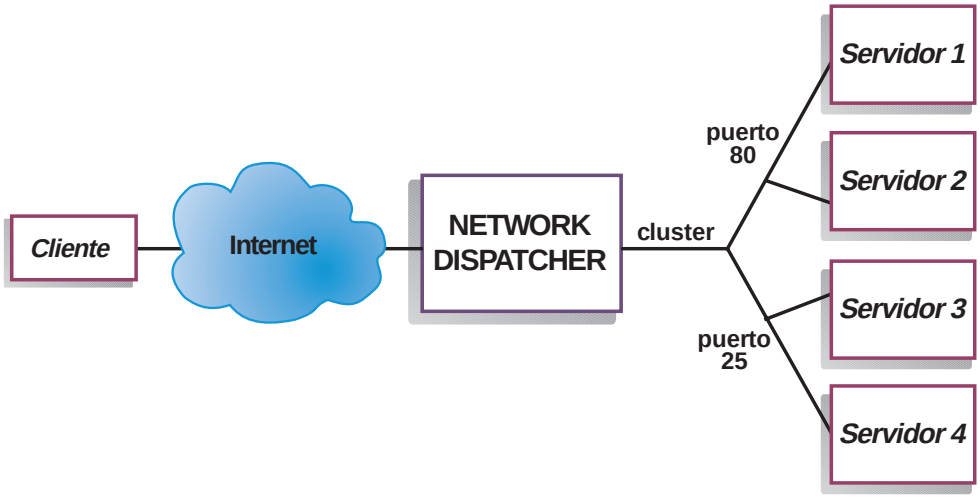


Figura 5. Ejemplo de Network Dispatcher configurado con un único cluster y 2 puertos

Sería necesaria otra forma de configuración del Network Dispatcher si su sitio contempla el alojamiento de contenedores para varias compañías o departamentos, cada uno de los cuales llegan al sitio con un URL diferente. En este caso, puede que desee definir un cluster para cada compañía o departamento y los puertos en los que desee recibir conexiones en dicho URL tal como se muestra en la Figura 6 en la página 117.

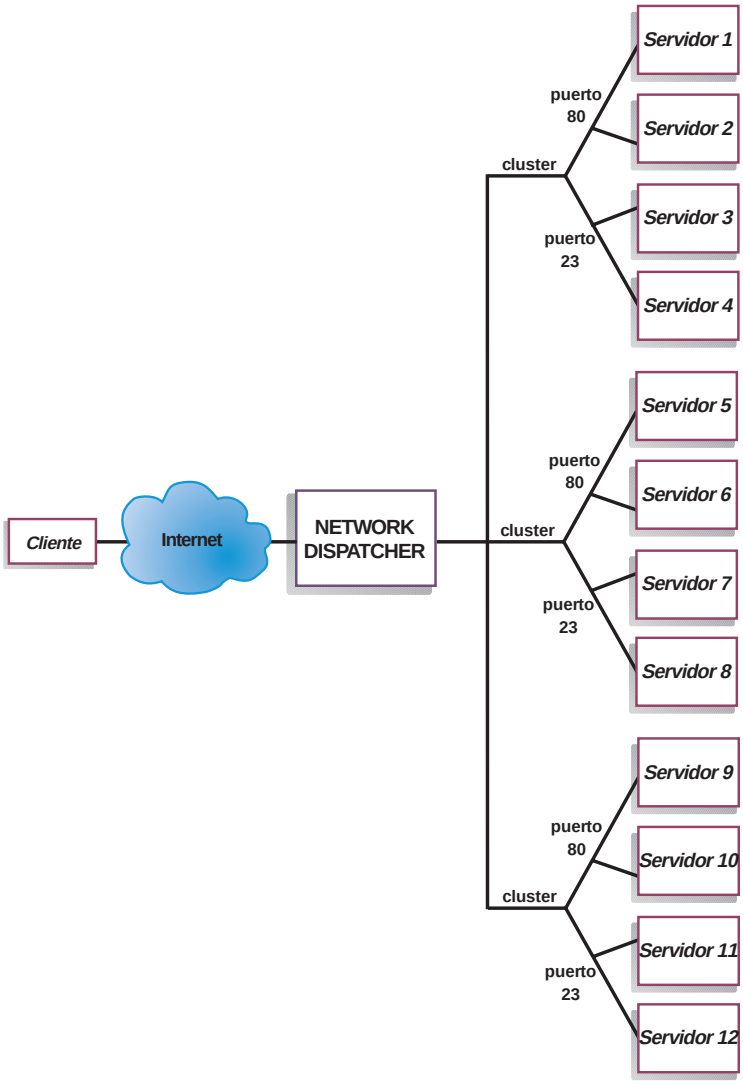


Figura 6. Ejemplo de Network Dispatcher configurado con 3 clusters y 3 URL

Una tercera manera de configurar el Network Dispatcher sería apropiada si su sitio es muy grande y tiene muchos servidores dedicados a cada protocolo soportado. Por ejemplo, puede optar por tener servidores FTP separados con líneas T3 directas para archivos descargables grandes. En este caso, puede que desee definir un cluster para cada protocolo con un único puerto pero con varios servidores, tal como se muestra en la Figura 7 en la página 118.

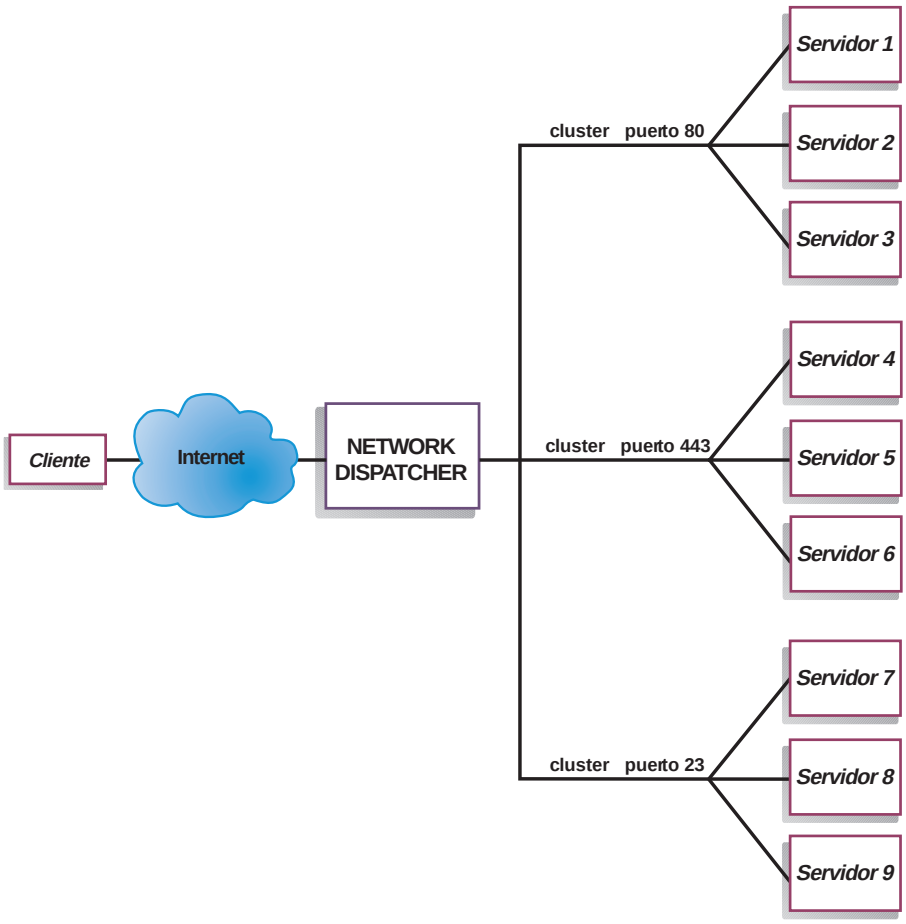


Figura 7. Ejemplo de Network Dispatcher configurado con 3 clusters y 3 puertos

Pasos de la configuración

Antes de configurar el Network Dispatcher:

1. Asegúrese de que Network Dispatcher tiene interfaces directas en los servidores (es decir, cada máquina servidor debe estar conectada directamente a una subred que sea local para la máquina de Network Dispatcher). Dado que la característica Network Dispatcher sólo ve el tráfico que circula desde el cliente al servidor, los servidores pueden tener conexiones independientes con el direccionador de empresa o la Internet, de forma que el tráfico de salida de los servidores a los clientes puede ignorar la máquina de Network Dispatcher. No existe ninguna configuración especial de Network Dispatcher necesaria para permitir estos tipos de conexiones de salida.

   Si la alta disponibilidad es importante para la red, en la Figura 8 en la página 119 se muestra una configuración de alta disponibilidad típica.

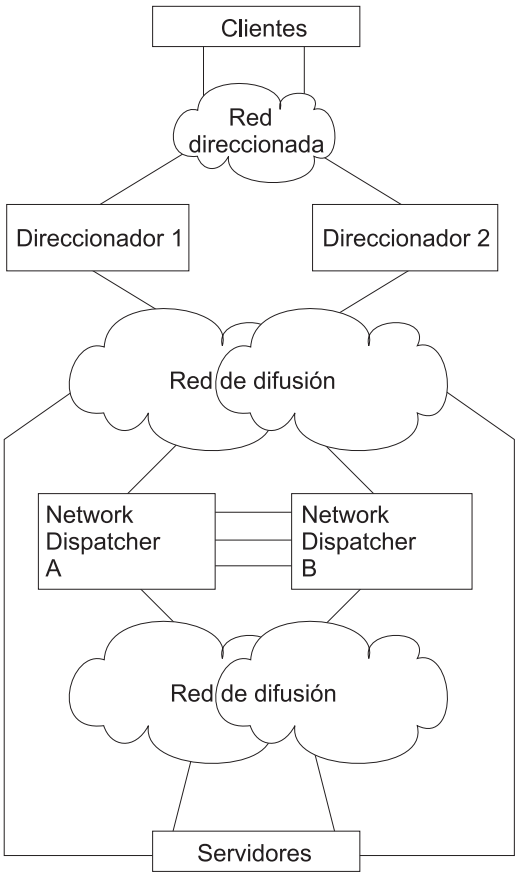


Figura 8. Configuración de Network Dispatcher de alta disponibilidad

2. Configure las interfaces de la máquina de Network Dispatcher. Este paso incluye la configuración de todas las interfaces, direcciones IP en todas las interfaces y cualquier protocolo de direccionamiento aplicable. El Network Dispatcher utiliza la dirección IP interna del direccionador, de modo que también debe configurarse utilizando el mandato set internal-ip-address. La dirección IP interna no debe coincidir con una dirección de cluster configurada en el Network Dispatcher. Consulte el capítulo Configuración y supervisión de IP en *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener más información sobre el mandato **set internal-ip-address**.
3. Rearranque o reinicie la máquina de Network Dispatcher.

Configuración del Network Dispatcher en un IBM 2210

Para configurar el Network Dispatcher en un IBM 2210:

1. En `talk 6`, acceda a la característica Network Dispatcher, utilizando el mandato **feature ndr**.
2. Habilite el ejecutor y el gestor utilizando los mandatos **enable executor** y **enable manager**.
3. Configure los clusters utilizando el mandato **add cluster**. Si configura las direcciones de cluster que se van a anunciar, consulte el apartado “Utilización del Network Dispatcher con anuncio de dirección de cluster” en la página 128 para obtener más información. Si elige que Network Dispatcher no anuncie las direcciones de cluster, deberá seleccionar direcciones de cluster que formen parte de una subred anunciada que sea local para el direccionador de Network

Dispatcher. Generalmente suele ser la subred en la que el Network Dispatcher recibe tráfico de clientes desde el direccionador de salto siguiente.

Nota: Las direcciones IP de cluster no deben coincidir con la dirección IP interna del direccionador y no deben coincidir con ninguna dirección IP de interfaz definida en el direccionador. Si está ejecutando Network Dispatcher y el servidor TN3270 en la misma máquina, la dirección de cluster puede coincidir con una dirección IP definida en la interfaz de bucle de retorno. Consulte el apartado “Utilización del Network Dispatcher con el servidor TN3270” en la página 125 para obtener información.

4. Configure los puertos de destino TCP y UDP utilizando el mandato **add port** para cada cluster de servidores que servirán el protocolo correspondiente. Lo siguiente son ejemplos de puertos típicos: 80 para HTTP, 20 y 21 para FTP y 23 para Telnet.
5. Configure los servidores utilizando los mandatos **add server**. Un servidor siempre está asociado con un puerto y un cluster. Un servidor puede servir más de un puerto (es decir, un servidor puede definirse bajo múltiples puertos para el mismo cluster) y un servidor puede pertenecer a más de un cluster, si el sistema operativo del servidor soporta múltiples seudónimos.
6. Configure los asesores utilizando el mandato **add advisor**.

   Notas:

   a. Para el asesor MVS, no defina el valor Port Number (valor por omisión = 10007) bajo ningún cluster. Este número de puerto sólo lo utiliza el asesor MVS para comunicarse con WLM en los sistemas MVS.

   b. Para el asesor TN3270, se entran dos valores de puerto. El valor Port Number (número de puerto) utilizado para la comunicación cliente-servidor (valor por omisión = 23) debe definirse bajo los clusters apropiados. No defina el valor Communication Port (puerto de comunicaciones) (valor por omisión = 10008) bajo ningún cluster. El valor Communication Port sólo lo utiliza el asesor TN3270 para reunir información de carga desde los servidores TN3270.
7. Habilite los asesores que ha configurado utilizando el mandato **enable advisor** y establezca las proporciones de gestor para incluir entrada de asesor en los cálculos de peso utilizando el mandato **set manager**.

Si configura el Network Dispatcher para alta disponibilidad, continúe con los pasos siguientes. De lo contrario, ha finalizado la configuración.

Nota: Realice estos pasos en el Network Dispatcher primario y, a continuación, en el Network Dispatcher de reserva. Para asegurar una sincronización de bases de datos correcta, el ejecutor del Network Dispatcher primario debe habilitarse antes que el ejecutor del Network Dispatcher de reserva.

8. Configure si este Network Dispatcher es el primario o el de reserva y si la conmutación es manual o automática utilizando el mandato **add backup**.
9. Configure todas las vías en las que va a tener lugar la transmisión de mensajes de pulso entre los Network Dispatcher primario y de reserva utilizando el mandato **add heartbeat**. Una vía se especifica mediante las direcciones IP de origen y de destino.

Nota: Es necesario configurar más de una vía de "pulso" entre los Network Dispatcher primario y de reserva para asegurar que la anomalía de una sola interfaz no interrumpirá la comunicación de "pulso" entre las máquinas primaria y de reserva.

Si sólo tiene una conexión LAN existente entre los dos Network Dispatcher, el segundo "pulso" puede configurarse a través de una conexión LAN simple (por ejemplo, un cable de cruce utilizado directamente entre dos puertos Ethernet) o una conexión serie de punto a punto (por ejemplo, la conexión PPP de parte posterior a parte posterior a través de un cable de módem nulo utilizando IP sin número).

10. Configure la lista de direcciones IP de sistemas principales a las que debe poder llegar el Network Dispatcher para asegurar un servicio completo, utilizando el mandato **add reach**. Por lo general, es un subconjunto de servidores, el direccionador de empresa o una estación de administración. Se deberá configurar al menos una dirección de alcance para cada interfaz en la que puede que circule el tráfico de Network Dispatcher.

Puede cambiar la configuración utilizando los mandatos **set**, **remove** y **disable**. Consulte el apartado “Configuración y supervisión de la característica Network Dispatcher” en la página 131 para obtener más información sobre estos mandatos.

Configuración de un servidor para el Network Dispatcher

Para configurar un servidor para utilizarlo con el Network Dispatcher:

1. Proporcione un seudónimo al dispositivo de bucle de retorno.

   Para que los servidores TCP y UDP funcionen, debe establecer (o preferiblemente proporcionar un seudónimo) el dispositivo de bucle de retorno (normalmente denominado ***lo0***) como la dirección de cluster. El Network Dispatcher no cambia la dirección IP de destino del paquete de IP antes de reenviar el paquete a un sistema servidor. Cuando establece o proporciona un seudónimo al dispositivo de bucle de retorno como dirección de cluster, el sistema servidor aceptará un paquete dirigido a la dirección de cluster.

   Es importante que el servidor utilice la dirección de cluster en lugar de su propia dirección IP para responder al cliente. Esto no afecta a los servidores TCP, pero algunos servidores UDP utilizan su propia dirección IP cuando responden a peticiones enviadas a la dirección de cluster. Cuando el servidor utiliza su propia dirección IP, algunos clientes descartan la respuesta del servidor porque no procede de una dirección IP de origen esperada. Sólo debe utilizar servidores UDP que utilicen la dirección IP de destino de la petición cuando responden al cliente. En este caso, la dirección IP de destino de la petición es la dirección de cluster.

   Si su sistema operativo soporta la asignación de seudónimos de interfaz de red como por ejemplo AIX, Solaris o Windows NT, debe proporcionar un seudónimo al dispositivo de bucle de retorno como la dirección de cluster. La ventaja de utilizar un sistema operativo que soporta seudónimos es que se pueden configurar los sistemas servidores para que sirvan múltiples direcciones de cluster.

   Si tiene un servidor con un sistema operativo que no soporta seudónimos, como por ejemplo HP-UX y OS/2, debe establecer ***lo0*** como la dirección de cluster.

Si el servidor es un sistema MVS que ejecuta TCP/IP V3R2, debe establecer la dirección VIPA como la dirección de cluster. Funcionará como una dirección de bucle de retorno. La dirección VIPA no debe pertenecer a una subred directamente conectada al nodo MVS. Si el sistema MVS ejecuta TCP/IP V3R3, debe establecer el dispositivo de bucle de retorno como la dirección de cluster. Si utiliza alta disponibilidad, debe habilitar RouteD en el sistema MVS para que el mecanismo de entrada en función de alta disponibilidad funcione correctamente.

Nota: Los mandatos que se listan en este capítulo se han probado en los sistemas operativos y niveles siguientes: AIX 4.2.1 y 4.3, HP-UX 10.2.0, Linux, OS/2 Warp Connect Versión 3.0, OS/2 Warp Versión 4.0, Solaris 2.6 (Sun OS 5.6), Windows NT 3.51 y 4.0 y OS/390.

Utilice el mandato para su sistema operativo tal como se muestra en la Tabla 10 en la página 123 para establecer o proporcionar un seudónimo al dispositivo de bucle de retorno.

Tabla 10. Mandatos para proporcionar un seudónimo al dispositivo de bucle de retorno (lo0) para el Asignador

Sistema	Mandato
AIX	**ifconfig lo0 alias** *dirección_cluster* **netmask** *máscarared*
HP-UX	**ifconfig lo0** *dirección_cluster*
Linux	**ifconfig lo:1** *dirección_cluster* **netmask** *máscarared* **up**
OS/2	**ifconfig lo** *dirección_cluster*
Solaris	**ifconfig lo0:1** *dirección_cluster* **127.0.0.1 up**
Windows NT	1. Pulse en **Inicio** y, a continuación, pulse en **Configuración**. 2. Pulse en **Panel de control** y, a continuación, efectúe una doble pulsación en **Red**. 3. Si todavía no lo ha hecho, añada el Controlador de Dispositivo MS Loopback. a. En la ventana Red, pulse en **Adaptadores**. b. Seleccione **Adaptador MS Loopback** y, a continuación, pulse en **Aceptar**. c. Cuando se le solicite, inserte el CD o discos de instalación. d. En la ventana Red, pulse en **Protocolos**. e. Seleccione **Protocolo TCP/IP** y, a continuación, pulse en **Propiedades**. f. Seleccione **Adaptador MS Loopback** y, a continuación, pulse en **Aceptar**. 4. Establezca la dirección de bucle de retorno en la dirección de cluster. Acepte la máscara de subred por omisión (255.0.0.0) y no entre ninguna dirección de pasarela. **Nota:** Puede que tenga que salir y volver a entrar en Valores de Red antes de que aparezca Controlador de MS Loopback bajo Configuración TCP/IP.

OS/390	Configuración de un seudónimo de bucle de retorno en el sistema OS/390.
	• En el miembro de parámetros IP (archivo), un Administrador necesitará crear una entrada en la lista de direcciones Home. Por ejemplo:
	`HOME`
	`;Address Link`
	`192.168.252.11 tr0`
	`192.168.100.100 ltr1`
	`192.168.252.12 loopback`
	• Se pueden definir varias direcciones para el bucle de retorno
	• Por omisión se configura la 127.0.0.1.

2. Compruebe si existe una ruta adicional.

   En algunos sistemas operativos puede que se haya creado una ruta por omisión y debe eliminarse.

   a. Compruebe si existe una ruta adicional en Windows NT con el siguiente mandato: **route print**

   b. Compruebe si existe una ruta adicional en todos los sistemas UNIX® y OS/2® con el mandato siguiente: **netstat -nr**

c. Ejemplo para Windows NT: Después de solicitar la impresión de ruta se visualizará una tabla similar a la siguiente. (En este ejemplo se muestra cómo buscar y eliminar una ruta adicional al cluster 9.67.133.158 con la submáscara de red por omisión 255.0.0.0.)

```
Rutas activas:
       Destino de red   Máscara de red   Puerta de acceso       Interfaz   Métrica
               0.0.0.0         0.0.0.0      9.67.128.1      9.67.133.67     1
               9.0.0.0       255.0.0.0    9.67.133.158     9.67.133.158     1
            9.67.128.0   255.255.248.0     9.67.133.67      9.67.133.67     1
           9.67.133.67 255.255.255.255       127.0.0.1        127.0.0.1     1
          9.67.133.158 255.255.255.255       127.0.0.1        127.0.0.1     1
       9.255.255.255 255.255.255.255     9.67.133.67      9.67.133.67     1
           127.0.0.0       255.0.0.0       127.0.0.1        127.0.0.1     1
           224.0.0.0       224.0.0.0    9.67.133.158     9.67.133.158     1
           224.0.0.0       224.0.0.0     9.67.133.67      9.67.133.67     1
     255.255.255.255 255.255.255.255     9.67.133.67      9.67.133.67     1
```

d. Busque su dirección de cluster en la columna "Puerta de acceso". Si tiene una ruta adicional, la dirección de cluster aparecerá dos veces. En el ejemplo proporcionado, la dirección de cluster (9.67.133.158) aparece en la fila 2 y la fila 8.

e. Busque la dirección de red en cada fila en la que aparezca la dirección de cluster. Necesita una de estas rutas y deberá suprimir la otra ruta, que es superflua. La ruta adicional que debe suprimirse será la ruta cuya dirección de red empieza por el primer dígito de la dirección de cluster, seguido de tres ceros. En el ejemplo que se muestra, la ruta adicional es la de la fila dos, que tiene la dirección de red 9.0.0.0:

```
9.0.0.0        255.0.0.0     9.67.133.158     9.67.133.158     1
```

3. Suprima las rutas adicionales.

   Utilice el mandato de la Tabla 11 para que su sistema operativo suprima las rutas adicionales.

Tabla 11. Mandatos para suprimir rutas para varios sistemas operativos

Sistema operativo	**Mandato**
AIX	**route delete -net** *dirección_red dirección_cluster*
HP-UNIX	**route delete** *dirección_cluster dirección_cluster*
Solaris	No es necesario suprimir ninguna ruta.
OS/2	No es necesario suprimir ninguna ruta.
Windows NT	**route delete** *dirección_red dirección_cluster* **Notas:** 1. Este mandato debe entrarse en un indicador de mandatos de MS-DOS. 2. Para Windows NT, debe suprimir la ruta adicional cada vez que rearranca el servidor. 3. Para evitar tener que eliminar manualmente la ruta adicional cada vez que reinicia el servidor, es aconsejable que cree e instale un Servicio utilizando el Kit de recursos de Windows NT que suprimirá automáticamente la ruta adicional después de cada rearranque del servidor.

Utilización del Network Dispatcher con el servidor TN3270

Network Dispatcher se puede utilizar con un cluster de 2210, 2212, Network Utilities o 2216 que ejecuten la función de servidor TN3270E para proporcionar soporte de servidor TN3270E para entornos 3270 grandes. El asesor TN3270 permite al Network Dispatcher reunir estadísticas de carga de cada servidor TN3270E en tiempo real para lograr la mejor distribución posible entre los servidores TN3270E. Además de los servidores TN3270E externos al direccionador de Network Dispatcher, uno de los servidores TN3270E del cluster puede ser interno - se puede ejecutar en el mismo direccionador que Network Dispatcher.

Claves para la configuración

La configuración de los servidores TN3270E externos (es decir, el servidor TN3270E no se ejecuta en el mismo direccionador que Network Dispatcher) es esencialmente igual que la configuración de un servidor TN3270E autónomo. De hecho, el servidor TN3270E ignora que el tráfico desde los clientes se envía a través de otra máquina. Sin embargo, existen algunos puntos que deben tenerse presentes al configurar servidores TN3270E externos para utilizarse con el Network Dispatcher:

- Cuando se configuran servidores TN3270E, la dirección IP del servidor TN3270E también se debe configurar en la máquina servidor como una dirección de interfaz. Los clientes envían paquetes a la dirección IP del servidor TN3270E y la máquina servidor acepta los paquetes para entregarlos a una función local, en este caso la función de servidor TN3270E. Con el Network Dispatcher delante de los servidores TN3270E, los clientes envían paquetes a la dirección IP del cluster del Network Dispatcher y Network Dispatcher reenvía los paquetes a los servidores sin cambiarlos, de modo que los paquetes llegan a las máquinas servidor con la dirección IP de destino igual a la dirección IP de cluster. Por consiguiente, la dirección IP de servidor TN3270 de cada servidor debe establecerse igual que la dirección IP de cluster y la dirección IP de cluster también debe definirse en cada máquina servidor como una dirección de interfaz (cualquier interfaz habilitada para IP será válida) para que la máquina servidor acepte los paquetes para la entrega local a la función de servidor TN3270E.
- Deberá asegurarse de que ningún protocolo de direccionamiento que se esté utilizando en los servidores TN3270E (por ejemplo OSPF o RIP) no anuncie la dirección de cluster. La dirección de cluster debe “pertenecer” al direccionador del Network Dispatcher por lo que respecta a la red del cliente.
- Si el tráfico del cliente al Network Dispatcher circula en la misma LAN que el tráfico del Network Dispatcher al servidor, deberá asegurarse de que los servidores no responden al ARP para la dirección de cluster, de modo que la dirección de cluster no puede definirse en la interfaz del servidor con esta LAN. El Network Dispatcher debe ser el único que responde a ARP en la LAN (o las LAN) en la(s) que recibe el tráfico de cliente de la red. La dirección de cluster puede configurarse alternativamente en el servidor TN3270E como una dirección de interfaz en otra interfaz o puede configurarse como la dirección IP interna del servidor TN3270E.
- Cada servidor TN3270E debe configurarse en el Network Dispatcher con una dirección IP de servidor exclusiva. Ésta es la dirección que Network Dispatcher utiliza para buscar el servidor. Esta dirección también debe configurarse como una dirección de interfaz en el direccionador que efectúa la función de servidor

TN3270E. Si la dirección IP de servidor exclusiva no forma parte de la subred que es local para la máquina del Network Dispatcher, éste debe poder encontrar el servidor a través de una ruta estática definida en la máquina de Network Dispatcher o a través de protocolos de direccionamiento que anuncien la dirección IP exclusiva del servidor.

- Para evitar que las conexiones TN3270 se eliminen de forma prematura de la tabla de conexiones de Network Dispatcher cuando un periodo de inactividad excede el tiempo de espera caducado para el cluster, deberá configurar el temporizador de mantenimiento de actividad del servidor TN3270E en modalidad de marca de temporización con un valor de tiempo de espera menor que el tiempo de espera caducado para el cluster. El servidor TN3270E envía un mensaje al cliente y espera una respuesta que evitará que la conexión caduque.

Cuando el servidor TN3270E está en el mismo direccionador que el Network Dispatcher, se aplica lo siguiente:

- Dado que los paquetes con equilibrio de carga en un servidor TN3270E interno seguirán teniendo la dirección de cluster como la dirección IP de destino del paquete, la dirección IP del servidor TN3270E debe configurarse como la dirección de cluster.
- Cuando el servidor TN3270E es externo a la máquina de Network Dispatcher, la dirección IP del servidor TN3270E debe definirse en el servidor como la dirección IP interna o como una dirección de interfaz para que el paquete pueda entregarse localmente a la función de servidor TN3270E. Sin embargo, cuando el servidor TN3270E es interno en el direccionador de Network Dispatcher, la dirección IP del servidor TN3270E no debe definirse en el direccionador como la dirección IP interna o como una dirección de interfaz. Si la dirección IP del servidor TN3270E (es decir, la dirección de cluster) se define como la dirección IP interna o como una dirección de interfaz, los paquetes no llegarán nunca al Network Dispatcher sino que irán directamente a la función de servidor TN3270E del direccionador.
- Cada servidor TN3270E debe configurarse en el Network Dispatcher con una dirección IP de servidor exclusiva. Para un servidor TN3270E interno, configure la dirección IP exclusiva del servidor igual que la dirección IP interna de la máquina de Network Dispatcher.
- Antes de la V3.4, se podía configurar un servidor TN3270E para el acceso interno o externo por parte de Network Dispatcher, pero no podía ser interno y externo y no podía conmutarse de uno a otro. Como resultado de ello, al implementar una solución de alta disponibilidad del Network Dispatcher con servidores TN3270E internos en ambos direccionadores de Network Dispatcher, el Network Dispatcher de un direccionador no podía equilibrar la carga del servidor TN3270E en el otro direccionador de Network Dispatcher.

  A partir de MRS V3.4, al implementar una solución de alta disponibilidad de Network Dispatcher con servidores TN3270E internos en ambos direccionadores de Network Dispatcher, los servidores TN3270E internos pueden configurarse para que pueda acceder a ellos cualquiera de los Network Dispatcher. Simplemente añada un dispositivo de bucle de retorno en ambos direccionadores de Network Dispatcher y defina la dirección IP de servidor TN3270E (es decir, la dirección de cluster) en cada interfaz de bucle de retorno. Cuando el Network Dispatcher esté en estado activo, la dirección de cluster de la interfaz de bucle de retorno se inhabilitará de modo que los

paquetes destinados a la dirección de cluster llegarán al Network Dispatcher. Cuando el Network Dispatcher esté en estado de espera, la dirección de cluster de la interfaz de bucle de retorno se habilitará de modo que los paquetes destinados a la dirección de cluster se entregarán localmente al servidor TN3270E. De este modo, ambos Network Dispatcher pueden utilizar un servidor TN3270E interno en una configuración de alta disponibilidad.

La máquina de Network Dispatcher activa debe ser la única máquina que responda a ARP para la dirección de cluster. Dado que la dirección de cluster está definida en ambas máquinas de Network Dispatcher en la interfaz de bucle de retorno, se deberá inhabilitar el ARP proxy en ambas máquinas de Network Dispatcher para evitar que la máquina de Network Dispatcher en espera responda a ARP para la dirección de cluster.

La máquina de Network Dispatcher activa también debe ser la propietaria de la dirección de cluster en lo que concierne a la red de cliente, de modo que la máquina de Network Dispatcher en espera (que tiene la dirección de cluster definida en la interfaz de bucle de retorno) no pueda anunciar la dirección de cluster. El RIP por omisión no anunciará rutas de sistema principal (rutas con la máscara 255.255.255.255), pero si se ha habilitado el anuncio de rutas de sistema principal, deberá definir la política de RIP para que inhabilite específicamente el anuncio de la dirección de cluster.

Este ejemplo muestra la política para evitar que RIP anuncie una dirección IP de cluster (aquí se supone que es 10.0.0.1). Observe que la segunda entrada de política permite a RIP anunciar cualquier otra ruta.

```
IP config> add route-policy
Route Policy Identifier [1-15 characters] []? rip-send
Use strictly linear policy? [No]: yes
IP config>change route-policy rip-send
rip-send IP Route Policy Configuration
IP Route Policy Config>add entry
Route Policy Index [1-65535] [0]? 1
IP Address [0.0.0.0]? 10.0.0.1
IP Mask [0.0.0.0]? 255.255.255.255
Address Match (Range/Exact) [Range]? exact
Policy type (Inclusive/Exclusive) [Inclusive]? exclusive
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]?
IP Route Policy Config> list

IP Address      IP Mask           Match  Index  Type
-------------------------------------------------------
10.0.0.1        255.255.255.255   Exact  1      Exclude
0.0.0.0         0.0.0.0           Range  2      Include
IP Route Policy Config> exit
IP config>enable sending policy global rip-send
IP config>
```

Para OSPF, si se habilitan el Direccionamiento de límites AS y la importación de rutas directas o si se habilita OSPF en la interfaz de bucle de retorno, se anunciará la dirección de cluster definida en la interfaz de bucle de retorno y se deberá definir la política OSPF para que inhabilite específicamente el anuncio de la dirección de cluster.

El ejemplo siguiente muestra una política para evitar que OSPF importe una dirección IP de cluster (aquí se supone que es 10.0.0.1). Observe que la segunda entrada de política permite a OSPF importar cualquier otra ruta directa.

```
IP> add route-policy ospf-send
Use strictly linear policy? [No]: yes
IP config> change route-policy ospf-send
ospf-send IP Route Policy Configuration
IP Route Policy Config> add entry
Route Policy Index [1-65535] [0]? 1
IP Address [0.0.0.0]? 10.0.0.1
IP Mask [0.0.0.0]? 255.255.255.255
Address Match (Range/Exact) [Range]? exact
Policy type (Inclusive/Exclusive) [Inclusive]? exclusive
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]?
IP Route Policy Config> add match-condition protocol direct
Route Policy Index [1-65535] [0]? 2
Route policy entry match condition updated or added
IP Route Policy Config> list

IP Address      IP Mask           Match  Index  Type
-----------------------------------------------------
10.0.0.1        255.255.255.255   Exact  1      Exclude
0.0.0.0         0.0.0.0           Range  2      Include
    Match Conditions:  Protocol: Direct
IP Route Policy Config> exit
IP config> exit
Config> protocol ospf
Open SPF-Based Routing Protocol configuration console
OSPF Config> enable as
Use route policy? [No]: yes
Route Policy Identifier [1-15 characters] []? ospf-send
Always originate default route? [No]:
Originate default if BGP routes available? [No]:
OSPF Config>
```

LU explícitas y el Network Dispatcher

Debe tenerse un cuidado especial para la definición de LU explícitas en un entorno de Network Dispatcher. Una petición de sesión para una LU implícita o explícita se puede enviar a cualquier servidor. Esto significa que la LU explícita debe definirse en cada servidor, puesto que no se sabe de antemano a qué servidor se enviará la sesión.

Utilización del Network Dispatcher con anuncio de dirección de cluster

El anuncio de dirección de cluster le permitirá configurar si los protocolos de direccionamiento habilitados en la máquina de Network Dispatcher deben anunciar o no cada dirección de cluster definida en el Network Dispatcher. Para las direcciones de cluster que no se anuncien, deberá seleccionar direcciones de cluster que formen parte de una subred anunciada que sea local para la máquina de Network Dispatcher. Las direcciones de cluster que se configuren para anunciarse se anunciarán como rutas de sistema principal y no tienen que formar parte de una subred anunciada. El anuncio de las direcciones de cluster es beneficioso en los escenarios siguientes:

- Puede que tenga múltiples ubicaciones de servidor geográficamente distribuidas que proporcionan el mismo contenido y desea que los clientes se conecten a la ubicación de servidor activa más próxima. Puede llevar a cabo este anuncio de dirección de cluster configurando la misma dirección de cluster en todas las ubicaciones de servidor y anunciando dichas direcciones de cluster desde todas las ubicaciones. Entonces los protocolos de

direccionamiento de la red dirigirán cada conexión de cliente a la ubicación de servidor más próxima. Si la ubicación más próxima está inactiva, la conexión irá a la siguiente ubicación de servidor más próxima. Tenga presente que los cambios en la red (un direccionador o un enlace de comunicaciones queda inactivo o vuelve a quedar activo) o los cambios en la disponibilidad de una ubicación de servidor pueden hacer que la ubicación de servidor más próxima cambie, incluso en medio de conexiones cliente-servidor existentes. Esto no es ningún problema con conexiones de vida corta como HTTP, pero puede considerarse como un problema para conexiones de vida larga como Telnet o TN3270.

- El anuncio de dirección de cluster le permite utilizar la alta disponibilidad de Network Dispatcher en una red IP ATM clásica. Cuando el Network Dispatcher en espera toma el control al Network Dispatcher activo, envía un ARP gratuito en todas las interfaces para hacer que el tráfico futuro destinado a la dirección de cluster se envíe a una nueva dirección MAC. Con la IP ATM clásica, el servidor ARP se actualiza pero no puede forzar a los clientes a que renueven sus antememorias. Las antememorias de cliente no se actualizarán hasta que caduque el tiempo de espera de renovación configurado en el cliente. Esto puede durar varios minutos. Las conexiones nuevas de clientes que no habían almacenado en antememoria la dirección ATM del Network Dispatcher primario irán inmediatamente al Network Dispatcher de reserva, pero las conexiones existentes en el momento de la entrada en función se perderán y no se podrán volver a establecer hasta que el temporizador de renovación de dicho cliente caduque y se actualice la antememoria del cliente. Mediante la definición de las direcciones de cluster que no forman parte de la subred ATM con el direccionador y mediante el anuncio de dichas direcciones de cluster, los protocolos de direccionamiento harán que el tráfico destinado a las direcciones de cluster se direccione al Network Dispatcher adecuado. El Network Dispatcher primario dejará de anunciar direcciones de cluster cuando pase al estado de espera y el Network Dispatcher de reserva empezará a anunciar direcciones de cluster cuando se convierta en el Network Dispatcher activo.

Los protocolos de direccionamiento de la máquina del Network Dispatcher deben configurarse adecuadamente para poder anunciar las direcciones de cluster:

- Para RIP, deberá habilitar rutas de sistema principal de envío.
- Para OSPF, deberá habilitar el direccionamiento de límites AS e importar rutas directas y de subred.
- Para BGP, deberá asegurarse de que el rango de direcciones de la política de origen incluye las direcciones de cluster anunciadas y deberá habilitar classless-bgp (bgp sin clase).

Utilización del Network Dispatcher con Antememoria de alta disponibilidad escalable (SHAC)

Puede utilizar el Network Dispatcher con un grupo de Antememorias de servidor Web para crear una Antememoria de alta disponibilidad escalable. Una Antememoria de alta disponibilidad escalable (SHAC) consta de una o dos máquinas de Network Dispatcher (la segunda se utilizará para proporcionar una reserva para la primera), dos o más máquinas de Antememoria de servidor Web y como mínimo un servidor de fondo. La Figura 9 en la página 130 muestra un ejemplo de una configuración SHAC. La máquina del Network Dispatcher equilibra

la carga del tráfico de cliente en las máquinas de antememoria y las máquinas de antememoria sirven los archivos de la antememoria u obtienen los archivos de los servidores de fondo si los archivos no se han almacenado en la antememoria,

En la máquina de Network Dispatcher, deberá configurar el cluster y el puerto y la modalidad del puerto deberá establecerse en *extcache* para indicar que está equilibrando la carga de una matriz de antememoria externa escalable. Consulte el mandato **add port** en la “Add” en la página 132. Bajo el puerto, las máquinas de antememoria se configuran como servidores. Al igual que con otros servidores, las direcciones IP de interfaz de las antememorias se utilizan para las direcciones IP de servidor exclusivas configuradas en la máquina de Network Dispatcher. El asesor y el gestor son críticos para SHAC. El asesor HTTP debe habilitarse en la máquina de Network Dispatcher en los puertos para los que existen antememorias externas (es decir, la modalidad de puerto es extcache). Las consultas del asesor se utilizan para determinar si las antememorias están operativas. El gestor debe habilitarse y las proporciones de gestor deben establecerse para que incluyan entrada de asesor en los cálculos de peso (es decir, establecer el porcentaje de asesor en un valor mayor que 0).

Cuando configure una antememoria como servidor bajo un cluster/puerto en la máquina de Network Dispatcher, deberá configurar también el mismo cluster y el mismo puerto en la función de Network Dispatcher de la máquina de antememoria. Los puertos definidos en las máquinas de antememoria deben establecerse en modalidad antememoria y los servidores de fondo se definen como servidores bajos dichos puertos. El asesor HTTP también deberá ejecutarse en las máquinas de antememoria de modo que éstas puedan determinar la carga y la disponibilidad del servidor de fondo.

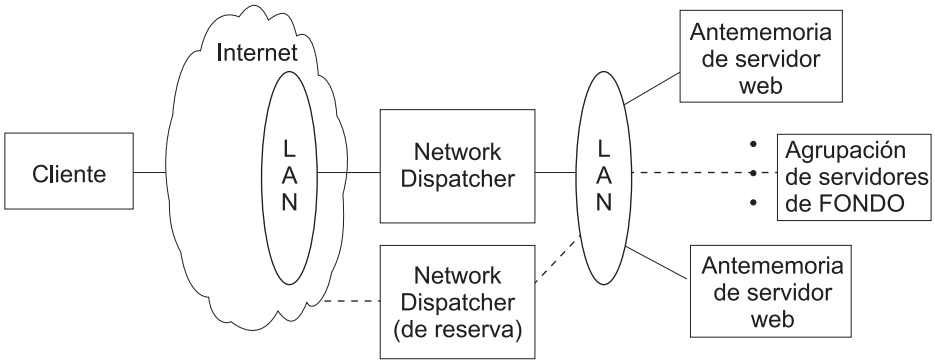


Figura 9. Servidores conectados a Lan

Configuración y supervisión de la característica Network Dispatcher

Este capítulo describe la configuración de la característica Network Dispatcher y los mandatos operativos. El capítulo contiene las secciones siguientes:

Acceso a los mandatos de configuración del Network Dispatcher

Para acceder al entorno de configuración del Network Dispatcher:

1. Entre **talk 6** en el indicador de mandatos OPCON (*).
2. Entre **feature ndr** en el indicador de mandatos `Config >`.

Mandatos de configuración del Network Dispatcher

La Tabla 12 resume los mandatos de configuración del Network Dispatcher y el resto de la sección explica estos mandatos. Entre estos mandatos en el indicador de mandatos `NDR Config >`.

Tabla 12. Mandatos de configuración del Network Dispatcher

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxx.
Add	Configura varios componentes del Network Dispatcher, entre los que se incluyen asesores, clusters, puertos y servidores.
Clear	Borra por completo la configuración del Network Dispatcher.
Disable	Inhabilita los componentes de reserva, ejecutor y gestor del Network Dispatcher. También inhabilita asesores específicos.
Enable	Habilita los componentes de reserva, ejecutor y gestor del Network Dispatcher. También habilita asesores específicos.
List	Visualiza toda la configuración del Network Dispatcher o partes específicas de la configuración.
Remove	Elimina partes específicas de la configuración del Network Dispatcher.
Set	Cambia los parámetros de configuración para asesores, clusters, puertos, servidores o el gestor de Network Dispatcher.
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 asesores, clusters, puertos, servidores y direcciones asequibles. Para Alta disponibilidad también puede configurar si este Network Dispatcher es primario o de reserva y qué direcciones IP deben utilizarse para la comunicación de "pulso".

Sintaxis:

add advisor . . .
backup . . .
cluster . . .
heartbeat . . .
port . . .
reach . . .
server . . .

Advisor *nombre núm-puerto intervalo tiempo-espera puerto-com*

Especifica el nombre y puerto para un asesor. Este parámetro también especifica la frecuencia con la que el asesor reunirá información acerca de un protocolo determinado y un periodo de tiempo después del cual se considera que el informe del asesor está atrasado.

nombre Especifica el tipo de asesor. Entre el número de asesor que corresponde al tipo de asesor que desea añadir.

Tabla 13. Nombres de asesor y números de puerto

Número de asesor	Nombre de asesor	Núm. de puerto por omisión
0	FTP	21
1	HTTP	80
2	MVS	10007
3	TN3270	23
4	SMTP	25
5	NNTP	119
6	POP3	110
7	TELNET	23
8	SSL	443

Valores válidos: 0 - 8

Valor por omisión: 1

núm-puerto

Especifica el número de puerto para este asesor.

Valores válidos: de 1 a 65535

Valores por omisión: Vea la Tabla 13.

intervalo Especifica la frecuencia, en segundos, con que el asesor consulta su protocolo para cada servidor. A la mitad de este valor sin ninguna respuesta desde el servidor, el asesor considera que el protocolo no está disponible.

Valores válidos: de 1 a 65535

Valor por omisión: 5

tiempo-espera
Especifica el intervalo de tiempo, en segundos, después del cual se considera que el informe del asesor está atrasado.

Para asegurarse de que el gestor no utiliza información atrasada en sus decisiones de equilibrio de carga, el gestor no utilizará información del asesor cuya indicación de la hora sea anterior a la hora establecida en este parámetro. El tiempo de espera del asesor debe ser mayor que el intervalo de sondeo del asesor. Si el tiempo de espera es menor, el gestor ignorará los informes que deben utilizarse. Por omisión, los informes del asesor no exceden el tiempo de espera.

Este valor de tiempo de espera generalmente se aplica si se inhabilita un asesor. No confunda este parámetro con el tiempo de espera de intervalo/2 previamente descrito, que hace referencia a un servidor que no responde.

Valores válidos: de 0 a 65535

Valor por omisión: 0, que significa que el informe del asesor no caduca nunca.

puerto-com
Especifica el número de puerto que utiliza el asesor TN3270 para comunicarse con los servidores TN3270. Este parámetro sólo se utiliza para el asesor TN3270. Debe coincidir con el número de puerto de asesor establecido en la configuración del servidor TN3270.

Valores válidos: de 1 a 65535

Valor por omisión:

- Valor por omisión de TN3270: 10008

Nota: Dado que el componente gestor es un requisito previo para el asesor, debe habilitar el gestor antes de habilitar cualquier asesor. También debe establecer las proporciones del gestor para que el gestor tenga en cuenta la entrada del asesor cuando establezca los pesos del servidor que se utilizan para tomar decisiones sobre el equilibrado de carga. También debe establecer la dirección IP interna utilizando el mandato **set internal-ip-address** para que el asesor se ejecute correctamente. Consulte Configuración y supervisión de IP en el manual *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener más información sobre el mandato **set internal-ip-address**.

Ejemplo 1:

```
add advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp,6=pop3,7=telnet,8=SSL) [1]? 1
Port number [80]?
Interval (seconds) [5]? 10
Timeout (0=unlimited) [0]? 10
```

Ejemplo 2:

```
add advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp,6=pop3,7=telnet,8=SSL) [1]? 3
Port number [23]?
Interval (seconds) [5]? 10
Timeout (0=unlimited) [0]? 10
Communication Port number [10008]?
```

backup *función estrategia*

Especifica si este Network Dispatcher es de reserva o primario.

función Define si es un Network Dispatcher primario o de reserva. Utilice este mandato solamente si desea tener una configuración redundante y desea ejecutar la función Alta disponibilidad. En este caso, también debe configurar la comunicación de "pulso" (**add heartbeat**) y la asequibilidad (**add reach**).

Valores válidos: 0 ó 1

0 = primario

1 = de reserva

Valor por omisión: 0

estrategia

Especifica si el Network Dispatcher conmutará de nuevo a la modalidad primaria automática o manualmente. Cuando falla un Network Dispatcher primario y queda en espera (lo que significa que uno de reserva ha realizado la entrada en función de IP) y, a continuación, queda disponible, se convertirá automáticamente en el Network Dispatcher activo si la estrategia se establece en *automática*. Si la estrategia se establece en *manual*, el antiguo primario pasará a modalidad de espera y el operador debe utilizar el mandato **switchover** en talk 5 para hacer que vuelva a estar activo. Consulte “Switchover” en la página 160.

Valores válidos: 0 ó 1

0 = automática

1 = manual

Valor por omisión: 0

Ejemplo:

```
add backup
Role (0=Primary, 1=Backup) [0]?
Switch back strategy (0=Auto, 1=Manual) [0]?
```

cluster *dirección cuenta-FIN tiempo-espera-FIN Temporizador-caducado Anunciar-dirección-cluster Anunciar-coste-ruta*

Especifica una dirección IP del cluster y la frecuencia con que el ejecutor realizará la recolección de basura de la base de datos del Network Dispatcher. Si configura direcciones de cluster que se van a anunciar, consulte el apartado “Utilización del Network Dispatcher con anuncio de dirección de cluster” en la página 128 para obtener más información.

Para las direcciones de cluster que no se han configurado para anunciarse, deberá seleccionar direcciones de cluster que formen parte de una subred anunciada que sea local para la máquina de Network Dispatcher. Generalmente, suele ser la subred en la que el Network Dispatcher recibe tráfico de clientes desde el direccionador de saltos siguiente.

Nota: Las direcciones IP de cluster no deben coincidir con la dirección IP interna del direccionador y no deben coincidir con ninguna dirección IP de interfaz definida en el direccionador. Si está ejecutando Network Dispatcher y el servidor TN3270 en la misma máquina, la dirección de cluster puede coincidir con una dirección IP definida en la interfaz de bucle de retorno. Consulte el apartado “Utilización del Network Dispatcher con el servidor TN3270” en la página 125 para obtener información.

dirección Especifica la dirección IP para el cluster.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

cuenta-FIN

Especifica el número de conexiones que deben estar en estado FIN antes de que el ejecutor intente eliminar la información de conexión no utilizada de la base de datos del Network Dispatcher una vez transcurrido el *Tiempo-espera-FIN* o *Temporizador-caducado*.

Valores válidos: de 0 a 65535

Valor por omisión: 4000

Tiempo-espera-FIN

Especifica el número de segundos, que una conexión ha estado en estado FIN, tras los cuales el ejecutor intenta eliminar la información de conexión no utilizada de la base de datos del Network Dispatcher.

Valores válidos: de 0 a 65535

Valor por omisión: 30

Temporizador-caducado

Especifica el número de segundos, que debe permanecer inactiva una conexión antes de que el ejecutor intente eliminar la información de una conexión de la base de datos del Network Dispatcher.

Valores válidos: de 0 a 65535

Valor por omisión: 1500

Anunciar-dirección-cluster

Especifica si la dirección de cluster debe anunciarse.

Valores válidos: yes o no

Valor por omisión: no

Anunciar-coste-ruta

Especifica el coste de la ruta anunciada. Esta pregunta sólo se formula si la respuesta a **anunciar dirección cluster** es *yes*.

Valores válidos: 0 a 4294967295

Valor por omisión: 0

Ejemplo:

```
NDR Config>add cluster
Cluster Address [0.0.0.0]? 113.3.1.12
FIN count [4000]?
FIN time out [30]?
Stale timer [1500]?
Advertise cluster address [No]? y
Advertise route cost [0]? 20
Cluster 113.3.1.12 has been added.
Fincount has been set to 4000 for cluster 113.3.1.12
Fintimeout has been set to 30 for cluster 113.3.1.12
Staletimer has been set to 1500 for cluster 113.3.1.12
NDR Config>
```

heartbeat *dirección1 dirección2*

Especifica una vía para los mensajes de "Pulso". El mensaje de "Pulso" circulará desde la *dirección1*, que pertenece a este Network Dispatcher, a la *dirección2*, que pertenece al Network Dispatcher similar.

Nota: Es necesario configurar más de una vía de "pulso" entre los Network Dispatcher primario y de reserva para asegurar que la anomalía de una sola interfaz no interrumpirá la comunicación de "pulso" entre las máquinas primaria y de reserva.

Si sólo tiene una conexión LAN existente entre los dos Network Dispatcher, el segundo "pulso" puede configurarse a través de una conexión LAN simple (un cable de cruce utilizado directamente entre los dos puertos Ethernet) o una conexión serie de punto a punto (conexión PPP de parte posterior a parte posterior a través de un cable de módem nulo utilizando IP sin número).

dirección1

Especifica la dirección IP de la interfaz de este Network Dispatcher desde la cual circularán los mensajes de "Pulso".

Valores válidos: Cualquier dirección IP.

Valor por omisión: 0.0.0.0

dirección2

Especifica la dirección IP de la interfaz del Network Dispatcher similar hasta la que circularán los mensajes de "Pulso". Esta dirección debe ser asequible desde la interfaz especificada en la *dirección1.*

Valores válidos: Cualquier dirección IP.

Valor por omisión: 0.0.0.0

Ejemplo:

```
add heartbeat
Source Heartbeat address [0.0.0.0]? 131.2.25.90
Target Heartbeat Address [0.0.0.0]? 131.2.25.92
```

port *dirección-cluster núm-puerto tipo-puerto peso-máx modalidad-puerto*

Especifica el puerto y los atributos del mismo.

dirección-cluster

Especifica la dirección IP del cluster.

Valores válidos: Cualquier dirección IP.

Valor por omisión: 0.0.0.0

núm-puerto

Especifica el número de puerto del protocolo para este cluster.

Valores válidos: de 1 a 65535

Valor por omisión: 80

tipo-puerto

Especifica los tipos de tráfico de IP para los que se puede equilibrar la carga en este puerto. Los tipos soportados son:

- 1 = TCP
- 2 = UDP
- 3 = ambos

Valores válidos: 1, 2, 3

Valor por omisión: 3

peso-máx

Especifica el peso máximo para los servidores en este puerto. Esto afecta al grado de diferencia que puede existir entre el número de peticiones que el ejecutor dará a cada servidor.

Valores válidos: de 0 a 100

Valor por omisión: 20

modalidad-puerto

Especifica si el puerto enviará todas las peticiones desde un único cliente a un único servidor (conocido como bloqueada), utilizará ftp pasivo (pftp), enviará una matriz de antememoria externa escalable (antememoriaext), o no utilizará ningún protocolo particular en este cluster (ninguna).

Valores válidos: 0, 1, 2, 4,, donde:

- 0 = ninguna
- 1 = bloqueada
- 2 = pftp
- 4 = antememoriaext

Valor por omisión: 0

Ejemplo:

```
Config>feature ndr
NDR>add cluster 1.2.3.4 4000 30 1500
NDR>add port
Cluster address [0.0.0.0]? 1.2.3.4
Port number [80]? 80
Port type [3]?
Maximum weight [20]?
Port mode [0=none, 1=sticky, 2=pftp, 4=extcache ]? 0
```

reach *dirección*

Especifica cualquier dirección de sistema principal a la que el Network Dispatcher debe poder acceder y ejecutar correctamente. Puede ser una dirección de servidor, una dirección de direccionador, una dirección de estación de administración u otro sistema principal de IP.

dirección Especifica la dirección IP de destino.

Valores válidos: Cualquier dirección IP

Valor por omisión: 0.0.0.0

Ejemplo:

```
add reach
Address to reach [0.0.0.0]?
```

server *dirección-cluster núm-puerto dirección-servidor peso-servidor estado-servidor*

Especifica los atributos de un servidor en un cluster.

dirección-cluster

Especifica la dirección IP del cluster al cual pertenece este servidor.

Valores válidos: Cualquier dirección IP

Valor por omisión: 0.0.0.0

núm-puerto

Especifica el protocolo que se ejecuta a través de la conexión con este servidor.

Valores válidos: de 1 a 65535

Valor por omisión: 80

dirección-servidor

Especifica la dirección IP del servidor.

Valores válidos: Cualquier dirección IP

Valor por omisión: 0.0.0.0

peso-servidor

Especifica el peso del servidor para el ejecutor. Esto afecta a la frecuencia con que el Network Dispatcher envía peticiones a este servidor determinado.

Valores válidos: de 0 al valor de *peso-máx* especificado en el mandato add port.

Valor por omisión: peso-máx en el mandato port

estado-servidor

Especifica si el ejecutor debe considerar el servidor como disponible o como no disponible cuando el ejecutor inicia el proceso.

Valores válidos: 0 (inactivo) o 1 (activo)

Valor por omisión: 1

Ejemplo:

```
add server
Cluster address [0.0.0.0]? 131.2.25.91
Port number [80]? 80
Server address [0.0.0.0]? 131.2.25.94
Server weight [35]?
Server state (down=0 up=1) [1]?
```

Límites de configuración de parámetros

La Tabla 14 lista los límites para los distintos elementos que se pueden configurar en un Network Dispatcher.

Tabla 14. Límites de configuración de parámetros

Parámetro	Límite
Asesores	8 por 2210
Clusters	32 por 2210
Pulsos	8 por 2210
Puertos	8 por cluster
Alcances	8 por 2210
Servidores	32 por puerto configurado, 128 para cada número de puerto bajo todos los clusters configurados.
Direcciones IP de servidor exclusivas	32 por 2210

Clear

Utilice el mandato **clear** para borrar toda la configuración del Network Dispatcher.

Sintaxis:

c**lear**

Disable

Utilice el mandato **disable** para inhabilitar un componente del Network Dispatcher.

Sintaxis:

d**isable** advisor . . .
backup
executor
manager

advisor *nombre núm-puerto*

Inhabilita un asesor del Network Dispatcher.

nombre Especifica el tipo de asesor. Entre el número de asesor que corresponde al tipo de asesor que desea inhabilitar.

Consulte la Tabla 13 en la página 132 para obtener información adicional.

Valores válidos: 0 - 8

Valor por omisión: 0

núm-puerto

Especifica el número de puerto para este asesor.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe entrar un número de puerto.

Ejemplo:

```
disable advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp,6=pop3,7=telnet,8=SSL) [1]? 1
Port number  [0]? 80
```

backup Inhabilita la función de reserva del Network Dispatcher.

Ejemplo:

```
disable backup
Backup is now disabled.
```

executor Inhabilita el ejecutor del Network Dispatcher. La inhabilitación del ejecutor inhabilita la característica Network Dispatcher.

Ejemplo:

```
disable executor
Executor is now disabled.
```

Nota: La inhabilitación del ejecutor detendrá el gestor, los asesores y la función de alta disponibilidad, si se ejecutan actualmente.

manager Inhabilita el gestor del Network Dispatcher. El gestor es un componente opcional. Sin embargo, si no utiliza el gestor, el Network Dispatcher equilibrará la carga utilizando un método de planificación rotatoria basado en los pesos actuales de los servidores.

Ejemplo:

```
disable manager
Manager is now disabled.
```

Nota: Dado que el componente gestor es un requisito previo para los asesores, la inhabilitación del gestor detendrá la ejecución de todos los asesores.

Enable

Utilice el mandato **enable** para habilitar un componente del Network Dispatcher.

Sintaxis:

enable advisor . . .

backup

executor

manager

advisor *nombre núm-puerto*

Habilita un asesor en el Network Dispatcher.

nombre Especifica el tipo de asesor. Entre el número de asesor que corresponde al tipo de asesor que desea habilitar.

Consulte la Tabla 13 en la página 132 para obtener información adicional.

Valores válidos: 0 - 8

Valor por omisión: 0

núm-puerto

Especifica el número de puerto para este asesor.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe entrar un número de puerto.

Ejemplo:

```
enable advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp=6=pop3,7=telnet,8=SSL) [1]? 1
Port number  [0]? 80
```

Nota: Dado que el componente gestor es un requisito previo para el asesor, debe habilitar el gestor antes de habilitar cualquier asesor. También debe establecer las proporciones del gestor para que el gestor tenga en cuenta la entrada del asesor cuando establezca los valores del servidor que se utilizan para tomar decisiones sobre el equilibrado de carga. También debe establecer la dirección IP interna utilizando el mandato **set internal-ip-address** para que el asesor se ejecute correctamente. Consulte el capítulo Configuración y supervisión de IP en *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener más información sobre el mandato **set internal-ip-address**.

backup Habilita la función de reserva del Network Dispatcher.

Ejemplo: `enable backup`

Nota: Antes de habilitar la reserva, debe añadir como mínimo una comunicación de pulso.

executor Habilita el ejecutor del Network Dispatcher.

Ejemplo:

```
enable executor
Executor is now enabled.
```

manager Habilita el gestor del Network Dispatcher.

Ejemplo:

```
enable manager
Manager interval was set to 2.
Manager proportions were set to  50   50   0   0
Manager refresh cycle was set to 2
Manager sensitivity was set to 5.
Manager smoothing factor was set to 1.50.
```

Cuando se habilita el gestor por primera vez, se crea un registro del gestor con los siguientes valores por omisión:

Intervalo: 2 segundos

Ciclo-Renovación: 2

Sensibilidad: 5 %

Alisado: 1,5

Proporciones:

Activo: 50%

Nuevo: 50%

Asesor: 0

Sistema: 0

Consulte el apartado “Set” en la página 146 para obtener una descripción de los parámetros anteriores.

List

Utilice el mandato **list** para visualizar información sobre el Network Dispatcher.

Sintaxis:

list
- all
- advisor
- backup
- cluster
- manager
- port
- server

all Visualiza toda la información de configuración del Network Dispatcher. Incluye la misma información visualizada para asesores, reserva, cluster, gestor, puertos y servidores.

Ejemplo:

```
NDR Config> list all

Executor: Enabled

Manager: Enabled

        Interval        Refresh-Cycle   Sensitivity     Smoothing
        2               2               5 %             1.50
        Proportions:    Active  New     Advisor         System
                        50 %    50 %    0 %             0 %

Advisor:
        Name    Port    Interval        TimeOut         State     CommPort
        http    80      5               0               Enabled
        MVS     10007   15              0               Enabled
        TN3270  23      5               0               Enabled   10008

Backup: Enabled
        Role            Strategy
        PRIMARY         AUTOMATIC

        Reachability:   Address         Mask            Type
                        131.2.25.93     255.255.255.255 HOST
                        131.2.25.94     255.255.255.255 HOST

        HeartBeat Configuration:
           Source Address:  131.2.25.90 Target Address:   131.2.25.92
           Source Address:  132.2.25.90 Target Address:   132.2.25.92

Clusters:
        Cluster-Addr    FIN-count       FIN-timeout     Stale-timer  Advertise/Cost
        131.2.25.91     4000            30              1500         Yes      / 20

Ports:
  Cluster-Addr    Port#   Weight  Port-Mode  Port-Type
  131.2.25.91     23      20 %    none       TCP
  131.2.25.91     80      20 %    none       Both

Servers:
        Cluster-Addr    Port#   Server-Addr     Weight  State
        131.2.25.91     23      131.2.25.93     20 %    up
        131.2.25.91     23      131.2.25.94     20 %    up
        131.2.25.91     80      131.2.25.93     20 %    up
        131.2.25.91     80      131.2.25.94     20 %    up
```

advisor Visualiza la configuración de los asesores del Network Dispatcher.

backup Visualiza la configuración de reserva del Network Dispatcher.

cluster Visualiza la configuración de los clusters del Network Dispatcher.

manager Visualiza la configuración del gestor del Network Dispatcher.

port Visualiza la configuración de los puertos del Network Dispatcher.

server Visualiza la configuración de los servidores asociados con los clusters del Network Dispatcher.

Remove

Utilice el mandato **remove** para suprimir parte de la configuración del Network Dispatcher.

Sintaxis:

remove
- advisor . . .
- backup
- cluster . . .
- heartbeat . . .
- port . . .
- reach . . .

server . . .

advisor *nombre núm-puerto*

Elimina un asesor específico de la configuración del Network Dispatcher.

nombre Especifica el tipo de asesor. Entre el número de asesor que corresponde al tipo de asesor que desea eliminar.

Consulte la Tabla 13 en la página 132 para obtener información adicional.

Valores válidos: 0 - 8

Valor por omisión: 0

núm-puerto

Especifica el número de puerto para este asesor.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe entrar un número de puerto.

Ejemplo:

```
remove advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp,6=pop3,7=telnet,8=SSL) [0]?
Advisor port [0]? 80
```

backup Elimina la función de alta disponibilidad.

Nota: Puesto que la reserva es un requisito previo para las funciones heartbeat y reach la eliminación de la reserva detendrá la ejecución de heartbeat y reach.

Ejemplo: `remove backup`

cluster *dirección*

Elimina un cluster de la configuración del Network Dispatcher.

dirección Especifica la dirección IP para el cluster.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

Nota: La eliminación de una dirección de cluster también elimina todos los puertos y servidores asociados con dicho cluster.

Ejemplo:

```
remove cluster
WARNING: Deleting a cluster will make any port or server
         associated with it to also be deleted.
Cluster address [0.0.0.0]? 131.2.25.91
```

heartbeat *dirección*

Elimina la dirección de "pulso" de la configuración del Network Dispatcher.

dirección Especifica la dirección IP para el Network Dispatcher de destino.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

Ejemplo:

```
remove heartbeat
Target address [0.0.0.0]? 131.2.25.92
```

port *dirección-cluster núm-puerto*

Elimina un puerto de un cluster específico de la configuración del Network Dispatcher.

dirección-cluster

Especifica la dirección IP del cluster.

Valores válidos: Cualquier dirección IP.

Valor por omisión: 0.0.0.0

núm-puerto

Especifica el número de puerto del protocolo para este cluster.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe entrar un número de puerto.

Ejemplo:

```
remove port
WARNING: Deleting a port will make any server
associated with it also be deleted.   [0.0.0.0]? 7.82.142.15
Port number  [0]? 80
Cluster address [0.0.0.0]? 20.21.22.15
```

reach *dirección*

Elimina un servidor de la lista de sistemas principales a los que debe poder llegar el Network Dispatcher.

dirección Especifica la dirección IP del cluster.

Valores válidos: Cualquier dirección IP.

Valor por omisión: 0.0.0.0

Ejemplo:

```
remove reach
Target address [0.0.0.0]? 9.82.142.15
```

server *dirección-cluster núm-puerto dirección-servidor*

Elimina un servidor de un cluster y un puerto de la configuración del Network Dispatcher.

dirección-cluster

Especifica la dirección IP del cluster.

Valores válidos: Cualquier dirección IP.

Valor por omisión: 0.0.0.0

núm-puerto

Especifica el número de puerto del protocolo para este cluster.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe entrar un número de puerto.

dirección-servidor

Especifica la dirección IP del cluster.

Valores válidos: Cualquier dirección IP.

Valor por omisión: 0.0.0.0

Ejemplo:

```
remove server
Cluster address [0.0.0.0]? 7.82.142.15
Port number  [0]? 80
Server address [0.0.0.0]? 20.21.22.15
```

Set

Utilice el mandato **set** para cambiar los atributos de un asesor, cluster, puerto o servidor existente. También puede definir atributos para el gestor del Network Dispatcher.

Sintaxis:

set advisor . . .

cluster . . .

manager . . .

port . . .

server . . .

advisor *nombre núm-puerto intervalo tiempo-espera puerto-com*

Cambia el número de puerto, intervalo y tiempo de espera para un asesor.

nombre Especifica el tipo de asesor. Entre el número de asesor que corresponde al tipo de asesor que desea establecer.

Consulte la Tabla 13 en la página 132 para obtener información adicional.

Valores válidos: 0 - 8

Valor por omisión: 0

núm-puerto

Especifica el número de puerto para este asesor.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe entrar un número de puerto.

intervalo Especifica la frecuencia con que el asesor consulta su protocolo para cada servidor. A la mitad de este valor sin ninguna respuesta del servidor, el asesor considera que el protocolo no está disponible.

Valores válidos: de 0 a 65535

Valor por omisión: 5

tiempo-espera

Especifica el intervalo de tiempo, en segundos, después del cual el asesor considera que el protocolo no está disponible.

Para asegurarse de que el gestor no utiliza información atrasada en sus decisiones de equilibrado de carga, el gestor no utilizará información del asesor cuya indicación de la hora sea anterior a la hora establecida en este parámetro. El tiempo de espera del asesor debe ser mayor que el intervalo

de sondeo del asesor. Si el tiempo de espera es menor, el gestor ignorará los informes que deben utilizarse. Por omisión, los informes del asesor no exceden el tiempo de espera.

Este valor de tiempo de espera generalmente se aplica si se inhabilita un asesor. No confunda este parámetro con el tiempo de espera de intervalo/2 previamente descrito, que hace referencia a un servidor que no responde.

Valores válidos: de 0 a 65535

Valor por omisión: 0, que significa que el protocolo se considera que está siempre disponible.

puerto-com

Especifica el número de puerto utilizado por el asesor TN3270 para comunicarse con los servidores TN3270 . Este parámetro sólo se utiliza para el asesor TN3270 .

Valores válidos: de 1 a 65535

Valor por omisión:

- Valor por omisión de TN3270: 10008

Ejemplo:

```
set advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp=6=pop3,7=telnet,8=SSL) [0]?
Port number [0]? 21
Interval (seconds) [5]? 10
Timeout (0=unlimited) [0]? 20
```

cluster *dirección cuenta-FIN tiempo-espera-FIN Temporizador-caducado*

Cambia la cuenta-FIN, tiempo-espera-FIN y Temporizador-caducado para un cluster en la configuración del Network Dispatcher.

dirección Especifica la dirección IP para el cluster.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

cuenta-FIN

Especifica el número de conexiones que deben estar en estado FIN antes de que el ejecutor intente eliminar la información de conexión no utilizada de la base de datos del Network Dispatcher una vez transcurrido el *Tiempo-espera-FIN* o *Temporizador-caducado*.

Valores válidos: de 0 a 65535

Valor por omisión: 4000

Tiempo-espera-FIN

Especifica el número de segundos después del cual el ejecutor intenta eliminar la información de conexión no utilizada de la base de datos del Network Dispatcher.

Valores válidos: de 0 a 65535

Valor por omisión: 30

Temporizador-caducado

Especifica el número de segundos que una conexión ha estado inactiva, después del cual el ejecutor intenta eliminar la información de una conexión de la base de datos del Network Dispatcher.

Valores válidos: de 0 a 65535

Valor por omisión: 1500

Ejemplo:

```
set cluster
Cluster address [0.0.0.0]? 131.2.25.91
FIN count [4000]? 4500
FIN timeout [30]? 40
Stale timer [1500]? 2000
```

manager *intervalo proporción renovación sensibilidad alisado*

Establece los valores que el gestor utiliza para determinar el mejor servidor para satisfacer una petición.

intervalo Especifica la cantidad de tiempo, en segundos, después del cual el gestor actualiza los pesos del servidor que el ejecutor utiliza al equilibrar la carga de conexiones.

Valores válidos: de 0 a 65535

Valor por omisión: 2

proporción

Especifica la importancia relativa de los factores externos en las decisiones de ponderación del gestor. La suma de las proporciones debe ser igual a 100. Los factores son:

activas El número de conexiones activas en cada servidor TCP/IP de las que efectúa un seguimiento el ejecutor.

Valores válidos: de 0 a 100

Valor por omisión: 50

nuevas El número de conexiones nuevas en cada servidor TCP/IP de las que efectúa un seguimiento el ejecutor.

Valores válidos: de 0 a 100

Valor por omisión: 50

asesor Entrada desde los asesores de protocolo definidos para el Network Dispatcher.

Valores válidos: de 0 a 100

Valor por omisión: 0

sistema Entrada desde el asesor del sistema MVS proporcionada por la herramienta de supervisión del sistema MVS WLM.

Valores válidos: de 0 a 100

Valor por omisión: 0

renovación

Especifica la frecuencia con la que el gestor solicita estados del ejecutor. Este parámetro se especifica como un número de *intervalos*.

Valores válidos: de 0 a 100

Valor por omisión: 2

sensibilidad

Especifica el cambio de porcentaje de peso para todos los servidores en un puerto, después del cual el gestor actualiza los pesos que utiliza el ejecutor al equilibrar la carga de conexiones.

Valores válidos: de 0 a 100

Valor por omisión: 5

alisado Especifica un límite para la variación del peso de un servidor. El alisado minimiza la frecuencia de cambio en la distribución de peticiones. Un índice de alisado más alto hará que los pesos cambien menos. Un índice de alisado más bajo hará que los pesos cambien más.

Valores válidos: un valor decimal entre 1,0 y 42 949 673,00

Valor por omisión: 1,5

Nota: Sólo puede especificar dos dígitos después de la coma decimal.

Ejemplo:

```
set manager
Interval (in seconds) [2]? 3
Active proportion [50]? 40
New proportion [50]? 38
Advisor proportion [0]? 20
System proportion [0]? 2
Refresh cycle [2]? 4
Sensitivity threshold [5]? 10
Smoothing index (>1.00) [1.50]? 200
```

port *dirección-cluster núm-puerto tipo-puerto peso-máx modalidad-puerto*

Cambia tipo-puerto, peso-máx y modalidad-puerto para un cluster y número de puerto específicos.

dirección-cluster

Especifica la dirección IP del cluster.

Valores válidos: Cualquier dirección IP.

Valor por omisión: 0.0.0.0

núm-puerto

Especifica el número de puerto del protocolo para este cluster.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe entrar un número de puerto.

tipo-puerto

Especifica el tipo de tráfico de IP para los que se puede equilibrar la carga en este puerto.

Valores válidos:

- 1 = TCP
- 2 = UDP
- 3 = ambos

Valor por omisión: 3

peso-máx

Especifica el peso para los servidores en este puerto. Esto afecta al grado de diferencia que puede existir entre el número de peticiones que el ejecutor dará a cada servidor.

Valores válidos: de 0 a 100

Valor por omisión: 20

modalidad-puerto

Especifica si el puerto enviará todas las peticiones de un solo cliente a un solo servidor (conocido como bloqueada), utilizará ftp pasivo (pftp), enviará una matriz de antememoria externa escalable, o no utilizará ningún protocolo en este cluster (ninguna).

Valores válidos:

- 0 = ninguna
- 1 = bloqueada
- 2 = pftp
- 4 = antememoriaext

Valor por omisión: 0 (ninguna)

Ejemplo:

```
set port
Cluster address [0.0.0.0]? 131.2.25.91
Port number [0]? 23
Port type (tcp=1, udp=2, both=3) [0]?
Max. weight (0-100) [20]? 30
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1, pftp=2 extcache=4) []?
```

server *dirección-cluster núm-puerto dirección-servidor peso estado*

Cambia el estado y el peso de un servidor específico de un cluster.

dirección-cluster

Especifica la dirección IP del cluster al cual pertenece este servidor.

Valores válidos: Cualquier dirección IP

Valor por omisión: 0.0.0.0

núm-puerto

Especifica el número de puerto del protocolo para este cluster.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe entrar un número de puerto.

dirección-servidor

Especifica la dirección IP del servidor.

Valores válidos: Cualquier dirección de servidor válida

Valor por omisión: 0.0.0.0

estado Especifica si el ejecutor debe considerar el servidor como disponible o como no disponible cuando el ejecutor inicia el proceso.

Valores válidos: 0 (inactivo) o 1 (activo)

Valor por omisión: 1

peso Especifica el peso del servidor para el ejecutor. Esto afecta a la frecuencia con que el Network Dispatcher envía peticiones a este servidor determinado.

Valores válidos: de 0 al valor de *peso-máx* especificado en el mandato add port.

Valor por omisión: peso-máx en el mandato port

Ejemplo:

```
set server
Cluster address [0.0.0.0]? 131.2.25.91
Port number [0]?
Server address [0.0.0.0]?
Server weight [20]? 25
Server state (down=0, up=1) [1]? 1
```

Acceso a los mandatos de supervisión del Network Dispatcher

Para acceder al entorno de supervisión del Network Dispatcher:

1. Entre **talk 5** en el indicador de mandatos OPCON (*).
2. Entre **feature ndr** en el indicador de mandatos GWCON (+).

El Network Dispatcher también se puede supervisar utilizando SNMP. Consulte "Gestión de SNMP" en la publicación *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener más información.

Mandatos de supervisión del Network Dispatcher

La Tabla 15 resume los mandatos de supervisión del Network Dispatcher y el resto de la sección explica estos mandatos. Entre estos mandatos en el indicador de mandatos `NDR >`.

Tabla 15. Mandatos de supervisión del Network Dispatcher

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxx.
List	Visualiza los atributos actualmente configurados del asesor, clusters, puertos o servidores.
Quiesce	Especifica que no debe enviarse a un servidor ninguna petición más de conexión. Además detiene temporalmente las funciones heartbeat y reach.
Report	Visualiza un informe de información relacionada con el asesor y el gestor.
Status	Visualiza el estado actual de los contadores, clusters, puertos, servidores, asesor, gestor y reserva.
Switchover	Obliga a que un Network Dispatcher que se ejecuta en modalidad de espera se convierta en el Network Dispatcher activo. La utilización de este mandato es necesaria si ha especificado manual como modalidad de conmutación.
Unquiesce	Permite que el gestor del Network Dispatcher asigne un peso mayor que 0 a un servidor inmovilizado previamente en cada puerto en el que está configurado el servidor. Esta acción permite que circulen peticiones de conexión nuevas al servidor seleccionado.
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 visualizar información sobre el Network Dispatcher.

Sintaxis:

list advisor
cluster
port

server

advisor Visualiza la configuración de los asesores del Network Dispatcher que están habilitados actualmente.

Ejemplo:

```
list advisor
Advisor list requested.

-------------------------------------------
| ADVISOR |  PORT  |  TIMEOUT  |  STATUS  |
-------------------------------------------
|  ftp    |    21  |       5   |   ACTIVE |
|  Http   |    80  | unlimited |   ACTIVE |
|  MVS    | 10007  | unlimited |   ACTIVE |
|  TN3270 |    23  | unlimited |   ACTIVE |
-------------------------------------------
```

cluster Visualiza la configuración de los clusters del Network Dispatcher.

Ejemplo:

```
list cluster
EXECUTOR INFORMATION:
 --------------------
Version: 01.01.00.00 - Tue Dec 10 14:15:58 EST 1996
Number of defined clusters: 2

CLUSTER LIST:
-------------
  131.2.25.91
  10.11.12.2
```

port Visualiza la configuración de los puertos del Network Dispatcher.

Ejemplo:

```
list port
Cluster Address [0.0.0.0]? 131.2.25.91

  ------------------------------------------------------------
   CLUSTER:       131.2.25.91
  ------------------------------------------------------------
     PORT        MAXWEIGHT      PORT MODE     PORT TYPE
  ------------------------------------------------------------
       23             30          none           TCP
       80             20          none           both
 ------------------------------------------------------------
```

server Visualiza la configuración de los servidores asociados con los clusters del Network Dispatcher.

Ejemplo:

```
list server
Cluster Address [0.0.0.0]? 131.2.25.91

PORT 23 INFORMATION:
 --------------------
Maximum weight.................. 20
Port mode....................... NONE
Port type....................... TCP
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 TCP Count: 0 UDP Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0 TCP Count: 0 UDP Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1
PORT 80 INFORMATION:
 --------------------
Maximum weight.................. 20
Port mode....................... NONE
Port type....................... BOTH
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 TCP Count: 0 UDP Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0 TCP Count: 0 UDP Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1
```

Consulte la página 159 para obtener una descripción de la información visualizada.

Quiesce

Utilice el mandato **quiesce** para detener temporalmente las funciones heartbeat o reach, o para especificar que no deben enviarse a un servidor más peticiones de conexión.

Sintaxis:

quiesce heartbeat
manager
reach

heartbeat *dirección*
Detiene la vía seleccionada para la función heartbeat. La *dirección* es la dirección IP del network dispatcher remoto al cual el Network Dispatcher envía mensajes de "Pulso".

Ejemplo:

```
quiesce heartbeat
Remote Address [0.0.0.0]? 131.2.25.94
```

manager *dirección*
Especifica que no se efectúen más peticiones de conexión al servidor especificado. *Dirección* es la dirección IP del servidor.

Ejemplo:

```
quiesce manager
Server Address [0.0.0.0]? 131.2.25.93
```

reach *dirección*

Detiene el sondeo del Network Dispatcher de la dirección especificada para determinar si es asequible, donde *dirección* es la dirección IP que forma parte del criterio de asequibilidad.

Ejemplo:

```
quiesce reach
Reach Address [0.0.0.0]? 131.2.25.92
```

Report

Utilice el mandato **report** para visualizar un informe del asesor o gestor

Sintaxis:

report advisor

manager

advisor *tipo núm-puerto*

Visualiza un informe sobre un asesor específico.

tipo Es el tipo de asesor. Entre el número de asesor que corresponde al tipo de asesor. Vea la Tabla 13 en la página 132 para conocer los tipos de asesor.

núm-puerto Es el número de puerto.

Ejemplo:

```
report advisor
0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp,6=pop3,7=telnet,8=SSL
Advisor name [0]? 1
Port number  [0]? 80

--------------------------------
|      ADVISOR:     http      |
|      PORT:          80      |
--------------------------------
| 131.2.25.93      |       0  |
| 131.2.25.94      |      16  |
--------------------------------
```

El valor mostrado para cada dirección de servidor representa:

≥0 Carga del servidor

-1 El asesor no ha podido ponerse en contacto con el servidor.

manager Visualiza un informe de la información de gestor actual.

Ejemplo:

```
report manager

----------------------------------
|  HOST TABLE LIST  |   STATUS   |
----------------------------------
|  131.2.25.93      |    ACTIVE  |
|  131.2.25.94      |    ACTIVE  |
----------------------------------
```

La información que se presenta es:

Status Visualiza el estado de la dirección de servidor.

Quiesce El servidor se ha inmovilizado.

Active El servidor no se ha inmovilizado.

```
-------------------------------------------------------------------------------
|131.2.25.91    |WEIGHT | ACTIVE % 50  |  NEW % 50    | PORT %  0 |SYSTEM %  0|
|               ---------------------------------------------------------------|
|PORT:   23     |NOW|NEW| WT | CONNECT | WT | CONNECT | WT | LOAD | WT | LOAD |
|-----------------------------------------------------------------------------|
|131.2.25.93    | 10| 10|  10|        0|  10|        0|   0|     0|-999|    -1|
|131.2.25.94    | 10| 10|  10|        0|  10|        0|   0|     0|-999|    -1|
|-----------------------------------------------------------------------------|
|PORT TOTALS:   | 20| 20|    |        0|    |        0|    |     0|    |    -2|
-------------------------------------------------------------------------------


-------------------------------------------------------------------------------
|131.2.25.91    |WEIGHT | ACTIVE % 50  |  NEW % 50    | PORT %  0 |SYSTEM %  0|
|               ---------------------------------------------------------------|
|PORT:   80     |NOW|NEW| WT | CONNECT | WT | CONNECT | WT | LOAD | WT | LOAD |
|-----------------------------------------------------------------------------|
|131.2.25.93    | 10| 10|  10|        0|  10|        1|  16|     0|-999|    -1|
|131.2.25.94    | 10| 10|  10|        0|  10|        1|   3|    16|-999|    -1|
|-----------------------------------------------------------------------------|
|PORT TOTALS:   | 20| 20|    |        0|    |        0|    |    16|    |    -2|
-------------------------------------------------------------------------------


-------------------------------------------
| ADVISOR |  PORT  |  TIMEOUT  |  STATUS  |
-------------------------------------------
|  http   |    80  | unlimited |   ACTIVE |
|  MVS    | 10007  | unlimited |   ACTIVE |
-------------------------------------------
Manager report requested.
```

La información que se presenta es:

Weight Cálculo de peso total para este servidor.

- **Now** Peso anterior asignado al servidor.
- **New** Peso más nuevo asignado al servidor.

Active % Proporción de conexiones activas para el cálculo de peso total del servidor. El valor de este parámetro se establece utilizando el mandato **set manager proportions**. Consulte la página 148.

- **Wt** Peso utilizado para el cálculo de peso total.
- **Connect** Número de conexiones activas para este servidor.

New % Nueva proporción de conexiones para el cálculo de peso total del servidor. El valor de este parámetro se establece utilizando el mandato **set manager proportions**. Consulte la página 148.

- **Wt** Peso utilizado para el cálculo de peso total.
- **Connect** Número de conexiones nuevas para este servidor.

Port % Proporción de asesor para el cálculo de peso total del servidor. El valor de este parámetro se establece utilizando el mandato **set manager proportions**. Consulte la página 148.

- **Wt** Peso utilizado para el cálculo de peso total.

Load Carga de servidor indicada por el asesor para este servidor.

System % Proporción de supervisión del sistema para el cálculo de peso total del servidor. El valor de este parámetro se establece utilizando el mandato **set manager proportions**. Consulte la página 148.

Wt Peso utilizado para el cálculo de peso total.

Load Carga de servidor indicada por el supervisor del sistema.

Status

Utilice el mandato **status** para obtener el estado de los asesores, reserva, contador, clusters, gestor, puertos y servidores.

Sintaxis:

st**atus** advisor
backup
cluster
counter
manager
ports
servers

advisor *nombre núm-puerto*
Obtiene el estado de un asesor específico.

nombre Especifica el tipo de asesor. Entre el número de asesor que corresponde al tipo de asesor. Vea la Tabla 13 en la página 132 para conocer los tipos de asesor.

núm-puerto
Es el número de puerto.

Ejemplo:

```
status advisor
0=ftp, 1=http, 2=MVS 3=TN3270, 4=SMTP, 5=NNTP, 6=POP3, 7=TELNET, 8=SSL
Advisor name [0]?
Port number [0]? 21

Advisor ftp on port 21 status:
==============================
Interval.................. 10
```

backup Obtiene el estado de la función de reserva.

Ejemplo:

```
status backup
 Dumping status ...
 Role : PRIMARY   Strategy : AUTOMATIC  State : ND_ACTIVE Sub-State : ND_SYNCHRONIZED
 <<Preferred Target : 132.2.25.92>>

 Dumping HeartBeat Status ...
 .....Heartbeat target : 131.2.25.92 Status : UNREACHABLE
 .....Heartbeat target : 132.2.25.92 Status : REACHABLE

 Dumping Reachability Status ...
 .....Host:131.2.25.93   Local:REACHABLE
 .....Host:131.2.25.94   Local:REACHABLE
```

cluster *dirección*

Obtiene el estado de un cluster especificado, donde *dirección* es la dirección IP del cluster.

Ejemplo:

```
status cluster
Cluster Address [0.0.0.0]? 131.2.25.91

EXECUTOR INFORMATION:
 ---------------------
Version: 01.01.00.00 - Tue Dec 10 14:15:58 EST 1996

CLUSTER INFORMATION:
 --------------------
Address........................ 131.2.25.91
Number of target ports......... 2
FIN clean up count............. 4000
Connection FIN timeout......... 30
Active connection stale timer... 1500
Advertise cluster address...... Yes
Advertise route cost........... 20

PORT 23 INFORMATION:
 --------------------
Maximum weight................. 20
Port mode...................... NONE
Port type...................... TCP
All up nodes are weight zero.... FALSE
Total target nodes............. 2
Currently marked down.......... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 TCP Count: 0 UDP Count: 0  Active:
0 FIN 0 Complete 0 Status: up Saved Weight: -1  Address: 131.2.25.94 Weight:
20 Count: 0 TCP Count: 0 UDP Count: 0  Active: 0 FIN 0 Complete 0 Status:
up Saved Weight: -1
PORT 80 INFORMATION:
 --------------------
Maximum weight................. 20
Port type...................... BOTH
Port mode...................... NONE
All up nodes are weight zero.... FALSE
Total target nodes............. 2
Currently marked down.......... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 TCP Count: 0 UDP Count: 0  Active:
0 FIN 0 Complete 0 Status: up Saved Weight: -1  Address: 131.2.25.94 Weight:
20 Count: 0 TCP Count: 0 UDP Count: 0  Active: 0 FIN 0 Complete 0 Status:
up Saved Weight: -1
```

Consulte la página 159 para obtener definiciones de los campos visualizados.

counter Obtiene el estado de todos los contadores.

Ejemplo:

```
status counter
Internal counters from executor:
--------------------------------
Total number of packets into executor...... 2684
Total packets for cluster processing (C)... 2684
Packets not addressed to a cluster(port)... 0

Cluster processing results:
---------------------------
Errors......................................... 0
Discarded...................................... 0
Own address.................................0
Forward requested.............................. 2684
Forward discarded with error................... 0

Other processing problems:
--------------------------
Total packets dropped (C)...................... 0
```

manager Obtiene el estado del gestor.

Ejemplo:

```
status manager
Number of defined hosts... 2
Sensitivity.............. 0%
Smoothing factor......... 2
Interval................. 3
Weights refresh cycle..... 4

Active connections gauge proportion......... 40%
New connections counter(delta) proportion... 38%
Advisor gauge proportion.................... 20%
System Metric proportion...................  2%

Manager status requested.
```

port *dirección-cluster núm-puerto*

Obtiene el estado de un puerto específico, donde:

dirección-cluster
: es la dirección IP del cluster.

núm-puerto
: es el número de puerto en el cluster.

Ejemplo:

```
status port
Cluster Address [0.0.0.0]? 131.2.25.91
Port number  [0]? 80

PORT 80 INFORMATION:
 --------------------
Maximum weight.................. 20
Port mode....................... NONE
Port type....................... BOTH
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 12345 TCP Count: 10000 UDP count 2345
Active: 3431 FIN 3780 Complete 3431  Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 7890  Active: 2980 FIN 2390 Status: up
Saved Weight: -1
```

La información de servidor que se presenta es:

Address
: Dirección IP del servidor

Weight
: Peso asignado actualmente a este servidor

Count
: Cuenta acumulativa de conexiones TCP y paquetes UDP

TCP Count
: Cuenta acumulativa de conexiones TCP

UDP Count
: Cuenta acumulativa de paquetes UDP

Active
: Número de conexiones TCP activas

FIN
: Las conexiones TCP están en estado FIN

Complete
: Las conexiones TCP que se han completado (se ve ACK después de FIN)

Status
: Estado de servidor configurado:

  active — El servidor está activo.

  down — El servidor está inactivo.

  quiesced — El servidor está inmovilizado.

  not responding — El servidor no está respondiendo al asesor.

Saved weight Peso de servidor antes de que el servidor se marcara como inactivo

server *dirección*

Obtiene el estado de un servidor específico, donde *dirección* es la dirección IP del cluster al cual pertenece el servidor.

Ejemplo:

```
status server
Cluster Address [0.0.0.0]? 131.2.25.91

PORT 23 INFORMATION:
 --------------------
Maximum weight.................. 20
Port mode....................... NONE
Port type....................... TCP
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 140 TCP Count: 100 UDP Count: 40
Active: 50 FIN 45 Complete 50  Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 250 TCP Count: 100 UDP Count: 40
Active: 60 FIN 54 Complete 50  Status: up Saved Weight: -1

PORT 80 INFORMATION:
 --------------------
Maximum weight.................. 20
Port mode....................... NONE
Port type....................... BOTH
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 12345 TCP Count: 10000 UDP Count: 2345
Active: 3431 FIN 3780 Complete 3431  Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 7890  TCP Count: 10000 UDP Count: 2345
Active: 2980 FIN 2390 Complete 3431  Status: up Saved Weight: -1
```

Switchover

Utilice el mandato **switchover** para hacer que un Network Dispatcher que se ejecuta en modalidad de espera se convierta en el Network Dispatcher activo cuando la estrategia de conmutación es manual. Este mandato debe entrarse en el sistema principal que ejecuta el Network Dispatcher que está en modalidad de espera.

Sintaxis:

sw**itchover**

Unquiesce

Utilice el mandato **unquiesce** para reiniciar una función heartbeat, manager o reach detenida previamente con el mandato **quiesce**.

Sintaxis:

u**nquiesce** heartbeat
manager
reach

heartbeat *dirección*

Reinicia la vía para mensajes de "Pulso", donde *dirección* es la dirección IP del Network Dispatcher remoto al cual envía mensajes de "Pulso" este Network Dispatcher.

Ejemplo:

```
unquiesce heartbeat
Remote Address [0.0.0.0]? 9.10.11.1
```

manager *dirección*

Reinicia el envío de peticiones de conexión al servidor especificado. *Dirección* es la dirección IP del servidor.

Ejemplo:

```
unquiesce manager
Server Address [0.0.0.0]? 20.21.22.15
```

reach *dirección*

Reinicia el sondeo del Network Dispatcher de la dirección especificada para determinar si es asequible, donde *dirección* es la dirección IP que forma parte del criterio de asequibilidad.

Ejemplo:

```
unquiesce reach
Reach address [0.0.0.0]? 20.3.4.5
```

Soporte de reconfiguración dinámica del Network Dispatcher

Esta sección describe la reconfiguración dinámica (DR) en lo que afecta a los mandatos de Talk 6 y Talk 5.

Delete interface de CONFIG (Talk 6)

El mandato de CONFIG (Talk 6) **delete interface** no es aplicable para la NDR. El Network Dispatcher es una característica y no se configura en una interfaz.

Activate interface de GWCON (Talk 5)

El mandato de GWCON (Talk 5) **activate interface** no es aplicable para la NDR. El Network Dispatcher es una característica y no se configura en una interfaz.

Reset interface de GWCON (Talk 5)

El mandato de GWCON (Talk 5) **reset interface** no es aplicable para la NDR. El Network Dispatcher es una característica y no se configura en una interfaz.

Mandatos de cambio inmediato de CONFIG (Talk 6)

La NDR soporta los mandatos de CONFIG siguientes que cambian inmediatamente el estado operativo del dispositivo. Estos cambios se guardan y se conservan si se vuelve a cargar o se reinicia el dispositivo o si se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
CONFIG, feature ndr, add advisor
CONFIG, feature ndr, add backup
CONFIG, feature ndr, add cluster
CONFIG, feature ndr, add heartbeat
CONFIG, feature ndr, add port
CONFIG, feature ndr, add reach
CONFIG, feature ndr, add server
CONFIG, feature ndr, disable advisor
CONFIG, feature ndr, disable backup
CONFIG, feature ndr, disable executor **Nota:** Cuando el ejecutor se inhabilita, elimina todos los clusters, puertos y servidores de las estructuras de código de ejecución, excepto *NOT SRAM*.
CONFIG, feature ndr, disable manager
CONFIG, feature ndr, enable advisor
CONFIG, feature ndr, enable backup
CONFIG, feature ndr, enable executor
CONFIG, feature ndr, enable manager
CONFIG, feature ndr, remove advisor
CONFIG, feature ndr, remove backup
CONFIG, feature ndr, remove cluster **Nota:** La eliminación de un cluster hace que todos los puertos y servidores asociados con dicho cluster se eliminen de las estructuras de código de ejecución y de la SRAM.
CONFIG, feature ndr, remove heartbeat
CONFIG, feature ndr, remove port
CONFIG, feature ndr, remove reach
CONFIG, feature ndr, remove server
CONFIG, feature ndr, set advisor
CONFIG, feature ndr, set cluster
CONFIG, feature ndr, set manager
CONFIG, feature ndr, set port
CONFIG, feature ndr, set server

Mandatos no reconfigurables dinámicamente

Todos los parámetros de configuración NDR pueden cambiarse dinámicamente.

Configuración y supervisión del subsistema de codificación

Las funciones de compresión y cifrado de datos se agrupan dentro del Subsistema de codificación (ES). El ES proporciona acceso al dispositivo de software de codificación para interfaces o protocolos y se activa automáticamente cuando se activa un enlace para compresión o cifrado. El dispositivo de software está formado por software operativo que lleva a cabo las funciones de compresión y cifrado. Los algoritmos de compresión y cifrado se ejecutan en el procesador del direccionador. No es necesario cambiar la configuración por omisión para utilizar el dispositivo de software.

Nota: Consulte el apartado “Configuración y supervisión de la compresión de datos” en la página 171 para obtener instrucciones sobre cómo configurar sesiones de compresión sobre PPP o Frame Relay, consulte el apartado “Utilización y configuración de protocolos de cifrado” en la página 217 para obtener instrucciones sobre cómo configurar sesiones de cifrado sobre PPP o Frame Relay y consulte el apartado “Configuración y supervisión de la seguridad de IP” en la página 343 para obtener instrucciones sobre cómo configurar sesiones de IPSec.

La supervisión de la actividad del ES se puede llevar a cabo entrando **feature es** en el indicador de mandatos (talk 5) de supervisión.

Los parámetros de configuración del ES le permiten limitar la cantidad de memoria utilizada por el dispositivo de software del ES. La configuración por omisión permite que el ES obtenga la memoria que necesite. Para limitar la utilización de memoria, utilice el mandato **set** bajo **feature es** en el proceso de configuración (Talk 6).

Este capítulo consta de las secciones siguientes:

Configuración del subsistema de codificación

Los parámetros de configuración del ES proporcionan un medio para controlar el número de sesiones de compresión y cifrado que utilizan el dispositivo de codificación de software a la vez. El dispositivo de codificación de software consiste esencialmente en un conjunto de bibliotecas de compresión y cifrado que se ejecutan en el procesador del direccionador. Una sesión consta de una conexión dúplex sobre una interfaz en particular que se ha configurado para utilizar compresión o cifrado.

Generalmente, la codificación de datos es una operación que requiere un uso intensivo del procesador. Mediante la limitación del número de sesiones de codificación de software, el impacto de la codificación de datos en el rendimiento del direccionador se puede controlar hasta cierto punto. Por ejemplo, si el direccionador tiene configuradas 20 interfaces de marcación de entrada para compresión y se ha determinado que la compresión de más de 10 interfaces a la vez tiene un efecto adverso en el rendimiento del direccionador, el número máximo de

sesiones de compresión debe establecerse en 10. Esto permite que 10 de las 20 interfaces utilicen la compresión.

Los requisitos de memoria del dispositivo de codificación de software también puede ser un motivo para limitar el número de sesiones. Cada sesión de compresión por software utiliza aproximadamente 30 KB de memoria de direccionador y una sesión de cifrado utiliza aproximadamente 2 KB. Si el ES utiliza demasiada memoria, es posible que otras funciones tengan restricciones de memoria y el rendimiento del direccionador puede verse afectado negativamente. Consulte el apartado “Consideraciones” en la página 174 para obtener información.

Puede establecer el número mínimo o máximo de sesiones del ES indicando el número de sesiones o especificando uno de los valores *unlimited*, *default* o un número. Los valores *unlimited* y *default* tienen el mismo significado; estos valores permiten que el direccionador soporte todas las sesiones que se han activado para cifrado o compresión, hasta que se agote la memoria.

Nota: Ninguno de los parámetros de configuración del ES (talk 6) se puede volver a configurar dinámicamente. Para activar los valores de los parámetros después de haberlos cambiado, debe reiniciar o volver a cargar el direccionador.

En el proceso Config (talk 6), entre **feature es** en el indicador de mandatos `Config>` para acceder a los mandatos de configuración del ES. Aparece el indicador de mandatos `ES Config>`. La Tabla 16 lista los mandatos.

Tabla 16. Mandatos de configuración del ES

Mandato	Acción
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
List	Visualiza el valor actual de las sesiones de compresión y cifrado.
Set	Establece el número máximo de sesiones de cifrado y compresión disponibles para todas las interfaces.
Exit	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 visualizar el valor actual de las sesiones de compresión y cifrado.

Sintaxis:

list

Ejemplo:

```
ES Config> list
Data Compression and Encryption System Configuration
----------------------------------------------------

Parameters used for host-based encoding:
  Compression sessions:
    Reserved at initial bootup:           0
    Maximum allowed:                      unlimited
  Encryption sessions:
    Reserved at initial bootup:           0
    Maximum allowed:                      unlimited
```

Set

Utilice el mandato **set** para establecer el número máximo de sesiones de cifrado o compresión de datos.

Sintaxis:

set sw minimum compression-sessions *n, unlimited o default*

sw maximum compression-sessions *n, unlimited o default*

sw minimum encryption-systems *n, unlimited o default*

sw maximum encryption-systems *n, unlimited o default*

Nota: Las letras sw son una abreviatura para software.

software minimum compression-sessions *n, unlimited o default*
Establece el número mínimo de sesiones de compresión disponibles para las interfaces. El direccionador reserva estas sesiones de modo que siempre están disponibles.

Valor por omisión: 0

Valores válidos: de 0 a *unlimited*; como alternativa, *default*

software maximum compression-sessions *n, unlimited o default*
Establece el número máximo de sesiones de compresión disponibles para las interfaces. Una vez activado este número de sesiones, no se pueden activar sesiones nuevas.

Valor por omisión: 0

Valores válidos: de 0 a *unlimited*; como alternativa, *default*

software minimum encryption-sessions *n, unlimited o default*
Establece el número mínimo de sesiones de crifrado disponibles para las interfaces. El direccionador reserva este número de sesiones de modo que siempre están disponibles.

Valor por omisión: 0

Valores válidos: de 0 a *unlimited*; como alternativa, *default*

software maximum encryption-sessions *n, unlimited o default*
Establece el número máximo de sesiones de cifrado disponibles para las interfaces. Una vez activado este número de sesiones, no se pueden activar sesiones nuevas.

Valor por omisión: 0

Valores válidos: de 0 a *unlimited*; como alternativa, *default*

Supervisión del subsistema de codificación

En el proceso de supervisión, entre **feature es** en el indicador de mandatos + para acceder a los mandatos de supervisión del ES. Aparece el indicador de mandatos `ES Monitor>`. La Tabla 17 lista los mandatos disponibles.

Tabla 17. Mandato de supervisión del ES

Mandato	Acción
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
List	Lista los puertos, los circuitos, los dispositivos, la configuración, el estado o el resumen del ES.
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 información sobre el ES. Consulte el mandato **list summary** para ver un ejemplo de la salida del mandato **list** que incluya puertos, dispositivos y estado.

Sintaxis:

list ports
circuits
devices
config
status
summary

ports El mandato **list ports** lista los puertos de codificación creados por clientes potenciales del sistema de codificación. Un puerto establece un enlace entre el sistema de codificación y los clientes configurados para utilizar el ES. Por ejemplo, si se configura la compresión o el cifrado sobre la Red 1 de interfaz PPP, existe un puerto asociado con esta interfaz. El campo QLen muestra la suma de todas las peticiones de compresión o cifrado pendientes para todos los circuitos asociados con el puerto. Un cliente, como por ejemplo PPP configurado sobre una interfaz particular, presenta una petición al ES cuando designa un almacenamiento intermedio de datos particular para codificación.

El campo Status (Estado) muestra *Idle* (Desocupado) no hay nada en cola en el puerto o *Busy* (Ocupado) o *Waiting* (En espera) si hay peticiones en proceso o en cola en el puerto.

circuits El mandato **list circuits** visualiza los circuitos que han definido los clientes del sistema de codificación. Cada circuito corresponde a una conexión dúplex. Cifrado o comprimido a una fecha en un extremo se descifra o descomprime en el otro.

Por omisión, sólo se visualizan los circuitos activos. Utilice el mandato **list circuits all** para incluir los circuitos activos y los inactivos.

Para cada circuito que se encuentra, el puerto y el usuario se visualizan igual que en el mandato **list ports**. Además, se muestran dos líneas de información, una línea Tx para el circuito de salida y una línea Rx para el circuito de entrada. El ID de circuito es un número arbitrario que proporciona el cliente para poder identificar cada circuito que crea. Para circuitos Frame Relay, este número corresponde al ID del circuito de enlace de datos (DLCI) Frame Relay asociado. Los enlaces punto a punto sólo crean un circuito, que se identifica siempre mediante el número *1*.

Además, se visualizan los elementos siguientes:

Dev Es el número que representa el dispositivo de codificación que sirve a dicha corriente. Es 1 cuando la codificación se realiza mediante la activación de software de la CPU y 2 cuando la codificación la realiza el adaptador de compresión/cifrado.

Cmpr Este campo visualiza el algoritmo de compresión o descompresión activo para dicha corriente. Si es *LZC*, se utiliza compresión STAC-LZC; si es *MPPC*, se utiliza Microsoft® PPC. Se añade un asterisco (*) al nombre del algoritmo si la corriente funciona en modalidad sin estado. La modalidad sin estado es una modalidad en la que la historia del paquete de datos no se mantiene una vez procesado el paquete, al contrario de la modalidad continua en la que la historia se mantiene después del manejo de un paquete para poder manejar el siguiente. Por ejemplo, en compresión continua, el codificador mantiene una antememoria de información obtenida de paquetes anteriores para comprimir más eficazmente los paquetes actuales.

Encr Este campo visualiza el algoritmo de cifrado o descifrado que se utiliza. Es *DES* para DES estándar, *3DES* para Triple DES o *RC4* si se utiliza el algoritmo RC4 de RSA. Se añade un asterisco (*) al nombre si la corriente funciona en modalidad sin estado. Esto es importante para RC4 pero no para DES/3DES. Tenga en cuenta que el nombre mostrado corresponde al algoritmo de cifrado básico que se utiliza, no al formato de encapsulación que utiliza el cliente. Por ejemplo, PPP soporta dos métodos de encapsulación: DESE (RFC 1969) que cifra con DES, y MPPE (no estándar Microsoft), que utiliza RC4.

QLen Este parámetro muestra el número de paquetes pendientes en la cola de la corriente que esperan para ser codificados o descodificados. Tenga en cuenta que este número sólo refleja paquetes que se han sometido realmente al ES para su proceso. Algunos clientes pueden mantener sus propias colas y enviar sólo unos cuantos paquetes nuevos a la vez al sistema de codificación desde estas colas privadas.

Status Una indicación rápida del estado de la corriente. No es inusual que todas las corrientes tengan un estado de espera y que ninguna parezca estar ocupada. Para ver un estado de ocupado es necesario interrumpir la actividad de la cola

durante un período bastante reducido de tiempo dentro del ciclo de proceso. Los estados posibles son los siguientes:

Desocupado No hay ningún paquete en cola en esta corriente

Ocupado El sistema está procesando actualmente paquetes en esta corriente (lo que significa que el elemento situado a la cabeza de la cola está pasando por el mecanismo de codificación en este momento).

En espera Hay peticiones pendientes, pero nada de dicha corriente está procesándose actualmente.

devices El mandato **list devices** lista los dispositivos de codificación que el sistema tiene a su disposición. Un dispositivo de codificación generalmente hace referencia a un adaptador de compresión/cifrado. El software que se utiliza cuando un acelerador de hardware no está disponible se implanta como un dispositivo virtual y también aparecerá en esta lista como un dispositivo *Host Software*. Existen dos formas para este mandato: **list devices** y **list device n**. La primera forma produce un breve listado de resumen de todos los dispositivos reconocidos por el sistema. La segunda forma producirá un listado detallado para un dispositivo específico n, donde n es el número de unidad. Unidad 1 representa software de sistema principal, que es un dispositivo de codificación virtual y unidad 2 representa el adaptador de compresión/cifrado. Se puede utilizar un asterisco (*) en lugar del número n, en cuyo caso se proporciona un listado para ambas unidades.

config El mandato **list config** visualiza los parámetros de configuración actuales. Son los parámetros leídos desde la memoria no volátil en el momento en que el direccionador se reinicia o se vuelve a cargar. La información visualizada es idéntica a la que se visualiza mediante el mandato **list config** de configuración (Talk 6).

status El mandato **list status** visualiza el estado del sistema de codificación, que consta de algunos identificadores de estado global y de estadísticas varias del sistema. Son las descripciones de los campos que se visualizan con el mandato **list status**:

Last Error

El último código de error devuelto a un cliente del sistema de codificación. Sirve para la depuración y debe utilizarlo el personal de servicio.

Internal Condition flags

Este campo muestra algunas condiciones internas, tal como se define en la lista siguiente:

Ready El sistema está activo y es operativo. Es la condición normal.

Not Working

El sistema de codificación no es operativo debido a un error interno.

No Devices Available

Indica que no hay ningún dispositivo disponible para realizar la codificación. Esta condición no

debe producirse si no hay presente un codificador basado en el hardware, la codificación la lleva a cabo el software interno.

Out of Memory
El sistema ha intentado asignar memoria y ha fallado. Esta condición indica que el direccionador está bajo de RAM y que el sistema de codificación se ha visto afectado de manera negativa.

Number of Ports
Este campo indica el número de clientes que han establecido puertos para sí mismos en el ES. Consulte el mandato **list ports** para obtener una definición de un puerto.

Number of Circuits
Consulte el mandato **list circuits** para obtener una definición de los circuitos.

Global Request pool size
El número de almacenamientos intermedios de peticiones asignados y libres. Aproximadamente se utiliza un almacenamiento intermedio de peticiones para cada paquete que se codifica. Si el número de almacenamientos intermedios libres es menor que el número asignado, la codificación está en proceso.

Total # of Requests processed
Este valor muestra el número total de almacenamientos intermedios que el mecanismo de codificación ha procesado. Este número corresponde aproximadamente al número total de paquetes que todos los clientes del sistema han comprimido o cifrado desde que se ha reiniciado o se ha vuelto a cargar el último direccionador.

summary Este mandato visualiza un resumen del sistema. Es un mandato compuesto que combina la salida de los mandatos **list status**, **list devices** y **list ports**.

Ejemplo:

```
list summary

Encoding System Status
----------------------

Last Error:                              14 (Stream not active)

Internal Condition flags:                0x00000001   -->
                                          Ready

Number of Ports:                         2

Global Request pool size:                Alloc: 32  Free: 32
Total # of Requests processed:           7059

 Encoding System Devices
 Encoding System Devices

Device Type                        Slot/Port  Status
------ --------------------------  ---------  ----------
     1 Host Software                  0/0     Ready
     0 Null Device                    0/0     Ready


                       Encoding System Ports
                       ---------------------

                                  +--Encoder State---+   +--Decoder State---+
Port  User                        QLen  Status           QLen  Status
----  -------------------------   ----  --------------   ----  --------------
   1  Net 2   (PPP/0)               0  Idle                0  Idle
   2  Net 3   (PPP/1)               0  Idle                0  Idle
```

Soporte de reconfiguración dinámica del subsistema de cifrado

Esta sección describe la reconfiguración dinámica (DR) en lo que afecta a los mandatos de Talk 6 y Talk 5.

Delete interface de CONFIG (Talk 6)

El Subsistema de codificación no soporta el mandato de CONFIG (Talk 6) **delete interface**.

Activate interface de GWCON (Talk 5)

El mandato GWCON (Talk 5) **activate interface** no es aplicable al Subsistema de codificación. Los parámetros de configuración del ES determinan cuánta memoria se asignará para el ES en el arranque y no están asociados con ninguna interfaz.

Reset interface de GWCON (Talk 5)

El mandato de GWCON (Talk 5) **reset interface** no es aplicable al Subsistema de codificación. Los parámetros de configuración del ES determinan cuánta memoria se asignará para el ES en el arranque y no están asociados con ninguna interfaz.

Mandatos no reconfigurables dinámicamente

El Subsistema de codificación no soporta cambios dinámicos de ninguna de sus parámetros de configuración.

Configuración y supervisión de la compresión de datos

Este capítulo describe la compresión de datos en un 2210 sobre interfaces Frame Relay y PPP. El capítulo incluye las secciones siguientes:

La compresión de datos está soportada en interfaces Frame Relay y PPP.

Visión general de la compresión de datos

El sistema de compresión de datos proporciona un medio de aumentar el ancho de banda de las interfaces de la red en el dispositivo. Básicamente está pensado para utilizarlo en enlaces de WAN de velocidad más lenta.

La compresión de datos en el dispositivo se soporta en interfaces PPP y Frame Relay.

- Para interfaces PPP, la compresión se implanta de acuerdo con el Compression Control Protocol (CCP) tal como se define en la RFC 1962 de Internet Engineering Task Force. El CCP proporciona los mecanismos básicos mediante los cuales se negocia la utilización de la compresión y un medio para elegir entre múltiples protocolos de compresión posibles.

  El dispositivo proporciona dos protocolos de compresión: el protocolo Stac-LZS, definido en la RFC 1974 y el protocolo Microsoft Point-to-Point Compression (MPPC), descrito en la RFC 2118. Ambos se basan en algoritmos de compresión proporcionados por Stac Electronics.

- Para interfaces Frame Relay, la compresión se implanta de acuerdo con el FRF.9, el *Data Compression over Frame Relay Implementation Agreement* producido por el Frame Relay Forum Technical Committee. El FRF.9 describe un Data Compression Protocol (DCP), modelado según el CCP de PPP y, de modo similar, proporciona un medio para negociar varios algoritmos de y opciones de compresión. El dispositivo soporta la negociación en "modalidad 1" de DCP. El FRF.9 también describe una "modalidad 2" más generalizada, que no está soportada. La compresión se lleva a cabo utilizando el mismo mecanismo de compresión que se utiliza para el protocolo PPP Stac-LZS.

Conceptos sobre la compresión de datos

La compresión de datos del dispositivo proporciona un medio para aumentar el rendimiento en los enlaces de la red haciendo que sea más eficaz la utilización del ancho de banda disponible en un enlace. El principio básico implícito es simple: representar los datos que circulan a través de un enlace del modo más compacto posible para que el tiempo necesario para transmitirlos sea lo más corto posible, según una velocidad establecida en un enlace.

La compresión de datos se puede llevar a cabo en varias capas del modelo de red. A un extremo del espectro, las aplicaciones pueden comprimir datos antes de trasmitirlos a aplicaciones similares en otro lugar de la red, mientras que en el otro extremo del espectro los dispositivos pueden realizar compresión en la capa de enlace de datos, trabajando estrictamente en la corriente de bits que pasan entre dos nodos. El modo de llevar a cabo esta compresión y su efectividad depende de varios factores, entre los que se incluyen en qué capa de la red se efectúa la compresión, el grado de conocimiento intrínseco que el compresor y el descompresor tienen sobre los datos que se comprimen, el algoritmo de compresión elegido y los datos reales que se están comprimiendo. Normalmente la mejor compresión se realiza en la capa de aplicación; por ejemplo, por lo general una aplicación de transferencia de archivos tiene la ventaja de tener todo un archivo de datos disponible antes de intentar la compresión y puede probar distintos algoritmos de compresión en el archivo para ver cuál funciona mejor en los datos del archivo determinado. Aunque de este modo se puede obtener una compresión excelente para este tipo de aplicación, no sirve para solucionar el problema general de comprimir la masa del tráfico que circula a través de una red, dado que la mayoría de aplicaciones de red actualmente no comprimen los datos a medida que los generan.

La compresión en el dispositivo tiene lugar en una capa de red más inferior, en la capa de enlace de datos. En el dispositivo, la compresión se realiza en los paquetes individuales que se transmiten a través de un enlace. La compresión se realiza en tiempo real a medida que los paquetes circulan a través del dispositivo: el emisor comprime un paquete justo antes de transmitirlo y el descompresor descomprime el paquete tan pronto como lo recibe. Esta operación es transparente para los protocolos de red capas superiores.

Conceptos básicos sobre la compresión de datos

Los compresores de datos funcionan reconociendo la información “redundante” en los datos y produciendo un conjunto de datos diferente que contiene la menor cantidad de redundancia posible. Una información “redundante” es cualquier información que se pueda deducir y volver a crear basándose en los datos que hay disponibles actualmente. Por ejemplo, un compresor puede funcionar reconociendo patrones de caracteres repetidos en una corriente de datos y sustituyendo estos patrones repetidos por una secuencia de código más corta para representar dicho patrón. Siempre y cuando el compresor y el descompresor estén de acuerdo sobre cuáles son estas secuencias de código, el descompresor siempre puede volver a crear los datos originales a partir de los datos comprimidos.

Esta correlación de secuencias de los datos originales con las secuencias correspondientes de la salida comprimida usualmente se llama ***diccionario de datos***. Estos diccionarios pueden definirse estáticamente (información basada en la experiencia disponible para el compresor y el descompresor) o se pueden generar dinámicamente, generalmente basándose en la información que se comprime. Los diccionarios estáticos son aplicables sobretodo a entornos en los que los datos que se procesan son de naturaleza conocida y limitados, y no son demasiado efectivos para compresores de propósito general. La mayoría de sistemas de compresión utilizan diccionarios dinámicos, incluyendo los compresores que se utilizan en el dispositivo. En un 2210 los diccionarios de datos se basan en el paquete actual que se procesa y posiblemente en los paquetes que ha visto anteriormente, pero no existe capacidad para “mirar más adelante” en la corriente de datos tal como sucede cuando la compresión se realiza en otras capas. Para sistemas en los que

el diccionario de datos se deriva dinámicamente y sólo se basa en los datos que se han visto previamente, el diccionario se conoce usualmente como ***histórico***. Los términos histórico y diccionario de datos se utilizarán indistintamente en el resto de este capítulo, pero debe entenderse que en otros entornos un histórico es una forma específica del diccionario de datos.

El hecho de que el dispositivo utilice diccionarios dinámicos y que el compresor y el descompresor deban mantener sus diccionarios en sincronización significa que la compresión de datos funciona en una corriente de datos que pasa entre dos puntos finales. Por lo tanto, la compresión en el direccionador es un proceso orientado a la conexión, donde los puntos finales de la conexión son los mismos compresor y descompresor. Cuando se inicia la compresión en la corriente, ambos extremos restauran sus diccionarios de datos a algún estado inicial conocido y, a continuación, actualizan dicho estado a medida que reciben datos.

La compresión se puede realizar en cada paquete individual, restaurando los históricos antes de procesar cada paquete. Sin embargo, normalmente los diccionarios de datos no se restauran entre paquetes, lo que significa que los históricos no sólo se basan en el contenido del paquete actual, sino que también en el contenido de los paquetes que han visto previamente. Con esto suele mejorar la eficacia global de la compresión, dado que aumenta la cantidad de datos que busca el compresor cuando busca redundancias a eliminar. Por ejemplo, considere el caso de un sistema principal “sondeando” otro sistema principal con IP: se envía una serie de paquetes, cada uno de los cuales es generalmente casi idéntico al último que se ha enviado. El compresor puede que no tenga demasiada suerte al comprimir el primer paquete, pero puede reconocer que cada paquete subsiguiente se parece mucho al último que se ha enviado y produce versiones sumamente comprimidas de dichos paquetes.

Puesto que los históricos del compresor y el descompresor cambian con cada paquete recibido, los mecanismos de compresión son sensibles a los paquetes perdidos, dañados o reordenados. Los protocolos de compresión empleados por el dispositivo incluyen mecanismos de señalización por medio de los cuales el compresor y el descompresor pueden detectar la pérdida de sincronización y resincronizarse el uno al otro, como puede ser necesario cuando se pierde un paquete debido a un error de transmisión. Generalmente se lleva a cabo incluyendo un número de secuencia en cada paquete que será comprobado por el descompresor para asegurarse de que recibe todos los paquetes, en orden. Si detecta un error, se restaurará a sí mismo a algún estado inicial conocido, indicará al compresor que haga lo mismo y, a continuación, esperará (descartando los paquetes de entrada comprimidos) a que el compresor reconozca que también se ha restaurado a sí mismo.

Normalmente, la compresión en un enlace se lleva a cabo en los datos que se transmiten en ambas direcciones a través del enlace. Generalmente, en cada extremo de una conexión se ejecuta un compresor y un descompresor, que se comunican con sus análogos en el otro extremo de la conexión, tal como se muestra en la Figura 10 en la página 174. El extremo de salida (compresión) se ejecuta independientemente respecto al extremo de entrada (descompresión). Es posible que se apliquen algoritmos de compresión completamente diferentes para cada dirección del enlace. Cuando se establece una conexión de enlace, el protocolo de control de compresión para el enlace se negociará con el similar para determinar los algoritmos de compresión que se utilizan para la conexión. Si los dos extremos no se ponen de acuerdo sobre los protocolos de compresión que van

a utilizar, no se realizará ninguna compresión y el enlace funcionará normalmente (es decir, los paquetes simplemente se enviarán en su forma descomprimida).

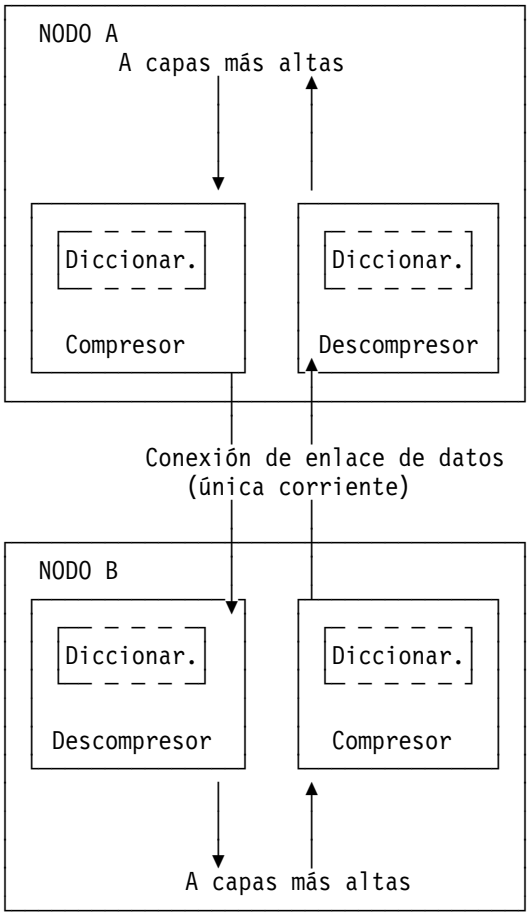


Figura 10. Ejemplo de compresión de datos bidireccional con diccionarios de datos

En realidad una corriente representa una conexión entre un proceso de compresión específico en un extremo de un enlace y un proceso de descompresión asociado en el otro extremo de un enlace y, de este modo, es más específico que únicamente una “conexión” entre dos nodos; es posible que un protocolo de compresión sofisticado pueda dividir los datos que circulan entre dos sistemas principales en varias corrientes, comprimiendo cada una de ellas de modo independiente. Por ejemplo, el CPP de PPP tiene la capacidad de negociar el uso de varios históricos a través de un enlace PPP, aunque el direccionador no soporte esta capacidad.

Consideraciones

La decisión sobre si debe utilizarse o no compresión de datos no siempre es fácil. Existen varios factores que deben considerarse antes de habilitar la compresión en una conexión.

Carga de la CPU

La compresión de datos es un procedimiento costoso desde el punto de vista informático. A medida que la cantidad de datos que se comprimen va aumentando (por tiempo de unidad), más cantidad de una carga se sitúa en el procesador del dispositivo. Si la carga se hace demasiado grande, el rendimiento del dispositivo disminuye (en todas las interfaces, no sólo en las que se lleva a cabo la compresión).

En realidad el dispositivo contiene varios procesadores y utiliza multiproceso asimétrico (por ejemplo, controladores de E/S de enlace que funcionan en tándem con el procesador principal) por lo que el efecto de la carga del procesador no siempre es fácil de medir. Puesto que el proceso de la compresión puede verse solapado por la transmisión de paquetes, de hecho esta carga puede ser totalmente transparente y no suponer ningún problema. No obstante, es posible que el procesador del dispositivo se sobrecargue y que disminuya el rendimiento.

Cómo método práctico general, la compresión sólo deberá habilitarse en enlaces de WAN lentos - probablemente sólo para enlaces con velocidades máximas de 64 kbps aproximadamente (la velocidad de un enlace de marcación ISDN típico). El ancho de banda total para los datos que se están comprimiendo en todos los enlaces debería limitarse probablemente a varios centenares de kbps. La ejecución de la compresión en todos los canales de un adaptador de Velocidad Primaria RDSI no sería prudente.

Los parámetros del Subsistema de codificación le permiten limitar el número de conexiones que pueden ejecutar simultáneamente la compresión. Entonces se pueden habilitar más interfaces para la compresión de las que realmente la ejecutan. Cuando se alcanza el límite del número de conexiones de compresión activas, las conexiones adicionales simplemente no negociarán el uso de la compresión, como mínimo no hasta que se cierre el enlace de compresión existente.

Utilización de la memoria

Otro tema a considerar al configurar la compresión es el requisito de memoria. Los históricos de compresión y descompresión ocupan una cantidad considerable de memoria, que es un recurso limitado del dispositivo. El algoritmo Stac-LZS, por ejemplo, necesita alrededor de 16 KB para un histórico de compresión y aproximadamente 8 KB para un histórico de descompresión. El problema aumenta por el hecho de que estos históricos deben existir para cada conexión que se establece: un histórico de compresión se sincroniza con un histórico de descompresión correspondiente en un direccionador similar. Para un enlace PPP, esto implica un histórico de compresión y un histórico de descompresión (suponiendo que la compresión de datos se ejecuta bidireccionalmente en el enlace). En un enlace Frame Relay, puede que hagan falta estos históricos, un par para cada conexión virtual (DLCI) que se establece.

El dispositivo crea una agrupación de históricos de compresión y descompresión cuando arranca. Estos históricos se asignan siempre en pares conocidos como ***sesiones de compresión*** - una sesión es simplemente un histórico de compresión emparejado con un histórico de descompresión. Técnicamente, la compresión y la descompresión son funciones independientes, pero a la práctica la compresión casi siempre se ejecuta bidireccionalmente y, por lo tanto, la memoria se gestiona y configura basándose en sesiones en lugar de históricos individuales para simplificar la operación. Dado que los distintos algoritmos de compresión tienen requisitos de memoria diferentes para la compresión y descompresión, se proporciona a

la sesión un tamaño aproximado de 30 KB para poder manejar el peor de los casos. La agrupación de sesiones de compresión está poblada según se haya configurado en la característica Subsistema de codificación. Consulte el apartado “Configuración y supervisión del subsistema de codificación” en la página 163 para obtener información detallada.

Cuando el dispositivo intenta establecer una conexión de compresión en un enlace, empieza reservando una sesión de la agrupación de sesiones asignada. Si no hay disponible ninguna sesión, no se lleva a cabo la compresión en dicha conexión. El direccionador puede intentar iniciar más adelante la compresión en dicha conexión, cuando las sesiones estén disponibles.

El número de sesiones de compresión que se asignan es un parámetro configurable. El establecimiento del número de sesiones asignadas limita la cantidad de memoria utilizada y el número máximo de conexiones que pueden funcionar simultáneamente con compresión. La limitación del número de conexiones de compresión que funcionan simultáneamente proporciona un medio para ayudar a controlar el problema de carga de la CPU.

Contenido de los datos

Debe considerarse la naturaleza real de los datos que se transmiten en una conexión antes de habilitar la compresión para dicha conexión. La compresión funciona mejor en algunos tipos de datos que en otros. Los paquetes que contienen mucha información prácticamente idéntica (por ejemplo, un conjunto de paquetes generado a partir de un “sondeo” de IP) normalmente se comprimen sumamente bien. Un conjunto típico de datos binarios y de texto aleatorios que se transmiten través de enlace generalmente se comprime en proporciones de 1,5:1 a 3:1. Algunos datos simplemente no se comprimen en absoluto. En particular, los datos que ya se han comprimido rara vez se comprimen más. De hecho, los datos que ya se han comprimido pueden ampliarse cuando pasan a través del mecanismo de compresión.

Si se sabe por avanzado que la mayoría de datos que pasan a través de una conexión serán datos comprimidos, se recomienda no habilitar la compresión para dicha conexión. Un ejemplo donde se puede producir esta situación es una conexión con un sistema principal configurado para ser básicamente un archivador de archivos FTP, en el cual todos los archivos disponibles que deben transferirse se almacenan en formato comprimido en el sistema principal.

Compresión de la capa de enlace

Un factor decisivo a considerar es la naturaleza del enlace de red entre dos sistemas principales. La compresión se puede realizar en una capa inferior que en las interfaces de hardware del dispositivo. En particular, muchos módems modernos incorporan mecanismos de compresión de datos en su hardware y firmware. Si se realiza compresión en el enlace en una capa inferior (fuera del dispositivo), es mejor no habilitar la compresión de datos en el dispositivo para dicha interfaz. Tal como ya se ha mencionado, la compresión de una corriente de datos ya comprimidos normalmente no es efectiva y, de hecho, puede reducir ligeramente el rendimiento. A menos que exista algún motivo particular para pensar que el direccionador realizará un mejor trabajo de compresión que el hardware de enlace, es mejor dejar que el hardware de enlace lleve a cabo la compresión.

Configuración y supervisión de la compresión de datos en enlaces PPP

El 2210 utiliza el Compression Control Protocol (CCP) de PPP para negociar la utilización del uso de compresión en un enlace. El CCP proporciona un mecanismo para negociar la utilización de un protocolo de compresión particular, posiblemente incluso utilizando un protocolo diferente en cada dirección del enlace y varias opciones específicas del protocolo. El software soporta los protocolos Stac-LZS y MPPC, de modo que el similar también debe proporcionar soporte para como mínimo uno de estos algoritmos para negociar satisfactoriamente la compresión de datos entre los dos nodos. Los dos nodos también deben ponerse de acuerdo sobre las opciones específicas del algoritmo para que la compresión funcione.

Configuración de la compresión de datos en enlaces PPP

Para configurar la compresión de datos en enlaces PPP:

1. Habilite el protocolo CCP en el enlace con el mandato **enable ccp**. Esto permite que el enlace negocie la compresión con el otro nodo. La negociación incluye el algoritmo de compresión que se va a utilizar y las opciones específicas del protocolo.
2. Seleccione los algoritmos de compresión que se pueden negociar utilizando el mandato **set ccp algorithms**.
3. Establezca los parámetros negociables para cada algoritmo de compresión utilizando el mandato **set ccp options**.

Puede visualizar la configuración de compresión actual utilizando el mandato **list ccp**.

La Tabla 18 lista los mandatos disponibles y la Figura 11 en la página 178 es un ejemplo de configuración de la compresión en un enlace PPP. Para obtener descripciones detalladas de estos mandatos, consulte 'Mandatos de la configuración Point-to-Point' en la publicación *Guía del usuario de software*.

Tabla 18. Mandatos de configuración de la compresión de datos PPP

Mandato de compresión de datos	Acción
disable ccp	Inhabilita la compresión de datos.
enable ccp	Habilita la compresión de datos.
set ccp options	Establece las opciones para el algoritmo de compresión.
set ccp algorithms	Especifica una lista con prioridad de algoritmos de compresión.
list ccp	Visualiza la configuración de la compresión.

```
Config>net 6 1
PPP 6 Config>enable ccp
PPP 6 Config>set ccp alg 2
Enter a prioritized list of compression algorithms (first is preferred),
all on one single line.
Choices (can be abbreviated) are:
STAC-LZS MPPC
Compressor list [STAC-LZS]? stac mppc
PPP 6 Config>set ccp options
STAC: check mode (0=none, 1=LCB, 2=CRC, 3=Seq, 4=Ext) [3]?
STAC: # histories [1]?
PPP 6 Config>li ccp

CCP Options
-----------
Data Compression enabled
Algorithm list: STAC-LZS MPPC
STAC histories: 1
STAC check_mode: SEQ

MPPE Options
------------
MPPE disabled
Optional encryption
Key generation: STATEFUL
```

Figura 11. Ejemplo de configuración de la compresión en un enlace PPP

Notas:

1. El mandato network selecciona la interfaz de red para el enlace PPP. Si el enlace es un circuito de marcación PPP, debe utilizar el mandato **encapsulator** para acceder al menú de configuración PPP.
2. Si habilita el CCP y no establece algoritmos para el enlace, el software establece automáticamente el enlace para utilizar los protocolos STAC y MPPC como si se hubiera entrado el mandato **set ccp algorithms stac mppc**.

   Si establece múltiples algoritmos, el orden de los algoritmos determina la preferencia de negociación para el enlace.

   Es posible que determinadas implantaciones de cliente de marcación de entrada no puedan conectarse si el direccionador soporta múltiples protocolos de compresión en un enlace. Si se produce esta situación, establezca el protocolo ccp en STAC o MPPC.

   Si entra **set ccp algorithms none**, el software inhabilitará automáticamente la compresión en el enlace.

   Si MPPE está habilitado y CCP está habilitado, el algoritmo de compresión es MPPC.

Supervisión de la compresión de datos en enlaces PPP

La compresión se supervisa tal como se haría en otros componentes PPP. El apartado ‘Accessing the Interface Monitoring Process’ de la publicación *Guía del usuario de software* describe cómo acceder al entorno de consola PPP y los detalles sobre los mandatos. La Tabla 19 en la página 179 lista los mandatos relacionados con la compresión. La Figura 12 en la página 179 muestra un ejemplo de listado de compresión en una interfaz PPP.

Tabla 19. Mandatos de supervisión de la compresión de datos PPP	
Mandato	**Función**
list control ccp	Lista el estado de CCP y la opciones negociadas.
list ccp	Lista las estadísticas de paquetes CCP.
list cdp o **list compression**	Lista las estadísticas del datagrama comprimido.

```
+ network 1
PPP > list control ccp

CCP State:                Open
Previous State:           Ack Sent
Time Since Change:        2 minutes and 52 seconds

Compressor:   STAC-LZS histories 1, check_mode SEQ
Decompressor: STAC-LZS histories 1, check_mode SEQ
MPPE:         Not negotiated

PPP > list ccp

CCP Statistic             In                      Out
-------------             --                      ---

Packets:                  2                       3
Octets:                   18                      27
Reset Reqs:               0                       0
Reset Acks:               0                       0
Prot Rejects:             1                       -

PPP > list cdp

Compression Statistic     In                      Out
---------------------     --                      ---

Packets:                  19541                   19542
Octets:                   2550673                 2740593
Compressed Octets:        821671                  899446
Incompressible Packets:   0                       0
Discarded Packets:        0                       -
Prot Rejects:             0                       -
Compression Ratios:       3.11                    3.24
```

Figura 12. Supervisión de la compresión en una interfaz PPP

Configuración y supervisión de la compresión de datos en enlaces Frame Relay

Después de configurar los parámetros de compresión globales y de habilitar la compresión en la interfaz, debe establecer los parámetros para cada circuito (PVC) individual en la interfaz Frame Relay. Cada circuito definido para la interfaz puede tener habilitada la compresión en el circuito y cada circuito que negocia satisfactoriamente la utilización de la compresión utiliza una sesión de compresión de la agrupación global. También puede inhabilitar la compresión en la interfaz lo que significa que ninguno de los circuitos de dicha interfaz será elegible para transportar tráfico de datos comprimidos.

Configuración de la compresión de datos en enlaces Frame Relay

Para configurar la compresión de datos en enlaces FR:

1. Habilite la compresión en la interfaz utilizando el mandato **enable compression**. Esto permite que el enlace negocie la compresión con el otro nodo.
2. Habilite la compresión en cada nuevo PVC que va a transportar datos comprimidos utilizando el mandato **add permanent-virtual-circuit**. Puede cambiar los PVC existentes utilizando el mandato **change permanent-virtual-circuit**.

Puede visualizar la configuración de la compresión actual utilizando los mandatos **list lmi** o **list permanent-virtual-circuit**.

La Tabla 20 en la página 182 lista los mandatos disponibles para configurar la compresión en un enlace Frame Relay y la Figura 13 en la página 181 es un ejemplo de configuración en un enlace Frame Relay. Consulte el apartado "Mandatos de la configuración Frame Relay" en la publicación *Guía del usuario de software* para obtener más detalles.

```
Config> net 2

Frame Relay user configuration

FR Config> enable compression
Maximum number of run-time compression circuits (zero means no limit) [0]? 0
Do you want orphan PVCs to perform compression [Y]? n
The number of currently defined non-compression PVCs is 4
Would you like to change them all to compression PVCs [N]? y

FR Config> add perm

Circuit number [16]? 22
Committed Information Rate (CIR) in bps [65536]?
Committed Burst Size (Bc) in bits [64000]?
Excess Burst Size (Be) in bits [0]?
Assign circuit name []? cir22
Is circuit required for interface operation [N]?
Do you want to have data compression performed [Y]?

FR Config>list lmi

                      Frame Relay Configuration


  LMI enabled            =      No  LMI DLCI                      =       0
  LMI type               =    ANSI  LMI Orphans OK                =     Yes
  CLLM enabled           =      No  Timer Ty seconds              =      11

  Protocol broadcast     =     Yes  Congestion monitoring         =     Yes
  Emulate multicast      =     Yes  CIR monitoring                =      No
  Notify FECN source     =      No  Throttle transmit on FECN     =      No

  Data compression       =     Yes  Orphan compression            =      No
  Compression PVC limit  =    None  Number of compression PVCs    =       2

  PVCs P1 allowed        =      64  Interface down if no PVCs     =      No
  Timer T1 seconds       =      10  Counter N1 increments         =       6
  LMI N2 error threshold =       3  LMI N3 error threshold window =       4
  MIR % of CIR           =      25  IR % Increment                =      12
  IR % Decrement         =      25  DECnet length field          =      No
  Default CIR            =   65536  Default Burst Size            =   64000
  Default Excess Burst   =       0

FR Config>list perm

  Maximum PVCs allowable =      64
  Total PVCs configured  =       2

            Circuit               Circuit   Circuit     CIR    Burst  Excess
             Name                 Number     Type      in bps  Size   Burst
--------------------------------- ------- ----------- ------- ------- -----
 circ16                             16    @ Permanent   65536   64000       0
 cir22                              22    @ Permanent   65536   64000       0

* = circuit is required
# = circuit is required and belongs to a required PVC group
@ = circuit is data compression capable
```

Figura 13. Ejemplo de configuración de la compresión en un enlace Frame Relay

Tabla 20. Mandatos de configuración de la compresión de datos	
Mandato	**Acción**
add permanent-virtual-circuit *número*	Se utiliza para habilitar la compresión de datos en un PVC específico en una interfaz.
change permanent-virtual-circuit *número*	Se utiliza para cambiar si un PVC específico va a comprimir datos.
disable compression	Inhabilita la compresión de datos.
enable compression	Habilita la compresión de datos.
list lmi	Visualiza la configuración actual de la interfaz.
list permanent	Lista la información de resumen sobre circuitos.

Nota: La habilitación de la compresión en circuitos huérfanos disminuirá el número de sesiones de compresión disponibles para los PVC nativos en el dispositivo.

Si habilita la compresión en una interfaz Frame Relay que ya tenga habilitada la compresión, el software le pregunta si desea cambiar los parámetros de compresión en la interfaz, tal como se muestra en el ejemplo siguiente. Puede cambiar la compresión en la interfaz sin inhabilitar la compresión.

Ejemplo sobre cómo cambiar la compresión en interfaces Frame Relay:

```
Config> net 2

Frame Relay user configuration

FR Config> enable compression
Data compression already enabled.
Do you wish to continue and change an interface parameter [Y]
Maximum number of run-time compression PVCs (zero means no limit) [0]? 32
Do you want orphan circuits to perform compression [Y]?
The number of currently defined circuits is 5
Change all of these circuits to perform compression?
```

Supervisión de la compresión de datos en enlaces Frame Relay

La compresión se supervisa tal como se haría en otros componentes Frame Relay. El apartado “Mandatos de supervisión de Frame Relay” de la publicación *Guía del usuario de software* describe cómo acceder al entorno de consola Frame Relay y proporciona detalles sobre los mandatos. La Tabla 21 lista los mandatos relacionados con la compresión. El “Ejemplo: Supervisión de la compresión en una interfaz o circuito Frame Relay” en la página 183 muestra un ejemplo de listado de compresión en una interfaz Frame Relay.

Tabla 21. Mandatos de supervisión de la compresión de datos Frame Relay	
Mandato	**Visualización**
list lmi	Lista el estado actual de la interfaz.
list permanent	Lista la información de resumen sobre circuitos.
list circuit	Lista el estado actual de un circuito.

Ejemplo: Supervisión de la compresión en una interfaz o circuito Frame Relay

```
+ network 2
FR 2 > list lmi

Management Status:
  ------------------

    LMI enabled          =      No  LMI DLCI                   =       0
    LMI type             =    ANSI  LMI Orphans OK             =     Yes
    CLLM enabled         =      No

    Protocol broadcast   =     Yes  Congestion monitoring      =     Yes
    Emulate multicast    =     Yes  CIR monitoring             =      No
    Notify FECN source   =      No  Throttle transmit on FECN  =      No
    PVCs P1 allowed      =      64  Interface down if no PVCs  =      No
    Line speed (bps)     =   64000  Maximum frame size         =    2048
    Timer T1 seconds     =      10  Counter N1 increments      =       6
    LMI N2 threshold     =       3  LMI N3 threshold window    =       4
    MIR % of CIR         =      25  IR % Increment             =      12
    IR % Decrement       =      25  DECnet length field        =      No
    Default CIR          =   65536  Default Burst Size         =   64000
    Default Excess Burst =       0

    Current receive sequence  =       0
    Current transmit sequence =       0
    Total status enquiries    =       0  Total status responses   =       0
    Total sequence requests   =       0  Total responses          =       0

    Data compression enabled  =     Yes  Orphan Compression       =      No

    Compression PVC limit     =    None  Active compression PVCs  =       1

  PVC Status:
  -----------

    Total allowed  =      64  Total configured  =       1
    Total active   =       1  Total congested   =       0
    Total left net =       0  Total join net    =       0


FR 2 > list permanent

 Circuit                                  Orphan  Type/   Frames      Frames
 Number            Circuit Name           Circuit State Transmitted  Received
 ------- -------------------------------- ------- ----- ----------- --------

     16  circ16                             No   @ P/A        58364      58355
     22  circ22                             No   & P/A        58364      58355

    A - Active   I - Inactive   R - Removed   P - Permanent   C - Congested
    * - Required               # - Required and belongs to a PVC group
    @ - Data compression capable but not operational
    & - Data compression capable and operational
```

```
FR 2 > list circuit 22

 Circuit name = circ22

     Circuit state        =    Active  Circuit is orphan   =           No
     Frames transmitted   =     58391  Bytes transmitted   =      2676894
     Frames received      =     58383  Bytes received      =      2671009
     Total FECNs          =         0  Total BECNs         =            0
     Times congested      =         0  Times Inactive      =            0
     CIR in bits/second   =     65536  Potential Info Rate =        64000
     Committed Burst (Bc) =     64000  Excess Burst (Be)   =            0
     Minimum Info Rate    =     16000  Maximum Info Rate   =        64000
     Required             =        No  PVC group name      =   Unassigned

     Compression capable  =       Yes  Operational         =          Yes
     R-R's received       =         0  R-R's transmitted   =            0
     R-A's received       =         0  R-A's transmitted   =            0
     R-R mode discards    =         0  Enlarged frames     =            0
     Decompress discards  =         0  Compression errors  =            0
     Rcv error discards   =         0

     Compression ratio    =  1.00 to 1  Decompression ratio =    1.00 to 1

     Current number of xmit frames queued                  =            0
     Xmit frames dropped due to queue overflow             =            0
```

Utilización de autentificación local o remota

La autentificación es el proceso de determinar quién es un usuario (o entidad). La autentificación del acceso del usuario para el protocolo PPP en el 2210 amplía la flexibilidad de la gestión de perfiles de usuario puesto que está relacionada con los protocolos de autentificación PPP PAP, MSCHAP, CHAP y SPAP. Consulte el apartado 'PPP Authentication Protocols' en la publicación *Guía del usuario de software* para obtener información adicional sobre cómo configurar PAP, MSCHAP, CHAP y SPAP.

La autentificación se puede configurar localmente o se puede configurar para consolidar la configuración de usuario utilizando servidores de autentificación que estén disponibles en la red para servir peticiones de autentificación para toda la red. El IBM 2210 implementa la autentificación mantenida localmente así como los protocolos de servidor de autentificación siguientes:

- Radius
- TACACS
- TACACS+

Utilización de la Seguridad de Autentificación, Autorización y Contabilidad (AAA)

La Seguridad de Autentificación, Autorización y Contabilidad (AAA) está formada por protocolos configurables que le permiten controlar el acceso a los servicios. Puede configurar AAA para que lleve a cabo autentificación local o remota.

Puede configurar un protocolo de seguridad para los tipos de funciones siguientes:

- Enlaces PPP
- Usuarios de inicio de sesión (Inicio de sesión Telnet/Consola)
- Túneles

La configuración se lleva a cabo estableciendo un servidor primario y uno secundario. La información del servidor se configura y almacena aparte de la configuración de AAA. Un perfil de servidor se utiliza mediante un nombre que se proporciona durante la configuración.

En todos los casos la contabilidad no se puede llevar a cabo localmente y debe ser Radius o TACACS+.

La autorización sólo se puede realizar localmente, o mediante autentificación remota que utilice Radius o TACACS+.

¿Qué es la seguridad AAA?

La Seguridad AAA es el nombre del sistema de seguridad para este dispositivo. Incluye:

Autentificación

El proceso de identificar a un usuario. La autentificación utiliza un nombre y una contraseña para el acceso.

Autorización
El proceso de determinar los servicios a los cuales puede acceder un usuario.

Contabilidad
El proceso de registrar cuándo un usuario ha iniciado o detenido una sesión. Existen dos tipos de registros de contabilidad soportados.

Registros de inicio
Indica que está a punto de iniciarse un servicio.

Registros de detención
Indica que ha finalizado un servicio.

Utilización del PPP

Para el Point-to-Point Protocol (PPP) puede configurar lo siguiente:

- Autentificación
- Autorización
- Contabilidad

Cada función puede tener su propio protocolo de seguridad configurado de modo independiente por el usuario.

- El establecimiento del protocolo de autentificación no tendrá efecto en la autorización ni la contabilidad.
- El establecimiento del protocolo de autorización no tendrá efecto sobre la autentificación ni la contabilidad.
- El establecimiento del protocolo no tendrá efecto sobre la autentificación ni la autorización.
- El establecimiento de AAA en remoto establecerá la autentificación en remota, la autorización en remota y la contabilidad en remota.
- El establecimiento de AAA en local establecerá la autentificación en local y la autorización en local. No se puede inhabilitar la autentificación ni la autorización.

Consulte el apartado Point-to-Point Configuration Commands en la publicación *Guía del usuario de software* para obtener detalles sobre los mandatos de configuración PPP que utilice en este entorno.

Protocolos de seguridad PPP válidos

A continuación se listan los protocolos de seguridad PPP válidos:

Métodos de autentificación
Local, RADIUS, TACACS+, TACACS

Métodos de autorización
Local, RADIUS, TACACS+

Métodos de contabilidad
RADIUS, TACACS+

Tabla 22. Establecimiento de protocolos de seguridad PPP

Acción	Autentificación	Autorización	Contabilidad
establecer AAA local	local	local	ignorar
establecer AAA remota	remota	remota	remota
establecer AUTHENT local	local	ignorar	ignorar
establecer AUTHOR local	ignorar	local	ignorar
establecer AUTHENT remota	remota	ignorar	ignorar
establecer AUTHOR remota	ignorar	remota	ignorar
establecer ACCOUNTING remota	ignorar	ignorar	remota
inhabilitar ACCOUNTING	ignorar	ignorar	inhabilitada

Utilización del inicio de sesión

Para la configuración del inicio de sesión de AAA, se puede seleccionar remoto o local. Si desea una autentificación local, también debe utilizarse autorización local. Si se selecciona autentificación remota, debe utilizarse autorización remota. La contabilidad no se soporta localmente, de modo que cuando se autentifica y autoriza localmente se debe inhabilitar la contabilidad.

Atención:

Si un servidor de autentificación remoto no responde, es posible utilizar un id de usuario y una contraseña de inicio de sesión local cuando se ha habilitado login-of-last-resort. Esto permite realizar un solo intento de inicio de sesión local si se excede el tiempo de espera de autentificación remota. Asimismo, si se ha habilitado tech-support-bypass, se puede utilizar un id y una contraseña de soporte técnico para iniciar la sesión y no se transmitirá la petición al servidor de autentificación.

Es importante especificar un nivel de privilegio al utilizar la autentificación remota. Los usuarios de inicio de sesión pueden entrar un id de usuario y una contraseña correctos, pero sin especificar un privilegio el usuario no puede acceder a la consola. Se pueden establecer tres niveles de privilegio: administrador, operador y supervisor. Para RADIUS, utilice el atributo SERVICE-TYPE número 6 o añada un atributo de proveedor número 216. Consulte el Apéndice A, “Atributos de AAA remota” en la página 573 para obtener detalles sobre atributos de RADIUS específicos.

Cuando se configura la autentificación remota, se puede establecer la autorización en otro protocolo de autorización remoto Radius o TACACS+ y establecer la contabilidad para que utilice Radius o TACACS+.

- El establecimiento de AAA en local establece la autentificación en local, la autorización en local y la contabilidad en inhabilitada.
- El establecimiento de AAA en remota establece la autentificación en remota, la autorización en remota y la contabilidad en remota.
- El establecimiento del protocolo de autentificación en local establece automáticamente el protocolo de autorización en lo mismo e inhabilita la contabilidad.

- El establecimiento del protocolo de autentificación en remota establece automáticamente el protocolo de autorización en lo mismo solamente si el protocolo de autorización está establecido en local e ignora el protocolo de contabilidad.
- El establecimiento del protocolo de autorización en remoto establece automáticamente el protocolo de autentificación en lo mismo solamente si el protocolo de autentificación está establecido en local e ignora el protocolo de contabilidad.
- El establecimiento del protocolo de contabilidad en remoto establece automáticamente el protocolo de autentificación en lo mismo solamente si el protocolo de autentificación está establecido en local, y establece el protocolo de autorización en lo mismo solamente si la autorización está establecida en local.
- El establecimiento del protocolo de contabilidad en inhabilitar no tiene efecto sobre el protocolo de autentificación o de autorización.
- La inhabilitación de la autentificación o autorización no está permitida.

Protocolos de seguridad de inicio de sesión/administración

A continuación se listan los protocolos de seguridad de inicio de sesión/administración válidos.

Métodos de autentificación/autorización
Local, RADIUS, TACACS Plus

Métodos de contabilidad
RADIUS, TACACS Plus

Tabla 23. Establecimiento de los protocolos de seguridad de inicio de sesión

Acción	Autentificación	Autorización	Contabilidad
establecer AAA local	local	local	inhabilitada
establecer AAA remota	remota	remota	remota
establecer AUTHENT local	local	local	inhabilitada
establecer AUTHOR local	local	local	inhabilitada
establecer AUTHENT remota	remota	remota, si es local en otro lugar ignorar	ignorar
establecer AUTHOR remota	remota, si es local en otro lugar ignorar	remota	ignorar
establecer ACCOUNTING remota	remota, si es local en otro lugar ignorar	remota, si es local en otro lugar ignorar	remota
inhabilitar ACCOUNTING	ignorar	ignorar	inhabilitada

Utilización de túneles

Establezca la autentificación de túnel en lo mismo que la autorización del túnel. Cuando se establece la autentificación del túnel en local o remota, a continuación puede habilitar la contabilidad. La autorización de túnel y el servidor de autentificación deben ser iguales.

La configuración de túnel para contabilidad también se aplica a los túneles IPSec. La autentificación y la autorización de túnel no se aplican a los túneles IPSec. No puede realizar la autentificación o la autorización para túneles IPSec utilizando AAA.

Protocolos de seguridad de túnel válidos

A continuación se proporcionan los protocolos de seguridad de Túnel válidos:

Métodos de autentificación/autorización
Local, RADIUS

Métodos de contabilidad
RADIUS, TACACS Plus

Tabla 24. Establecimiento de los protocolos de seguridad de túnel

Acción	Autentificación	Autorización	Con-tabilidad
establecer AAA local	local	local	ignorar
establecer AAA remota	remota	remota	remota
establecer AUTHENT local	local	local	ignorar
establecer Author local	local	local	ignorar
establecer AUTHENT remota	remota	remota	ignorar
establecer AUTHOR remota	remota	remota	ignorar
establecer ACCOUNTING remota	ignorar	ignorar	remota
inhabilitar ACCOUNTING	ignorar	ignorar	inhabilitada

Normas para la contraseña

La autentificación local le permite utilizar una contraseña para controlar el acceso al inicio de sesión. La contraseña se puede comprobar con alguna o todas las normas siguientes.

Nota: Las normas siguientes sólo se aplican al inicio de sesión de usuario de PPP, no al inicio de sesión de consola.

- Debe tener un número mínimo de caracteres de longitud. El usuario establece el número de caracteres necesarios.
- Debe contener como mínimo un carácter alfabético.
- Debe contener como mínimo un carácter no alfabético.
- Debe contener un carácter no numérico en la primera posición.
- Debe contener un carácter no numérico en la última posición.
- Debe contener no más de tres caracteres consecutivos idénticos utilizados en la última contraseña.
- No debe contener más de dos caracteres consecutivos.
- No debe contener el id de usuario como parte de la contraseña.
- No debe ser igual que ninguna de las tres últimas contraseñas.

- Debe cambiarse después de un número determinado de días. Debe establecer el número de días entre cambios de contraseña.
- Se bloquea después de un número específico de anomalías de inicio de sesión. El usuario establece el número de anomalías.

Comprensión de los servidores de autentificación

Un ***servidor de autentificación*** es un servidor en la red que valida los id de usuario y las contraseñas para la red. Si se configura un dispositivo para autentificación mediante un servidor de autentificación y el dispositivo recibe un paquete de un protocolo de autentificación, el dispositivo pasa un id de usuario y una contraseña al servidor para la autentificación. Si el id de usuario y la contraseña son correctos, el servidor responde positivamente. A continuación, el dispositivo puede comunicarse con el originador de la petición. Si el servidor no encuentra el id de usuario y la contraseña que recibe desde el dispositivo, responde negativamente al dispositivo. A continuación, el dispositivo rechaza la sesión desde la cual ha recibido la petición de autentificación.

Soporte de SecurID

El 2210 puede autentificar clientes de marcación de entrada que utilicen SecurID con un Security Dynamics ACE/Server. Este soporte utiliza TACACS, TACACS+ o RADIUS en el ACE/Server para la autentificación del cliente. Los clientes de marcación de entrada se configuran igual que los otros clientes de marcación de entrada en el 2210.

El cliente de marcación de entrada inicia la sesión de la manera habitual, pero utiliza el código de paso SecurID para la contraseña. El código de paso SecurID consta de un número PIN de 4 a n dígitos seguido del número de la tarjeta de señales SecurID. (El número máximo de dígitos del PIN depende del servidor.) El id de usuario y la contraseña pueden aparecer como:

```
Nombusu.: John Customer

Contras.: 1234098765
```

Figura 14. Nombre de usuario y código de paso SecurID

Cuando el ACE/Server autentifica el inicio de sesión, puede que solicite la siguiente señal desde el cliente. La siguiente señal es la siguiente señal de la tarjeta de señales. El número máximo de dígitos de la siguiente señal depende de la tarjeta de señales SecurID que utiliza el cliente. Cuando se le solicite la contraseña, el cliente puede entrar el código de paso y la siguiente señal utilizando el formato `códigopaso*señal` como se muestra a continuación:

```
Nombusu.: John Customer

Contras.: 1234098765*111111
```

Figura 15. Código de paso SecurID con la siguiente señal

Nota: Cuando el servidor solicita al cliente que entre la señal siguiente, el cliente debe:

1. Entrar el PIN
2. Esperar una nueva señal desde la tarjeta y entrar dicha señal
3. Entrar un * seguido de la siguiente señal de la tarjeta

El administrador de ACE/Server configura las condiciones que hacen que el servidor solicite la siguiente señal o el nuevo PIN.

Los clientes de marcación de entrada deben utilizar SPAP para poder recibir alertas desde el sistema de autentificación cuando tienen que entrar la siguiente señal. Si un cliente no utiliza SPAP y no inicia la sesión satisfactoriamente, debe intentar entrar un nuevo código de paso utilizando el formato `códigopaso*señal`. Si el cliente todavía no consigue iniciar la sesión satisfactoriamente, puede que existan otros problemas entre el cliente y el ACE/Server.

Limitaciones de SecurID

Existen las limitaciones siguientes:

- Security Dynamics Inc. (SDI) y el cifrado DES no están soportados.
- La función “New PIN” de SecurID no está soportada.
- TACACS no soporta las funciones “New PIN” o “Next-Token”. El cliente puede especificar una "next-token" (señal siguiente) al iniciar la sesión, pero el servidor no la utilizará.
- Los clientes configurados para devolución de llamada no están soportados.
- Cuando utilice CHAP con TACACS o TACACS+, establezca el intervalo de recomprobación de CHAP en 0.
- No utilice CHAP cuando utilice la autentificación RADIUS y SecurID.
- Los clientes pueden obtener los mejores resultados utilizando TACACS+ y SPAP.
- El cliente DIAL de Windows 3.1 con autentificación de SecurID utilizando multienlace no está soportado.
- Cuando se utiliza autentificación de SecurID, se recomienda utilizar el último software de cliente (por ejemplo, Windows 95 u OS/2).

Configuración de la autentificación

Este capítulo describe la configuración y los mandatos operativos para la autentificación. El capítulo incluye las secciones siguientes:

- “Acceso al indicador de mandatos de configuración de la autentificación”
- “Mandatos de configuración de autentificación”
- “Soporte de reconfiguración dinámica de autentificación (AAA)” en la página 215

Acceso al indicador de mandatos de configuración de la autentificación

Para acceder al indicador de mandatos `AAA Config>`:

1. Entre **talk 6** en el indicador de mandatos `*`.
2. Entre **feature auth** en el indicador de mandatos `Config>`.

Mandatos de configuración de autentificación

La Tabla 25 lista los mandatos disponibles en el indicador de mandatos `AAA Config >`.

Tabla 25. Mandatos de configuración de la autentificación

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Disable	Inhabilita diversas opciones de AAA.
Enable	Habilita diversas opciones de AAA.
List	Visualiza los parámetros de configuración de AAA.
Login	Configura AAA para inicio de sesión.
Nets-info	Visualiza información sobre autentificación de PPP local.
Password-rules	Configura normas de la contraseña (habilita o inhabilita).
PPP	Configura AAA para PPP.
Servers	Configura servidores AAA remotos individuales.
Set	Configura parámetros de Autentificación independientemente del tipo.
Tunnel	Configura AAA para túneles.
User-profiles	Configura usuarios PPP locales.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Disable

Utilice el mandato **disable** para inhabilitar la opción de contabilidad seleccionada.

Sintaxis:

disable accounting

ipsec-accounting

login-last-resort

tech-support-bypass

unauthent-accounting

accounting
Especifica que la contabilidad AAA debe inhabilitarse.

ipsec-accounting
Especifica que la contabilidad IPSec debe inhabilitarse.

login-last-resort
Especifica que el último recurso de inicio de sesión debe inhabilitarse.

tech-support-bypass
Especifica que la acción de ignorar el soporte técnico debe inhabilitarse.

unauthent-accounting
Especifica que la contabilidad no autentificada debe inhabilitarse. Las sesiones PPP que queden activas sin autentificar al usuario mediante la habilitación de la autentificación PPP no se contabilizarán. No se transmitirán los registros de inicio y detención.

Enable

Utilice el mandato **enable** para habilitar la opción de contabilidad seleccionada.

Sintaxis:

enable accounting

ipsec-accounting

login-last-resort

tech-support-bypass

unauthent-accounting

accounting
Especifica que la contabilidad AAA debe habilitarse.

ipsec-accounting
Especifica que la contabilidad IPSec debe habilitarse.

login-last-resort
Especifica que el último recurso de inicio de sesión debe habilitarse. En el caso de que se produzca un tiempo de espera excedido mientras se transmite información de autentificación a un servidor de autentificación remoto, se visualizará un solo indicador de mandatos para permitir iniciar la sesión a un usuario autentificado localmente.

tech-support-bypass
Especifica que la acción de ignorar soporte técnico debe habilitarse.

unauthent-accounting
Especifica que la contabilidad no autentificada debe habilitarse.

List

Utilice el mandato **list** para visualizar los parámetros de AAA.

Sintaxis:

list	accounting
	all
	authentication
	authorization
	config
	options

Ejemplos de salida del mandato list

Los ejemplos siguientes muestran la salida típica para las opciones soportadas del mandato list:

```
AAA Config> list all
ppp AAA configuration...
 ppp authentication        : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 ppp authorization         : localllist
 ppp accounting            : Disabled
tunnel AAA configuration...
 tunnel authentication     : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 tunnel authorization      : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 tunnel accounting         : Disabled
login AAA configuration...
 login authentication      : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 login authorization       : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 login accounting          : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>


AAA Config> list accounting all
accounting AAA configuration...
accounting ppp            : Disabled
accounting tunnel         : Disabled
accounting login          : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
```

```
AAA Config> list accounting config
accounting ppp            : Disabled
accounting login          : Radius        serv01
accounting tunnel         : Disabled


AAA Config> list authentication all
authentication AAA configuration...
 authentication ppp        : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 authentication tunnel     : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>


AAA Config> list options
Login Last Resort  : disabled
Tech Support Bypass: disabled
IPSEC Accounting   : enabled

INBYTES              enabled
OUTBYTES             enabled
INPKTS               enabled
OUTPKTS              enabled
```

Login

Utilice el mandato **login** para configurar AAA para inicio de sesión.

La Tabla 26 lista los submandatos disponibles con el mandato **login**.

Tabla 26. Submandatos de login

Mandato	Función
Disable	Inhabilita la contabilidad para inicio de sesión.
List	Visualiza los parámetros de configuración de AAA para inicio de sesión.
Set	Establece los parámetros de configuración de AAA para inicio de sesión.

Disable

Utilice el mandato **login disable** para inhabilitar la contabilidad.

Sintaxis:

lo**gin disable** ac**counting**

List

Utilice el mandato **login list** para visualizar los parámetros de configuración de AAA.

Sintaxis:

login list all
accounting
authentication
authorization
config

Set

Utilice el mandato **login set** para configurar los parámetros de autentificación.

Sintaxis:

login set aaa
accounting
authentication
authorization

aaa *tipo-aut*

Establece el tipo de autentificación, autorización y contabilidad. El *tipo-aut* puede ser uno de los siguientes:

local Establece el tipo de autentificación, autorización y contabilidad para utilizar una base de datos de usuario mantenida localmente.

remota Establece el tipo de autentificación, autorización y contabilidad para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

accounting *tipo-aut*

Establece el tipo de contabilidad. El *tipo-aut* puede ser uno de los siguientes:

remota Establece el tipo de autentificación para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

authentication *tipo-aut*

Establece el tipo de autentificación. El *tipo-aut* puede ser uno de los siguientes:

local Establece el tipo de autentificación para utilizar una base de datos de usuario mantenida localmente.

remota Establece el tipo de autentificación para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

authorization *tipo-aut*

Establece el tipo de autorización. El *tipo-aut* puede ser uno de los siguientes:

local Establece el tipo de autorización para utilizar una base de datos de usuario mantenida localmente.

remota Establece el tipo de autorización para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

Nets-info

Utilice el mandato **nets-info** para visualizar el protocolo de autentificación PPP configurado actualmente en cada interfaz PPP.

Sintaxis:

n**ets-info**

Password-rules

Utilice el mandato **password-rules** para configurar la contraseña (habilitar o inhabilitar).

La Tabla 27 lista los submandatos disponibles con el mandato **password-rules**.

Tabla 27. Submandatos de login

Mandato	Función
Disable	Inhabilita una norma de contraseña.
Enable	Habilita una norma de contraseña.
List	Visualiza el estado actual de las normas de contraseña (habilitada o inhabilitada).

Disable

Utilice el mandato **password-rules disable** para inhabilitar alguna o todas las normas de contraseña.

Sintaxis:

pa**ssword-rules disable** all

compare-ident-prev

change-days

first-non-numeric

ident-chars

last-non-numeric

lockout

minimum-length

one-alpha

one-nonalpha

prev-three

userid-contained

compare-ident-prev
Compara la identidad del usuario anterior con el usuario que solicita un cambio de contraseña.

change-days
El número máximo de días antes de que sea necesario un cambio de contraseña.

Valores válidos: de 0 a 360

Valor por omisión: 180

first_non-numeric
El primer carácter de una contraseña no puede ser numérico.

Valores válidos: cualquier carácter no numérico

Valor por omisión: ninguno

ident-chars
No puede contener más de 3 caracteres utilizados en una contraseña anterior en la misma posición.

last-non-numeric
El último carácter de la contraseña no puede ser numérico.

Valores válidos: cualquier carácter no numérico

Valor por omisión: ninguno

lockout El número de veces que se puede probar una contraseña antes de que se bloquee el acceso.

Valores válidos: de 0 a 360

Valor por omisión: 3

minimum-length
El número mínimo de caracteres necesario para tener una contraseña válida.

Valores válidos: de 1 a 31

Valor por omisión: 8

maximum-length
El número máximo de caracteres que puede contener una contraseña.

Valores válidos: de 1 a 31

Valor por omisión: 8

one-alpha
Como mínimo un carácter de la contraseña debe ser alfabético.

one-nonalpha
Como mínimo un carácter de la contraseña debe ser numérico.

prev-three
La contraseña no puede ser la misma que ninguna de las tres últimas contraseñas.

userid-contained
La contraseña no puede contener el id de usuario como parte de la contraseña.

Enable

Utilice el mandato **password-rules enable** para habilitar alguna o todas las normas de contraseña. Consulte el mandato **disable** para obtener una lista de descripciones de normas de contraseña.

Sintaxis:

pa**ssword-rules enable** all
compare-ident-prev
change-days
first-non-numeric
ident-chars
last-non-numeric
lockout
minimum-length
one-alpha
one-nonalpha
prev-three
userid-contained

List

Utilice el mandato **password-rules list** para visualizar el estado actual de las normas de contraseña (inhabilitada o habilitada).

Sintaxis:

pa**ssword-rules list**

PPP

Utilice el mandato **ppp** para configurar AAA para PPP.

La Tabla 28 lista los submandatos disponibles con el mandato **ppp**.

Tabla 28. Submandatos de PPP

Mandato	Función
Disable	Inhabilita la contabilidad para PPP.
List	Visualiza los parámetros de configuración de AAA para PPP.
Set	Establece los parámetros de configuración de AAA para PPP.

Disable

Utilice el mandato **ppp disable** para inhabilitar la contabilidad para PPP.

Sintaxis:

ppp disable accounting

List

Utilice el mandato **ppp list** para visualizar los parámetros de configuración de AAA para PPP.

Sintaxis:

ppp list all
accounting
authentication
authorization
config

Set

Utilice el mandato **ppp set** para establecer los parámetros de configuración de AAA para PPP.

Sintaxis:

ppp set aaa
accounting
authentication
authorization

aaa *tipo-aut*
Establece el tipo de autentificación, autorización y contabilidad. El *tipo-aut* puede ser uno de los siguientes:

local Establece el tipo de autentificación, autorización y contabilidad para utilizar una base de datos de usuario mantenida localmente.

remota Establece el tipo de autentificación, autorización y contabilidad para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

accounting *tipo-aut*
Establece el tipo de contabilidad. El *tipo-aut* puede ser uno de los siguientes:

remota Establece el tipo de autentificación para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

authentication *tipo-aut*

Establece el tipo de autentificación. El *tipo-aut* puede ser uno de los siguientes:

local Establece el tipo de autentificación para utilizar una base de datos de usuario mantenida localmente.

remota Establece el tipo de autentificación para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

authorization *tipo-aut*

Establece el tipo de autorización. El *tipo-aut* puede ser uno de los siguientes:

local Establece el tipo de autorización para utilizar una base de datos de usuario mantenida localmente.

remota Establece el tipo de autorización para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

Servers

Utilice el mandato **servers** para configurar servidores de AAA remotos individuales.

La Tabla 29 lista los submandatos disponibles con el mandato **servers**.

Tabla 29. Submandatos de server

Mandato	Función
Add	Añade un perfil de servidor de AAA remoto.
Change	Cambia un perfil de servidor remoto.
Delete	Suprime un perfil de servidor remoto.
Lists	Visualiza la información de un perfil de servidor de AAA.

Add

Utilice el mandato **servers add** para añadir un perfil de servidor remoto.

Sintaxis:

ser**vers add** name

radius Establece el tipo de autentificación para utilizar el protocolo de servidor de autentificación radius.

Se pueden establecer valores para los siguientes parámetros:

nivel-contabilidad

Especifica el nivel de información de contabilidad a registrar. Un nivel más alto registra toda la información listada bajo los niveles de valores más bajos.

Rango: 0 a 10

Valor por omisión: 0

>**0** Información de registro para:

- INBYTES_AH
- OUTBYTES_AH
- INBYTES_ESP
- OUTBYTES_ESP

>**1** Información de registro para:

- INPKTS_AH
- OUTPKTS_AH
- INPKTS_ESP
- OUTPKTS_ESP

>**2** Información de registro para:

- INBYTES_BAD
- OUTBYTES_BAD
- INPKTS_BAD
- OUTPKTS_BAD

>**3** Información de registro para:

- INPKTS_BAD_AH
- OUTPKTS_BAD_AH
- INPKTS_BAD_ESP
- OUTPKTS_BAD_ESP

>**4** Información de registro para:

- INPKTS_BAD_AH_RPLY
- INPKTS_BAD_ESP_RPLY

puerto-contabilidad
Especifica el puerto de contabilidad del servidor RADIUS.

Rango: 1 a 10000

Valor por omisión: 1646

puerto-autentificación
Especifica el puerto de autentificación del servidor RADIUS.

Rango: 1 a 1000

Valor por omisión: 1645

autentificación-autor
Especifica si los atributos de autorización se transfieren durante la autentificación.

Valores válidos: sí, no

Valor por omisión: sí

contabilidad-para-paquetes
Especifica si se deben enviar las cuentas de paquetes al detenerse la contabilidad.

Valores válidos: sí, no

Valor por omisión: sí

clave-para-cifrado:
Especifica la clave de cifrado.

Valores válidos: Cualquier serie de caracteres alfanuméricos con una longitud máxima de 32 caracteres.

Valor por omisión: Ninguno.

dirección-servidor-primario:
Especifica la dirección del servidor de autentificación primario.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

reintentos

Valores válidos: de 1 a 100

Valor por omisión: 3

intervalo-reintento

Valores válidos: de 1 a 60

Valor por omisión: 3

dirección-servidor-secundario:
Especifica la dirección del servidor de autentificación secundario.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

tacacs Establece el tipo de autentificación para utilizar el protocolo de servidor de autentificación TACACS.

Se pueden establecer valores para los siguientes parámetros:

dirección-servidor-primario:
Especifica la dirección del servidor de autentificación primario.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

reintentos

Valores válidos: de 1 a 100

Valor por omisión: 3

intervalo-reintento

Valores válidos: de 1 a 60

Valor por omisión: 3

dirección-servidor-secundario:
Especifica la dirección del servidor de autentificación secundario.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

tacacsplus
Establece el tipo de autentificación para utilizar el protocolo de servidor de autorización TACACS+.

Se pueden establecer valores para los siguientes parámetros:

cifrado: Especifica si se utilizará cifrado.

Valores válidos: sí, no

Valor por omisión:

clave-para-cifrado:
Especifica la clave de cifrado que debe utilizarse.

Valores válidos: Cualquier valor de 16 dígitos hexadecimales

Valor por omisión:

dirección-servidor-primario:
Especifica la dirección del servidor de autentificación primario.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

nivel-privilegio

Valores válidos: de 0 a 15

Valor por omisión: 0

reinicios Establece el número de reinicios. Este parámetro no incluye reinicios de tiempo de espera y sólo pertenece a los reinicios solicitados por el servidor.

Valores válidos: de 0 a 3200

Valor por omisión: 0

tiempo-de-conexión
La cantidad de tiempo para permitir obtener la autentificación del servidor.

Valores válidos: de 1 a 60

Valor por omisión: 9

dirección-servidor-secundario:
Especifica la dirección del servidor de autentificación secundario.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

Change

Utilice el mandato **servers change** para cambiar un perfil de servidor remoto. Consulte el mandato **add** para obtener las descripciones de perfil de servidor remoto.

Sintaxis:

ser**vers change** radius

tacacs

tacacsplus

Consulte el mandato **servers add** para obtener descripciones de perfiles de servidor remoto.

Delete

Utilice el mandato **servers delete** para suprimir un perfil de servidor remoto. Consulte el mandato **add** para obtener las descripciones de perfil de servidor remoto.

Sintaxis:

ser**vers delete** radius

tacacs

tacacsplus

Consulte el mandato **servers add** para obtener las descripciones de perfil de servidor remoto.

List

Utilice el mandato **servers list** para visualizar la información de perfil de servidor AAA.

Sintaxis:

ser**vers list** all

names

profile

Set

Utilice el mandato **set** para establecer los parámetros para inicio de sesión, PPP y túnel L2TP.

Sintaxis:

s**et** aaa

accounting

authentication

authorization

aaa *tipo-aut*

Establece el tipo de autentificación, autorización y contabilidad. El *tipo-aut* puede ser uno de los siguientes:

local Establece el tipo de autentificación, autorización y contabilidad para utilizar una base de datos de usuario mantenida localmente.

remota Establece el tipo de autentificación, autorización y contabilidad para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

accounting *tipo-aut*

Establece el tipo de contabilidad para inicio de sesión, PPP y túnel. El *tipo-aut* puede ser uno de los siguientes:

options Le permite entrar opciones de contabilidad.

bytes Especifica que la contabilidad debe efectuarse a nivel de byte.

incoming Especifica que la contabilidad debe efectuarse para los bytes de entrada.

enable Habilita la contabilidad para las opciones especificadas.

disable Inhabilita la contabilidad para las opciones especificadas.

outgoing Especifica que la contabilidad debe efectuarse para los bytes de salida.

enable Habilita la contabilidad para las opciones especificadas.

disable Inhabilita la contabilidad para las opciones especificadas.

packets Especifica que la contabilidad debe efectuarse a nivel de paquete.

incoming Especifica que la contabilidad debe efectuarse para los paquetes de entrada.

enable Habilita la contabilidad para las opciones especificadas.

disable Inhabilita la contabilidad para las opciones especificadas.

outgoing Especifica que la contabilidad debe efectuarse para los paquetes de salida.

enable Habilita la contabilidad para las opciones especificadas.

disable Inhabilita la contabilidad para las opciones especificadas.

remota Establece el tipo de autentificación para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

authentication *tipo-aut*

Establece el tipo de autentificación para inicio de sesión, PPP y túnel.El *tipo-aut* puede ser uno de los siguientes:

local Establece el tipo de autentificación para utilizar una base de datos de usuario mantenida localmente.

remota Establece el tipo de autentificación para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

authorization *tipo-aut*

Establece el tipo de autorización para inicio de sesión, PPP y túnel. El *tipo-aut* puede ser uno de los siguientes:

local Establece el tipo de autorización para utilizar una base de datos de usuario mantenida localmente.

remota Establece el tipo de autorización para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

Tunnel

Utilice el mandato **tunnel** para configurar AAA para el túnel L2TP.

La Tabla 30 lista los submandatos disponibles con el mandato **tunnel**.

Tabla 30. Submandatos de tunnel

Mandato	Función
Disable	Inhabilita la contabilidad para el túnel L2TP.
List	Visualiza los parámetros de configuración de AAA para el túnel L2TP.
Set	Establece los parámetros de configuración de AAA para el túnel L2TP.

Disable

Utilice el mandato **tunnel disable** para inhabilitar la contabilidad para el túnel L2TP.

Sintaxis:

t**unnel disable** accounting

List

Utilice el mandato **tunnel list** para visualizar la AAA para el túnel L2TP.

Sintaxis:

tu**nnel list** all

accounting

authentication

authorization

config

Set

Utilice el mandato **tunnel set** para establecer los parámetros de configuración de AAA para el túnel L2TP.

Sintaxis:

tunnel set aaa

accounting

authentication

authorization

aaa *tipo-aut*

Establece el tipo de autentificación, autorización y contabilidad. El *tipo-aut* puede ser uno de los siguientes:

local Establece el tipo de autentificación, autorización y contabilidad para utilizar una base de datos de usuario mantenida localmente.

remota Establece el tipo de autentificación, autorización y contabilidad para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

accounting *tipo-aut*

Establece el tipo de contabilidad. El *tipo-aut* puede ser uno de los siguientes:

remota Establece el tipo de autentificación para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

authentication *tipo-aut*

Establece el tipo de autentificación. El *tipo-aut* puede ser uno de los siguientes:

local Establece el tipo de autentificación para utilizar una base de datos de usuario mantenida localmente.

remota Establece el tipo de autentificación para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

authorization *tipo-aut*

Establece el tipo de autorización. El *tipo-aut* puede ser uno de los siguientes:

local Establece el tipo de autorización para utilizar una base de datos de usuario mantenida localmente.

remota Establece el tipo de autorización para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

User-profiles

Utilice el mandato **user-profiles** para acceder al indicador de mandatos `User profile config>`. Desde este indicador de mandatos puede acceder a los mandatos siguientes.

Tabla 31. Mandatos de configuración de perfil de usuario

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Add	Añade un perfil de usuario PPP.
Change	Cambia un perfil de usuario PPP.
Delete	Suprime un perfil de usuario PPP.
Disable	Inhabilita un perfil de usuario PPP.
Enable	Habilita un perfil de usuario PPP.
List	Lista la información de perfil de usuario PPP.
Report	Genera un informe de perfil de usuario PPP.
Reset-user	Restablece un perfil de usuario PPP.
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 **user profiles add** para añadir el perfil de usuario de un usuario remoto a la base de datos de usuario PPP local o para proporcionar acceso de similar de túnel a través de una red IP al direccionador.

Sintaxis:

add ppp-user

tunnel

ppp-user Añade un perfil de usuario de un usuario remoto a la base de datos de usuario PPP local. Puede añadir un máximo de 500 usuarios. Puede añadir un usuario PPP para cada direccionador remoto o cliente DIAL que se pueda conectar al dispositivo que está configurando.

Consulte el mandato Add en el capítulo “El proceso CONFIG (CONFIG - Talk 6) y mandatos” en la publicación *Guía del usuario de software* para obtener una descripción de la sintaxis y las opciones del mandato.

Ejemplo:

```
Config> add ppp-user
Enter name:  [ ]? pppusr01
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [yes]
Will user be tunneled? (Yes, No): [No]
Number of days before account expiry[0-1000] [0]? 10
Number of grace logins allowed after an expiry[0-100] [0]? 5
IP address: [0.0.0.0]? 1.1.1.1
Set ECP encryption key for this user? (Yes, No): [No] no
Disable user ? (Yes, No): [No]

     PPP user name: pppusr01
   User IP address: 1.1.1.1
      Virtual Conn: disabled
        Encryption: disabled
            Status: enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0
   Account expires: Sun 17Feb2036 06:28:16
  Account duration: 10 days  00.00.00
   Password Expiry: <unlimited>

User 'pppusr01' has been added
```

Ejemplo:

```
Config> add ppp-user
Enter name:  [ ]? tunusr01
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [yes]
Will user be tunneled? (Yes, No): [No] yes
Enter hostname to use when connection to this peer: []? host01
Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.1

                  PPP user name: tunusr01
                       Endpoint: 1.1.1.1
                       Hostname: host01

User 'tunusr01' has been added
```

tunnel Proporciona acceso de similar de túnel a través de una red IP hacia el direccionador. A continuación se autoriza el similar para iniciar sesiones PPP de túnel en el direccionador.

Consulte el mandato Add en el capítulo “Configuring the CONFIG Process” de la publicación *Guía del usuario de software* para obtener una descripción de la sintaxis y las opciones del mandato.

Ejemplo:

```
Config> add tunnel
Enter name:  []? tunnel02
Enter hostname to use when connecting to this peer: []? host02
Set shared secret? (Yes, No): [No]? yes
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 2.2.2.22

       Tunnel name: tunnel02
          Endpoint: 2.2.2.22
```

Change

Utilice el mandato **change** para cambiar un perfil de usuario.

Sintaxis:

change ppp-user

tunnel

Delete

Utilice el mandato **delete** para suprimir un perfil de usuario.

Sintaxis:

delete ppp-user

tunnel

Disable

Utilice el mandato **disable** para inhabilitar un perfil de usuario.

Sintaxis:

disable *nombre*

Enable

Utilice el mandato **enable** para habilitar un perfil de usuario.

Sintaxis:

enable *nombre*

List

Utilice el mandato **list** para listar la información de perfil de usuario.

Sintaxis:

list ppp-user

tunnel

```
User profile config> list ppp-user
List  (Name, Verb, User, Addr, Encr, zdump): [Verb]
     PPP user name: ppp01
        Expiry: <unlimited>
   User IP address: Interface Default
        Encryption: Not Enabled
            Status: Enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0
1 record displayed.
```

List Especifica cómo acceder a la información listada.

Valores válidos: name, verb, user, addr, encr, zdump

Valor por omisión: verb

PPP user name

Lista el nombre de usuario.

Expiry Lista la fecha de caducidad.

User IP address
Lista la dirección IP del usuario.

Encryption
Lista si el cifrado está habilitado o no.

Status Lista si el estado está habilitado o no.

Login attempts
Lista el número de veces que el usuario ha intentado iniciar la sesión.

Login failures
Lista el número de intentos de iniciar la sesión que han fallado.

Lockout attempts
Lista el número de intentos de bloqueo.

Report

Utilice el mandato **report** para generar un informe de perfil de usuario PPP.

Sintaxis:

report addresses
all
callback
dialout
dump
encrypt
name
password
time
user

```
User profile config> report addresses
PPP user name      User IP address
-----------------  ------------------
ppp01              Interface Default
1 record displayed.


User profile config> report all
     PPP user name: ppp01
        Expiry: <unlimited>
   User IP address: Interface Default
        Encryption: Not Enabled
            Status: Enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0
1 record displayed.


User profile config> report callback
PPP user name      Callback type        Phone Number
-----------------  -------------------  --------------------
ppp01
1 record displayed.
```

```
User profile config> report dialout
PPP user name      Dial-out
-----------------  ---------------
ppp01
1 record displayed.


User profile config> report dump
Enter user name:  []? user01


User profile config> report encrypt
PPP user name      Encryption
-----------------  ---------------
ppp01              Not Enabled
1 record displayed.


User profile config> report name
PPP user name
-----------------
ppp01
1 record displayed.


User profile config> report password
PPP user name      Expiry        Grace
-----------------  ------------  ------
ppp01              <unlimited>
1 record displayed.


User profile config> report time
PPP user name      Time allotted
-----------------  -------------------
ppp01
1 record displayed.


User profile config> report user
Enter user name:  []? login01
     PPP user name: login01
        Expiry: <unlimited>
   User IP address: Interface Default
        Encryption: Not Enabled
```

Reset-user

Utilice el mandato **reset-user** para restablecer un perfil de usuario.

Sintaxis:

res**et-user** *nombre*

Soporte de reconfiguración dinámica de autentificación (AAA)

Esta sección describe la reconfiguración dinámica (DR) en lo que afecta a los mandatos de Talk 6 y Talk 5.

Delete interface de CONFIG (Talk 6)

AAA no soporta el mandato de CONFIG (Talk 6) **delete interface**.

Activate interface de GWCON (Talk 5)

AAA no soporta el mandato de GWCON (Talk 5) **activate interface**.

Reset interface de GWCON (Talk 5)

AAA no soporta el mandato de GWCON (Talk 5) **reset interface**.

Mandatos de cambio inmediato de CONFIG (Talk 6)

AAA soporta los mandatos de CONFIG siguientes que cambian inmediatamente el estado operativo del dispositivo. Estos cambios se guardan y se conservan si se vuelve a cargar o se reinicia el dispositivo o si se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
CONFIG, add ppp-user
CONFIG, feature authentication, enable login-last-resort
CONFIG, feature authentication, disable login-last-resort **Nota:** Efectivo para la secuencia de inicio de sesión siguiente.
CONFIG, feature authentication, enable tech-support-bypass
CONFIG, feature authentication, disable tech-support-bypass **Nota:** Efectivo para la secuencia de inicio de sesión siguiente.
CONFIG, feature authentication, enable unauthent-accounting
CONFIG, feature authentication, disable unauthent-accounting

Mandatos no reconfigurables dinámicamente

La tabla siguiente describe los mandatos de configuración AAA que no se pueden cambiar dinámicamente. Para activar estos mandatos, es necesario volver a cargar o reiniciar el dispositivo.

Mandatos
CONFIG, feature authentication, server add
CONFIG, feature authentication, server change
CONFIG, feature authentication, server delete
CONFIG, feature authentication, enable ipsec-accounting
CONFIG, feature authentication, disable ipsec-accounting
CONFIG, feature authentication, ppp set
CONFIG, feature authentication, tunnel set
CONFIG, feature authentication, login set
CONFIG, feature authentication, set accounting options
CONFIG, feature authentication, password-rules enable
CONFIG, feature authentication, password-rules disable

Utilización y configuración de protocolos de cifrado

El objetivo del cifrado es transformar datos a una forma no legible para asegurar el secreto. Los datos ***cifrados*** deben descifrarse para obtener los datos originales.

El 2210 soporta:

- El algoritmo de cifrado RC4 con claves de 40 y 128 bits para MPPE (Microsoft Point-to-Point Encryption) (Cifrado de punto a punto de Microsoft) en interfaces PPP.
- El algoritmo Data Encryption Standard in Cipher Block Chaining Mode (DES-CBC) con claves de 56 bits para soporte del Encryption Control Protocol para PPP tal como se describe en las RCF 1968 y 1969.
- El commercial Data Masking Facility (CDMF) que utiliza claves de 40 bits para Cifrado Frame Relay. Este soporte está patentado.
- Frame Relay también utiliza triple-DES y una clave de 128 bits.

Cifrado de PPP utilizando el Encryption Control Protocol

El Encryption Control Protocol (ECP) se utiliza en el direccionador para negociar el uso del cifrado en enlaces punto a punto que se comunican utilizando el protocolo PPP. El Encryption Control Protocol proporciona un mecanismo generalizado para negociar qué algoritmos de cifrado y descifrado se utilizarán en un enlace PPP. Los distintos algoritmos de cifrado se pueden negociar en cada dirección del enlace PPP.

Un método de cifrado y descifrado recibe el nombre de ***algoritmo de cifrado***. Los algoritmos de cifrado utilizan una clave para controlar el cifrado y el descifrado. A diferencia de la compresión, el direccionador cifra en ambas direcciones del enlace, ya que el cifrado en una única dirección supone un riesgo para la seguridad. El enlace se termina cada vez que el ECP no puede negociar algoritmos de cifrado en ambas direcciones.

Configuración del cifrado de ECP para PPP

Para configurar el dispositivo a fin de utilizar el cifrado en la capa de enlace de datos:

1. Establecer las claves de cifrado para los dispositivos remotos y las interfaces PPP locales.

   Establezca la clave de cifrado para el dispositivo remoto utilizando el mandato **add ppp-user** en el indicador de mandatos `Config>`. Consulte el mandato **Add** en el capítulo “Configuración del proceso CONFIG” de la publicación *Guía del usuario de software* para obtener una descripción de la sintaxis y las opciones del mandato.

   Establezca la clave de cifrado para la interfaz PPP local utilizando el mandato **enable ecp** (consulte el mandato talk 6 `PPP Config>` **enable** en la publicación *Guía del usuario de software*).

2. Configurar enlaces PPP individuales para utilizar el Encryption Control Protocol (ECP) utilizando el mandato **enable ecp** en el indicador de mandatos `PPP Config>`.

3. Habilitar PAP, CHAP o SPAP.

También puede inhabilitar el cifrado, cambiar la clave de cifrado para un usuario, listar el estado del cifrado o establecer el nombre que utiliza el dispositivo cuando solicita cifrado. Para obtener información para:

- Inhabilitar el cifrado, consulte el mandato `PPP Config>` **disable ecp** en la publicación *Guía del usuario de software*.
- Cambiar la clave de cifrado y la contraseña del usuario remoto, consulte el mandato `Config>` **change ppp-user** en la publicación *Guía del usuario de software*.
- Listar el estado de cifrado, consulte el mandato `PPP Config>` **list ecp** en la publicación *Guía del usuario de software*.
- Establecer el nombre del dispositivo, consulte el mandato `PPP Config>` **set name** en la publicación *Guía del usuario de software*.

Supervisión del cifrado de ECP para PPP

Puede supervisar los distintos valores de cifrado en las interfaces:

1. Accediendo al indicador de mandatos de supervisión utilizando el mandato **talk 5**.
2. Seleccionando la interfaz que desea supervisar utilizando el mandato **network**. Este mandato lo sitúa en el indicador de mandatos `PPP n>`, donde *n* representa el número de la red. Consulte “Configuración y supervisión de interfaces Point-to-Point Protocol” en la publicación *Guía del usuario de software* para obtener instrucciones sobre cómo utilizar el mandato **network**.

Desde este indicador de mandatos, puede:

- Listar el estado actual del cifrado, la negociación de cifrado más reciente, el tiempo transcurrido desde un cambio de estado de cifrado y los algoritmos que utilizan los codificadores. (Consulte el mandato **list control ecp** en la publicación *Guía del usuario de software*.)
- Listar los paquetes de control de cifrado recibidos y transmitidos en la interfaz. (Consulte el mandato **list ecp** en la publicación *Guía del usuario de software*.)
- Listar los paquetes de datos cifrados transmitidos o recibidos en la interfaz. (Consulte el mandato **list edp** en la publicación *Guía del usuario de software*.)

Cifrado punto a punto de Microsoft (MPPE)

El Cifrado punto a punto de Microsoft (MPPE) proporciona un medio para que las estaciones de trabajo Windows conectadas remotamente conocidas como clientes de Microsoft Dial-Up Networking (DUN) puedan cifrar los datos que se transmiten a través de un enlace PPP entre ellas y el 2210. El MPPE también se puede utilizar para cifrar los datos que se transmiten a través de un enlace PPP entre direccionador y direccionador. El MPPE siempre se negocia en ambas direcciones.

MPPE utiliza algoritmos de clave secreta para realizar el cifrado. En algoritmos de clave secreta, se utiliza la misma clave para el cifrado y el descifrado. Esta clave no la configura el usuario, sino que se genera en el proceso de negociación del MPPE entre las estaciones de trabajo de envío y de recepción. Para utilizar el MPPE, debe configurar el protocolo de autentificación Microsoft Challenge/Handshake Authentication Protocol (MS-CHAP).

Si la interfaz PPP se ha autentificado con MS-CHAP, el direccionador pasa a una "modalidad Microsoft", en la que sólo negociará MPPC si se ha habilitado la compresión y sólo negociará MPPE si se ha habilitado el cifrado. En la "modalidad Microsoft", el direccionador ignora la lista de prioridades de algoritmos de compresión e inhabilita la negociación del ECP.

Configuración del MPPE

Para configurar el MPPE, debe llevar a cabo estos pasos para cada interfaz:

1. Configurar MS-CHAP. En la publicación *Guía del usuario de software*, consulte "Microsoft PPP CHAP Authentication (MS-CHAP)" y "Configuración y supervisión de interfaces Point-to-Point Protocol" para obtener información sobre cómo utilizar y configurar MS-CHAP.
2. Si configura una conexión de direccionador a direccionador, establezca el nombre para la interfaz PPP local utilizando el mandato **set name** (consulte el mandato `PPP Config>` **set name** en la publicación *Guía del usuario de software*).
3. Si desea compresión de datos, habilite MPPC utilizando el mandato talk 6 **enable ccp** en el indicador de mandatos `PPP Config>`. El MPPE no necesita compresión de datos.
4. Habilite el MPPE. Utilice el mandato **enable mppe** en el indicador de mandatos `PPP Config>` (consulte el mandato `PPP Config>` **enable** en la publicación *Guía del usuario de software*).
5. Reinicie el direccionador para activar la configuración.

También puede inhabilitar el MPPE y listar las opciones del MPPE.

- Utilice el mandato talk 6 **disable mppe** en el indicador de mandatos `PPP Config>` para inhabilitar el MPPE.
- Utilice el mandato talk 6 **list ccp** en el indicador de mandatos `PPP Config>` para listar las opciones del MPPE que se han configurado.

Supervisión del MPPE

Active el indicador de mandatos `PPP>` tal como se describe en "Supervisión del cifrado de ECP para PPP" en la página 218. Utilice el mandato **list mppe** para ver las estadísticas de datos del MPPE y el mandato **list control ccp** para ver el estado del MPPE. Pueden encontrarse ejemplos de estos mandatos en "Configuración y supervisión de interfaces Point-to-Point Protocol" en la publicación *Guía del usuario de software*.

Configuración del cifrado en interfaces Frame Relay

Nota: Frame relay utiliza un esquema de cifrado patentado.

El cifrado de datos está soportado en todas las interfaces en las que se ha habilitado el cifrado. Puede configurar circuitos individuales en una interfaz con el cifrado habilitado para llevar a cabo o no el cifrado, según se desee.

Para configurar el dispositivo para utilizar el cifrado en enlaces frame relay:

1. Acceda al indicador de mandatos de configuración de frame relay utilizando el mandato **talk 6**.

2. Seleccione la interfaz frame relay que desee que tenga capacidad de cifrado utilizando el mandato **net** *número*.
3. Habilite el cifrado en la interfaz frame relay utilizando el mandato **enable encryption**. Consulte los mandatos de configuración de Frame Relay en la publicación *Guía del usuario de software*.
4. Añada circuitos virtuales permanentes con capacidad de cifrado y defina la clave de cifrado para cada uno de los PVC utilizando el mandato **add permanent-virtual-circuit**. Consulte los mandatos de configuración de Frame Relay en la publicación *Guía del usuario de software*.
5. Repita los pasos del 1 al 4 para cada interfaz con capacidad de cifrado que esté configurando.

Nota: Si el cifrado está habilitado para un circuito virtual permanente FR, los datos no circularán por el circuito a menos que el cifrado se negocie satisfactoriamente con el dispositivo en el otro extremo del circuito virtual. El cifrado no está soportado para circuitos huérfanos puesto que debe configurarse el PVC para poder entrar la clave de cifrado.

También puede inhabilitar el cifrado para una interfaz, cambiar los valores de cifrado para un PVC o listar el estado del cifrado. Para obtener información para

- Inhabilitar el cifrado en una interfaz, consulte el mandato **disable encryption** de Configuración de Frame Relay en la publicación *Guía del usuario de software*.
- Cambiar los valores de cifrado para un PVC, consulte el mandato **change permanent-virtual-circuit** de Configuración de Frame Relay en la publicación *Guía del usuario de software*.
- Listar estados de cifrado, consulte los mandatos **list all,**, **list lmi** y **list permanent-virtual-circuit** de Configuración de Frame Relay en la publicación *Guía del usuario de software*.

Supervisión del cifrado en interfaces Frame Relay

Puede supervisar los distintos valores de cifrado en las interfaces:

1. Accediendo al indicador de mandatos de supervisión utilizando el mandato **talk 5**.
2. Seleccionando la interfaz que desea supervisar utilizando el mandato **network** *número*. Este mandato lo sitúa en el indicador de mandatos FR x>.

Desde este indicador de mandatos puede listar el estado de cifrado actual para una interfaz, un PVC o un circuito. Consulte el mandato **list** de Supervisión de Frame Relay en la publicación *Guía del usuario de software*.

Configuración y supervisión de Calidad de los servicios (QoS)

Este capítulo describe la configuración de Calidad de los servicios (QoS) y los mandatos operativos para interfaces LAN y ELAN en el dispositivo. El capítulo contiene las secciones siguientes:

Visión general de Calidad de los servicios

La característica QoS mejora las ventajas de las capacidades de QoS ATM para los VCC directos de datos de Emulación de LAN. A este soporte se hace referencia como "QoS configurable para Emulación de LAN". Los atributos clave y las ventajas de esta característica son los siguientes:

- Un Cliente LE utiliza los parámetros de QoS configurados para sus VCC directos de datos.
- Los parámetros de QoS se pueden configurar para:
  - Cliente LE
  - Interfaz ATM
- El conjunto de parámetros de QoS configurados se utilizan con señalización ATM Forum UNI 3.0/3.1. Los parámetros incluyen Peak Cell Rate, Sustained Cell Rate, QoS Class y Maximum Burst Size.
- Se puede configurar el Maximum Reserved Bandwidth por VCC para proteger un Cliente LE al aceptar/establecer los VCC para cuyos parámetros de tráfico no tiene soporte.
- El mecanismo de QoS Negotiation permite que los Clientes LE participantes puedan conocer los parámetros de QoS de cada uno de ellos. Un VCC directo de datos se configura utilizando parámetros negociados.

Ventajas del QoS

- La utilización de QoS para el Cliente LE, Interfaz ATM o LAN emulada proporciona las siguientes ventajas para los VCC directos de datos de LANE.
  - Un Cliente LE puede configurarse con QoS si la QoS que necesita el cliente es diferente de la QoS que necesitan otros clientes de la ELAN. Por ejemplo, si un Cliente LE sirve un servidor de archivos, puede que el usuario desee configurar los parámetros de QoS adecuados para todo el tráfico desde y hacia el servidor de archivos.

– Se puede configurar una Interfaz ATM con QoS si un usuario desea que todos los Clientes LE en dicha interfaz ATM utilicen el mismo conjunto de parámetros. Por ejemplo, si se conecta una interfaz ATM a 25 Mbps, el usuario puede configurar parámetros apropiados que sean diferentes de los de una interfaz a 155 Mbps.

Parámetros de configuración de QoS

Esta sección describe nueve parámetros que se utilizan para la configuración de QoS. Los seis parámetros siguientes se pueden configurar para un Cliente LE, Interfaz ATMy una LAN emulada:

1. max-reserved-bandwidth
2. traffic-type
3. peak-cell-rate
4. sustained-cell-rate
5. max-burst-size
6. qos-class

Los dos parámetros siguientes se pueden configurar para una LAN emulada y un Cliente LE:

1. *validate-pcr-of-best-effort-vccs*
2. *negotiate-qos*

El parámetro *accept-qos-parms-from-lecs* solamente se puede configurar para un Cliente LE.

Los seis primeros parámetros controlan las características de tráfico de los VCC directos de datos establecidos por el Cliente LE mientras que el primer parámetro también hace referencia a las llamadas recibidas por el Cliente LE. Las características siguientes están asociadas con todos los VCC directos de datos establecidos por el Cliente LE:

- El ancho de banda no está reservado para el tráfico de mayor eficacia.
- Los parámetros de tráfico hacen referencia a ambas direcciones, hacia adelante y hacia atrás.
- Cuando se rechaza una conexión de ancho de banda debido a los parámetros de tráfico o a la Clase de QoS, la llamada se reintenta como una conexión de mayor eficacia con la velocidad mayor de célula configurada (se utilizan códigos de causa en mensajes de liberación o liberación completada para determinar por qué se ha liberado un VCC).
- Cuando se rechaza una conexión de mayor eficacia debido a la Velocidad mayor de célula (PCR), la llamada se puede reintentar automáticamente con una PCR menor. Los reintentos se realizan bajo las condiciones siguientes:
  1. Si la PCR rechazada es mayor que 100 Mbps, la llamada se reintenta con una PCR de 100 Mbps.
  2. De lo contrario, si la PCR rechazada es mayor que 25 Mbps, la llamada se reintenta con una PCR de 25 Mbps.

Ancho de banda máximo reservado (max-reserved-bandwidth)

El ancho de banda máximo reservado aceptable para un VCC directo de datos. Este parámetro hace referencia tanto a llamadas de VCC directo de datos recibidas por el Cliente LE como a llamadas de VCC directo de datos efectuadas al Cliente LE. Para las llamadas de entrada, este parámetro define la SCR máxima aceptable para un VCC directo de datos. Si no se especifica la SCR en la llamada de entrada, este parámetro define la PCR máxima aceptable para un VCC directo de datos con ancho de banda reservado.

Las llamadas recibidas con parámetros de tráfico que especifican velocidades más altas se liberarán. Si se especifica la SCR en la llamada de entrada, la llamada no se rechazará debido a la PCR o al Maximum Burst Size. La limitación que impone este parámetro no es aplicable a conexiones de mayor eficacia. Para llamadas de salida, este parámetro establece un límite superior para la cantidad de ancho de banda reservado que puede solicitar un VCC directo de datos. Por lo tanto, los parámetros traffic-type y sustained-cell-rate dependen de este parámetro.

Valores válidos:

Entero en el rango de 0 a la velocidad de línea del dispositivo ATM en kbps

Valor por omisión:

0

Tipo de tráfico (traffic-type)

El tipo de tráfico deseado para los VCC directos de datos. Si los parámetros de QoS no se negocian, este parámetro especifica el tipo de llamadas que realiza el Cliente LE. De lo contrario, si se negocian los parámetros de QoS, este parámetro especifica el tipo deseado de características de tráfico para los VCC directos de datos. Cuando se negocian los parámetros de QoS, si tanto el LEC de origen como el de destino desean una conexión de ancho de banda reservado y ambos LEC soportan conexiones de ancho de banda reservado (es decir, max-reserved-bandwidth > 0), se realizará un intento de establecer un VCC directo de datos de ancho de banda reservado entre los dos LEC. De lo contrario, el VCC directo de datos será una conexión de mayor eficacia. Dependencias: max-reserved-bandwidth

Valores válidos:

best_effort o reserved_bandwidth

Valor por omisión:

best_effort

Velocidad mayor de célula (peak-cell-rate)

La velocidad mayor de célula que se desea para los VCC directos de datos. Si no se negocian los parámetros de QoS, este parámetro especifica el parámetro de tráfico de PCR para las llamadas de VCC directo de datos realizadas por el Cliente LE. De lo contrario, si se negocian los parámetros de QoS, este parámetro especifica el parámetro de tráfico de PCR deseado para los VCC directos de datos. Se utiliza la mínima de las PCR deseadas de los dos LEC para los VCC de mayor eficacia negociados.

Cuando se negocia un VCC de ancho de banda reservado y sólo uno de los Clientes LE solicita una conexión de ancho de banda reservado, la PCR deseada de dicho LEC se utiliza para el VCC directo de datos sujeta al límite superior que

impone la velocidad de línea del dispositivo ATM local. Si ambos LEC solicitan una conexión de ancho de banda reservado, se utiliza la máxima de las PCR deseadas de los Clientes LE para el VCC directo de datos sujeto al límite superior que impone la velocidad de línea del dispositivo ATM local.

Valores válidos:

Un valor entero en el rango de 0 a la velocidad de línea del dispositivo ATM en kbps

Valor por omisión:

Velocidad de línea del dispositivo LEC ATM en kbps.

Velocidad sostenida de célula (sustained-cell-rate)

La velocidad sostenida de célula deseada para los VCC directos de datos. Si no se negocian parámetros de QoS, este parámetro especifica el parámetro de tráfico de SCR para llamadas de VCC directo de datos realizadas por el Cliente LE. De lo contrario, si se negocian parámetros de QoS, este parámetro especifica el parámetro de tráfico de SCR deseado para los VCC directos de datos.

Cuando se negocia un VCC de ancho de banda reservado y sólo uno de los Clientes LE solicita una conexión de ancho de banda reservado, la SCR deseada de dicho LEC se utiliza para el VCC directo de datos (sujeta al límite superior que impone el parámetro max-reserved-bandwidth del otro LEC). Si ambos LEC solicitan una conexión de ancho de banda reservado, se utiliza la máxima de las SCR deseadas de los Clientes LE para el VCC directo de datos (sujeta al límite superior impuesto por los parámetros max-reserved-bandwidth de ambos LEC). En cualquier caso (con o sin negociación), si la SCR que debe señalarse es igual a la PCR que debe señalarse, la llamada se señala con sólo PCR.

Dependencias: max-reserved-bandwidth, traffic-type y peak-cell-rate. Este parámetro sólo es aplicable cuando el traffic-type es anchobanda_reservado.

Valores válidos:

Un valor entero en el rango de 0 al mínimo de max-reserved-bandwidth y peak-cell-rate, especificado en kbps

Valor por omisión

Ninguno

Tamaño máximo de ráfaga (max-burst-size)

El tamaño máximo de ráfaga deseado para los VCC directos de datos. Si no se negocian parámetros de QoS, este parámetro especifica el parámetro de tráfico Maximum Burst Size para las llamadas de VCC directo de datos realizadas por el Cliente LE. De lo contrario, si se negocian los parámetros de QoS, este parámetro especifica el parámetro de tráfico Maximum Burst Size deseado para los VCC directos de datos.

Cuando se negocia un VCC de ancho de banda reservado y sólo uno de los Clientes LE solicita una conexión de ancho de banda reservado, se utiliza el Maximum Burst Size deseado de dicho LEC para el VCC directo de datos. Si ambos LEC solicitan una conexión de ancho de banda reservado, se utiliza el Maximum Burst Size deseado de los Clientes LE para el VCC directo de datos.

En cualquier caso (con o sin negociación), el Maximum Burst Size sólo se señala cuando se señala la SCR. Aunque este parámetro se expresa en unidades de

células, se configura como un múltiplo entero del Maximum Data Frame Size (especificado en el parámetro C3 del LEC) con un límite inferior de 1.

Dependencias: Este parámetro sólo es aplicable cuando el traffic-type es anchobanda_reservado.

Valores válidos:
Un número entero de tramas; debe ser mayor que 0

Valor por omisión:
1 trama

Clase de QoS (qos-class)

La clase de QoS que se desea para las llamadas de ancho de banda reservado. Si no se negocian parámetros de QoS, este parámetro especifica la clase de QoS que debe utilizarse para las llamadas de VCC directo de datos de ancho de banda reservado efectuadas por el Cliente LE. De lo contrario, si se negocian parámetros de QoS, este parámetro especifica la Clase de QoS que se desea para los VCC directos de datos. Siempre se utiliza una Clase de QoS sin especificar en llamadas de mayor eficacia. Las clases de QoS especificadas definen valores objetivos para el rendimiento de ATM. Las clases de QoS especificadas definen los valores objetivos para los parámetros de rendimiento de ATM, como por ejemplo proporción de pérdida de célula y retardo de transferencia de célula.

La Especificación UNI declara que:

La Clase 1 de QoS especificada
debe proporcionar un rendimiento comparable al rendimiento de la línea privada digital actual.

La Clase 2 de QoS especificada
está indicada para vídeo y audio empaquetados en teleconferencias y aplicaciones multimedia.

La Clase 3 de QoS especificada
está indicada para la interoperación de protocolos orientados a la conexión, como por ejemplo Frame Relay.

La Clase 4 de QoS especificada
está indicada para la interoperación de protocolos sin conexión, como por ejemplo IP o SMDS.

Los LEC deben poder aceptar llamadas con cualquiera de las Clases de QoS anteriores. Cuando se negocian parámetros de QoS, se comparan las Clases de QoS configuradas de los dos LEC y se utiliza la Clase de QoS con los requisitos más estrictos.

Valores válidos:
0: para Clase de QoS sin especificar

1: para Clase 1 de QoS especificada

2: para Clase 2 de QoS especificada

3: para Clase 3 de QoS especificada

4: para Clase 4 de QoS especificada

Valor por omisión:
0 (Clase de QoS sin especificar)

Para validar la PCR de los VCC de mayor eficacia (validate-pcr-of-best-effort-vccs)

Validar Peak Cell Rate de los VCC de mayor eficacia. Cuando es FALSE, los VCC de mayor eficacia se aceptan sin tener en cuenta la PCR hacia adelante señalada. Cuando es TRUE, los VCC de mayor eficacia se rechazan si la PCR hacia adelante señalada excede la velocidad de línea del dispositivo Cliente LE ATM. Las llamadas no se rechazan debido a la PCR hacia atrás. La PCR hacia atrás señalada se mantendrá si no se excede la velocidad de línea; de lo contrario, las transmisiones al emisor serán a la velocidad de línea.

Notas:

1. La aceptación de los VCC de mayor eficacia con PCR hacia adelante que excedan la velocidad de línea puede dar como resultado un rendimiento bajo debido a un exceso de retransmisiones; sin embargo, el rechazo de estos VCC puede provocar problemas de interoperabilidad.
2. El valor sí es útil cuando los emisores vayan a reintentar con una PCR más baja después de un rechazo de llamada debido a una velocidad de célula no disponible.

Valores válidos:
yes, no

Valor por omisión:
no

Negociar QoS (negotiate-qos)

Habilitar la negociación de parámetros de QoS para los VCC directos de datos. Este parámetro sólo debe habilitarse cuando se conecta a un IBM MSS LES. Cuando este parámetro es sí, el Cliente LE incluirá un TLV de Parámetro de tráfico de IBM en las tramas LE_JOIN_REQUEST y LE_ARP_RESPONSE enviadas al LES. Este TLV incluirá los valores de max-reserved-bandwidth, traffic-type, peak-cell-rate, sustained-cell-rate, max-burst-size y qos-class. Un TLV de Parámetro de tráfico de IBM también se puede incluir en una LE_ARP_RESPONSE devuelta al Cliente LE por el LES.

Si no existe ningún TLV en una LE_ARP_RESPONSE recibida por el Cliente LE, deben utilizarse los parámetros de configuración local para configurar el VCC directo de datos. Si se incluye un TLV en una LE_ARP_RESPONSE, el Cliente LE debe comparar el contenido del TLV con los valores locales correspondientes para determinar el conjunto de parámetros “negociado” o “mejor” aceptable para ambas partes antes de señalar para el VCC directo de datos.

Valores válidos:
yes, no

Valor por omisión:
no

Aceptar parámetros de QoS de LECS (accept-qos-parms-from-lecs)

Este parámetro proporciona la posibilidad de configurar un Cliente LE para aceptar/rechazar parámetros de QoS de un LECS. Cuando este parámetro es sí, el Cliente LE debe utilizar los parámetros de QoS obtenidos de los Clientes LE en las tramas LE_CONFIGURE_RESPONSE, es decir, los parámetros de QoS de los Clientes LE prevalecen sobre los parámetros de QoS configurados. Si este parámetro es no el Cliente LE ignorará los parámetros de QoS recibidos en una trama LE_CONFIGURE_RESPONSE desde los Clientes LE.

Valores válidos:

yes, no

Valor por omisión:

no

Acceso al indicador de mandatos de configuración de QoS

Utilice el mandato **feature** desde el proceso CONFIG para acceder a los mandatos de configuración de Calidad de los servicios. Entre **feature** seguido del número de característica (6) o nombre abreviado (QoS). Por ejemplo:

```
Config> feature qos
Quality of Service - Configuration
QoS Config>
```

Después de acceder al indicador de mandatos `QoS Config>`, puede configurar la Calidad de los servicios (QoS) de un Cliente LE o una Interfaz ATM. Para volver al indicador de mandatos `Config>` en cualquier momento, entre el mandato **exit** en el indicador de mandatos `QoS Config>`.

Alternativamente, puede configurar parámetros de QoS para un Cliente LE o una Interfaz ATM accediendo a las entidades de la siguiente manera:

- Cliente LE
  1. En el indicador de mandatos `Config>`, entre el mandato **network** y el número de interfaz de Cliente LE.
  2. En el indicador de mandatos `LE Client configuration>`, entre **qos-configuration**.

     Ejemplo:

     ```
     config> network 3
     Token Ring Forum Compliant LEC Config> qos-configuration
      LEC QoS Config>
     ```

- Interfaz ATM
  1. En el indicador de mandatos `Config>`, entre el mandato **network** y el número de interfaz ATM para llegar al indicador de mandatos `ATM Config>`.
  2. Entre el parámetro **interface** para llegar al indicador de mandatos `ATM Interface Config>`.
  3. En el indicador de mandatos `ATM InterfaceConfig>`, entre **qos-configuration**.

     Ejemplo:

     ```
        config> network 0
      ATM Config> interface
      ATM Interface Config> qos-configuration
    ATM-I/F 0 QoS>
     ```

Mandatos de Calidad de los servicios

Esta sección resume los mandatos de configuración de QoS. Utilice los mandatos siguientes para configurar la Calidad de los servicios. Entre los mandatos desde el indicador de mandatos `QoS Config>`.

Tabla 32. Resumen de los mandatos de configuración de la Calidad de los servicios (QoS)

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
le-client	Le conduce al indicador de mandatos `LE Client QoS configuration >` para el cliente LE seleccionado.
atm-interface	Le conduce al indicador de mandatos `ATM Interface QoS configuration>` para la interfaz ATM seleccionada.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Mandatos de configuración de QoS para Cliente LE

Esta sección resume y explica los mandatos para configurar QoS para un Cliente LE específico.

Utilice los mandatos siguientes en el indicador de mandatos `LEC QoS config>`.

Tabla 33. Resumen de los mandatos de configuración de Calidad de los servicios (QoS) para un Cliente LE

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
List	Lista la configuración de QoS del Cliente LE.
Set	Establece los parámetros de QoS del Cliente LE.
Remove	Elimina la configuración de QoS del Cliente LE.
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 configuración de QoS de este Cliente LE. Los parámetros de QoS sólo se listan si como mínimo se ha configurado uno específicamente (vea el Ejemplo 1). De lo contrario, no se lista ningún parámetro (vea el Ejemplo 2).

Sintaxis:

list

Ejemplo 1:

```
LEC QoS Config> list

             LE Client QoS Configuration for Data Direct VCCs
           ========================================
       (ATM interface number = 0,  LEC interface number = 3)

  Maximum Reserved Bandwidth for a Data-Direct VCC = 10000 Kbps
     Data-Direct VCC Type ........................... = Best-Effort
     Data-Direct VCC Peak Cell Rate ................. = 155000 Kbps
     Data-Direct VCC Sustained Cell Rate ............ = 155000 Kbps
     Desired QoS Class of Reserved Connections ...... = 0
     Max Burst Size of Reserved Connections    ...... = 0 frames

     Validate Peak Rate of Best-Effort connections .. = No
  Enable QoS Parameter Negotiation ............... = Yes
     Accept QoS Parameters from LECS ................ = Yes

  LEC QoS Config>
```

Ejemplo 2:

```
LEC QoS Config> list

   QoS has not been configured for this LEC.
   Please use the SET option to configure QoS.

  LEC QoS Config>
```

Set

Utilice el mandato **set** para especificar parámetros de QoS de Cliente LE.

Sintaxis:

set accept-qos-parms-from-lecs
all-default-values
max-burst-size
max-reserved-bandwidth
negotiate-qos
peak-cell-rate
qos-class
sustained-cell-rate
traffic-type
validate-pcr-of-best-effort-vccs

accept-qos-parms-from-lecs

Utilice esta opción para habilitar/inhabilitar el LE Client para aceptar/rechazar los parámetros de QoS recibidos desde un LECS como TLV. Consulte el apartado “Aceptar parámetros de QoS de LECS (accept-qos-parms-from-lecs)” en la página 227 para obtener una descripción más detallada de este parámetro.

Valores válidos:

yes, no

Valor por omisión:

sí

Ejemplo:

```
LEC QoS Config> se acc y
LEC QoS Config>
```

all-default-values

Utilice esta opción para establecer los parámetros de QoS en los valores por omisión. En el ejemplo siguiente también se listan los valores por omisión.

Ejemplo:

```
LEC QoS Config> set all-default-values
   Failed to locate existing QoS configuration record!
   Using a new set of default values ...
   Initializing all parameters to default values
   LEC QoS Config>  list

              LE Client QoS Configuration for Data Direct VCCs
              ========================================
        (ATM interface number = 0,  LEC interface number = 3)

     Maximum Reserved Bandwidth for a Data-Direct VCC = 0 Kbps
     Data-Direct VCC Type ........................... = Best-Effort
     Data-Direct VCC Peak Cell Rate ................. = 155000 Kbps
     Data-Direct VCC Sustained Cell Rate ............ = 155000 Kbps
     Desired QoS Class of Reserved Connections ...... = 0
     Max Burst Size of Reserved Connections    ...... = 0 frames

     Validate Peak Rate of Best-Effort connections .. = No
     Enable QoS Parameter Negotiation ............... = No
     Accept QoS Parameters from LECS ................ = Yes

  LEC QoS Config>
```

max-burst-size

Establece el tamaño máximo de ráfaga que se desea en las tramas. Consulte el apartado “Tamaño máximo de ráfaga (max-burst-size)” en la página 224 para obtener una descripción más detallada de este parámetro.

Valores válidos:

Un número entero de tramas; debe ser mayor que 0

Valor por omisión:

1 trama

Ejemplo:

```
LEC QoS Config> se ma
   Maximum Burst Size in Kbps [1]? 10000
   LEC QoS Config>
```

max-reserved-bandwidth

Utilice esta opción para establecer el ancho de banda máximo reservado permitible por VCC directo de datos. Consulte el apartado “Ancho de banda máximo reservado (max-reserved-bandwidth)” en la página 223 para obtener una descripción más detallada de este parámetro.

Valores válidos:

Entero en el rango de 0 a la velocidad de línea del dispositivo ATM en kbps

Valor por omisión:

0

Ejemplo:

```
   LEC QoS Config> set max-reserved-bandwidth
   Maximum reserved bandwidth acceptable for a data-direct VCC (in Kbps) [0]? 20000
   LEC QoS Config>
```

negotiate-qos

Utilice esta opción para habilitar/inhabilitar la participación del Cliente LE en la negociación de QoS. Consulte el apartado “Negociar QoS (negotiate-qos)” en la página 226 para obtener una descripción más detallada de este parámetro.

Valores válidos:

yes, no

Valor por omisión:

no

Ejemplo:

```
LEC QoS Config> se neg y
LEC QoS Config>
```

peak-cell-rate

Establece la velocidad mayor de célula que se desea para los VCC directos de datos. Consulte el apartado “Velocidad mayor de célula (peak-cell-rate)” en la página 223 para obtener una descripción más detallada de este parámetro.

Valores válidos:

Un valor entero en el rango de 0 a la velocidad de línea del dispositivo ATM en kbps

Valor por omisión:

Velocidad de línea del dispositivo LEC ATM en kbps.

Ejemplo:

```
LEC QoS Config> set peak-cell-rate
Data-Direct VCC Peak Cell Rate in Kbps [1]? 25000
LEC QoS Config>
```

qos-class

Establece la Clase de QoS que se desea para los VCC directos de datos. Consulte el apartado “Clase de QoS (qos-class)” en la página 225 para obtener una descripción más detallada de este parámetro.

Valores válidos:

0: para Clase de QoS sin especificar

1: para Clase 1 de QoS especificada

2: para Clase 2 de QoS especificada

3: para Clase 3 de QoS especificada

4: para Clase 4 de QoS especificada

Valor por omisión:

0 (Clase de QoS sin especificar)

Ejemplo:

```
LEC QoS Config> se qos
Desired QoS Class for Data Direct VCCs [0]? 1
LEC QoS Config>
```

sustained-cell-rate

Establece la velocidad sostenida de célula que se desea para los VCC de datos directos. Consulte el apartado “Velocidad sostenida de célula (sustained-cell-rate)” en la página 224 para obtener una descripción más detallada de este parámetro.

Valores válidos:

Un valor entero en el rango de 0 al mínimo de max-reserved-bandwidth y peak-cell-rate, especificado en kbps

Valor por omisión

Ninguno

Ejemplo:

```
LEC QoS Config> se sus
Data-Direct VCC Sustained Cell Rate in Kbps [1]? 10000
LEC QoS Config>
```

traffic-type

Establece el tráfico que se desea para los VCC directos de datos. Consulte el apartado “Tipo de tráfico (traffic-type)” en la página 223 para obtener una descripción más detallada de este parámetro.

Valores válidos:

mayor eficacia o ancho de banda reservado

Valor por omisión:

mayor eficacia

Ejemplo:

```
LEC QoS Config>set traffic-type
  Choose from:
     (0): Best-Effort
     (1): Reserved-Bandwidth
Data Direct VCC Type [0]? 1
Note: Peak Cell Rate has been reset to 1
      Sustained Cell Rate has been reset to 1
      Max Reserved Bandwidth has been reset to 1
      Please configure appropriate values.
LEC QoS Config>
```

validate-pcr-of-best-effort-vccs

Utilice esta opción para habilitar/inhabilitar la validación del parámetro de tráfico Peak Cell Rate de las llamadas de VCC directo de datos recibidas por este Cliente LE. Consulte el apartado “Para validar la PCR de los VCC de mayor eficacia (validate-pcr-of-best-effort-vccs)” en la página 226 para obtener una descripción más detallada de este parámetro.

Valores válidos:

yes, no

Valor por omisión:

no

Ejemplo:

```
LEC QoS Config> se val y
LEC QoS Config>
```

Remove

Utilice el mandato **remove** para eliminar la configuración de QoS de este Cliente LE.

Sintaxis:

r**emove**

Ejemplo:

```
LEC QoS Config> remove
WARNING: This option deletes the QoS configuration.
         To re-configure use any of the SET options.
Should the LEC QoS configuration be deleted? [No]: yes
Deleted QoS configuration successfully
LEC QoS Config>
```

Mandatos de configuración de QoS de Interfaz ATM

Tabla 34. Resumen de los mandatos de configuración de Calidad de los servicios (QoS) para un Cliente LE

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
List	lista la configuración de QoS de la Interfaz ATM actual.
Set	Establece los parámetros de QoS de la Interfaz ATM.
Remove	Elimina la configuración de QoS de la Interfaz ATM.
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 configuración de QoS de esta Interfaz ATM. Los parámetros de QoS sólo se listan si se ha configurado como mínimo un parámetro (vea el ejemplo siguiente). De lo contrario, no se lista ningún parámetro.

Sintaxis:

list

Ejemplo:

```
ATM-I/F 0 QoS> list

          ATM Interface `Quality of Service' Configuration
          ================================================
                    (ATM interface number = 0  )

     Maximum Reserved Bandwidth for a VCC = 15000 Kbps
     VCC Type ........................... = RESERVED-BANDWIDTH
     Peak Cell Rate ..................... = 20000 Kbps
     Sustained Cell Rate ................ = 5000 Kbps
     QoS Class .......................... = 4
     Maximum Burst Size ................. = 5 frames
ATM-I/F 0 QoS>
```

Set

Utilice el mandato **set** para especificar parámetros de QoS de la interfaz ATM.

Sintaxis:

set max-burst-size

max-reserved-bandwidth

peak-cell-rate

qos-class

sustained-cell-rate

traffic-type

max-burst-size

Establece el tamaño máximo de ráfaga que se desea en las tramas. Consulte el apartado “Tamaño máximo de ráfaga (max-burst-size)” en la página 224 para obtener una descripción más detallada de este parámetro.

Valores válidos:

Un número entero de tramas; debe ser mayor que 0

Valor por omisión:

1 trama

Ejemplo:

```
ATM-I/F 0 QoS Config> se ma
Maximum Burst Size in Kbps [1]? 10000
ATM-I/F 0 QoS Config>
```

max-reserved-bandwidth

Utilice esta opción para establecer el ancho de banda máximo reservado permitible para cada VCC directo de datos. Consulte el apartado “Ancho de banda máximo reservado (max-reserved-bandwidth)” en la página 223 para obtener una descripción más detallada de este parámetro.

Valores válidos:

Entero en el rango de 0 a la velocidad de línea del dispositivo ATM en kbps

Valor por omisión:

0

Ejemplo:

```
   ATM-I/F 0 QoS> se max-reserved-bandwidth
   Maximum reserved bandwidth acceptable for a data-direct VCC (in Kbps) [0]?
15000
ATM-I/F 0 QoS>
```

peak-cell-rate

Establece la velocidad mayor de célula que se desea para los VCC directos de datos. Consulte el apartado “Velocidad mayor de célula (peak-cell-rate)” en la página 223 para obtener una descripción más detallada de este parámetro.

Valores válidos:

Un valor entero en el rango de 0 a la velocidad de línea del dispositivo ATM en kbps

Valor por omisión:

Velocidad de línea del dispositivo LEC ATM en kbps.

Ejemplo:

```
ATM-I/F 0 QoS Config> set peak-cell-rate
Data-Direct VCC Peak Cell Rate in Kbps [1]? 25000
ATM-I/F 0 QoS Config>
```

qos-class

Establece la Clase de QoS que se desea para los VCC directos de datos. Consulte el apartado “Clase de QoS (qos-class)” en la

página 225 para obtener una descripción más detallada de este parámetro.

Valores válidos:

0: para Clase de QoS sin especificar

1: para Clase 1 de QoS especificada

2: para Clase 2 de QoS especificada

3: para Clase 3 de QoS especificada

4: para Clase 4 de QoS especificada

Valor por omisión:

0 (Clase de QoS sin especificar)

Ejemplo:

```
ATM-I/F 0 QoS Config> se qos
Desired QoS Class for Data Direct VCCs [0]? 1
ATM-I/F 0 QoS Config>
```

sustained-cell-rate

Establece la velocidad sostenida de célula que se desea para los VCC de datos directos. Consulte el apartado “Velocidad sostenida de célula (sustained-cell-rate)” en la página 224 para obtener una descripción más detallada de este parámetro.

Valores válidos:

Un valor entero en el rango de 0 al mínimo de max-reserved-bandwidth y peak-cell-rate, especificado en kbps

Valor por omisión

Ninguno

Ejemplo:

```
ATM-I/F 0 QoS Config> se sus
Data-Direct VCC Sustained Cell Rate in Kbps [1]? 10000
ATM-I/F 0 QoS Config>
```

traffic-type

Establece el tráfico que se desea para los VCC directos de datos. Consulte el apartado “Tipo de tráfico (traffic-type)” en la página 223 para obtener una descripción más detallada de este parámetro.

Valores válidos:

best_effort o reserved_bandwidth

Valor por omisión:

best_effort.

Ejemplo:

```
ATM-I/F 0 QoS> set traffic-type
  Choose from:
     (0): Best-Effort
     (1): Reserved Bandwidth
  Traffic Type of VCCs [1]? 0
ATM-I/F 0 QoS>
```

Remove

Utilice el mandato **remove** para eliminar la configuración de QoS de esta Interfaz ATM.

Sintaxis:

r**emove**

Ejemplo:

```
ATM-I/F 0 QoS> remove
WARNING: This option deletes the QoS configuration.
         To re-configure use any of the SET options.
Should the ATM Interface QoS configuration be deleted? [No]: yes
Deleted QoS SRAM record successfully
ATM-I/F 0 QoS>
```

Acceso a los mandatos de supervisión de QoS

Utilice el mandato **feature** desde el proceso GWCON para acceder a los mandatos de supervisión de Calidad de los servicios. Entre **feature** seguido del número de característica (6) o nombre abreviado (QoS). Por ejemplo:

```
+feature qos
Quality of Service (QoS) - User Monitoring
QoS+
```

Cuando haya accedido al indicador de mandatos de supervisión de QoS, puede seleccionar la supervisión de un Cliente LE particular. Para volver al indicador de mandatos GWCON en cualquier momento, entre el mandato exit en el indicador de mandatos de supervisión de QoS.

Alternativamente, puede acceder a la Supervisión de QoS de un Cliente LE del modo siguiente:

1. En el indicador de mandatos GWCON (+), entre el mandato network y el número de interfaz de Cliente LE.
2. En el indicador de mandatos de supervisión de Cliente LE, entre **qos-information**.

   Ejemplo:

   ```
   +network 3
   ATM Emulated LAN Monitoring
   LEC+qos information
   LE Client QoS Monitoring
   LEC 3 QoS+
   ```

Mandatos de supervisión de Calidad de los servicios

Esta sección resume los mandatos de supervisión de QoS. Entre estos mandatos en el indicador de mandatos QoS+.

Tabla 35. Resumen de los mandatos de supervisión de Calidad de los servicios (QoS)	
Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
le-client	Le conduce al indicador de mandatos `LE Client QoS console +` para el cliente LE seleccionado.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Mandatos de supervisión de QoS de Cliente LE

Esta sección resume los mandatos de supervisión de QoS de Cliente LE. Entre los mandatos desde el indicador de mandatos `LEC num QoS+`.

Tabla 36. Resumen de los mandatos de supervisión de QoS de Cliente LE	
Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
List	Lista la información de QoS de Cliente LE actual. Las opciones incluyen: parámetros de configuración, TLV, VCC y estadísticas.
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 relacionada con QoS de este Cliente LE.

Sintaxis:

list configuration-parameters

data-direct-VCCs (Detailed Information)

statistics

tlv-information

vcc-information

configuration-parameters

Lista los parámetros de configuración de QoS. Dado que se pueden configurar parámetros para un Cliente LE, Interfaz ATM o ELAN, estos parámetros se visualizan junto con un conjunto resuelto de parámetros utilizados por el Cliente LE.

le-client Los parámetros configurados para este Cliente LE que se obtienen de los registros de la SRAM. Si los registros de la SRAM contienen un conjunto no válido de parámetros, esta columna no visualizará ningún valor de parámetro.

ATM Interface
Los parámetros configurados para la Interfaz ATM utilizados por este Cliente LE. Estos parámetros se obtienen de los registros de la SRAM local. Si los registros de la SRAM contienen un conjunto no válido de parámetros, esta columna no visualizará ningún valor de parámetro.

From LECS
Los parámetros recibidos por este Cliente LE desde el Servidor de configuración de LE. Los parámetros se reciben como TLV individuales en el mensaje de control LE_CONFIGURE_RESPONSE.

used El conjunto resuelto de parámetros de tráfico utilizados por sus VCC directos de datos. Si ninguna de las entidades se ha configurado con parámetros de QoS, los parámetros USED (utilizados) representan los parámetros por omisión. Si se configuran parámetros para como mínimo una entidad, se resuelven de la siguiente forma:

- Si solamente el Cliente LE o la Interfaz ATM se ha configurado con parámetros y accept-parms-from-lecs es FALSE o no se han recibido parámetros desde el LECS, se utilizan los parámetros de Cliente LE o de Interfaz ATM configurados.
- Si tanto el Cliente LE como la Interfaz ATM tienen parámetros configurados, se utilizan los parámetros de Cliente LE.
- Si accept-params-from-lecs es TRUE y se han recibido parámetros desde el LECS, los parámetros de Cliente LE (o los valores por omisión si no se ha configurado el Cliente LE) se combinan con los recibidos desde el LECS para formar un conjunto completo de los seis primeros parámetros de QoS que se describen en “Parámetros de configuración de QoS” en la página 222.
- Si el conjunto de los seis primeros parámetros de QoS que se describe en “Parámetros de configuración de QoS” en la página 222 contiene una combinación no válida, los parámetros del LECS se rechazan. Tenga en cuenta que los dos distintivos negotiate-qos y validate-pcr-of-best-effort-vccs se validan independientemente.

Ejemplo:

```
LEC 1 QoS+ list configuration parameters


                ATM LEC Configured QoS  Parameters
                ==================================

      QoS                                        |    LEC      ATM-IF    FROM

   PARAMETER                             USED    |    SRAM     SRAM      LECS

 ------------------------------------------------------------------------------
 Max Reserved Bandwidth (cells/sec) :    23584   |    23584        0     none
                        (Kbits/sec) :    10000   |    10000        0     none
 VCC Type ......................... :   ResvBW   |   ResvBW   BstEft        0
 Peak Cell Rate ........(cells/sec) :    18867   |    18867   365566   365566
                        (Kbits/sec) :     8000   |     8000   155000   155000
 Sustained Cell Rate ...(cells/sec) :    18867   |    18867   365566     none
                        (Kbits/sec) :     8000   |     8000   155000     none
 QoS Class ........................ :        4   |        4        0     none
 Max Burst Size ............(cells) :       95   |       95        0     none
                             (frames) :        1   |        1        0     none
 Validate PCR of Best-Effort VCCs . :       no   |       no      n/a     none
 Enable QoS Negotiation ........... :      yes   |      yes      n/a     none
 Accept QoS Parameters from LECS .. :      yes   |      yes      n/a      n/a
 ------------------------------------------------------------------------------
(BstEft = Best Effort, ResvBW = Reserved Bandwidth)
(n/a = not applicable, none = no value is specified)

LEC 1 QoS+
```

data-direct-vccs (Detailed Information)

Esta opción lista la información de VCC directo de datos de este Cliente LE. También se lista información similar utilizando **list vcc-information**.

Ejemplo:

```
LEC 1 QoS+ list data direct vccs

          LEC Data Direct VCCs - QoS Information
          ======================================

Conn Handle = 80, VPI = 0, VCI = 546
        Connection Type = RETRIED CONNECTION PARAMETERS
          TrafficType    = BEST EFFORT VCC
          PCR            = 58962 (25 Mbps)
          SCR            = 58962 (25 Mbps)
          QoS Class      = 0
          Max Burst Size = 0

Conn Handle = 78, VPI = 0, VCI = 544
        Connection Type = PARAMETERS SET BY DESTINATION
          TrafficType    = RESERVED BANDWIDTH VCC
          PCR            = 58962 (25 Mbps)
          SCR            = 16509 (7 Mbps)
          QoS Class      = 1
          Max Burst Size = 95

LEC 1 QoS+
```

statistics Se mantienen contadores para las estadísticas siguientes:

Conexiones de QoS satisfactorias

Número de conexiones RESERVED-BANDWIDTH establecidas por el Cliente LE.

Conexiones de mayor eficacia satisfactorias

Número de conexiones BEST-EFFORT establecidas por el Cliente LE.

Conexiones de QoS que han fallado

Número de peticiones de conexiones RESERVED-BANDWIDTH realizadas por el Cliente LE que han fallado.

Conexiones de mayor eficacia que han fallado
Número de peticiones de conexiones BEST-EFFORT realizadas por el Cliente LE que ha fallado.

Negociación de QoS aplicada
Número de veces que se ha aplicado la ampliación de negociación de QoS. Los parámetros se negocian si el Cliente LE recibe los parámetros del Cliente LE de destino en un mensaje de control LE_ARP_RESPONSE.

Propuesta de PCR (IBM) aplicada
Número de veces que se ha aplicado la Propuesta de Velocidad mayor de célula de IBM. Esta propuesta recomienda utilizar parámetros de velocidad específicos si se señaliza a 100 Mbps o a 155 Mbps para conexiones BEST-EFFORT. Esto permite que otros productos IBM participantes (por ejemplo, adaptadores ATM de 25 Mbps) rechacen una conexión basada en las velocidades mayores de célula señaladas.

Conexiones de QoS aceptadas
Número de conexiones RESERVED-BANDWIDTH aceptadas por este Cliente LE.

Conexiones de mayor eficacia aceptadas
Número de conexiones BEST-EFFORT aceptadas por este Cliente LE.

Conexiones de QoS rechazadas
Número de peticiones de conexiones RESERVED-BANDWIDTH recibidas por este Cliente LE que se han rechazado.

Conexiones de mayor eficacia rechazadas
Número de peticiones de conexión BEST-EFFORT recibidas por este Cliente LE que se han rechazado.

Rechazadas debido a validación de PCR
Número de conexiones BEST-EFFORT rechazadas por el Cliente LE debido a la validación de Peak Cell Rate cuando el parámetro validate-pcr-of-best-effort-vccs es TRUE.

Ejemplo:

```
LEC 1 QoS+ li stat

QoS Statistics: of Data Direct Calls Placed by the LEC
------------------------------------------------------
    Successful QoS Connections          = 0
    Successful Best-Effort Connections  = 1
    Failed QoS Connections              = 1
    Failed Best-Effort Connections      = 1
    Qos Negotiation Applied             = 0
    PCR Proposal (IBM) Applied          = 0

QoS Statistics: of Data Direct Calls Received by the LEC
--------------------------------------------------------
    QoS Connections Accepted            = 1
    Best-Effort Connections Accepted    = 0
    QoS Connections Rejected            = 0
    Best-Effort Connections Rejected    = 0
    Rejected due to PCR Validation      = 0

LEC 1 QoS+
```

tlv-information

Lista TLV de Información de tráfico de IBM que este Cliente LE ha registrado con el Servidor LE. TLV sólo se registra si el Cliente LE participa en la Negociación de QoS.

Ejemplo:

```
LEC 1 QoS+ list tlv

  Traffic Info TLV of the LEC (registered with the LES)
  =====================================================
    TLV Type .........................= 268458498
    TLV Length .......................= 24
    TLV Value:
           Maximum Reserved Bandwidth = 23584 cells/sec (10 Mbps)
           Data Direct VCC Type...... = RESERVED BANDWIDTH VCC
           Data Direct VCC PCR....... = 18867 cells/sec (8 Mbps)
           Data Direct VCC SCR....... = 18867 cells/sec (8 Mbps)
           Data Direct VCC QoS Class  = 4
           Maximum Burst Size         = 95 cells (1 frames)

LEC 1 QoS+
```

vcc-information

Lista todos los VCC activos del Cliente LE. La información incluye los parámetros de tráfico de las conexiones. Para conexiones BEST-EFFORT, Sustained Cell Rate se visualiza para que sea igual que Peak Cell Rate, QoS Class y Maximum Burst Size se visualizan como 0.

Las entradas del Descriptor de parámetros son las siguientes:

SrcParms

Parámetros de una conexión establecida por este Cliente LE.

DestParms

Parámetros de una conexión recibida por este Cliente LE.

NegoParms

Parámetros de una conexión establecida por el Cliente LE para los cuales se ha utilizado Negociación de QoS.

RetryParms

Parámetros de una conexión establecidos por este Cliente LE después de haber fallado como mínimo una vez.

Ejemplo:

```
LEC 1 QoS+ li vcc

                          LEC VCC Table
                          =============

                                                                        Burst
Conn   Conn              Conn          VCC    PCR    SCR   QoS   Size    Parameters
Index  Handle VPI   VCI   Type  Status  Type  (kbps) (kbps) Class (cells) Descriptor
-------------------------------------------------------------------------------------
   2)     69    0   535  Cntrl  Ready  BstEft 155000 155000    0      0   SrcParms
   3)     71    0   537  Cntrl  Ready  BstEft      0      0    0      0   DestParms
   4)     72    0   538  Mcast  Ready  BstEft 155000 155000    0      0   SrcParms
   5)     74    0   540  Mcast  Ready  BstEft      0      0    0      0   DestParms
   6)     78    0   544  Data   Ready  ResvBW  25000   7000    1     95   DestParms

LEC 1 QoS+
```

Soporte de reconfiguración dinámica de QoS

Esta sección describe la reconfiguración dinámica (DR) en lo que afecta a los mandatos de Talk 6 y Talk 5.

Delete interface de CONFIG (Talk 6)

La Calidad de los servicios (QoS) soporta el mandato de CONFIG (Talk 6) **delete interface** con la consideración siguiente:

QoS se configura para una interfaz LEC o ATM específica. Los cambios de QoS entran en vigor cuando se emite el mandato en dicha interfaz en concreto.

Activate interface de GWCON (Talk 5)

La Calidad de los servicios (QoS) soporta el mandato de GWCON (Talk 5) **activate interface** con la consideración siguiente:

QoS se configura para una interfaz LEC o ATM específica. Los cambios de QoS entran en vigor cuando se emite el mandato en dicha interfaz en concreto.

El mandato de GWCON (Talk 5) **activate interface** soporta todos los mandatos específicos de interfaz de Calidad de los servicios (QoS).

Reset interface de GWCON (Talk 5)

La Calidad de los servicios (QoS) soporta el mandato de GWCON (Talk 5) **reset interface** con la consideración siguiente:

QoS se configura para una interfaz LEC o ATM específica. Los cambios de QoS entran en vigor cuando se emite el mandato en dicha interfaz en concreto.

El mandato de GWCON (Talk 5) **reset interface** soporta todos los mandatos específicos de interfaz de de Calidad de los servicios (QoS).

Mandatos de cambio temporal de GWCON (Talk 5)

La Calidad de los servicios (QoS) soporta los mandatos de GWCON siguientes que cambian temporalmente el estado operativo del dispositivo. Estos cambios se pierden siempre que se vuelve a cargar o se reinicia el dispositivo o se ejecuta cualquier mandato reconfigurable dinámicamente.

Todas las modificaciones de QoS en Talk 5 efectúan un cambio operativo inmediato cuando se emite el mandato en la interfaz para la que está configurado.

Utilización de la característica de política

Este capítulo describe cómo interactúa la característica de política con otros componentes de software de direccionador para tomar decisiones acerca de la QoS, la seguridad o ambas. También describe los conceptos y mandatos de configuración específicos relacionados con la característica de política. La característica de política también permite utilizar un servidor de directorios LDAP como depósito central para información de política. Los conceptos y pasos de configuración necesarios para habilitar las funciones de LDAP también se describen en este capítulo. Los temas siguientes explican estos conceptos, el modo cómo los direccionadores imponen las políticas y también se proporcionan ejemplos.

Visión general de la política

La característica de política facilita la gestión de tráfico IPv4 en una red. Puede configurar políticas para normas de filtro muy simples (excluir o pasar) o para escenarios de QoS y seguridad complejos. La combinación de políticas determina cómo manejan los direccionadores el tráfico IPv4 en una red.

Decisión e imposición de una política

La implantación de una política en esta familia de direccionadores constituye la base para tomar decisiones de política y el medio para imponerlas. A menudo se hace referencia a estos conceptos como punto de decisión de política (PDP) y punto de imposición de política (PEP).

La base de datos de políticas, que reside en la memoria del direccionador está formada por el conjunto de políticas cargadas desde la configuración local y las políticas que se han leído desde LDAP. La base de datos de políticas se crea bajo las condiciones siguientes:

- Nueva carga o reinicio del dispositivo
- Mandato de supervisión **reset database**
- Renovación automática
- Petición de conjunto SNMP

La base de datos de políticas sirve de PDP y está formada por un conjunto de políticas que determinan cómo los componentes relacionados con la característica de política manejan los paquetes. Cuando una política determina una decisión (basada en información como por ejemplo la hora del día, información de paquete de IP e información específica del protocolo, como por ejemplo identificación), la decisión se pasa al componente de imposición (PEP) para llevar a cabo la acción. La Figura 16 en la página 244 muestra la relación entre estos componentes.

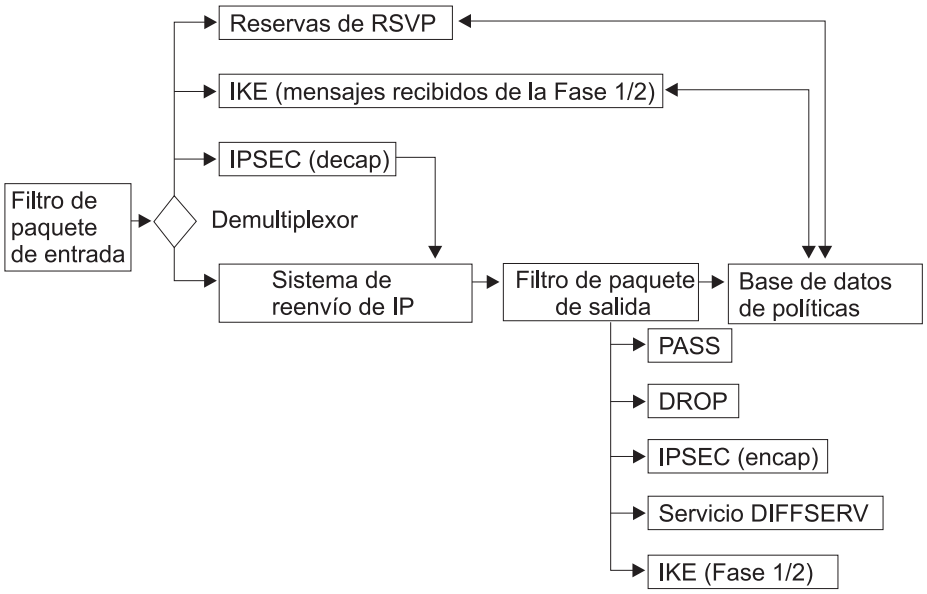


Figura 16. Flujo de paquetes de IP y base de datos de políticas

Decisión de política y flujo de paquetes

Los Paquetes de IP deben pasar el filtro de paquete de entrada para poder llevar a cabo cualquier otra acción. Si el filtro de paquete de entrada tiene normas presentes, es posible que se realice alguna acción en el paquete. Si existe una coincidencia de filtro que excluya el paquete, o no se encuentra ninguna coincidencia en el filtro de paquete de entrada, el paquete se excluye.

Si el paquete pasa el filtro de paquete de entrada, a continuación se somete a un filtro de demultiplexado, que comprueba si el paquete tiene un destino local. Si es así, según el tipo del paquete se pasa a otros módulos. Estos módulos pueden ser IPSec, IKE, RSVP u otros. Si el paquete tiene un destino local para IPSec, IKE o RSVP, estos módulos pueden consultar la base de datos de políticas para determinar la acción que debe realizarse.

Si el paquete no tiene un destino local, se pasa al sistema de reenvío y se toma una decisión de direccionamiento. Si la decisión de direccionamiento no excluye el paquete (el Direccionamiento basado en la política puede decidir excluir el paquete), el paquete pasa al filtro de paquete de salida. Si hay presentes normas de filtro en el paquete de salida, el paquete puede someterse a conversión de dirección (NAT), puede ser aceptado o puede excluirse. Si no existen normas de filtro, el paquete es aceptado. Si existen normas de filtro y no se encuentra ninguna coincidencia el paquete se excluye. Si el paquete pasa el filtro de Paquete de salida, el Sistema de IP consulta la base de datos de políticas para determinar si debe aplicarse alguna otra acción en este paquete.

Nota: Si los filtros de paquete de entrada y de salida están habilitados para una interfaz (o varias interfaces) y se espera que los paquetes que debe controlar la base de datos de política atraviesen estas interfaces, debe haber presente una norma de filtro que incluya estos paquetes en los filtros de paquete de entrada y de salida para que no se excluyan los paquetes antes de consultar la base de datos de políticas. Una sugerencia es utilizar la base de datos de políticas para configurar todas las normas de aceptar/excluir y no utilizar filtros de paquete.

Consultas de política de IP

Cuando el sistema de reenvío de IP consulta la base de datos de políticas, se pueden devolver los siguientes tipos combinaciones de decisiones:

- No se ha encontrado ninguna coincidencia—pasar el paquete
- Se ha encontrado una coincidencia—excluir el paquete
- Se ha encontrado una coincidencia—aceptar el paquete
- Se ha encontrado una coincidencia—asegurar el paquete en túnel x manual de IPSec
- Se ha encontrado una coincidencia—asegurar el paquete en túnel x IPSec negociado de IKE
- Se ha encontrado una coincidencia—iniciar negociaciones de ISAKMP para la Fase 1 y 2, excluir paquete
- Se ha encontrado una coincidencia—proporcionar DiffServ QoS x, asegurar el paquete con IPSec

Consultas de política de IPSec

Si IPSec recibe un paquete, primero debe eliminar la encapsulación del paquete y después debe decidir si el paquete ha llegado al túnel de IPSec correcto (a menudo se hace referencia a este proceso como comprobación de conformidad). Para ello consulta la base de datos de políticas. La base de datos de políticas puede devolver los siguientes tipos de decisiones para esta consulta:

- Comprobación de conformidad pasada—reenviar el paquete
- Comprobación de conformidad fallada—excluir el paquete

Decisiones de política de IKE

IKE puede consultar la base de datos de políticas y se pueden devolver las decisiones de política de IP de *Fase 1* que se muestran en la Tabla 37.

Tabla 37. Consultas de Fase 1 de IKE y decisiones devueltas

Tipo de consulta	Decisión
Mensaje 1 (Modalidad principal)	No se ha encontrado ninguna coincidencia, excluir paquete
Mensaje 1 (Modalidad principal)	Se ha encontrado una coincidencia, negociar con política x de Fase 1
Mensaje 5 (Modalidad principal)	No se ha encontrado ninguna coincidencia, detener negociaciones con similar, excluir paquete
Mensaje 5 (Modalidad principal)	No se ha encontrado ninguna coincidencia, detener negociaciones con similar, excluir paquete
Mensaje 5 (Modalidad principal)	Se ha encontrado una coincidencia, política x coincidente, finalizar Fase 1
Mensaje 5 (Modalidad principal)	Se ha encontrado una coincidencia, política y coincidente, detener Fase 1 actual e iniciar Fase 1 nueva con política nueva
Mensaje 1 (Modalidad agresiva)	No se ha encontrado ninguna coincidencia, excluir paquete
Mensaje 1 (Modalidad agresiva)	Se ha encontrado una coincidencia, política x coincidente

IKE puede consultar la base de datos de políticas y se pueden devolver las decisiones de política de IP de *Fase 2* que se muestran en la Tabla 38 en la página 246.

Tabla 38. Consultas de Fase 2 de IKE y decisiones devueltas

Tipo de consulta	Decisión
Mensaje 2 (emisor de respuesta)	No se ha encontrado ninguna coincidencia, excluir paquete
Mensaje 2 (emisor de respuesta)	Se ha encontrado una coincidencia, negociar con política x

Decisiones de política de RSVP

Si un paquete es un mensaje de control RSVP, RSVP consulta la base de datos de políticas para determinar si debe aceptar o denegar la reserva. Si se acepta, RSVP determina qué atributos de la reserva deben limitarse, basándose en la política. Las políticas de la base de datos pueden controlar la duración de la reserva, la cantidad de ancho de banda que debe asignarse y el retardo mínimo que debe garantizarse.

Objetos de política

Una política está formada por un perfil, que contiene un conjunto de atributos de paquete en los que basar las decisiones, las acciones que deben llevarse a cabo si los atributos de un paquete coinciden con los del perfil y el período de validez durante el cual se toman las decisiones y qué acciones se imponen. Estos elementos se explican más detalladamente en los temas siguientes:

Las partes que forman una política son objetos con nombres diferentes. Los objetos de política pueden hacer referencia entre ellos y como grupo de elementos relacionados forman una política. Separando la información de configuración en objetos diferentes individuales, puede volver a utilizar muchos de ellos en varias definiciones de política, con lo cual se ahorra tiempo y se reducen los esfuerzos de mantenimiento. Los objetos de política individuales se explican con más detalle en los temas siguientes.

Política

El objeto política describe qué condiciones deben comprobarse y si se encuentran coincidencias en la comprobación, qué acciones deben imponerse. La política crea referencias con nombre para el período de validez y el perfil. Para que la política sea válida, son necesarias estas referencias. La política también debe crear una referencia con nombre para una o más de las acciones siguientes: un objeto de túnel de clave manual de IPSec, una acción de IPSec, una acción de ISAKMP, una acción de RSVP o una acción de DiffServ. Las combinaciones válidas son:

- Túnel de clave manual de IPSec
- Acción de IPSec para excluir paquetes
- Acción de IPSec para aceptar paquetes (sin seguridad)
- Acción de IPSec para asegurar paquetes, acción de ISAKMP
- Acción de DiffServ (excluir)
- Túnel de clave manual de IPSec y acción de DiffServ (aceptar)

- Acción de IPSec para asegurar paquetes, acción de ISAKMP, acción de DiffServ (aceptar)
- Acción de RSVP
- Acción de RSVP y acción de DiffServ (aceptar)

Nota: En estas combinaciones un túnel manual de IPSec no puede existir en la misma definición de política que una acción de IPSec (túnel de IPSec negociado por IKE) y una acción de RSVP no debe estar asociada con ningún tipo de acción de IPSec. Si una acción de IPSec para asegurar paquetes está asociada con una política, también debe asociar una acción ISAKMP con la política.

Cada política también tiene un número de prioridad asociado (cuanto más alto es el número en el atributo de prioridad, más alta es la prioridad). La prioridad determina si esta política tiene prioridad sobre otra política. Generalmente, sólo debe definirse el número de prioridad si existen dos o más perfiles de políticas que entren en conflicto entre ellos de algún modo. La política con el perfil más específico debe tener la prioridad más alta. Por ejemplo, supongamos que una política especifica que el tráfico desde la subred A a la subred B debe asegurarse con IPSec (DES) y otra política especifica que el tráfico desde el punto a′ (un sistema principal particular dentro de la subred A) hasta la subred B debe asegurarse con IPSec (3DES). La política más específica (de a′ a B) debe tener una prioridad más alta que la política con de A a B.

Es una buena idea designar valores de prioridad iniciales formados por 5 o más dígitos por separado para dejar espacio para especificar valores de prioridad adicionales para políticas que entren en conflicto más adelante. Cada política también tiene habilitado un atributo, que determina si la política debe habilitarse cuando se carga en la base de datos de políticas. Si se encuentra una coincidencia de política durante una búsqueda en la base de datos de políticas pero la política está inhabilitada, se impone la política específica más cercana.

Puede iniciar una comprobación de coherencia y conflictos dentro de una política individual y entre todas las políticas definidas utilizando el mandato de supervisión **check-consistency**. Este mandato no intenta resolver problemas, pero los identifica para que se pueda realizar la acción correctiva. Consulte el apartado “Mandatos de supervisión de política” en la página 313 para obtener detalles sobre el mandato.

Perfil

El perfil determina qué información debe utilizarse para seleccionar una política determinada. El perfil consta de información de dirección de origen y de dirección de destino, y de información de puerto de origen y de destino.

Nota: Cuando se definen políticas para IPSec/ISAKMP, cada pasarela que proporciona la seguridad debe tener una política para definir la asociación de seguridad. El perfil en cada pasarela debe asociar el origen con el destino y el destino con el origen. El perfil para una política de IPSec especifica la dirección de origen como el tráfico que debe encapsularse en el túnel y la dirección de destino debe estar en el extremo remoto del túnel.

El perfil también puede seleccionar basándose en el byte de tipo-de-servicio (TOS) y la dirección IP de entrada y de salida. Por omisión, el paquete recibido en cualquier interfaz de entrada y que sale de cualquier interfaz de salida se comprueba

con los otros selectores. En algunos casos, puede que sea necesaria la flexibilidad para especificar exactamente las interfaces a las que debe llegar el paquete y la interfaz de la que debe salir el paquete. Para ello debe añadir objetos de par de interfaces y asociar el nombre de grupo para los objetos de par de interfaces con el perfil. Para asignar objetos de par de interfaces a un grupo proporcióneles el mismo nombre. Esto le permite especificar combinaciones como por ejemplo (cualquier paquete que llegue a IPaddrX y salga de cualquier interfaz *O* cualquier paquete que llegue a cualquier interfaz y salga de IPaddrX). Esto es especialmente útil si define una norma de exclusión general para una interfaz pública.

Par de interfaces: Identifica la interfaz de entrada y la interfaz de salida. Especifique las direcciones IP para la interfaz para esta selección. Un valor de 255.255.255.255 implica cualquier interfaz.

Si desea utilizar el perfil para seleccionar una política de IPSec/ISAKMP, tiene la opción de especificar el ID local que debe enviarse durante la Fase 1 y la lista de ID remotos aceptables durante las negociaciones de la Fase 1. Por omisión, el ID local es el punto final del túnel local para el tráfico de IPSec/IKE y la lista de ID remotos es *Cualquiera*. Opcionalmente, puede especificar el nombre de dominio completamente calificado (FQDN), el FQDN de usuario e ID de clave. Normalmente esto es suficiente porque todas las negociaciones de la Fase 1 de ISAKMP se autentifican con certificados públicos o claves previamente compartidas. Sin embargo, en algunas situaciones de acceso remoto en las que la política no es comodín para las direcciones de destino, puede que sea aconsejable especificar una lista de usuarios de acceso remoto a las que debe permitirse acceder a los recursos de la red.

Estos usuarios aún se autentifican con los métodos de autentificación de ISAKMP normales, pero la base de datos de políticas realiza un paso de autentificación adicional que asegura que el ID local que envía el similar remoto coincide con uno de los ID especificados en el Grupo de usuarios remotos del perfil de la política. Esto es necesario si una autorización de certificado (CA) pública administra certificados al público general y el administrador de la red sólo desea que tenga acceso un conjunto específico de estos usuarios (por ejemplo, empleados de la empresa). El grupo de usuarios remotos está formado por una lista de usuarios que pertenecen al mismo grupo. Estos usuarios se entran añadiendo uno o más *USUARIO*s. Un grupo de usuarios se puede crear haciendo que el nombre de grupo sea el mismo para cada usuario. A continuación, este grupo se puede asociar opcionalmente a un perfil.

Período de validez

El período de validez especifica la duración de la política—el año, los meses del año, los días de la semana y las horas del día que es válida. Esta flexibilidad permite que el administrador de la red pueda especificar cuándo es válida una política, por ejemplo “todo el tiempo” o “sólo este año, durante los meses de enero, febrero y marzo, de lunes a viernes, de 9 AM a 5 PM.” Cuando una política de la base de datos de políticas deja de ser válida, se impone la siguiente política más específica. De este modo se puede definir una política que especifique de lunes a viernes, de 9 am a 5 am, para asegurar todo el tráfico de la subred A a la subred B y que en cualquier otro momento elimine todo el tráfico de la subred A a la subred B. En este caso, la primera política debe tener una prioridad más alta (especificada al entrar el mandato de supervisión **add policy**).

Acción de DiffServ

La acción de DiffServ describe la calidad del servicio que debe proporcionarse a los paquetes que coinciden con una política que especifica una acción de DiffServ. Puede configurar la acción de DiffServ para excluir paquetes. También puede utilizar la acción de DiffServ para correlacionar paquetes con calidades de los servicios relativas. Puede configurar el ancho de banda asignado como un porcentaje del ancho de banda de salida o como un valor absoluto en kbps. Debe especificar si la cola asegurada (AF)/de mayor eficacia o la cola de primera calidad (EF) debe proporcionar la asignación de ancho de banda. Para obtener más información sobre estas colas y cómo definirlas, consulte “Utilización de la característica Servicios diferenciados” en la página 383 y “Configuración y supervisión de la característica Servicios diferenciados” en la página 393.

La acción de DiffServ también especifica cómo marcar el elemento de código DS (byte TOS) para el tráfico EF y AF antes de que se envíe en la interfaz de salida. El tráfico EF y AF se mide y el tráfico que no se ajusta se vigila. El tráfico EF que no se ajusta se elimina y, opcionalmente, el byte DS del tráfico AF que no se ajusta se vuelve a marcar utilizando el esquema TCM (Three Color Marker) (Marcador de tres colores). El marcado, la medición y la vigilancia del paquete permiten al direccionador central de una red habilitada para DiffServ clasificar el paquete basándose en elementos de código DS y controlar la congestión eliminando primero el tráfico que no se ajusta. Esto ayuda a obtener un mayor rendimiento y un retardo menor para el tráfico preferido en las redes habilitadas para DiffServ.

Acción de RSVP

La acción de RSVP especifica si deben permitirse o denegarse flujos de RSVP si se produce una reserva de RSVP y la petición de reserva coincide con el perfil de la política. Si desea que se permita la reserva, la acción de RSVP también indica la duración permitida de la reserva, el ancho de banda permitido y, opcionalmente, una referencia a una acción de DiffServ. La referencia a la acción de DiffServ permite que RSVP determine cómo marcar el byte de TOS antes de que el paquete salga del direccionador. Esto es útil cuando los paquetes pasan de una red RSVP a una red DiffServ. RSVP puede proporcionar la QoS hasta el límite de RSVP y luego marcar el byte TOS apropiadamente de modo que la red DiffServ pueda aplicar el ancho de banda correcto.

Acción de IPSec

La acción de IPSec puede especificar una acción de excluir, aceptar o asegurar. Si la acción es excluir, se excluyen todos los paquetes que coinciden con esta política. Si la acción es aceptar sin seguridad, se aceptan todos los paquetes libres de sospecha. Si la acción es aceptar con seguridad, se aseguran todos los paquetes mediante la asociación de seguridad (SA) especificada por esta acción. La acción de IPSec también contiene las direcciones IP de los puntos finales del túnel para el túnel de IPSec y las SA de IKE.

Los atributos de la SA los determinan las propuestas de IPSec a las que hace referencia la acción de IPSec. La acción de IPSec puede especificar múltiples propuestas de IPSec que se envían y comparan según el orden con el que se han especificado. El hecho de tener múltiples propuestas en una acción de IPSec permite que la configuración contenga todas las combinaciones aceptables de seguridad, reduciendo de este modo el número de no coincidencias de configuración potenciales entre pasarelas VPN.

Propuesta de IPSec

La propuesta de IPSec contiene la información sobre qué ESP, AH, (o ambos) convertir para proponer o comparar durante las negociaciones de ISAKMP de la Fase 2. Si necesita un secreto de reenvío perfecto (un cálculo Diffie Hellman reciente), la propuesta de IPSec identifica qué grupo DH debe utilizarse. Las conversiones a las que hace referencia la propuesta de IPSec se envían o se comprueban según el orden con el que se han especificado. La primera conversión de ESP o AH de la lista debe ser la más apropiada para utilizar. Si hay más de una conversión en la lista, cada una se compara con la lista de transformaciones del similar para encontrar una coincidencia. Si ninguna de las conversiones configuradas coinciden con la lista del similar, la negociación falla. La propuesta de IPSec puede listar una combinación de conversiones AH y ESP, pero las únicas combinaciones válidas son:

- Lista de sólo AH (modalidad de túnel o transporte)
- Lista de sólo ESP (modalidad de túnel o transporte)
- Lista de AH (modalidad de transporte) y lista de ESP (modalidad de túnel)

Conversión de IPSec

Los atributos de la conversión de IPSec contienen información sobre los parámetros de cifrado y autentificación de IPSec y también especifican con qué frecuencia se renuevan las claves. La conversión es AH (sólo autentificación) o ESP (cifrado, autentificación o ambos) y se puede configurar para funcionar en modalidad de túnel o de transporte.

Acción de ISAKMP

La acción de ISAKMP especifica la información de gestión de clave para la Fase 1. Especifica si las negociaciones de la Fase 1 deben iniciarse en modalidad principal (proporciona protección de identidad) o en modalidad agresiva. También especifica si la asociación de seguridad de la Fase 1 debe negociarse al arrancar el dispositivo o a petición. La acción de ISAKMP también debe hacer referencia a una o más propuestas de ISAKMP. La primera referencia debe ser la propuesta de ISAKMP más aceptable.

Propuesta de ISAKMP

La propuesta de ISAKMP especifica los atributos de cifrado y autentificación de la asociación de seguridad de la Fase 1. También especifica qué grupo Diffie Hellman debe utilizarse para generar las claves y la duración de la asociación de seguridad de la Fase 1. Debe seleccionar el método de autentificación en la propuesta de ISAKMP. Puede ser clave previamente compartida o modalidad de certificado.

Usuario

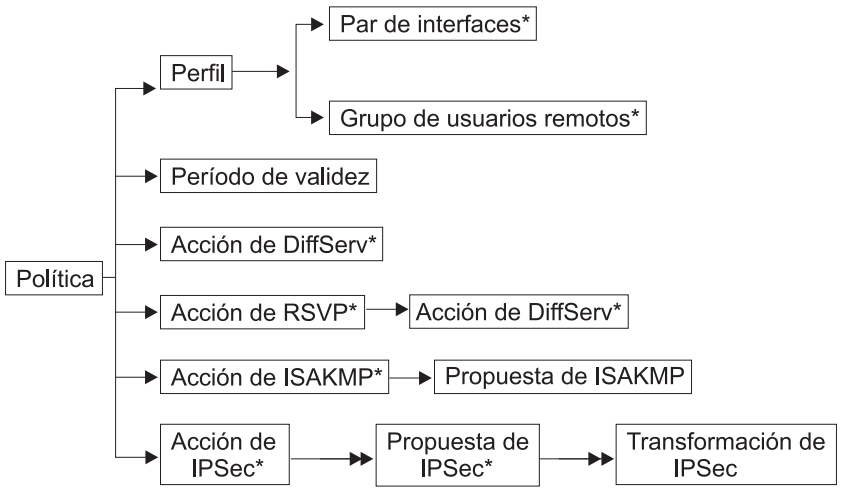
Debe configurar un USER (USUARIO) para cualquier política que utilice una negociación de ISAKMP con clave previamente compartida como método de autentificación. La configuración de USER identifica la clave previamente compartida que debe utilizarse para el similar de ISAKMP. El objeto de usuario contiene la información de identificación para un similar ISAKMP remoto, es decir dirección IP, FQDN, FQDN de usuario o ID de clave, y qué método de usuario desea utilizar para la autentificación. Puede seleccionar clave previamente compartida o modalidad de certificado. Si selecciona clave previamente compartida, también debe especificar si la clave previamente compartida debe entrarse en ASCII o hexadecimal, y el valor de la clave. Los USERs (USUARIOSs) se pueden agrupar asignándolos al mismo nombre de grupo. A continuación, este grupo se puede

asociar opcionalmente con un perfil de la política para llevar a cabo una búsqueda de política más estricta para la Fase 1.

Túnel de clave manual de IPSec

El túnel de clave manual de IPSec es una configuración estática de los parámetros de cifrado y autentificación. No se lleva a cabo ninguna negociación para el túnel de modo que los similares deben tener exactamente la misma configuración. De hecho las claves se entran como parte de esta configuración y deben coincidir en ambos extremos del túnel. Dado que no se lleva a cabo ninguna negociación, las claves no se renuevan nunca. Para obtener más información sobre túneles de clave manual de IPSec, consulte la descripción de la característica IPSec en “Utilización de Seguridad de IP” en la página 323.

La Figura 17 muestra la relación entre los objetos de configuración de política.



Notas:

1. El → indica una sola referencia.
2. El →→ indica una referencia múltiple.
3. El * indica una referencia opcional.
4. En una política de seguridad para ISAKMP/IPSec, el perfil de tráfico define el tráfico que entra en el túnel de seguridad.

Figura 17. Relación de los objetos de configuración de política

Interacción entre LDAP y la base de datos de políticas

Esta familia de direccionadores permite que un servidor de Lightweight Directory Access Protocol (LDAP) sea el depósito de la información de políticas (la base de datos de políticas). LDAP es un protocolo que permite buscar y efectuar modificaciones en un servidor de directorios. LDAP es una versión ligera del estándar X.500. Los direccionadores soportan la capacidad de buscar información (no modificar) en el servidor de directorios. El agente de búsqueda de política en el direccionador recupera toda la información de política del servidor de directorios específica de dicho dispositivo. Cualquier servidor de LDAP que utilice LDAP Versión 2 ó 3 funciona con la implantación en el direccionador. Una ventaja importante de utilizar un servidor de directorios para almacenar información de políticas de un modo contrario al de los métodos más tradicionales consiste en la capacidad de efectuar un cambio en un lugar y hacer que dicho cambio se aplique más allá

de todos los dispositivos de la red ampliada. Entre los dispositivos se incluyen tanto los dispositivos del dominio administrativo como los dispositivos más allá de los límites públicos.

Por ejemplo, supongamos que tiene una definición de conversión de IPSec que reside en el directorio. Si desea cambiar la política incorporada para el cifrado de DES a 3DES, normalmente haría falta un cambio en cada configuración de dispositivo más allá de cada límite de la red. Si utiliza el directorio para ampliar las políticas, tan solo debe cambiar una conversión de IPSec. A continuación, cada dispositivo con política habilitada de la red necesitaría volver a crear la base de datos. Como otro ejemplo, supongamos que debe cambiar una acción de DiffServ llamada “GoldService” para aumentar el valor de ancho de banda de 40% a 45% de ancho de banda. El servidor de LDAP y la infraestructura de política permiten que estos tipos de cambios de configuración se adapten mucho mejor y reducen las no coincidencias de configuración.

Si es el administrador de la red, también puede aprovechar la capacidad de renovar la base de datos automáticamente a una hora especificada cada día. Seleccione esta opción entrando el mandato **set refresh** de la característica de política. Puede especificar si la renovación está habilitada o no y, si está habilitada, la hora en la que debe renovarse la base de datos. Esta opción es útil para realizar cambios automatizados. Por ejemplo, supongamos que debe añadir una política nueva de modo que el departamento de marketing de los EE.UU. pueda hablar con el departamento de desarrollo del Japón a través de Internet, y que las pasarelas de seguridad son SG1 y SG2. Puede simplemente entrar esta información en el directorio y a medianoche SG1 y SG2 automáticamente recogen este cambio si están habilitadas para renovación automática.

Al leer satisfactoriamente la información de política del servidor LDAP, puede que desee almacenar esta información en la antememoria de un almacenamiento permanente del dispositivo. Una vez realizada esta acción, puede elegir leer siempre la información almacenada en antememoria, eliminando de este modo el tiempo necesario para interrogar al servidor LDAP. También puede elegir que el sistema de búsqueda de política lea la copia almacenada en antememoria si el servidor LDAP no está disponible cuando se solicita una renovación. Para obtener detalles, consulte los mandatos de supervisión **cache-ldap-plcys** y **flush-cache** en el apartado “Mandatos de supervisión de política” en la página 313 y el mandato de configuración **enable ldap** en el apartado “Mandatos de configuración de servidor de políticas de LDAP” en la página 308.

El sistema de búsqueda de política de LDAP le permite especificar el nivel de seguridad que debe utilizarse mientras se crea la base de datos de políticas. Estas opciones de seguridad se definen con el mandato **set default** de la característica de política. Las opciones son:

- Aceptar todo el tráfico durante la búsqueda (valor por omisión).
- Excluir todo el tráfico *excepto* las peticiones y los resultados de búsqueda de política de LDAP.
- Excluir todo el tráfico *excepto* las peticiones y los resultados de peticiones de búsqueda de política de LDAP protegidos por IPSec.

En algunas situaciones cualquiera de las dos primeras opciones es suficiente. Sin embargo, si el tráfico de LDAP va a atravesar la infraestructura pública, debe asegurar y autentificar la información seleccionando la tercera opción. Para ello debe

seleccionar las opciones de autentificación y cifrado de la Fase 1 y la Fase 2. También debe entrar las direcciones IP para los puntos finales del túnel (servidores de LDAP primarios y secundarios). Este túnel de IKE/IPSec de rutina de carga se negociará antes de enviar tráfico de LDAP. Esta característica le permite establecer la configuración que se muestra en la Figura 18.

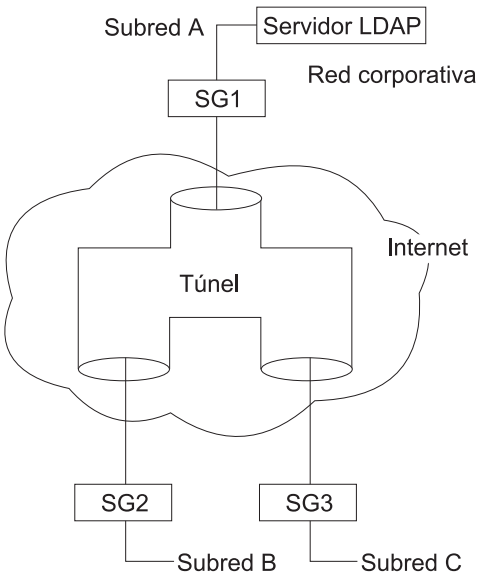


Figura 18. Asegurar el tráfico a través de Internet

Esta figura muestra un servidor de LDAP en la Subred A de la red incorporada. SG1, SG2 y SG3 obtienen sus políticas del servidor de LDAP. Esta búsqueda de política para SG2 y SG3 se produce a través de la Internet y está protegida mediante IPSec.

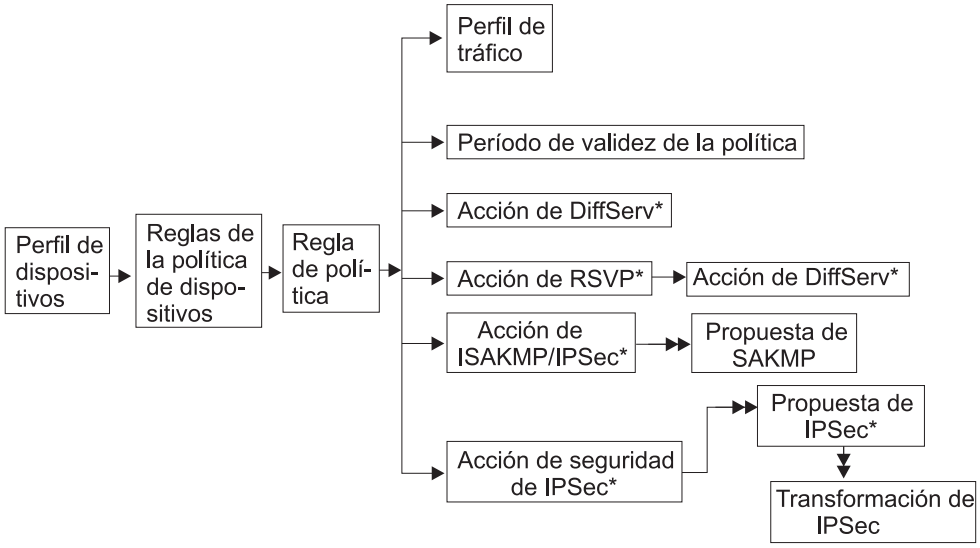
La información de configuración necesaria para que la base de datos de políticas recupere satisfactoriamente las políticas del directorio es la siguiente:

- Dirección IP de servidor primario (también se puede configurar un servidor secundario de reserva)
- Número de puerto en el cual el servidor está a la escucha (Nota: SSL y TLS no están soportados)
- Información de nombre de usuario y contraseña si es necesaria
- Nombre distinguido base del objeto DeviceProfile para este direccionador o clase de direccionadores.
- Información de política por omisión

Una vez entrada esta información de configuración, la próxima vez que se renueva la base de datos de políticas se realiza un intento de interrogar el servidor de directorios para obtener información de política. La base de datos de políticas permite una combinación de políticas configuradas localmente y normas leídas desde el servidor de LDAP. Si se encuentran dos normas que entran en conflicto y tienen la misma prioridad, la norma leída desde la configuración local tiene prioridad sobre la norma leída desde el directorio del servidor.

Esquema de política

El esquema de LDAP es el conjunto de normas e información que forman las definiciones de clase y atributo que determinan el contenido de las entradas del directorio. Generalmente, el esquema de LDAP se escribe con sintaxis ASN1, similar a las MIB de SNMP. El esquema de política que soporta esta familia de direccionadores es una estructura que incluye los esfuerzos preestándares efectuados en IETF. Se basa en el trabajo de seguimiento de estándares que llevan a cabo IPSec y los Grupos de trabajo de política de IETF y el Grupo de trabajo de política de DMTF. El esquema de política coincide exactamente con los objetos de configuración existentes en la característica de política del direccionador. Los archivos de definición del esquema de política y los archivos de configuración del servidor de LDAP pueden encontrarse accediendo al siguiente URL: **http://www.networking.ibm.com/support**. Por favor, seleccione el producto de direccionador que desee y, a continuación, seleccione el enlace *Downloads*. La Figura 19 muestra la estructura global del esquema de política.



Notas:

1. El → indica una sola referencia.
2. El →→ indica una referencia múltiple.
3. El * indica una referencia opcional.
4. En una política de seguridad para ISAKMP/IPSec, el perfil de tráfico define el tráfico que entra en el túnel de seguridad.

Figura 19. Estructura del esquema de política

PerfilDispositivo y NormasPolíticaDispositivo son dos objetos claves en el esquema de política. Permite que el agente de búsqueda de política localice las políticas necesarias para el dispositivo. PerfilDispositivo contiene información sobre la dirección IP administrativa del dispositivo y una referencia a NormasPolíticaDispositivo obligatoria. Puede agrupar dispositivos en un PerfilDispositivo o cada dispositivo de la red puede tener su propio PerfilDispositivo. La elección depende de si más de un dispositivo de la red debe obtener el mismo conjunto de normas. Generalmente, no suele se así para las pasarelas de seguridad puesto que cada pasarela tiene un punto final de túnel diferente. Para dispositivos sólo de QoS, es concebible que todos los dispositivos de un grupo lean el mismo conjunto de políticas.

El objeto NormasPolíticaDispositivo se recupera basándose en el PerfilDispositivo que se obtiene para el dispositivo. Una vez recuperado el objeto NormasPolíticaDispositivo, se puede recuperar la lista de NormasPolítica para dicho dispositivo. Si no se encuentra algún objeto o si se detecta un error durante una comprobación de coherencia para un objeto, la búsqueda se cancela anormalmente y se visualizan mensajes al ELS (mensajes PLCY) que identifican el error. Si se produce un error, el administrador de la red puede configurar una de las siguientes opciones para manejarlo:

- Suprimir todas las políticas leídas localmente y volver a una norma de excluir o aceptar todo
- Mantener todas las políticas leídas localmente. Especifique esta opción con el mandato **set default** de la característica de política.

En cualquiera de los casos, la búsqueda se vuelve a intentar una vez transcurrido el intervalo de reintento configurado. Si no es posible contactar con el servidor de LDAP primario, al cabo de 5 intentos se prueba el servidor secundario. Si no se puede contactar con el servidor secundario, al cabo de 5 intentos se vuelve a probar el servidor primario. Puede especificar el intervalo de reintento con el mandato **set ldap retry-interval** de la característica de política. Si falla una búsqueda debido a un estado latente de la red, puede cambiar el tiempo de espera de búsqueda del valor por omisión de 3 segundos utilizando el mandato **set ldap search-timeout** de la característica de política.

Generación de normas

Configure una política para especificar cómo desea que funcione la red. El direccionador convierte la información de la política en un conjunto de normas que compara con flujos de tráfico. Antes se tenía que hacer manualmente definiendo filtros de paquetes de entrada y de salida para cada patrón de tráfico. Con la base de datos de políticas ya no es necesario porque con ello sólo se configura una única política.

La mayor parte del trabajo se lleva a cabo internamente cada vez que se crea la base de datos de políticas. En algunos casos un direccionador convierte una política directamente en una única norma. En el caso de ISAKMP/IPSec, convierte una política en cinco normas. Se necesitan cinco normas para responder a las direcciones de tráfico (de entrada y de salida) y a los flujos de control que se producen durante las negociaciones de IKE de la Fase 1 y la Fase 2. La relación entre políticas es la siguiente:

Una política de DiffServ → Una norma de DiffServ

Una política de RSVP → Una norma de RSVP

Una política de ISAKMP/IPSec → Cinco normas de ISAKMP/IPSec

Ejemplo: Asegure el tráfico desde la subred A hasta la subred B; los puntos finales del túnel son SGa y SGb.

1. Fase 1 Entrada (Perfil = de SGb a SGa, Proto UDP, Puerto origen 500, Puerto destino 500): Esta norma es necesaria para filtrar las negociaciones

de la Fase 1 de entrada desde el similar ISAKMP remoto si el dispositivo funciona como un emisor de respuesta ISAKMP.

2. Fase 1 de salida (Perfil = de SGa a SGb, Proto UDP, Puerto origen 500, Puerto destino 500): Esta norma es necesaria para filtrar la información de la Fase 1 necesaria si el tráfico inicia negociaciones de la Fase 1 de ISAKMP. En este caso el dispositivo funciona como un iniciador de ISAKMP.
3. Fase 2 Entrada (Perfil = de SGb a SGa, Proto UDP, Puerto origen 500, Puerto destino 500): Esta norma es necesaria para filtrar el tráfico de la Fase 2 de entrada desde el similar ISAKMP remoto. Este tráfico es el resultado de la iniciación por parte del similar remoto de una renovación o negociación inicial de la Fase 2. Una norma de salida de la Fase 2 no es necesaria puesto que el tráfico de salida (norma 5) siempre inicia las negociaciones si es necesario.
4. Tráfico desde el túnel de seguridad (Perfil = de Subred A a Subred B): Esta norma es necesaria para situar el tráfico no protegido en un túnel de seguridad. Si la asociación de seguridad no se ha negociado, también se obtiene la norma de la Fase 1 e IKE inicia la Fase 1 y la Fase 2. Una vez establecidas las SA, los paquetes que coinciden con esta norma se pasan a IPSec para encapsulación y transmisión.
5. Tráfico desde el túnel de seguridad (Perfil = de Subred B a Subred A): Esta norma es necesaria para asegurar que los paquetes que deben llegar a un túnel de seguridad han llegado realmente a un túnel de seguridad. Si IPSec no ha desencapsulado el paquete y existe esta norma, el paquete se excluye. Esta norma maneja cualquier tráfico que se haya colado en la red.

Un túnel de clave manual de IPSec → Dos normas de IPSec

Ejemplo: Asegure el tráfico desde la subred A hasta la subred B; los puntos finales del túnel son SGa y SGb.

1. Tráfico desde el túnel de seguridad (Perfil = de Subred A a Subred B): Esta norma es necesaria para situar el tráfico no protegido en un túnel de seguridad. Es un túnel configurado estáticamente de modo que siempre está disponible y los paquetes que coinciden con esta norma se pasan directamente a IPSec para encapsulación y transmisión.
2. Tráfico desde el túnel de seguridad (Perfil = de Subred B a Subred A): Esta norma es necesaria para asegurar que los paquetes que deben llegar a un túnel de seguridad han llegado realmente a un túnel de seguridad. Si IPSec no ha desencapsulado el paquete y existe esta norma, el paquete se excluye. Esta norma maneja cualquier tráfico que se haya colado en la red.

Puede ver estas normas utilizando el mandato de supervisión **list rule** de la característica de política.

Ejemplos de configuración

Los ejemplos siguientes muestran cómo puede utilizar la característica de política para configurar los direccionadores en una red. Primero, acceda a la característica de política tal como se muestra a continuación:

```
* talk 6
Config>feature policy
IP Network Policy configuration
```

Política IPSec/ISAKMP con QoS

Puede entrar a la información de política de dos modos posibles. El primer modo consiste en definir los objetos de política individuales y, a continuación, agruparlos. Para utilizar este método, primero defina las conversiones de IPSec y, después, la propuesta de IPSec (que hace referencia a las conversiones de IPSec). Después, defina la acción de IPSec (que hace referencia a las propuestas de IPSec) y así sucesivamente hasta definir por completo la política. Utilizando la Figura 20 como referencia, este método empieza en el lado derecho de los objetos de política y actúa hacia la izquierda.

El segundo enfoque, que puede parecerle más fácil, consiste en definir primero las opciones de política de alto nivel y, cuando se le solicita, entrar las definiciones para los objetos de política individuales a medida que avanza. A continuación de la Figura 20 se proporciona un procedimiento de configuración de ejemplo en el cual se utilizan los valores que corresponden a los de la figura. Utiliza el método de izquierda a derecha y se inicia con el mandato **add policy**.

Si se ha definido un objeto previamente que se ajuste a sus necesidades, puede volverlo a utilizar en lugar de crear una nueva definición. Por ejemplo, si se ha configurado un período de validez para allTheTime (todoElTiempo) para una política anterior, puede volverlo a utilizar. El procedimiento siguiente muestra el proceso completo, pero no muestra la reutilización de la información de política previamente definida. Para obtener un ejemplo sobre cómo utilizar la información previamente definida, consulte “Única política de IPSec/ISAKMP” en la página 268.

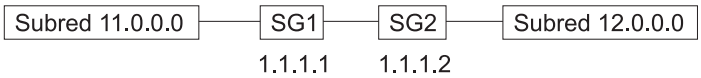


Figura 20. Configuración de IPSec/ISAKMP con QoS

El escenario de configuración de política que se describe en el texto siguiente se presenta bajo la perspectiva de SG1. La declaración de la política es:

Asegure el tráfico de la subred 11 a la subred 12, siendo los puntos finales del túnel SG1 y SG2, y proporcione una QoS para el tráfico de este túnel por medio de DiffServ GoldService

1. Añada la política.

   ```
   Policy config>add policy
   Enter a Name (1-29 characters) for this Policy []? examplePolicySecure11to12
   Enter the priority of this policy (This number is used to
   determine the policy to enforce in the event of policy conflicts) [5]? 10
   ```

2. No hay perfiles configurados por lo que debe definir uno nuevo.

```
List of Profiles:
        0: New Profile

Enter number of the profile for this policy [0]?
```

3. Nueva definición de perfil; en este caso el tráfico en el que estamos interesados es desde la subred 11 hasta la subred 12.

```
Enter a Name (1-29 characters) for this Profile []? trafficFrom11NetTo12Net
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Source Address [0.0.0.0]? 11.0.0.0
Enter IPV4 Source Mask [255.0.0.0]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Destination Address [0.0.0.0]? 12.0.0.0
Enter IPV4 Destination Mask [255.0.0.0]?

Protocol IDs:
     1)  TCP
     2)  UDP
     3)  All Protocols
     4)  Specify Range

Select the protocol to filter on (1-4) [3]?
Enter the Starting value for the Source Port [0]?
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]:
Limit this profile to specific interface(s)? [No]:


Here is the Profile you specified...


Profile Name    = trafficFrom11NetTo12Net
        sAddr:Mask=       11.0.0.0 : 255.0.0.0       sPort=    0 : 65535
        dAddr:Mask=       12.0.0.0 : 255.0.0.0       dPort=    0 : 65535
        proto     =              0 : 255
        TOS       =            x00 : x00
        Remote Grp=All Users
Is this correct? [Yes]:
```

4. Ha finalizado la definición del perfil y ha vuelto al menú de configuración de política.

```
List of Profiles:
        0: New Profile
        1: trafficFrom11NetTo12Net

Enter number of the profile for this policy [1]? 1
```

5. No hay períodos de validez configurados por lo que debe definir uno nuevo.

```
List of Validity Periods:
        0: New Validity Period

Enter number of the validity period for this policy [0]?
```

6. Preguntas sobre la configuración de período de validez; en este ejemplo el período de validez es de 9 AM a 5 PM, de lunes a viernes, cada mes de 1999.

```
Enter a Name (1-29 characters) for this Policy Valid Profile []?
              MonToFri-9am:5pm-1999
Enter the lifetime of this policy. Please input the
information in the following format:
                yyyymmddhhmmss:yyyymmddhhmmss OR '*' denotes forever.
 [*]? 19990101000000:19991231000000
During which months should policies containing this profile
be valid.  Please input any sequence of months by typing in
the first three letters of each month with a space in between
each entry, or type ALL to signify year round.
 [ALL]?
During which days should policies containing this profile
be valid.  Please input any sequence of days by typing in
the first three letters of each day with a space in between
each entry, or type ALL to signify all week
 [ALL]? mon tue wed thu fri
Enter the starting time (hh:mm:ss or * denotes all day)
 [*]? 00:00:00
Enter the ending time (hh:mm:ss)
 [00:00:00]? 17:00:00

Here is the Policy Validity Profile you specified...

Validity Name   = MonToFri-9am:5pm-1999
        Duration  = 19990101000000 : 19991231000000
        Months    = ALL
        Days      = MON TUE WED THU FRI
        Hours     = 09:00:00 : 17:00:00
Is this correct? [Yes]:
```

7. Ha finalizado la definición del período de validez y ha vuelto al menú de configuración de política.

```
List of Validity Periods:
        0: New Validity Period
        1: MonToFri-9am:5pm-1999

Enter number of the validity period for this policy [1]? 1
Should this policy enforce an IPSEC action? [No]: yes
```

8. Debe definir siempre una nueva acción de IPSec dado que el punto final del túnel siempre será diferente. Las excepciones se producen cuando existen varios túneles entre las dos mismas pasarelas, y en las configuraciones de acceso remoto comodín en las que el punto final del túnel no es conocido.

```
IPSEC Actions:
        0: New IPSEC Action

Enter the Number of the IPSEC Action [0]?
```

9. Menú de acción de IPSec.

```
Enter a Name (1-29 characters) for this IPsec Action []? secure11NetTo12Net
List of IPsec Security Action types:
     1)  Block (block connection)
     2)  Permit

Select the Security Action type (1-2) [2]? 2
Should the traffic flow into a secure tunnel or in the clear:
     1) Clear
     2) Secure Tunnel
 [2]?
Enter Tunnel Start Point IPV4 Address
 [11.0.0.5]? 1.1.1.1
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
 [0.0.0.0]? 1.1.1.2
Does this IPSEC tunnel flow within another IPSEC tunnel? [No]:
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?

Security Association Refresh Threshold, in percent (1-100) [85]?
Options for DF Bit in outer header (tunnel mode):
     1)  Copy
     2)  Set
     3)  Clear
Enter choice (1-3) [1]?
Enable Replay prevention (1=enable, 2=disable) [2]?
Do you want to negotiate the security association at
system initialization(Y-N)? [No]:
You must choose the proposals to be sent/checked against during phase 2
negotiations.  Proposals should be entered in order of priority.
```

10. No hay propuestas de IPSec definidas de modo que debe definir una nueva. Tenga en cuenta que una vez definida la propuesta de IPSec se puede volver a utilizar en varias acciones de IPSec.

```
List of IPSEC Proposals:
        0: New Proposal

Enter the Number of the IPSEC Proposal [0]?
```

11. Configuración de propuesta de IPSec.

```
Enter a Name (1-29 characters) for this IPsec Proposal []? genP2Proposal
Does this proposal require Perfect Forward Secrecy?(Y-N)? [No]:
Do you wish to enter any AH transforms for this proposal? [No]:
Do you wish to enter any ESP transforms for this proposal? [No]: yes
```

12. No hay conversiones ESP configuradas por lo que debe definir una nueva. Una vez definida la conversión ESP puede volverla a utilizar cualquier propuesta de IPSec.

```
List of ESP Transforms:
        0: New Transform

Enter the Number of the ESP transform [0]? 0
```

13. Configuración de conversión de IPSec.

```
Enter a Name (1-29 characters) for this IPsec Transform []? esp3DESwSHA
List of Protocol IDs:
     1)  IPSEC AH
     2)  IPSEC ESP

Select the Protocol ID (1-2) [1]? 2
List of Encapsulation Modes:
     1)  Tunnel
     2)  Transport

Select the Encapsulation Mode(1-2) [1]? 1
List of IPsec Authentication Algorithms:
     0)  None
     1)  HMAC-MD5
     2)  HMAC_SHA

Select the ESP Authentication Algorithm (0-2) [2]? 2
List of ESP Cipher Algorithms:
     1)  ESP DES
     2)  ESP 3DES
     3)  ESP CDMF
     4)  ESP NULL

Select the ESP Cipher Algorithm (1-4) [1]? 2
Security Association Lifesize, in kilobytes (1024-65535) [50000]?
Security Association Lifetime, in seconds (120-65535) [3600]?

Here is the IPSec transform you specified...

Transform Name  = esp3DESwSHA
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =3DES
Is this correct? [Yes]:
```

14. Vuelva al menú de propuesta de IPSec.

```
List of ESP Transforms:
        0: New Transform
        1: esp3DESwSHA

Enter the Number of the ESP transform [1]?
Do you wish to add another ESP transform to this proposal? [Yes]: no

Here is the IPSec proposal you specified...

Name  = genP2Proposal
        Pfs   = N
        ESP Transforms:
                esp3DESwSHA
Is this correct? [Yes]:
```

15. Vuelva al menú de acción de IPSec.

```
List of IPSEC Proposals:
        0: New Proposal
        1: genP2Proposal

Enter the Number of the IPSEC Proposal [1]?
Are there any more Proposal definitions for this IPSEC Action? [No]:

Here is the IPSec Action you specified...

IPSECAction Name = secure11NetTo12Net
        Tunnel Start:End         =        1.1.1.1 : 1.1.1.2
        Tunnel In Tunnel         =             No
        Min Percent of SA Life   =             75
        Refresh Threshold        =             85 %
        Autostart                =             No
        DF Bit                   =           COPY
        Replay Prevention        =       Disabled
        IPSEC Proposals:
                genP2Proposal
Is this correct? [Yes]:
```

16. Vuelva al menú de política.

```
IPSEC Actions:
        0: New IPSEC Action
        1: secure11NetTo12Net

Enter the Number of the IPSEC Action [1]? 1
```

17. Ha especificado un tipo de acción de IPSec de seguridad, por lo que debe identificar una acción de ISAKMP para las negociaciones de la Fase 1. No hay ninguna definida, por lo que debe entrar una nueva. En la mayoría de casos, una acción y propuesta de ISAKMP es suficiente para todas las políticas de seguridad.

```
ISAKMP Actions:
        0: New ISAKMP Action

Enter the Number of the ISAKMP Action [0]?
```

18. Configuración de acción de ISAKMP.

```
Enter a Name (1-29 characters) for this ISAKMP Action []? genPhase1Action

List of ISAKMP Exchange Modes:
     1)  Main
     2)  Aggressive

Enter Exchange Mode (1-2) [1]?
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?

ISAKMP Connection Lifesize, in kilobytes (100-65535) [5000]?
ISAKMP Connection Lifetime, in seconds (120-65535) [30000]?
Do you want to negotiate the security association at
system initialization(Y-N)? [Yes]: no
You must choose the proposals to be sent/checked against during phase 1
negotiations.  Proposals should be entered in order of priority.
```

19. No hay configurada ninguna propuesta de ISAKMP, por lo que debe crear una nueva.

```
List of ISAKMP Proposals:
        0: New Proposal
```

20. Configuración de propuesta de ISAKMP.

```
Enter the Number of the ISAKMP Proposal [0]?
Enter a Name (1-29 characters) for this ISAKMP Proposal []? genP1Proposal

List of Authentication Methods:
     1)  Pre-Shared Key
     2)  RSA SIG

Select the authentication method (1-2) [1]? 2

List of Hashing Algorithms:
     1)  MD5
     2)  SHA

Select the hashing algorithm(1-2) [1]? 2

List of Cipher Algorithms:
     1)  DES
     2)  3DES

Select the Cipher Algorithm (1-2) [1]? 2
Security Association Lifesize, in kilobytes (100-65535) [1000]?
Security Association Lifetime, in seconds (120-65535) [15000]?

List of Diffie Hellman Groups:
     1)  Diffie Hellman Group 1
     2)  Diffie Hellman Group 2

Select the Diffie Hellman Group ID from this proposal (1-2) [1]?


Here is the ISAKMP Proposal you specified...

Name = genP1Proposal
        AuthMethod = Pre-Shared Key
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = SHA
        Encr Algo  = 3DES CB
Is this correct? [Yes]:
```

21. Vuelva a la configuración de la acción de ISAKMP.

```
List of ISAKMP Proposals:
        0: New Proposal
        1: genP1Proposal

Enter the Number of the ISAKMP Proposal [1]?
Are there any more Proposal definitions for this ISAKMP Action? [No]:

Here is the ISAKMP Action you specified...

ISAKMP Name     = genPhase1Action
        Mode                    =           Main
        Min Percent of SA Life  =            75
        Conn LifeSize:LifeTime  =           5000 : 30000
        Autostart               =            No
        ISAKMP Proposals:
                genP1Proposal
Is this correct? [Yes]:
```

22. Vuelva a la configuración de política.

```
ISAKMP Actions:
        0: New ISAKMP Action
        1: genPhase1Action

Enter the Number of the ISAKMP Action [1]?
Do you wish to Map a DiffServ Action to this Policy? [No]: yes
```

23. Defina la acción GoldService de DiffServ.

```
DiffServ Actions:
        0: New DiffServ Action

Enter the Number of the DiffServ Action [0]?
```

24. Configuración de acción de DiffServ.

    Si la acción de DiffServ es para la cola asegurada:

```
Enter a Name (1-29 characters) for this DiffServ Action [AF11]? GoldService
Enter the permission level for packets matching this DiffServ
Action (1. Permit, 2. Deny) [2]? 1
List of DiffServ Queues:
   1) Premium
   2) Assured/BE
Enter the Queue Number(1-2) for outgoing packets matching
this DiffServ Action [2]?
How do you want to specify the bandwidth allocated to this service?
Enter absolute kbps(1) or percentage of output bandwidth(2) [2]?
Enter the percentage of output bandwidth allocated to this service [10]? 20

List of Assured Forwarding Class:
  1) AF11 Class DS Byte
  2) AF21 Class DS Byte
  3) AF31 Class DS BYte
  4) AF41 Class DS Byte
  5) New Class DS Byte

Enter the AF Class (1-5) for outgoing packets matching
this DiffServ Action [5]? 1

List of Policing Type in AF Class:
  1) Single Rate Color Blind TCM
  2) Single Rate Color Aware TCM
  3) Two Rate Color Blind TCM
  4) Two Rate Color Aware TCM
  5) None
Enter the AF Class (1-5) Policing for outgoing packets matching
this DiffServ Action [5]? 1

Single Rate TCM:
Committed Info Rate (CIR in bytes/sec) [0]? 25000
Committed Burst Size (CBS in bytes) [4000]?
Excess Burst Size (EBS in bytes) [4000]?

Here is the DiffServ Action you specified...

DiffServ Name   = GoldService                   Type =Permit

        DS mask:modify=xFC:x20
        Queue:BwShare  =Assured    : 20 %
        TCM:Class = SR,CB:AF11
        CIR = 25000 bytes/sec;   CBS = 4000 bytes
        EBS = 4000 bytes

Is this correct? [Yes]:
```

    Si la acción de DiffServ es para la cola de primera calidad:

```
Name (1-29 characters) for this DiffServ Action []? ExpService
Enter the permission level for packets matching this DiffServ
Action (1. Permit, 2. Deny) [2]? 1
List of DiffServ Queues:
   1) Premium
   2) Assured/BE
Enter the Queue Number(1-2) for outgoing packets matching
this DiffServ Action [2]? 1
How do you want to specify the bandwidth allocated to this service?
Enter absolute kbps(1) or percentage of output bandwidth(2) [2]?
Enter the percentage of output bandwidth allocated to this service [10]? 19

Transmitted DS-byte mask [0]? fc
Transmitted DS-byte modify value [0]? b8

List of EF Policing Config Type
   1) Default
   2) Custom

Enter the Parameter Type [1]? 2
Enter the Token Rate (in bytes/sec) [0]? 25000
Enter the Token Bucket Size (in bytes) [0]? 4000


Here is the DiffServ Action you specified...


DiffServ Name   = ExpService                    Type =Permit
        DS mask:modify =xFC:xB8
        Queue:BwShare  =Premium    : 19 %
        Token Rate:    = 25000 bytes/sec
        Token Bucket:  = 4000 bytes
Is this correct? [Yes]:
```

25. Vuelva a la configuración de política.

```
DiffServ Actions:
        0: New DiffServ Action
        1: GoldService

Enter the Number of the DiffServ Action [1]? 1
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?

Here is the Policy you specified...

Policy Name     = examplePolicySecure11to12
        State:Priority =Enabled    : 10
        Profile        =trafficFrom10NetTo12Net
        Valid Period   =MonToFri-9am:5pm-1999
        IPSEC Action   =secure11NetTo12Net
        ISAKMP Action  =genPhase1Action
        DiffServ Action=GoldService
Is this correct? [Yes]:
```

26. Si no está habilitado DiffServ o IPSec, se le avisa de que para poder imponer la política primero debe habilitar DiffServ, IPSec o ambos (característica DiffServ o característica IPSec).

```
You must enable and configure DiffServ in feature DS before
QoS can be ensured for this policy
```

27. El paso final de este proceso consiste en añadir una definición de perfil de USER (USUARIO) para el similar ISAKMP remoto. Este paso no es necesario si las negociaciones de ISAKMP deben autentificar el similar con certificados públicos. Sin embargo, en el ejemplo precedente se elige clave previamente compartida como método de autentificación, por lo que es necesario identificar

al usuario y entrar la clave previamente compartida que se espera que utilice el similar.

```
Policy config>add user
Choose from the following ways to identify a user:
        1: IP Address
        2: Fully Qualified Domain Name
        3: User Fully Qualified Domain Name
        4: Key ID (Any string)
Enter your choice(1-4) [1]?
Enter the IP Address that distinguishes this user
 [0.0.0.0]? 1.1.1.2
Group to include this user in []? peers
Authenticate user with 1:pre-shared key or 2: Public Certificate [1]?
Mode to enter key (1=ASCII, 2=HEX) [1]?
Enter the Pre-Shared Key (an even number of 2-128 ascii chars):
Enter the Pre-Shared Key again (10 characters) in ascii:

Here is the User Information you specified...

Name      = 1.1.1.2
Type      = IPV4 Addr
        Group     =peers
        Auth Mode =Pre-Shared Key
        Key(Ascii)=exampleKey
Is this correct? [Yes]:
```

28. Los pasos de configuración de política han finalizado. Si desea configurar DiffServ, IPSec o cualquier configuración de red o IP, debe hacerlo antes de que el túnel IPSec sea funcional. El ejemplo del mandato list siguiente muestra la configuración que se acaba de completar. Para activar estos cambios, vuelva a cargar el dispositivo o entre el mandato de supervisión **reset database** de la característica de política.

```
Policy config>list all

Configured Policies....

Policy Name     = examplePolicySecure11to12
        State:Priority =Enabled    : 10
        Profile        =trafficFrom11NetTo12Net
        Valid Period   =MonToFri-9am:5pm-1999
        IPSEC Action   =secure11NetTo12Net
        ISAKMP Action  =genPhase1Action
        DiffServ Action=GoldService
--More--

Configured Profiles....

Profile Name    = trafficFrom11NetTo12Net
        sAddr:Mask=       11.0.0.0 : 255.0.0.0       sPort=    0 : 65535
        dAddr:Mask=       12.0.0.0 : 255.0.0.0       dPort=    0 : 65535
        proto     =              0 : 255
        TOS       =            x00 : x00
        Remote Grp=All Users
--More--

Configured Validity Periods

Validity Name   = MonToFri-9am:5pm-1999
        Duration  = 19990101000000 : 19991231000000
        Months    = ALL
        Days      = MON TUE WED THU FRI
        Hours     = 09:00:00 : 17:00:00
--More--

Configured DiffServ Actions....

DiffServ Name   = GoldService                    Type =Permit

 DS mask:modify=xFC:x20
 Queue:BwShare  =Assured    : 20 %
 TCM:Class = SR, CB, AF11
 CIR = 25000 bytes/sec;   CBS = 4000 bytes
 EBS = 4000 bytes
--More--

Configured IPSEC Actions....

IPSECAction Name = secure11NetTo12Net
        Tunnel Start:End         =        1.1.1.1 : 1.1.1.2
        Tunnel In Tunnel         =             No
        Min Percent of SA Life   =             75
        Refresh Threshold        =             85 %
        Autostart                =             No
        DF Bit                   =           COPY
        Replay Prevention        =       Disabled
        IPSEC Proposals:
                genP2Proposal
--More--

Configured IPSEC Proposals....

Name  = genP2Proposal
        Pfs   = N
        ESP Transforms:
                esp3DESwSHA
--More--
```

```
Configured IPSEC Transforms....

Transform Name  = esp3DESwSHA
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =3DES
--More--

Configured ISAKMP Actions....

ISAKMP Name     = genPhase1Action
        Mode                    =            Main
        Min Percent of SA Life  =             75
        Conn LifeSize:LifeTime  =            5000 : 30000
        Autostart               =             No
        ISAKMP Proposals:
                genP1Proposal
--More--

Configured ISAKMP Proposals....
Name = genP1Proposal
        AuthMethod = Pre-Shared Key
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = SHA
        Encr Algo  = 3DES CB
--More--

Configured Policy Users....
Name      = 1.1.1.2
Type      = IPV4 Addr
        Group     =peers
        Auth Mode =Pre-Shared Key
        Key(Ascii)=exampleKey
--More--

Configured Manual IPSEC Tunnels....

                            IPv4 Tunnels
-------------------------------------------------------------------------------

   ID         Name        Local IPv4 Addr  Rem IPv4 Addr    Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------
```

Única política de IPSec/ISAKMP

Un procedimiento de configuración de ejemplo, proporcionado después de la Figura 21 y que utiliza valores que corresponden a los de la figura, utiliza el método de izquierda a derecha y muestra cómo crear el procedimiento de muestra anterior volviendo a utilizar información creada en el anterior.

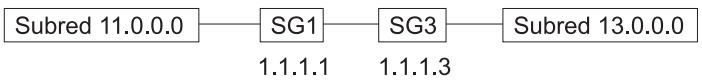


Figura 21. Configuración de IPSec y reutilización de una definición anterior

El escenario de configuración de política que se describe en el texto siguiente se presenta bajo la perspectiva de SG1. La declaración de política de este escenario es:

Asegure el tráfico de la subred 11 a la subred 13 (sólo tráfico TCP), siendo los puntos finales de túnel SG1 y SG3, y no proporcione ninguna QoS.

1. Añada la política.

```
Policy config>add policy
Enter a Name (1-29 characters) for this Policy []? examplePolicySecure11to13
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]? 10
List of Profiles:
        0: New Profile
        1: trafficFrom10NetTo12Net

Enter number of the profile for this policy [1]? 0
Enter a Name (1-29 characters) for this Profile []? trafficFrom11NetTo13Net
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Source Address [0.0.0.0]? 11.0.0.0
Enter IPV4 Source Mask [255.0.0.0]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Destination Address [0.0.0.0]? 13.0.0.0
Enter IPV4 Destination Mask [255.0.0.0]?

Protocol IDs:
     1)  TCP
     2)  UDP
     3)  All Protocols
     4)  Specify Range

Select the protocol to filter on (1-4) [3]? 1
Enter the Starting value for the Source Port [0]?
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]:
Limit this profile to specific interface(s)? [No]:

Here is the Profile you specified...

Profile Name    = trafficFrom11NetTo13Net
        sAddr:Mask=       11.0.0.0 : 255.0.0.0       sPort=    0 : 65535
        dAddr:Mask=       13.0.0.0 : 255.0.0.0       dPort=    0 : 65535
        proto     =              6 : 6
        TOS       =            x00 : x00
        Remote Grp=All Users
Is this correct? [Yes]:
List of Profiles:
        0: New Profile
        1: trafficFrom10NetTo12Net
        2: trafficFrom11NetTo13Net

Enter number of the profile for this policy [1]? 2
```

2. Vuelva a utilizar el período de validez.

```
List of Validity Periods:
        0: New Validity Period
        1: MonToFri-9am:5pm-1999

Enter number of the validity period for this policy [1]?
Should this policy enforce an IPSEC action? [No]: yes
IPSEC Actions:
        0: New IPSEC Action
        1: secure11NetTo12Net

Enter the Number of the IPSEC Action [1]? 0
Enter a Name (1-29 characters) for this IPsec Action []? secure11To13
List of IPsec Security Action types:
     1)  Block (block connection)
     2)  Permit

Select the Security Action type (1-2) [2]?
Should the traffic flow into a secure tunnel or in the clear:
     1) Clear
     2) Secure Tunnel
 [2]?
Enter Tunnel Start Point IPV4 Address
 [11.0.0.5]? 1.1.1.1
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
 [0.0.0.0]? 1.1.1.3
Does this IPSEC tunnel flow within another IPSEC tunnel? [No]:
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?

Security Association Refresh Threshold, in percent (1-100) [85]?
Options for DF Bit in outer header (tunnel mode):
     1)  Copy
     2)  Set
     3)  Clear
Enter choice (1-3) [1]?
Enable Replay prevention (1=enable, 2=disable) [2]?
Do you want to negotiate the security association at
system initialization(Y-N)? [No]:
You must choose the proposals to be sent/checked against during phase 2
negotiations.  Proposals should be entered in order of priority.
```

3. Vuelva a utilizar la propuesta de IPSec de la configuración previamente definida.

```
List of IPSEC Proposals:
        0: New Proposal
        1: genP2Proposal

Enter the Number of the IPSEC Proposal [1]?
Are there any more Proposal definitions for this IPSEC Action? [No]:


Here is the IPSec Action you specified...


IPSECAction Name = secure11To13
        Tunnel Start:End         =        1.1.1.1 : 1.1.1.3
        Tunnel In Tunnel         =             No
        Min Percent of SA Life   =             75
        Refresh Threshold        =             85 %
        Autostart                =             No
        DF Bit                   =           COPY
        Replay Prevention        =       Disabled
        IPSEC Proposals:
                genP2Proposal
Is this correct? [Yes]:
IPSEC Actions:
        0: New IPSEC Action
        1: secure11NetTo12Net
        2: secure11To13

Enter the Number of the IPSEC Action [1]? 2
```

4. Vuelva a utilizar la acción ISAKMP de la configuración anterior.

```
ISAKMP Actions:
        0: New ISAKMP Action
        1: genPhase1Action

Enter the Number of the ISAKMP Action [1]?
Do you wish to Map a DiffServ Action to this Policy? [No]:
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?

Here is the Policy you specified...

Policy Name     = examplePolicySecure11to13
        State:Priority =Enabled    : 10
        Profile        =trafficFrom11NetTo13Net
        Valid Period   =MonToFri-9am:5pm-1999
        IPSEC Action   =secure11To13
        ISAKMP Action  =genPhase1Action
Is this correct? [Yes]:
```

Excluir todo el tráfico público (norma de filtro)

Este ejemplo de política muestra cómo configurar una norma de exclusión simple para la interfaz pública que excluye todo el tráfico que no se ha asegurado mediante IPSec. Esta norma es muy general y **debe** tener la prioridad más baja de cualquier norma configurada.

1. Añada la política.

```
Policy config>add policy
Enter a Name (1-29 characters) for this Policy []? dropAllPublicTraffic
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]?
List of Profiles:
        0: New Profile
        1: trafficFrom10NetTo12Net
        2: trafficFrom11NetTo13Net

Enter number of the profile for this policy [1]? 0
```

2. Defina un nuevo perfil que incluya todo el tráfico que llegue a la interfaz pública o salga de la misma (1.1.1.1).

```
Enter a Name (1-29 characters) for this Profile []? allPublicTraffic
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Source Address [0.0.0.0]?
Enter IPV4 Source Mask [0.0.0.0]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Destination Address [0.0.0.0]?
Enter IPV4 Destination Mask [0.0.0.0]?

Protocol IDs:
     1)  TCP
     2)  UDP
     3)  All Protocols
     4)  Specify Range

Select the protocol to filter on (1-4) [3]?
Enter the Starting value for the Source Port [0]?
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]:
```

3. Dado que la información de origen y de destino (o ambas) no es comodín, debe especificar las interfaces en las que espera que este tráfico llegue y salga.

```
The Source and/or Destination Address information you specified
includes all addresses.  You must specify an Interface Pair
with this profile to further qualify what traffic you wish to filter
to this policy.  The interface pair should at least specify the
Limit this profile to specific interface(s)? [No]: yes
Interface Pair Groups:
        0: New Ifc Pair
Number of Ifc Pair Group [1]? 0
```

4. Añada un par de interfaces para el tráfico que sale a través de la interfaz pública.

```
Enter a Group Name (1-29 characters) for this Interface Pair []? inOutPublic
Ingress Interface IP Address (255.255.255.255 = any ingress)
 [255.255.255.255]?
Egress Interface IP Address (255.255.255.255 = any egress)
 [255.255.255.255]? 1.1.1.1
Interface Pair Groups:
        0: New Ifc Pair
        1) Group Name: inOutPublic
                  In:Out=255.255.255.255 : 1.1.1.1

Number of Ifc Pair Group [1]? 0
```

5. Añada otro par de interfaces para el tráfico que llega a través de la interfaz pública. Proporciónele el mismo nombre que el del par de interfaces anterior para asignarlo al mismo grupo.

```
Enter a Group Name (1-29 characters) for this Interface Pair []? inOutPublic
Ingress Interface IP Address (255.255.255.255 = any ingress)
 [255.255.255.255]? 1.1.1.1
Egress Interface IP Address (255.255.255.255 = any egress)
 [255.255.255.255]?
Interface Pair Groups:
        0: New Ifc Pair
        1) Group Name: inOutPublic
                  In:Out=255.255.255.255 : 1.1.1.1
                  In:Out=        1.1.1.1 : 255.255.255.255

Number of Ifc Pair Group [1]?

Here is the Profile you specified...

Profile Name    = allPublicTraffic
        sAddr:Mask=        0.0.0.0 : 0.0.0.0         sPort=    0 : 65535
        dAddr:Mask=        0.0.0.0 : 0.0.0.0         dPort=    0 : 65535
        proto     =              0 : 255
        TOS       =            x00 : x00
        Remote Grp=All Users
        1.  In:Out=255.255.255.255 : 1.1.1.1
        2.  In:Out=        1.1.1.1 : 255.255.255.255
Is this correct? [Yes]:
List of Profiles:
        0: New Profile
        1: trafficFrom10NetTo12Net
        2: trafficFrom11NetTo13Net
        3: allPublicTraffic

Enter number of the profile for this policy [1]? 3
```

6. Añada un nuevo período de validez que especifique `all the time` (todo el tiempo).

```
List of Validity Periods:
        0: New Validity Period
        1: MonToFri-9am:5pm-1999

Enter number of the validity period for this policy [1]? 0
Enter a Name (1-29 characters) for this Policy Valid Profile []? allTheTime
Enter the lifetime of this policy. Please input the
information in the following format:
                yyyymmddhhmmss:yyyymmddhhmmss OR '*' denotes forever.
 [*]?
During which months should policies containing this profile
be valid.  Please input any sequence of months by typing in
the first three letters of each month with a space in between
each entry, or type ALL to signify year round.
 [ALL]?
During which days should policies containing this profile
be valid.  Please input any sequence of days by typing in
the first three letters of each day with a space in between
each entry, or type ALL to signify all week
 [ALL]?
Enter the starting time (hh:mm:ss or * denotes all day)
 [*]?

Here is the Policy Validity Profile you specified...

Validity Name   = allTheTime
        Duration  = Forever
        Months    = ALL
        Days      = ALL
        Hours     = All Day
Is this correct? [Yes]:
List of Validity Periods:
        0: New Validity Period
        1: MonToFri-9am:5pm-1999
        2: allTheTime

Enter number of the validity period for this policy [1]? 2
Should this policy enforce an IPSEC action? [No]: yes
IPSEC Actions:
        0: New IPSEC Action
        1: secure11NetTo12Net
        2: secure11To13
```

7. Añada una nueva acción de IPSec para excluir todo el tráfico (acción de filtro).

```
Enter the Number of the IPSEC Action [1]? 0
Enter a Name (1-29 characters) for this IPsec Action []? dropTraffic
List of IPsec Security Action types:
     1)  Block (block connection)
     2)  Permit

Select the Security Action type (1-2) [2]? 1

Here is the IPSec Action you specified...

IPSECAction Name = dropTraffic
        Action   = Drop
Is this correct? [Yes]:
IPSEC Actions:
        0: New IPSEC Action
        1: secure11NetTo12Net
        2: secure11To13
        3: dropTraffic

Enter the Number of the IPSEC Action [1]? 3
Do you wish to Map a DiffServ Action to this Policy? [No]:
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?

Here is the Policy you specified...

Policy Name     = dropAllPublicTraffic
        State:Priority =Enabled    : 5
        Profile        =allPublicTraffic
        Valid Period   =allTheTime
        IPSEC Action   =dropTraffic
Is this correct? [Yes]:
```

Configuración y habilitación del sistema de búsqueda de política de LDAP

Este ejemplo muestra cómo configurar y habilitar el sistema de búsqueda de política de LDAP. En este ejemplo existen dos directorios de LDAP (uno primario y uno secundario) con direcciones IP de 11.0.0.2 y 13.0.0.1 respectivamente. Ambos están a la escucha en el puerto TCP 389 y el dispositivo debe enlazarse al servidor de LDAP como cn=router, contraseña (password) myPassWord. La entrada base en el árbol de directorios para las políticas del direccionador es cn=RouterDeviceProfile,o=ibm,c=us.

Nota: Actualmente tanto el servidor de LDAP primario como el secundario deben estar a la escucha en el mismo puerto y deben tener las mismas credenciales de autentificación para el direccionador. El DeviceProfile debe ser el mismo para el direccionador en ambos servidores de directorios.

Este ejemplo también muestra cómo establecer la política por omisión para que las comunicaciones de LDAP sean seguras a través de IPSec. Este ejemplo utiliza la modalidad de clave previamente compartida para la autentificación de ISAKMP, y SHA y 3DES para los parámetros de autentificación y cifrado para la Fase 1 y la Fase 2. El punto de inicio del túnel es 1.1.1.4 para el dispositivo que lleva a cabo la búsqueda de política de LDAP y los puntos finales del túnel son 1.1.1.1 para el servidor de LDAP 11.0.0.1 y 1.1.1.3 para el servidor de LDAP 13.0.0.1.

1. Configure y habilite el sistema de búsqueda de política de LDAP y liste los resultados.

```
Policy config>set ldap primary-server 11.0.0.1
Policy config>set ldap secondary-server 13.0.0.1
Policy config>set ldap port 389
Policy config>set ldap bind-name cn=router
Policy config>set ldap bind-pw myPassWord
Policy config>set ldap anonymous-bind no
Policy config>set ldap policy-base cn=RouterDeviceProfile,o=ibm,c=us
Policy config>enable ldap policy-search
Policy config>list ldap
LDAP CONFIGURATION information:

        Primary Server Address:              11.0.0.1
        Secondary Server Address:            13.0.0.1


        Search timeout value:                3 sec(s)
        Retry interval on search failures:   1 min(s)
        Server TCP port number:              389
        Server Version number:               2


        Bind Information:
        Bind Anonymously:                    No
          Device Distinguished Name:         cn=router
          Device Password:                   myPassWord


        Base DN for this device's policies:  cn=RouterDeviceProfile,o=ibm,c=us


        Search policies from LDAP Directory: Enabled
```

2. Establezca la política por omisión

```
Policy config>set default-policy
List of default policy rules:
  1)  Accept and Forward all IP Traffic
  2)  Permit LDAP traffic, drop all other IP Traffic
  3)  Permit and Secure LDAP traffic, drop all other IP Traffic

Select the default policy rule to use during policy refresh periods [1]? 3
List of default error handling procedures:
  1)  Reset Policy Database to Default Rule
  2)  Flush any rules read from LDAP, load local rules

Select the error handling behavior for when loading Policy Database  [1]?

Please enter the set of Security Information for encrypting and
authenticating the LDAP traffic generated by the device when
retrieving policy information from the LDAP Server

Enter phase 1 ISAKMP negotiation parameters:

List of Diffie Hellman Groups:
     1)  Diffie Hellman Group 1
     2)  Diffie Hellman Group 2

Select the Diffie Hellman Group ID from this proposal (1-2) [1]?

List of Hashing Algorithms:
     1)  MD5
     2)  SHA

Select the hashing algorithm(1-2) [1]? 2

List of Cipher Algorithms:
     1)  DES
     2)  3DES

Select the Cipher Algorithm (1-2) [1]? 2
Authentication: (1)Pre-shared Key or (2)Certificate(RSA Sig) [2]? 1
Enter the Pre-Shared Key []? test

Enter phase 2 IPSEC negotiation parameters:
List of IPsec Authentication Algorithms:
     0)  None
     1)  HMAC-MD5
     2)  HMAC_SHA

Select the ESP Authentication Algorithm (0-2) [1]? 2
List of ESP Cipher Algorithms:
     1)  ESP DES
     2)  ESP 3DES
     3)  ESP CDMF
     4)  ESP NULL

Select the ESP Cipher Algorithm (1-4) [1]? 2
Tunnel Start IPV4 Address (Primary LDAP Server)
 [0.0.0.0]? 1.1.1.4
Tunnel End Point IPV4 Address (Primary LDAP Server)
 [0.0.0.0]? 1.1.1.1
Tunnel Start IPV4 Address (Secondary LDAP Server)
 [1.1.1.4]?
Tunnel End Point IPV4 Address (Secondary LDAP Server)
 [1.1.1.1]? 1.1.1.3
Policy config>list default-policy

Default Policy Rule:                  Drop All IP Traffic except secure LDAP
Default error handling procedure:     Reset Policy Database to Default Rule
```

```
Phase 1 ISAKMP negotiation parameters:
Diffie Hellman Group ID:               1
Hashing Algorithm:                     SHA
ISAKMP Cipher Algorithm:               ESP 3DES CBC
Per-shared key value:                  test

Phase 2 IPSEC negotiation parameters:
IPsec ESP Authentication Algorithm:    HMAC SHA
ESP Cipher Algorithm:                  3DES
Local Tunnel Addr (Primary Server):    1.1.1.4
Remote Tunnel Addr (Primary Server):   1.1.1.1
Local Tunnel Addr (Secondary Server):  1.1.1.4
Remote Tunnel Addr (Secondary Server): 1.1.1.3
```

En este punto está preparado para gestionar los direccionadores de la red con la característica de política. Para obtener información detallada sobre los mandatos que se utilizan para configurar los parámetros de política necesarios, como por ejemplo, perfiles, propuestas, conversiones y acciones, consulte “Mandatos de configuración de política” en la página 287, “Mandatos de configuración de servidor de políticas de LDAP” en la página 308 y “Mandatos de supervisión de política” en la página 313.

Ejemplo de configuración rápida de política

El mandato **qconfig** disponible en la característica de política le permite añadir de forma rápida una política basándose en uno de cuatro escenarios. Se le harán unas cuantas preguntas simples y, a continuación, basándose en las respuestas, se generarán los objetos de política. El mandato **qconfig** aprovecha las plantillas de política predefinidas para minimizar las preguntas de configuración que se le hacen. Mediante **qconfig** no puede cambiar los objetos de política; sólo es un medio para añadir una política rápidamente. Consulte el apartado “Mandatos de configuración de política” en la página 287 para obtener más información sobre este mandato.

El ejemplo siguiente reproduce el ejemplo de IPSec/ISAKMP que se ha descrito anteriormente en este capítulo. Básicamente, el objetivo es proteger y autentificar el tráfico de la subred 11.0.0.0 a la subred 12.0.0.0 con SG1 y SG2. Adicionalmente, al tráfico que está asegurado a través de estas pasarelas de seguridad se le deberá proporcionar una QoS. En este ejemplo, la QoS es AF11 y se selecciona seguridad fuerte.

```
Policy config>qconfig
Enter a Name (1-29 characters) for this Policy [policyQC_1]?
Please choose from one of the following Scenarios:

1: Branch Office Scenario
2: Remote Access User Scenario (IPSEC and L2TP)
3: Drop Traffic not matched on Untrusted Interface
4: Custom
Selection [1]?
Local Subnet (Base Address) [0.0.0.0]? 11.0.0.0
Local Subnet (Net Mask) [255.0.0.0]?
Local Tunnel Endpoint [11.0.0.5]? 1.1.1.1
Remote Subnet (Base Address) [0.0.0.0]? 12.0.0.0
Remote Subnet (Net Mask) [255.0.0.0]?
Remote Tunnel Endpoint [0.0.0.0]? 1.1.1.2
Configure Ports and Protocols? [No]:
1: Strong Security, 2: Very Strong Security, 3: Help [1]?
Authenticate Peer using 1:Pre-shared Key or 2:Certificate(RSA Signatures) [2]? 1
Enter the Pre-Shared Key (an even number of 2-128 ascii chars):
Enter the Pre-Shared Key again (4 characters) in ascii:
Select from the following DiffServ Actions:
        0: Best Effort (No DiffServ)
        1: EF
        2: AF11
        3: AF21
        4: AF31
        5: AF41
        6: GoldService

Enter Selection [0]? 2
Configure advanced options? [No]:


Here is the information you entered...

Policy Name:  policyQC_1 (Branch Office Scenario)
Local Information:
------------------
            Subnet:  11.0.0.0/255.0.0.0
   Tunnel Endpoint:  1.1.1.1
        Port Range:  00000-65535

Remote Information:
-------------------
            Subnet:  12.0.0.0/255.0.0.0
   Tunnel Endpoint:  1.1.1.2
        Port Range:  00000-65535

Other Information:
------------------
          Protocol:  000-255
          Priority:  10
          Security:  Strong Security
        Encap Mode:  Tunnel
         Auth Mode:  Pre-Shared Key
   Validity Period:  allTheTime
   DiffServ Action:  AF11
Continue? [Yes]:
-----------------------------------------

Based on the input to these simple questions, the QCONFIG mechanism generated
the following objects:
```

1.

```
Policy config>list policy by-name policyQC_1

Policy Name     = policyQC_1
        State:Priority =Enabled    : 10
        Profile        =policyQC_1
        Valid Period   =allTheTime
        IPSEC Action   =policyQC_1
        ISAKMP Action  =generalPhase1Action
        DiffServ Action=AF11
```

2.

```
Policy config>list ipsec-action by-name policyQC_1
IPSECAction Name = policyQC_1
        Tunnel Start:End         =        1.1.1.1 : 1.1.1.2
        Tunnel In Tunnel         =             No
        Min Percent of SA Life   =              1
        Refresh Threshold        =             85 %
        Autostart                =             No
        DF Bit                   =           COPY
        Replay Prevention        =       Disabled
        IPSEC Proposals:
                strongP2EspProp
                strongP2EspAhProp
                veryStrongP2EspProp
                veryStrongP2EspAhProp
```

3.

```
Policy config>list profile by-name policyQC_1

Profile Name    = policyQC_1
        sAddr:Mask=       11.0.0.0 : 255.0.0.0       sPort=    0 : 65535
        dAddr:Mask=       12.0.0.0 : 255.0.0.0       dPort=    0 : 65535
        proto     =              0 : 255
        TOS       =            x00 : x00
        Remote Grp=All Users
```

4.

```
Policy config>list user by-name
List of Users:
  num: User Info                          :Group Name
    1: 1.1.1.2                            :IKE-Peers
Enter the number of user [1]?
Name      = 1.1.1.2
Type      = IPV4 Addr
        Group     =IKE-Peers
        Auth Mode =Pre-Shared Key
```

Objetos de política predefinidos

Se han predefinido los objetos de política siguientes para que el usuario los utilice. Estos objetos representan las configuraciones más típicas y están destinados a poderse utilizar para muchas configuraciones de política. Estas definiciones de objetos de política predefinidos, junto con el mandato **qconfig**, proporcionan un modo fácil de añadir políticas a una configuración de red. Las plantillas predefinidas no se pueden cambiar ni suprimir. Si desea cambiar un objeto, deberá copiarlo utilizando el mandato **copy**, especificando un nombre nuevo. Una vez hecho esto, puede cambiar la copia. Si actualiza a un nuevo release o a una versión de PTF del código y ha habido un cambio en las plantillas, necesitará utilizar el mandato de configuración **refresh-templates** de la característica de política

para obtener las plantillas más actuales; de lo contrario, se continuarán utilizando las definiciones originales.

Existen los objetos predefinidos siguientes para la característica de política:

Periodos de validez

Se han predefinido los objetos de periodo de validez siguientes:

```
Validity Name   = allTheTime
        Duration  = Forever
        Months    = ALL
        Days      = ALL
        Hours     = All Day

Validity Name   = allTheTimeMonThruFri
        Duration  = Forever
        Months    = ALL
        Days      = MON TUE WED THU FRI
        Hours     = All Day

Validity Name   = 9to5MonThruFri
        Duration  = Forever
        Months    = ALL
        Days      = MON TUE WED THU FRI
        Hours     = 09:00:00 : 17:00:00

Validity Name   = 5to9MonThruFri
        Duration  = Forever
        Months    = ALL
        Days      = MON TUE WED THU FRI
        Hours     = 17:00:00 : 09:00:00
```

Acciones de DiffServ

Se han predefinido los objetos de acciones de DiffServ siguientes:

```
DiffServ Name   = EF                            Type =Permit
        DS mask:modify =xFC:xB8
        Queue:BwShare  =Premium    : 19 %
        Token Rate:    = 0 bytes/sec
        Token Bucket:  = 0 bytes

DiffServ Name   = AF11                           Type =Permit
        DS mask:modify =xFC:x28
        Queue:BwShare  =Assured    : 15 %
        No Policing Selected

DiffServ Name   = AF21                           Type =Permit
        DS mask:modify =xFC:x48
        Queue:BwShare  =Assured    : 10 %
        No Policing Selected

DiffServ Name   = AF31                           Type =Permit
        DS mask:modify =xFC:x68
        Queue:BwShare  =Assured    : 10 %
        No Policing Selected

DiffServ Name   = AF41                           Type =Permit
        DS mask:modify =xFC:x88
        Queue:BwShare  =Assured    : 5 %
```

Acciones de IPSec

Se han predefinido los objetos de acciones de IPSec siguientes:

```
IPSECAction Name = ipsecDropTraffic
        Action   = Drop

IPSECAction Name = ipsecPassTrafficClear
        Action   = Clear
```

Propuestas de IPSec para la fase 2 de IKE

Se han predefinido los objetos de propuestas de IPSec siguientes para la fase 2 de IKE:

```
Name  = strongP2EspProp
        Pfs   = N
        ESP Transforms:
                espTunnelMD5andDES
                espTunnelSHAandDES

Name  = strongP2EspAhProp
        Pfs   = N
        AH Transforms:
                ahTunnelMD5
                ahTunnelSHA
        ESP Transforms:
                espTunnelDES

Name  = veryStrongP2EspProp
        Pfs   = N
        ESP Transforms:
                espTunnelSHAand3DES
                espTunnelMD5and3DES

Name  = veryStrongP2EspAhProp
        Pfs   = N
        AH Transforms:
                ahTunnelSHA
                ahTunnelMD5
        ESP Transforms:
                espTunnel3DES

Name  = veryStrongP2EspPropPFS
        Pfs   = Y     DHGrp= 1
        ESP Transforms:
                espTunnelSHAand3DES
                espTunnelMD5and3DES

Name  = strongP2EspPropXport
        Pfs   = N
        ESP Transforms:
                espTransportMD5andDES
                espTransportSHAandDES

Name  = strongP2EspAhPropXport
        Pfs   = N
        AH Transforms:
                ahTransportMD5
                ahTransportSHA
        ESP Transforms:
                espTransportDES
```

```
Name  = veryStrongP2EspPropXport
        Pfs   = N
        ESP Transforms:
                espTransportSHAand3DES
                espTransportMD5and3DES

Name  = strongP2EspAhPropXport
        Pfs   = N
        AH Transforms:
                ahTransportMD5
                ahTransportSHA
        ESP Transforms:
                espTransportDES

Name  = veryStrongP2EspPropXport
        Pfs   = N
        ESP Transforms:
                espTransportSHAand3DES
                espTransportMD5and3DES

Name  = veryStrongP2EspAhPropXport
        Pfs   = N
        AH Transforms:
                ahTransportSHA
                ahTransportMD5
        ESP Transforms:
                espTransport3DES

Name  = veryStrongP2EspPropXport
        Pfs   = N
        ESP Transforms:
                espTransportSHAand3DES
                espTransportMD5and3DES

Name  = veryStrongP2EspAhPropXport
        Pfs   = N
        AH Transforms:
                ahTransportSHA
                ahTransportMD5
        ESP Transforms:
                espTransport3DES

Name  = veryStrongP2EspPropPFSXport
        Pfs   = Y     DHGrp= 1
        ESP Transforms:
                espTransportSHAand3DES
                espTransportMD5and3DES

Name  = veryStrongP2EspAhPropPFSXport
        Pfs   = Y     DHGrp= 1
        AH Transforms:
                ahTransportSHA
                ahTransportMD5
        ESP Transforms:
                espTransport3DES
```

Transformaciones de IPSec

Se han predefinido los objetos de transformaciones de IPSec siguientes:

```
Transform Name  = ahTransportMD5
        Type =AH    Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =None

Transform Name  = ahTransportSHA
        Type =AH    Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =None

Transform Name  = ahTunnelMD5
        Type =AH    Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =None

Transform Name  = ahTunnelSHA
        Type =AH    Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =None

Transform Name  = espTunnelMD5andDES
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =DES

Transform Name  = espTunnelSHAandDES
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =DES

Transform Name  = espTunnelMD5and3DES
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =3DES

Transform Name  = espTunnelSHAand3DES
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =3DES

Transform Name  = espTunnelDES
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =None  Encr =DES

Transform Name  = espTunnel3DES
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =None  Encr =3DES

Transform Name  = espTransportMD5andDES
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =DES

Transform Name  = espTransportSHAandDES
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =DES

Transform Name  = espTransportMD5and3DES
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =3DES

Transform Name  = espTransportSHAand3DES
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =3DES

Transform Name  = espTransportDES
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =None  Encr =DES
```

```
Transform Name  = espTransport3DES
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =None  Encr =3DES
```

Acciones de ISAKMP

Se han predefinido los objetos de acciones de ISAKMP siguientes:

```
ISAKMP Name     = generalPhase1Action
        Mode                    =            Main
        Min Percent of SA Life  =               1
        Conn LifeSize:LifeTime  =            5000 : 30000
        Autostart               =              No
        ISAKMP Proposals:
                veryStrongP1PropRSACert
                strongP1PropRSACert
                veryStrongP1PropSharedKey
                strongP1PropSharedKey
```

Propuestas de ISAKMP

Se han predefinido los objetos de propuestas de ISAKMP siguientes:

```
Name = strongP1PropSharedKey
        AuthMethod = Pre-Shared Key
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = MD5
        Encr Algo  = DES CBC

Name = strongP1PropRSACert
        AuthMethod = Certificate (RSA SIG)
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = MD5
        Encr Algo  = DES CBC

Name = veryStrongP1PropSharedKey
        AuthMethod = Pre-Shared Key
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = SHA
        Encr Algo  = 3DES CB

Name = veryStrongP1PropRSACert
        AuthMethod = Certificate (RSA SIG)
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = SHA
        Encr Algo  = 3DES CB
```

Configuración y supervisión de la característica de política

Este capítulo describe el LDAP y los mandatos de política proporcionados por la característica de política para configurar y utilizar los dispositivos del direccionador en una red. El capítulo incluye las secciones siguientes:

Acceso al indicador de mandatos de configuración de política

Para entrar mandatos de configuración de política:

1. Entre **talk 6** en el indicador de mandatos OPCON (*).
2. Entre **feature policy** en el indicador de mandatos `Config>`.

Se visualiza el indicador de mandatos `Policy config>`. Ahora se pueden entrar mandatos de configuración de política.

Mandatos de configuración de política

Estos mandatos le permiten configurar la información contenida en las políticas. La Tabla 39 resume los mandatos de configuración de política y el resto de la sección los describe detalladamente. Entre estos mandatos en el indicador de mandatos `Policy config>`. Puede entrar el mandato y las opciones en una línea o entrar solamente el mandato y responder a las solicitudes. Para ver una lista de las opciones de mandatos válidas, entre el mandato con un interrogante en lugar de las opciones.

Tabla 39. Mandatos de configuración de política

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxx.
Add	Añade la información utilizada para crear una política.
Change	Cambia la información que compone una política.
Copy	Copia información de una política a otra.
Delete	Suprime información de una política.
Disable	Inhabilita una política.
Enable	Habilita una política.
List	Visualiza la información de una política.
Qconfig	Le permite añadir una política basada en plantillas predefinidas.
refresh-templates	Le permite instalar o quitar las plantillas más actuales para la versión de código que se ejecuta en una plataforma específica. Esto facilita el cambio entre diversos niveles de PTF y de release de software, haciendo que sea más simple tomar la decisión de efectuar dicho cambio.
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 a una política.

Sintaxis: add
- diffserv-action
- interface-pair
- ipsec-action
- ipsec-manual-tunn
- ipsec-proposal
- ipsec-transform
- isakmp-action
- isakmp-proposal
- policy
- profile
- rsvp-action
- user
- validity-period

diffserv-action Le solicita información sobre qué selecciones de DiffServ-action deben aplicarse. Para obtener detalles, consulte el apartado “Utilización de la característica Servicios diferenciados” en la página 383 y el apartado “Configuración y supervisión de la característica Servicios diferenciados” en la página 393.

name El nombre exclusivo de la acción de DiffServ para la política.

permission level Especifica si el direccionador debe reenviar paquetes que coincidan con esta acción de DiffServ.

1
Permitir

2
Denegar

Valor por omisión: 2

queue number La cola en la que se sitúan los paquetes de salida que coinciden con la acción de DiffServ.

1
Primera calidad (EF)

2
Asegurada (AF)/Mayor eficacia

Valor por omisión: 2

bwshare type El tipo de asignación de compartimiento de ancho de banda.

1
Absoluta (en kbps)

2
Porcentaje (del ancho de banda de salida total)

Valor por omisión: 2

bwshare El ancho de banda (en kbps o como porcentaje del ancho de banda de salida) asignado a este servicio.

Reenvío asegurado

Assured forwarding class Especifica la clase de reenvío asegurado para los paquetes de salida que coincidan con esta acción de DiffServ.

1
Byte DS de clase AF1

2
Byte DS de clase AF2

3
Byte DS de clase AF3

4
Byte DS de clase AF4

5
Clase nueva

Assured forwarding policing type Especifica el tipo de política AF para los paquetes de salida que coincidan con esta acción de DiffServ.

1
TCM sin distinción de color, de velocidad única

2
TCM con distinción de color, de velocidad única

3
TCM sin distinción de color, de dos velocidades

4
TCM con distinción de color, de dos velocidades

5
Ninguno

Parámetros de TCM de velocidad única

Committed information rate (CIR) Especifica la velocidad de información comprometida.

Committed burst size (CBS) Especifica el tamaño de ráfaga comprometido.

Excess burst size (EBS) Especifica el tamaño de ráfaga excesivo.

Notas:

1. Especifique la CIR en bytes de paquetes IP por segundo. Esto incluye la cabecera IP, pero no la cabecera específica del enlace.
2. Especifique el CBS y el EBS en bytes. Estos valores deben configurarse de forma que al menos uno de ellos sea mayor que cero. Se recomienda que, cuando el valor del CBS o del EBS sea mayor que cero, sea mayor que, o igual a, el tamaño del paquete IP más grande posible de la corriente.

Parámetros de TCM de dos velocidades

Committed information rate (CIR) Especifica la velocidad de información comprometida.

Committed burst size (CBS) Especifica el tamaño de ráfaga comprometido.

Peak information rate (PIR) Especifica la velocidad máxima de la información.

Peak burst size (PBS) Especifica el tamaño máximo de ráfaga.

Notas:

1. Especifique la CIR y la PIR en bytes de paquetes IP por segundo. Esto incluye la cabecera IP, pero no la cabecera específica del enlace. El valor de PIR debe ser igual o mayor que la CIR.
2. Especifique el CBS y el PBS en bytes. Ambos deben configurarse en valores mayores que cero y mayores que, o iguales a, el tamaño del paquete IP más grande posible de la corriente.

Reenvío acelerado

transmitted ds-byte mask Máscara que debe aplicarse a los bytes ds transmitidos para el reenvío acelerado. Este valor designa qué bits de un byte DS de un paquete deben cambiarse cuando se transmite el paquete. Un cero en alguna posición de bit de este byte implica que el bit no debe cambiarse.

Valor por omisión: 00 (no cambie ningún bit)

transmitted ds-byte modify value Marca del byte IP DS (TOS) para el reenvío acelerado que debe aplicarse a los paquetes que debe reenviar este dispositivo. Ceros en la máscara implican que el bit correspondiente no se cambiará. Un uno implica que el bit se marcará con el valor de bit en el byte de marca. La operación es: nuevoByteTOS = (Máscaraˆ & ByteTOSrecibido) | (Máscara&Marca) El ˆ ^ ∧ es un complemento basado en el bit (Máscara:Marca)

Ejemplo:

```
11111101:00000001
```

Utilizando este ejemplo, un valor recibido 0x07 se enviaría con un valor de 0x03

Valor por omisión: X'00' (no cambiar ningún bit)

EF policing type Especifica el tipo de configuración de política de reenvío acelerado.

1

Configuración por omisión

Los parámetros de velocidad de señal y de tamaño de cubeta de señales se calcularán a partir de la configuración de parámetros de ancho de banda.

2

Configuración personalizada

Token Rate: Velocidad de reaprovisionamiento de señales.

Token Bucket Size: Tamaño de cubeta de señales.

Notas:

1. Especifique la velocidad de señal en bytes de paquetes IP por segundo. Esto incluye la cabecera IP, pero no las cabeceras específicas del enlace.
2. Especifique el tamaño de cubeta de señales en bytes. El valor debe ser mayor que cero y mayor que, o igual a, el tamaño del paquete IP más grande de la corriente.

interface-pair
El par de interfaces asociado a un perfil con una interfaz o conjunto de interfaces específicas. Por omisión, el objeto de perfil no restringe la aplicación de la política a cualquier interfaz. Si esto fuera necesario, puede añadir pares de interfaces para conseguirlo. El par de interfaces especifica la dirección IP de la interfaz a la que debe llegar el tráfico y la dirección IP de la interfaz de la que debe salir el tráfico.

El ejemplo siguiente muestra dos pares de interfaces con el mismo nombre, que representan el tráfico que procede de cualquier interfaz y que sale de la interfaz pública, y viceversa.

```
1) Group Name: inOutPublic
        In:Out=255.255.255.255 : 1.1.1.1
        In:Out=1.1.1.1 : 255.255.255.255
```

Name
El nombre del par de interfaces.

Ingress interface
Dirección IPv4 de la interfaz de entrada.

Valor por omisión: 255.255.255.255 (cualquiera)

Egress interface
Dirección IPv4 de la interfaz de salida.

Valor por omisión: 255.255.255.255 (cualquiera)

IPSec-action
Le solicita información para configurar el túnel de la Fase 2.

Name
El nombre de la acción IPSec.

Action type
La acción que debe aplicarse a los paquetes que coinciden con el perfil de una política que contiene esta acción.

1 Bloquear (bloquear conexión).

2 Permitir (Permitir paquetes que coincidan con esta acción.) Si no existe ninguna proposición de IPSec, pasar el paquete; si existe una proposición de IPSec, aplicar el proceso de seguridad de IPSec al paquete.

Valor por omisión: 2

La opción siguiente sólo está disponible si especifica pasar como tipo de acción:

Traffic flow type
Tipo de flujo de tráfico (túnel de seguridad o fiable).

1
Borrar

2
Túnel de seguridad

Valor por omisión: 2

La opción siguiente sólo está disponible si especifica el flujo de tráfico como seguro:

Tunnel start point
Dirección IPv4 del punto de inicio del túnel.

Tunnel end point
Dirección IPv4 del punto final del túnel. (0.0.0.0 para acceso remoto)

Valor por omisión: 0.0.0.0

Tunnel-in-tunnel
Especifica si el tráfico protegido por este túnel debe protegerse adicionalmente mediante otra política configurada en este dispositivo.

Opciones válidas: Yes (Sí) o No

Valor por omisión: No

Percentage of SA lifesize/lifetime to accept
Tamaño/duración mínimo de SA (como porcentaje) del tamaño/duración de SA. Un tamaño/duración de SA recibido con un valor menor que éste no se acepta.

Valor por omisión: 75

SA refresh threshold
El porcentaje del valor de duración o tamaño de SA que la SA debe renovar automáticamente.

Valor por omisión: 85

DF-Bit-Setting
Especifica si debe copiarse el bit Don't Fragment (No Fragmentar) del paquete original y si debe establecerse o borrarse en la cabecera exterior del paquete IPSec si se ejecuta en modalidad de túnel.

1
Copiar

2
Establecer

3
Borrar

Valor por omisión: 1

Replay-Prevention
Especifica si IPSec debe imponer la prevención de reproducción para los paquetes IPSec recibidos. En esta modalidad IPSec asegura que los números de secuencia sean válidos y que no se reciban más de una vez.

1
Habilitar

2
Inhabilitar

Valor por omisión: 2

Negotiate SA Automatically
Especifica si la SA de la Fase 2 se negocia automáticamente durante la inicialización del sistema.

Yes (Sí) o No

Valor por omisión: No

IPSec proposal
El nombre de la propuesta de IPSec (puede especificar un máximo de cinco propuestas) a enviar o comprobar durante la Fase 2. El orden con el que se especifican determina su prioridad, siendo la primera la que tiene la máxima prioridad.

IPSec-manual-tunn
Le solicita información para configurar manualmente el túnel de la Fase 2.

Tunnel name
El nombre del túnel manual IPSec.

Tunnel lifetime
La duración del túnel (en minutos).

Valor por omisión: 46080

Encapsulation mode
La modalidad de encapsulación que debe utilizarse.

tunn
Modalidad de túnel

trans
Modalidad de transporte

Valor por omisión: tunn

Policy
El tipo de política de túnel que debe utilizarse.

AH
Cabecera de autentificación

ESP
Carga de seguridad de encapsulación

AH-ESP
Para paquetes de salida, especifica que el cifrado se ejecuta antes que la autentificación.

ESP-AH
Para paquetes de salida, especifica que la autentificación se ejecuta antes que el cifrado.

Valor por omisión: AH-ESP

Local IP address (Dirección IP local)
La dirección IPv4 de origen.

Valor por omisión: 11.0.0.5

Local encryption SPI
El valor de índice de los parámetros de seguridad de origen.

Valor por omisión: 256

Local encryption algorithm
El algoritmo de cifrado de origen.

Null (Nulo)
Sin cifrado.

CDMF
Commercial Data Masking Facility.

DES-CBC
Data Encryption Standard y Cipher Block Chaining.

3DES
Triple Data Encryption Standard.

Valor por omisión: DES-CBC

Local encryption key
Una clave de 16 caracteres.

Padding
Relleno adicional para el cifrado local.

Valor por omisión: 0

Local ESP authentication
Especifica si debe utilizarse autentificación ESP local.

Yes (Sí) o No

Valor por omisión: Yes (Sí)

Remote IP address
La dirección IPv4 de destino.

Valor por omisión: 0.0.0.0

Remote encryption SPI
El valor de índice de los parámetros de seguridad de destino.

Valor por omisión: 256

Remote encryption algorithm
El algoritmo de cifrado de destino.

Null (Nulo)
Sin cifrado.

CDMF
Commercial Data Masking Facility.

DES-CBC
Data Encryption Standard y Cipher Block Chaining.

3DES
Triple Data Encryption Standard.

Valor por omisión: DES-CBC

Remote encryption key
Una clave de 16 caracteres.

Verify remote encryption padding
Especifica si debe verificarse o no el relleno de cifrado remoto.

Yes (Sí) o No

Valor por omisión: No

Remote ESP authentication
Especifica si debe utilizarse o no autentificación ESP remota.

Yes (Sí) o No

Valor por omisión: Yes (Sí)

DF bit
Especifica cómo procesar el bit de Don't Fragment (No Fragmentar).

Copy
Copia el bit DF.

Set
Activa el bit DF.

Clear
Desactiva el bit DF.

Valor por omisión: COPY

Enable tunnel
Especifica si debe habilitarse o no el túnel cuando se crea.

Yes (Sí) o No

Valor por omisión: Yes (Sí)

IPSec-proposal
Le solicita información para crear una propuesta de IPSec.

IPSec proposal name
El nombre de la propuesta de IPSec.

Perfect forward secrecy
Especifica si debe utilizarse IKE, para evitar que nadie determine una clave actual a partir de una clave previamente comprometida.

Yes (Sí) o No

Valor por omisión: No

Diffie Hellman Group ID
El tipo de grupo Diffie Hellman.

1
Grupo Diffie Hellman 1

2
Grupo Diffie Hellman 2

Valor por omisión: 1

AH transform
El nombre de la conversión AH (puede especificar un máximo de cinco conversiones) para esta propuesta. El orden con el que se especifican determina su prioridad, siendo la primera la que tiene la máxima prioridad.

ESP transform
El nombre de la conversión ESP (puede especificar un máximo de cinco propuestas) para esta propuesta. El orden con el que se especifican determina su prioridad, siendo la primera la que tiene la máxima prioridad.

IPSec-transform
Le solicita información sobre conversiones de IPSec.

IPSec transform name
El nombre de la conversión de IPSec.

Protocol ID
El protocolo de seguridad que debe utilizarse.

1
IPSec-AH

2
IPSec-ESP

Valor por omisión: 1

AH Authentication Algorithm
El algoritmo de autentificación de AH que debe utilizarse.

1
HMAC-MD5

2
HMAC-SHA

Valor por omisión: 1

Encapsulation mode
La modalidad de encapsulación que debe utilizarse.

1
Túnel

2
Transporte

Valor por omisión: 1

ESP Authentication Algorithm
El algoritmo de autentificación ESP que debe utilizarse.

0
Ninguno

1
HMAC-MD5

2
HMAC-SHA

Valor por omisión: 2

ESP cipher algorithm
El algoritmo de cifrado ESP que debe utilizarse.

1
ESP DES

2
ESP 3DES

3
ESP CDMF

4
ESP Nulo (sin cifrado)

Valor por omisión: 1

SA lifesize
Duración (en kb) de la SA para esta propuesta.

Valor por omisión: 50000

SA lifetime
La duración (en segundos) de la SA para esta propuesta.

Valor por omisión: 3600

ISAKMP-Action
Le solicita información sobre qué acción de ISAKMP debe aplicarse.

Name
El nombre de la acción de ISAKMP.

Exchange mode
El tipo de modalidad de intercambio para las negociaciones de la Fase 1.

1
Principal

2
Agresiva

Valor por omisión: 1

Percentage of Minimum SA lifesize/lifetime
Tamaño/duración mínimo de SA (como porcentaje) del tamaño/duración de SA. Un tamaño/duración de SA con un valor menor que éste no se acepta.

Valor por omisión: 75

ISAKMP connection lifesize
Duración (en kb) de la conexión de la Fase 1. Una vez caducada la conexión de la Fase 1, la próxima vez que debe renovarse la SA de la Fase 2, la Fase 1 vuelve a negociarse por completo para poder iniciar la Fase 2.

Valor por omisión: 5000

ISAKMP connection lifetime
La duración (en segundos) de la conexión de la Fase 1. Una vez caducada la conexión de la Fase 1, la próxima vez que debe renovarse la Fase 2, la Fase 1 se inicia de nuevo por completo.

Valor por omisión: 5000

Negotiate SA automatically
Especifica si la SA se negocia automáticamente durante la inicialización del sistema.

Yes (Sí) o No

Valor por omisión: No

ISAKMP proposal
El nombre de la propuesta de ISAKMP (puede especificar un máximo de cinco propuestas) a enviar o comprobar durante la modalidad rápida de la Fase 2. El orden con el que se especifican determina su prioridad, siendo la primera la que tiene la máxima prioridad.

ISAKMP-Proposal
Le solicita la información de propuesta de ISAKMP que se utiliza en las negociaciones de ISAKMP.

ISAKMP proposal name
El nombre de la proposición de ISAKMP.

Authentication method
El tipo de autentificación que debe utilizarse durante las negociaciones de la Fase 1 de ISAKMP.

1
Clave precompartida

2
RSA SIG (modalidad certificada)

Valor por omisión: 1

Hash algorithm
El tipo de algoritmo hash que debe utilizarse durante las negociaciones de la Fase 1.

1
MD5

2
SHA

Valor por omisión: 1

Cipher algorithm
El tipo de algoritmo de cifrado que debe utilizarse durante las negociaciones de la Fase 1.

1
DES

2
3DES

Valor por omisión: 1

Diffie Hellman Group ID
El tipo de grupo Diffie Hellman que debe utilizarse durante las negociaciones de la Fase 1.

1
Grupo Diffie Hellman 1

2
Grupo Diffie Hellman 2

Valor por omisión: 1

SA lifesize
Duración (en kb) de la SA para esta propuesta.

Valor por omisión: 50000

SA lifetime
La duración (en segundos) de la SA para esta propuesta.

Valor por omisión: 5000

Policy
Le solicita información sobre la configuración de política: Nombre de perfil (necesario), nombre de RSVP (opcional), nombre de DiffServ (opcional), nombre de IPSec (opcional), nombre de ISAKMP (opcional) y Perfil de período de validez (opcional). Debe especificar DiffServ, IPSec, ISAKMP o RSVP para que la política sea válida.

Valor por omisión: Válida todo el tiempo

Name El nombre de la configuración de política

Priority La prioridad relativa de esta política respecto a otras políticas (cuando más alto es el número, más alta es la prioridad). Se utiliza para resolver conflictos si se aplican varias políticas a un paquete.

Valor por omisión: 5

Profile El nombre de un perfil de tráfico de datos previamente configurado para utilizar esta política.

Validity period
El nombre de un período de validez configurado previamente para utilizar esta política.

IPSec action
Si esta política va a imponer una acción de IPSec, el nombre de una acción de IPSec previamente configurada a utilizar para esta política. Si especifica una acción de IPSec segura, también debe especificar una acción de ISAKMP.

ISAKMP action
El nombre de una acción de ISAKMP previamente configurada a utilizar para esta política. Si especifica una acción de ISAKMP, también debe especificar una acción de IPSec.

Diffserv action
Si desea correlacionar una acción de DiffServ con esta política, el nombre de una acción de DiffServ previamente configurada.

RSVP action
El nombre de una acción de RSVP para esta política a imponer.

Profile
Le solicita información para definir un conjunto de selectores (condicionales) para un perfil de política en el cual deben realizarse acciones.

name
El nombre del perfil de política.

ipv4-src-address-format
El formato de la dirección IPv4 de origen (rango, máscara de red, única dirección).

ipv4-src-address
La dirección IPv4 de origen (dirección baja si el formato de dirección es de tipo *rango*).

Valor por omisión: 0.0.0.0

ipv4-src-mask
La máscara IPv4 de origen (dirección alta si el formato de dirección es de tipo *rango*).

Valor por omisión: 255.0.0.0

ipv4-dest-address-format
El formato de la dirección IPv4 de destino (rango, máscara de la red, única dirección).

ipv4-dest-address
La dirección IPv4 de destino (dirección baja si el formato de dirección es de tipo *rango*).

Valor por omisión: 0.0.0.0

ipv4-dest-mask
La máscara IPv4 de destino (dirección alta si el formato de dirección es de tipo *rango*).

Valor por omisión: 255.0.0.0

protocol-id
ID de protocolo en el que se debe filtrar.

1
TCP

2
UDP

3
Todos los protocolos

4
Especificar rango

Valor por omisión: 3

src-port-start
El primer número de puerto dentro del rango de números de puerto de origen.

Valor por omisión: 0

src-port-end
El último número de puerto dentro del rango de números de puerto de origen.

Valor por omisión: 65535

dest-port-start
El primer número de puerto dentro del rango de números de puerto de destino.

Valor por omisión: 0

dest-port-end
El último número de puerto dentro del rango de números de puerto de destino.

Valor por omisión: 65535

src-id-type
El tipo de ID de origen, que se envía al remoto. Este valor se utiliza para determinar qué política contiene la información de ISAKMP necesaria durante las negociaciones de la Fase 1 de ISAKMP. Se compara con la información contenida en la carga útil de identificación del paquete de ISAKMP. Esta información es necesaria si el similar remoto debe identificar el dispositivo con un valor que no sea la dirección IP.

1
Punto final de túnel local

2
Nombre de dominio completamente calificado de sistema principal

3
Nombre de dominio completamente calificado de usuario

4
ID de clave

any-user-access
Permitir el acceso a cualquier usuario dentro de la definición de perfil. Si especifica No, se le solicita el nombre del grupo de usuarios remotos para este perfil. Este atributo sólo es necesario si desea limitar el acceso de los similares de acceso remoto a una política específica.

Yes (Sí) o No

Valor por omisión: Yes (Sí)

Received DS byte mask
Máscara de 8 bits a aplicar al byte DS (TOS) de un paquete de entrada.

Valor por omisión: 0

Received DS byte match
Patrón de 8 bits a comparar con el resultado de aplicar AND entre el byte DS (TOS) de entrada y el valor de Received DS byte mask.

Valor por omisión: 0

Interface pairs
Si esta política debe limitar los flujos de tráfico a interfaces específicas, es el nombre del grupo de pares de interfaces.

RSVP-Action
Le solicita información sobre qué acciones de RSVP deben aplicarse.

Name
El nombre de la acción de RSVP.

Permission
Especifica el nivel de permiso para las sesiones de RSVP que coinciden con esta acción.

1
Permitir

2
Denegar

Valor por omisión: 2

Max token rate
Cantidad máxima de ancho de banda (en kbps) que RSVP debe asignar para un flujo individual.

Valor por omisión: 100

Max duration
La cantidad máxima de tiempo (en segundos) que puede durar un flujo (0 implica eternamente).

Valor por omisión: 600

RSVP-to-DS
Especifica si deben correlacionarse flujos de RSVP que coincidan con esta acción con una acción de DiffServ configurada. RSVP utiliza la información de la acción de DiffServ para marcar el byte de TOS para el siguiente dispositivo de comunicaciones en sentido inverso con DiffServ habilitado. Se utiliza en una red en la que los paquetes salen de una red con RSVP habilitado y se dirigen a una red con DiffServ habilitado.

Yes (Sí) o No

Valor por omisión: No

User
Le solicita información acerca de la definición de perfil de usuario para el similar IKE remoto. Esta información incluye cómo debe identificarse a sí mismo el similar durante las negociaciones de la fase 1, el método de autentificación a utilizar para este similar y, si el mecanismo de autentificación es de clave precompartida, el valor de clave a utilizar. Si utiliza la clave precompartida, **deberá** definir un usuario a fin de asociar la clave precompartida con un nombre y un tipo de ID. Este mandato establece la clave que se utiliza en la negociación de la fase 1 para un usuario determinado. La clave se utiliza en los mensajes 1 y 5 para los iniciadores y en los mensajes 2 y 6 para los respondedores.

Identification
Identificación del usuario. Para la autentificación en modalidad principal, el tipo de identificación de usuario **debe** ser la dirección IP. Para la autentificación en modalidad agresiva, el tipo de identificación debe ser uno de los demás tipos. El motivo de ello es que, dado que en modalidad principal los ID no se intercambian hasta los mensajes 5 y 6, lo cual es demasiado tarde para la clave precompartida, el único mecanismo de búsqueda es mediante la dirección IP del similar IKE. En modalidad agresiva, dado que los ID se intercambian en los mensajes 1 y 2, la búsqueda de clave precompartida puede efectuarse a través del tipo de ID y del valor correspondiente.

1 Dirección IP.

2 Nombre de dominio completamente calificado.

3 Nombre de dominio completamente calificado de usuario.

4 ID de clave (cualquier serie).

Valor por omisión: 1

Group
Nombre del grupo en el que debe colocarse este usuario.

Valor por omisión: ninguno

Authentication
Método de autentificación que debe utilizarse con el similar.

1 Clave precompartida.

1 Clave en formato ASCII.

Valores válidos: Un número par de 2 a 128 caracteres

2 Clave en formato hexadecimal.

Valores válidos: Un número par de 2 a 256 dígitos hexadecimales

2 Certificado público.

Valor por omisión: 1

VALIDITY-PERIOD
Le solicita información sobre el período durante el cual la política es válida y crea un perfil de política.

Name
El nombre del perfil de período de validez.

yyyymmddhhmmss:yyyymmddhhmmss
(aaaammddhhmmss:aammddhhmmss)
El período durante el cual las políticas que contienen este perfil de período de validez son válidas.

Ejemplo:

```
19980101000000:19981231000000
```

Months
Los meses durante los cuales las políticas que contienen este perfil de período de validez son válidas. Puede especificar cualquier secuencia de meses, utilizando las tres primeras letras de cada mes (por ejemplo, jan para enero o dic para diciembre), con los meses separados por espacios o puede especificar `all` (todos) para indicar todos los meses del año.

Days
Las fechas durante las cuales las políticas que contienen este perfil de período de validez son válidas. Puede especificar cualquier secuencia de fechas, utilizando las tres primeras letras de cada día (por ejemplo, mon para lunes o fri para viernes), con los días separados por espacios o puede entrar `all` (todos) para indicar todos los días de la semana.

Starting time
La hora en la que las políticas que contienen este perfil de período de validez son válidas. Especifíquela con el formato hh:mm:ss o especifique * si desea que la política sea válida todo el día.

Valor por omisión: *

Ending time
La hora en la que la que caduca la validez de las políticas que contienen este perfil de período de validez. Especifíquela con el formato hh:mm:ss.

Valor por omisión: Ninguna

Change

Utilice el mandato **change** para cambiar la información de un objeto de política. Consulte la descripción del mandato **add** para conocer cuáles son los objetos disponibles.

Copy

Utilice el mandato **copy** para copiar información de un objeto de política a otro. Consulte la descripción del mandato **add** para conocer cuáles son los objetos disponibles. (Las opciones de par de interfaces (interface-pair), túnel manual y usuario (user) no se aplican al mandato **copy**).

Delete

Utilice el mandato **delete** para suprimir información de un objeto de política. Consulte la descripción del mandato **add** para conocer cuáles son los objetos disponibles.

Disable

Utilice el mandato **disable** para inhabilitar una configuración de política.

Sintaxis: disable policy

Policy
Le solicita el nombre de la configuración de política que debe inhabilitarse.

Enable

Utilice el mandato **enable** para habilitar una configuración de política.

Sintaxis: enable policy

Policy
Le solicita el nombre de la configuración de política que debe habilitarse.

List

Utilice el mandato **list** para visualizar toda la información de configuración de política o una parte de la misma.

Sintaxis: list all
default-policy
ldap
refresh

All Visualiza toda la información de configuración de política.

Default-policy
Visualiza el nombre de la política por omisión.

LDAP
Visualiza los nombres de las configuraciones de LDAP definidas.

Refresh
Lista el estado de renovación de política (Habilitar o Inhabilitar) y la hora del intervalo de renovación.

Qconfig

Utilice el mandato **qconfig** para crear rápidamente políticas de seguridad para un dispositivo de red. Una vez que ha seleccionado un escenario de configuración en una lista corta, el mandato visualiza una serie breve de preguntas simples basándose en la selección. Entonces crea una política entera utilizando plantillas predefinidas relacionadas con el escenario (conjuntos completos de opciones de política compatibles). Esto elimina la necesidad de que especifique cada detalle de la política, reduciendo el tiempo necesario para configurar una política y las posibilidades de cometer un error.

Este mandato le solicita que especifique un nivel de seguridad para todos los escenarios excepto el escenario Custom (Personalizado).

Sintaxis: qconfig *nombre-política*
escenario

nombre-política
Especifica un nombre (de un máximo de 29 caracteres) a asignar a la política.

Valor por omisión: Nombre exclusivo generado por el sistema.

escenario
Especifica el escenario para el que se debe crear una política.

Valor por omisión: ninguno

1 Branch office scenario.

Esta selección le permite especificar las opciones de política para una conexión protegida entre dos Pasarelas de seguridad que protegen subredes locales.

Las opciones son:

Local IP Subnet

Local IP Tunnel Endpoint

Remote IP Subnet

Remote IP Tunnel Endpoint

Ports and Protocols

Security Level

1: Seguridad fuerte. Seleccione esta opción si desea seguridad, rendimiento y flexibilidad. Negocia un conjunto de propuestas (sin PFS) que incluye combinaciones de algoritmos de autentificación SHA y MD5 y algoritmos de cifrado DES y 3DES. Las propuestas potentes se negocian primero, seguidas de las propuestas más potentes, a fin de no comprometer el rendimiento.

2: Seguridad muy fuerte. Seleccione esta opción si necesita el nivel más alto de seguridad. Negocia un pequeño conjunto de propuestas (con PFS, Grp 1) que incluye combinaciones de

algoritmos de autentificación SHA y MD5 y algoritmos de cifrado 3DES.

Authentication Method

1: Clave precompartida - clave ASCII

2: Certificado (Firmas RSA) - ID local

DiffServe Actions

0:Best Effort (No DiffServ)

1:EF

2:AF11

3:AF21

4:AF31

5:AF41

Cualquier otra acción DiffServ configurada localmente también aparece en esta lista.

Validity Periods

1. 1: allTheTime
2. 2: allTheTimeMonThruFri
3. 3: 9to5MonThruFri
4. 4: 5to9MonThruFri

Cualquier otro periodo de validez configurado localmente también aparece en esta lista.

Priority of Policy

2 Remote access user scenario (IPSec and L2TP).

Esta selección le permite especificar las opciones de política para una conexión protegida entre una Pasarela de seguridad y usuarios de acceso remoto. Este escenario supone que el cliente de acceso remoto tiene la posibilidad de ejecutar L2TP sobre IPSec en modalidad de transporte.

L2TP configura una conexión de punto a punto entre la dirección IP pública del cliente de acceso remoto y la dirección IP pública de la pasarela de seguridad. UDP proporciona la conexión de la capa de transporte y los puertos de origen y destino son 1701. Es importante que L2TP se configure para el puerto de origen udp fijo (fixed-udp-source-port) en el direccionador que efectúa la función de pasarela de seguridad. IPSec proporciona la protección para la conexión L2TP en estos puertos y protocolos.

Una vez que se ha completado el escenario de configuración, deberá añadir usuarios en la característica de política para cualquiera que se vaya a autentificar utilizando la clave precompartida. Para la autentificación de certificado, deberá configurar los parámetros PKI en el direccionador y asegurarse de que se han cargado los certificados apropiados.

Las opciones son:

IP address of secure interface.

Normalmente es el mismo valor que el punto final de túnel IP local. Representa la dirección IP de la interfaz en la que los paquetes se envían protegidos y llegan protegidos.

Security Level

1: Seguridad fuerte

2: Seguridad muy fuerte

DiffServe Actions

0:Best Effort (No DiffServ)

1:EF

2:AF11

3:AF21

4:AF31

5:AF41

Cualquier otra acción DiffServ configurada localmente también aparece en esta lista.

Validity Periods

1. 1: allTheTime
2. 2: allTheTimeMonThruFri
3. 3: 9to5MonThruFri
4. 4: 5to9MonThruFri

Cualquier otro periodo de validez configurado localmente también aparece en esta lista.

Priority of Policy

3 Excluir tráfico que no coincide en interfaz no fiable. Este escenario es necesario para configuraciones en las que el dispositivo actúa como cortafuegos. En muchas configuraciones de red hay un cortafuegos delante de la pasarela de seguridad y no se necesita ninguna norma de exclusión. Si necesita una regla de exclusión, seleccione este escenario.

Las opciones son:

IP address of untrusted interface.

Es la dirección IP de la interfaz para la que se excluyen los paquetes no deseables. Normalmente, es la dirección IP de la conexión a la red pública o no fiable.

4 **Custom scenario.**

Esta selección proporciona la mayor flexibilidad al utilizar **qconfig** para definir una política. Se le solicita que seleccione una modalidad de encapsulación (Túnel o Transporte). Si elige la modalidad de túnel, se le presentan las mismas preguntas que en el escenario Branch Office. Si elige la modalidad de transporte, se le presentan las mismas pre-

guntas del escenario Branch Office excepto las que tratan sobre las subredes local y remota, porque no son aplicables.

Mandatos de configuración de servidor de políticas de LDAP

Los mandatos de configuración de servidor de políticas de LDAP le permiten especificar opciones de servidor de LDAP para recuperar información de política. La Tabla 40 resume los mandatos de configuración de LDAP y el resto de esta sección los describe con detalle. Éntrelos en el indicador de mandatos `Policy config>`. Puede entrar el mandato y las opciones en una línea o entrar solamente el mandato y responder a las solicitudes. Para ver una lista de las opciones de mandatos válidas, entre el mandato con un interrogante en lugar de las opciones.

Tabla 40. Mandatos de configuración de LDAP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Disable ldap	Inhabilita opciones de configuración de LDAP.
Enable ldap	Habilita opciones de configuración de LDAP.
Set ldap	Especifica opciones de configuración de LDAP.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Disable LDAP

Utilice el mandato **disable ldap** para inhabilitar las funciones de búsqueda de política de LDAP en el directorio o para inhabilitar la lectura de políticas almacenadas en antememoria del servidor LDAP en almacenamiento permanente.

Sintaxis: disable ldap cached-search
policy-search

cached-search
Inhabilita a LDAP para la lectura de políticas almacenadas en antememoria del servidor en el almacenamiento permanente.

policy-search
Inhabilita LDAP para realizar funciones de búsqueda de política en el directorio.

Enable LDAP

Utilice el mandato **enable ldap** para habilitar las funciones de búsqueda de política de LDAP en el directorio o para habilitar la lectura de políticas almacenadas en antememoria del servidor LDAP en el almacenamiento permanente.

Sintaxis: enable ldap cached-search
policy-search

cached-search
Habilita LDAP para que efectúe funciones de búsqueda de política en el directorio o para que lea políticas almacenadas en antememoria del servidor LDAP en el almacenamiento permanente.

Si habilita esta opción cuando está inhabilitada la opción de búsqueda de política, el sistema de búsqueda de política sólo lee políticas de la antememoria

local. Si habilita la opción de búsqueda en antememoria y la opción de búsqueda de política, el sistema de búsqueda de política intenta leer primero en el servidor LDAP y, si la operación no es satisfactoria, lee en los objetos de política LDAP almacenados en antememoria. Consulte el mandato **cache-ldap-polcys** en el apartado “Mandatos de supervisión de política” en la página 313 para obtener una explicación sobre cómo almacenar en antememoria las políticas LDAP.

policy-search
Habilita LDAP para realizar funciones de búsqueda de política en el directorio.

Set Default-Policy

Utilice el mandato **set default-policy** para especificar las opciones de política que deben utilizarse mientras se renueva la base de datos de política. El mandato establece las opciones de manejo de errores y la seguridad por omisión necesaria para acceder al servidor de políticas de LDAP.

Sintaxis: set default-policy
default-error-handling
default-security

default-error-handling
Especifica las opciones de manejo de errores que deben utilizarse mientras se renueva la base de datos de políticas.

Nota: El valor del manejo de errores por omisión determina el comportamiento del dispositivo si se produce un error mientras se vuelve a crear la base de datos de políticas. Si se produce un error, existen opciones sobre cómo debe comportarse el dispositivo. Son las siguientes:

1. Restablecer la base de datos de políticas en la seguridad por omisión.
2. Desechar cualquier norma leída desde LDAP y cargar las normas locales, además de la seguridad por omisión.

Estos valores sólo son válidos si se produjo un error al volver a crear la base de datos de políticas. Cada una de las opciones hereda la seguridad por omisión de excluir o aceptar mientras se produce un error. Si selecciona la opción 2, se excluye o se acepta todo el tráfico a menos que coincida con una política definida localmente. Si la base de datos de políticas se crea satisfactoriamente, no se utiliza esta opción.

default-security
Especifica las opciones de seguridad que deben utilizarse cuando se renueva la base de datos de políticas.

Nota: Cuando la base de datos de políticas se ha creado satisfactoriamente, el comportamiento por omisión se define como aceptar. Esto significa que si un paquete no coincide con ninguna norma de política, se aceptará sin sospecha. Si desea que los paquetes que no coinciden con ninguna norma se excluyan globalmente o tan solo para determinadas interfaces, debe definir una política para llevarlo a cabo.

1 Aceptar y reenviar todo el tráfico IP.

2 Permitir tráfico de LDAP, excluir todo el tráfico IP restante.

Si selecciona esta opción, a continuación se le solicitan las direcciones IP locales del dispositivo al cual debe enviarse y recibirse el tráfico de LDAP.

3 Permitir y asegurar tráfico de LDAP, excluir todo el tráfico IP restante.

Si selecciona esta opción, a continuación se le solicitará la información siguiente:

DHGroupId
El Id de Grupo Diffie-Hellman que debe utilizarse durante las negociaciones de la Fase 1 de ISAKMP.

1 Grupo DH 1.

2 Grupo DH 2.

Phase1-Hash-Algorithm
El algoritmo de hash que debe utilizarse durante las negociaciones de la Fase 1. El algoritmo de hash proporciona la autentificación de los mensajes de la Fase 1.

1 MD5.

2 SHA.

Phase1-Cipher-Algorithm
El algoritmo de cifrado que debe utilizarse durante las negociaciones de la Fase 1. El algoritmo de cifrado proporciona protección de cifrado para las negociaciones de la Fase 1.

1 DES

2 3DES

Phase1-Authentication-Method
El método de autentificación que debe utilizarse con el similar remoto. Especifica cómo ISAKMP determina si el similar remoto es realmente el dispositivo correcto con el que debe negociarse.

1 Clave precompartida

2 Certificado (RSA SIG)

Pre-Shared-Key-Value
Si ha especificado el método de autentificación de Fase 1 como clave precompartida, a continuación se le solicitará que entre el valor de la clave en ASCII.

Phase2-ESP-Authentication-Algorithm
ESP es el único protocolo de IPSec que se permite para la seguridad por omisión. Se le solicitará el algoritmo de autentificación que debe utilizarse durante las negociaciones de ISAKMP de la Fase 2.

0 Ninguno

1 HMAC-MD5

2 HMAC-SHA

Phase2-ESP-Cipher-Algorithm
ESP es el único protocolo de IPSec que se permite para la seguridad por omisión. Se le solicitará el algoritmo de cifrado que debe utilizar durante las negociaciones de ISAKMP de la Fase 2.

1 ESP DES

2 ESP 3DES

3 ESP CDMF

4 ESP NULL

Primary-Tunnel-Start
La dirección IP en el dispositivo que debe utilizarse para el tráfico de IKE e IPSec entre el dispositivo y la pasarela de seguridad que protege al servidor de LDAP primario.

Primary-Tunnel-End
La dirección IP en la pasarela de seguridad remota que protege al servidor de LDAP primario que debe utilizarse para el tráfico de IKE e IPSec.

Secondary-Tunnel-Start
La dirección IP en el dispositivo que debe utilizarse para el tráfico de IKE e IPSec entre el dispositivo y la pasarela de seguridad que protege al servidor LDAP secundario.

Secondary-Tunnel-End
La dirección IP en la pasarela de seguridad remota que protege al servidor de LDAP secundario que debe utilizarse para el tráfico de IKE e IPSec.

Set LDAP

Utilice el mandato **set ldap** para configurar los parámetros operativos de LDAP.

Sintaxis: set ldap anonymous-bind

yes

no

bind-name <*nombre*>
bind-pw <*ctr*>
policy-base <*serie*>
primary <*dirección-ip*>
secondary <*dirección-ip*>
version <*valor*>

anonymous-bind [Yes o No]
Especifica si desea enlazar el directorio de LDAP anónimamente o con el nombre de enlace y la contraseña de enlace especificados.

Valor por omisión: Yes (Sí)

bind-name <*nombre*>
Le solicita la información necesaria para enlazar con el servidor de LDAP para poder realizar una búsqueda en su directorio. El parámetro *nombre* especifica el nombre distinguido que utiliza el direccionador para identificarse a sí mismo. Si no entra este parámetro, el enlace se emite como una petición anónima.

bind-pw <*ctr*>
Le solicita la información necesaria para enlazar con el servidor de LDAP para poder realizar una búsqueda en su directorio. El parámetro *ctr* es la contraseña relacionada con el nombre distinguido. Si no entra este parámetro, el enlace se emite como una petición anónima.

policy-base <*serie*>
Le solicita que entre una serie de caracteres que debe utilizarse para definir el ámbito de la búsqueda de políticas en la SRAM del direccionador y en el servidor de LDAP. Por ejemplo, puede utilizar esta opción para devolver políticas que tan solo se apliquen al direccionador A, o para NHD, o para IBM-US. La "policy-base" (base-política) es el nombre distinguido del objeto DeviceProfile en el servidor de LDAP.

primary <*dirección-ip*>
Le solicita la dirección IPv4 del servidor de LDAP desde el que deben recuperarse políticas.

secondary <*dirección-ip*>
Le solicita la dirección IPv4 de un servidor de LDAP de reserva que se utiliza si no se puede llegar al servidor por omisión.

version <*valor*>
Le solicita el número de versión de LDAP soportada por el servidor de LDAP.

Valor por omisión: 2 (Los únicos valores aceptables son 2 ó 3.)

Set Refresh

Utilice el mandato **set refresh** para habilitar o inhabilitar la renovación automática de la base de datos de políticas una vez cada día. Si está habilitada, la base de datos de políticas se renueva automáticamente una vez al día a la hora especificada. Esto permite que todos los direccionadores con política habilitada de la red incorporen automáticamente los cambios de política que se hayan producido en el directorio de LDAP. Para restablecer este parámetro, utilice el mandato Talk 5 **reset refresh** de la característica de política.

Sintaxis: set refresh

enabled
yes
no
<*hora*>

enabled [yes (sí) o no]
Especifica si debe realizarse la renovación automática.

<*hora*>
Si ha especificado yes (sí), indica la hora del día (en formato de 24 horas) en la que debe producirse la renovación.

Acceso al indicador de mandatos de supervisión de política

La parte consola de política de la característica de política le permite ver las políticas que existen en la base de datos de políticas y habilitar o inhabilitar políticas individuales. Para acceder al entorno de supervisión de política, escriba **talk 5** en el indicador de mandatos de OPCON (*):

```
* t 5
```

A continuación, entre el mandato siguiente en el indicador de mandatos **+**:

```
+ feature policy
Policy>
```

Mandatos de supervisión de política

Estos mandatos le permiten ver los perfiles definidos en la base de datos de políticas y le permiten habilitar o inhabilitar políticas individuales. La Tabla 41 resume los mandatos de supervisión de política y el resto de esta sección los describe. Entre los mandatos en el indicador de mandatos `Policy console>`. Puede entrar el mandato y las opciones en una línea o entrar solamente el mandato y responder a las solicitudes. Para ver una lista de las opciones de mandatos válidas, entre el mandato con un interrogante en lugar de las opciones.

Tabla 41. Mandatos de supervisión de política

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Cache-ldap-plcys	Almacena una copia de la información de política más reciente leída del servidor LDAP en el almacenamiento de configuración permanente del direccionador.
Check-consistency	Comprueba la coherencia dentro de las políticas individuales y entre todas las políticas configuradas.
Disable	Inhabilita una política que se ha cargado en la base de datos de políticas.
Enable	Habilita una política que se ha cargado en la base de datos de políticas.
Flush-cache	Borra la información de política almacenada en antememoria del almacenamiento de configuración permanente del direccionador.
Reset	Renueva o restablece los criterios relacionados con la política.
Search	Prueba o depura la actividad entre el cliente y el servidor de LDAP.
Status	Visualiza información sobre la base de datos de políticas.
List	Visualiza información sobre la configuración de LDAP y las políticas definidas.
Test	Consulta el sistema de política y recupera las normas seleccionadas.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Cache-LDAP-Plcys

Utilice el mandato **cache-ldap-plcys** para almacenar una copia de la información de política más reciente leída del servidor LDAP en el almacenamiento de configuración permanente del direccionador. Esto elimina cualquier información de política almacenada en antememoria del almacenamiento permanente.

Sintaxis: cache-policy

Nota: En las plataformas 2212 y 2216, la entrada de este mandato también graba la configuración entera del direccionador, como lo hace el mandato de Talk 6 **write**.

Check-Consistency

Utilice el mandato **check-consistency** para comprobar las incoherencias potenciales entre las opciones configuradas en una política individual (interna) y entre políticas con definiciones que se solapan (externas). Entonces puede efectuar la acción correctiva para resolver cualquier conflicto.

Una incoherencia *interna* es aquella que existe entre objetos de acción dentro de una sola política, por ejemplo, una política con un tipo de acción DiffServ de Deny también tiene un tipo de acción IPSec de Permit. Una incoherencia *externa* es aquella que existe entre políticas independientes que tienen perfiles que se solapan, por ejemplo, una política tiene un tipo de acción DiffServ de Block y otra política tiene un tipo de acción IPSec de Permit. Otro ejemplo de ello son las políticas que se solapan que especifican tipos de acción IPSec diferentes.

Sintaxis: check-consistency

Ejemplo:

Suponga que las políticas se han configurado del modo siguiente:

Nombre de política: dsDown

Cargada de: Local

Estado: Enabled and Valid

Prioridad: 5

Aciertos: 0

Perfil: DSUP

Validez: always

DiffServ: dsDown

RSVP: rsvpActUp

Nombre de política: ManualTunnel

Cargada de: Local

Estado: Enabled and Valid

Prioridad: 5

Aciertos: 0

Perfil: DSUP

Validez: always

ID túnel: 1

Nombre de política: ike

Cargada de: Local

Estado: Enabled and Valid

Prioridad: 30

Aciertos: 0

Perfil: DSUP

Validez: always

IPSec: ipsecUP

ISAKMP: generalPhase1Action

La salida del mandato **consistency-check** aparecería del modo siguiente:

```
Policy console>check-consistency
Checking for inconsistencies with a policy...
Rule dsDown contains two conflicting actions:
   RSVP Action is of type PERMIT
   DiffServ Action is of type BLOCK

Checking for inconsistencies among policies with overlapping profiles...
  Mismatching IPSec and DiffServ actions at Priority 181 between:
        Rule: ike.traffic     State: ENABLE  Prio: 5 IPSec Action: PERMIT
        Rule: dsDown          State: ENABLE  Prio: 5 DiffServ Action: BLOCK

  Two rules with IPSec actions:
        Rule: ike.traffic     State: ENABLE  Prio: 30 Action: PERMIT
        Rule: Man             State: ENABLE  Prio: 5 Action: PERMIT

   Two rules with IPSec actions:
        Rule: ike.inBoundTunnel State: ENABLE  Prio: 30 Action: PERMIT
        Rule: Man.inBoundTunnel State: ENABLE  Prio: 5 Action: PERMIT

   Two rules with IPSec actions:
        Rule: Man.inBoundTunnel State: ENABLE  Prio: 5 Action: PERMIT
        Rule: ike.inBoundTunnel State: ENABLE  Prio: 30 Action: PERMIT

   Two rules with IPSec actions:
        Rule: Man             State: ENABLE  Prio: 5 Action: PERMIT
        Rule: ike.traffic     State: ENABLE  Prio: 30 Action: PERMIT

   Mismatching IPSec and DiffServ actions at Priority 5 between:
        Rule: Man             State: ENABLE  Prio: 5 IPSec Action: PERMIT
        Rule: dsDown          State: ENABLE  Prio: 5 DiffServ Action: BLOCK

  Mismatching IPSec and DiffServ actions at Priority 5 between:
        Rule: dsDown          State: ENABLE  Prio: 5 DiffServ Action: BLOCK
        Rule: ike.traffic     State: ENABLE  Prio: 30 IPSec Action: PERMIT

  Mismatching IPSec and DiffServ actions at Priority 5 between:
        Rule: dsDown          State: ENABLE  Prio: 5 DiffServ Action: BLOCK
        Rule: Man             State: ENABLE  Prio: 5 IPSec Action: PERMIT
```

Disable

Utilice el mandato **disable** para inhabilitar una política actualmente cargada en la base de datos de políticas. Se aplicarán decisiones por omisión a cualquier paquete de datos que coincida con los criterios de una política que haya inhabilitado.

Sintaxis: disable *nombre-política*

Enable

Utilice el mandato **enable** para habilitar una política actualmente cargada en la base de datos de políticas. A cualquier paquete que coincida con los criterios de una política que haya habilitado se le aplicarán las decisiones configuradas para dicha política.

Sintaxis: enable *nombre-política*

Flush-Cache

Utilice el mandato **flush-cache** para borrar la copia almacenada en antememoria más recientemente de la información de política leída desde el servidor LDAP del almacenamiento de configuración permanente del direccionador.

Sintaxis: flush-cache

Reset

Utilice el mandato **reset** para renovar o restablecer criterios relacionados con una política.

Sintaxis: reset ldap-config
policy-database
refresh-time

ldap-config
Carga dinámicamente la configuración de LDAP (tal como se especifica en el mandato **set ldap**) en la memoria. Los cambios se activan durante la próxima operación de búsqueda. Este mandato también impone un restablecimiento de la base de datos de políticas e inactiva la hora de renovación de base de datos de políticas.

policy-database
Renueva la base de datos de políticas. Detiene todos los túneles, las SA de la Fase 1 y la Fase 2, restablece las estructuras de datos de RSVP y DiffServ y desecha la base de datos de políticas. A continuación, las políticas se cargan desde el servidor de LDAP y se realiza un arranque automático. Mientras se vuelve a crear la base de datos, no se permitirá que entre o salga ningún paquete del direccionador, salvo los paquetes que entran o salen del servidor de LDAP.

refresh-time
Establece la hora en la que la base de datos de políticas se renovará automáticamente, según una base diaria. Si ha inhabilitado la hora de renovación, la base de datos no se renovará hasta que se vuelva a arrancar o se reinicie el direccionador.

Search

Utilice el mandato **search** para probar o depurar la actividad entre el cliente y el servidor de LDAP. Puede realizar búsquedas en el directorio y hacer que los resultados de las búsquedas se visualicen en talk 5.

Sintaxis: search *filtro*
dirección-ip

filtro
Especifica un valor de filtro para la operación de búsqueda.

dirección-ip
Especifica la dirección IP del servidor.

Status

Utilice el mandato **status** para visualizar información sobre la base de datos de políticas.

Sintaxis: status

status
Visualiza los resultados de la renovación más reciente de la base de datos de políticas, el tiempo que ha transcurrido desde la renovación y la hora en que está planificada la siguiente renovación.

Ejemplo:

```
Policy>status
Status of Last Search:       Failed
Time since last refresh:     4 seconds
Next Policy Refresh not scheduled
```

List

Utilice el mandato **list** para visualizar información sobre configuraciones y políticas de LDAP.

Sintaxis: list default-policy
ldap
policy
refresh
rule
stats

default-policy
Lista la política por omisión utilizada durante las renovaciones de la base de datos de políticas.

ldap
Lista las configuraciones de LDAP en la SRAM.

policy

basic Lista los componentes de política por nombre de política lógico. Puede seleccionar una política o listar todas las políticas. El listado visualiza los nombres de los componentes de las políticas tal como se entraron durante la configuración en Talk 6.

complete Hace lo mismo que list policy basic, salvo que el listado visualiza un listado completo de todos los valores de parámetros para cada política lógica.

generated Hace lo mismo que list policy basic, salvo que el listado visualiza los nombres de todas las normas generadas para cada política lógica.

refresh
Lista el estado de renovación de política (Habilitar o Inhabilitar) y la hora del intervalo de renovación.

rule
Lista información sobre las normas generadas según las opciones siguientes:

basic Lista todas las normas generadas. Puede seleccionar una norma de la lista o listar todas las normas. El listado visualiza los nombres de los componentes de las normas. Los componentes son:

nombre de política
cargado desde (LDAP o local)
estado
prioridad
número de coincidencias
perfil
validez (seguida de una lista de acciones que son las siguientes)
IPSec (y/o)
ISAKMP (y/o)
DiffServ (y/o)
RSVP

complete Hace lo mismo que rule basic, salvo que el listado visualiza los nombres de todos los parámetros para cada componente.

stats
Lista las normas que coinciden y el número de aciertos. Una norma puede tener varias acciones y que no todas ellas coincidan, por lo que estas opciones también indican qué acción de la norma coincide y el número de veces.

Test

Utilice el mandato **test** para verificar el funcionamiento de la base de datos de políticas. Este mandato le permite entrar un conjunto de selectores, que consulta el sistema de políticas y recupera las normas que coinciden. Se le solicitan las direcciones de origen y de destino, los puertos de origen y de destino, el ID de protocolo y el valor de TOS. Si una norma coincide, el mandato devuelve el nombre de la norma. De lo contrario, indica *No se ha encontrado ninguna coincidencia* (No match found).

Sintaxis: test forwarder
ISAKMP
IPSec
RSVP

forwarder
Simula una consulta de base de datos desde el sistema de reenvío de IP y devuelve las decisiones de política que resulten de dicha consulta. El tipo de política que se devuelve puede incluir información de DiffServ, información de la Fase 1 y de IKE de la Fase, e identificadores de túnel manual de IPSec.

ISAKMP
Simula una consulta de base de datos desde IKE para obtener información de política de la Fase 1 y devuelve las decisiones de política que resulten de dicha consulta. Si utiliza esta opción, debe establecer las direcciones de origen y de destino en las direcciones IP de punto final del túnel, el protocolo en 17 y los puertos de origen y de destino en 500.

IPSec
Simula una consulta de base de datos desde IKE para obtener información de política de la Fase 2 y devuelve las decisiones de política que resulten de dicha consulta. Si utiliza esta opción, debe establecer las direcciones de origen y de destino en las direcciones IP de punto final del túnel, el protocolo en 17 y los puertos de origen y de destino en 500.

RSVP

Simula un consulta de base de datos desde RSVP y devuelve las decisiones de política de RSVP que resulten de dicha consulta.

Soporte de reconfiguración dinámica de política

Esta sección describe la reconfiguración dinámica (DR) en lo que afecta a los mandatos de Talk 6 y Talk 5.

Delete interface de CONFIG (Talk 6)

La característica de política no soporta el mandato de CONFIG (Talk 6) **delete interface**.

Activate interface de GWCON (Talk 5)

El mandato de GWCON (Talk 5) **activate interface** no es aplicable para la característica de política. La configuración para la característica de política determina el conjunto de normas y las acciones subsiguientes que deben aplicarse al tráfico IP, que es independiente de una interfaz determinada.

Reset interface de GWCON (Talk 5)

El mandato de GWCON (Talk 5) **reset interface** no es aplicable para la característica de política. La configuración para la característica de política determina el conjunto de normas y las acciones subsiguientes que deben aplicarse al tráfico IP, que es independiente de una interfaz determinada.

Mandatos reset de componente GWCON (Talk 5)

La Característica de política soporta los mandatos **reset** de GWCON (Talk 5) específicos de Característica de política:

Mandato GWCON, Feature Policy, Reset, Database

Descripción: Todas las políticas configuradas en la política de característica se leerán de la configuración local. Si se ha habilitado la búsqueda de LDAP, las políticas para este dispositivo se leerán del servidor LDAP. Otros cambios en los objetos de política subyacentes, por ejemplo objetos de política IKE, IPSec y Acciones DIFFSERV utilizados por políticas, también se volverán a cargar de la configuración.

Una vez que se han leído todas las políticas, se creará la base de datos de políticas a partir del conjunto de normas que se generan desde estas políticas. Durante el periodo en el que se están leyendo las políticas, se crea una base de datos por omisión con la norma por omisión configurada en Talk 6, utilizando el mandato **feature policy, set default-policy**.

Efecto en la red: Durante el periodo en el que se está creando la base de datos de políticas, el tráfico de distribución única IPv4 se reenviará basándose en la política por omisión configurada en Talk 6. La política por omisión pasa todo el tráfico, excluye todo el tráfico excepto el tráfico LDAP hacia y desde el 2210 o excluye todo el tráfico excepto el tráfico LDAP protegido utilizando IPSec hacia y desde el 2210.

Limitaciones: Ninguna.

La tabla siguiente resume los cambios de configuración de la Característica de política que se activan cuando se invoca el mandato **GWCON, feature policy, reset, database**:

Mandatos cuyos cambios activa el mandato GWCON, feature policy, reset, database
CONFIG, feature policy, add, policy
CONFIG, feature policy, delete, policy
CONFIG, feature policy, change, policy
CONFIG, feature policy, disable, policy
CONFIG, feature policy, enable, policy

Mandato GWCON, feature policy, reset, LDAP

Descripción: Se renovarán los parámetros de configuración LDAP para la característica de política.

Efecto en la red: La siguiente vez que se renueve la base de datos de políticas, se utilizarán los parámetros de configuración LDAP nuevos para determinar si se debe realizar la búsqueda en el servidor y, en caso afirmativo, qué parámetros se deben utilizar.

Limitaciones: Ninguna.

La tabla siguiente resume los cambios de configuración de la Característica de política que se activan cuando se invoca el mandato **GWCON, feature policy, reset, ldap**:

Mandatos cuyos cambios activa el mandato GWCON, feature policy, reset, ldap
CONFIG, feature policy, set, ldap, anonymous-bind
CONFIG, feature policy, set, ldap, bind-name
CONFIG, feature policy, set, ldap, bind-pw
CONFIG, feature policy, set, ldap, policy-base
CONFIG, feature policy, set, ldap, port
CONFIG, feature policy, set, ldap, primary-server
CONFIG, feature policy, set, ldap, retry-interval
CONFIG, feature policy, set, ldap, search-timeout
CONFIG, feature policy, set, ldap, secondary-server
CONFIG, feature policy, set, ldap, version
CONFIG, feature policy, enable, ldap, cached-search
CONFIG, feature policy, enable, ldap, policy-search
CONFIG, feature policy, disable, ldap, cached-search
CONFIG, feature policy, disable, ldap, policy-search

GWCON, Feature Policy, Reset, Refresh

Descripción: Se volverán a cargar los parámetros de renovación de la base de datos de políticas. Los parámetros de renovación determinan si la base de datos debe renovarse automáticamente una vez al día y, si se habilitan, cuándo durante el día.

Efecto en la red: Si se habilita la característica de renovación de política, se renovará la base de datos de políticas cuando se produzca el suceso de tiempo especificado en la configuración de renovación. Esto tiene exactamente el mismo efecto que si se ejecuta manualmente un mandato **reset database**.

Limitaciones: Ninguna.

La tabla siguiente resume los cambios de configuración de la Característica de política que se activan cuando se invoca el mandato **GWCON, feature policy, reset, refresh**:

Mandatos cuyos cambios activa el mandato GWCON, feature policy, reset, refresh
CONFIG, feature policy, set, refresh

Mandatos de cambio inmediato de CONFIG (Talk 6)

La característica de política soporta los mandatos de CONFIG siguientes que cambian inmediatamente el estado operativo del dispositivo. Estos cambios se guardan y se conservan si se vuelve a cargar o se reinicia el dispositivo o si se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
CONFIG, feature policy, set, default-policy **Nota:** La siguiente vez que se renueve la base de datos de políticas, se utilizarán los valores para la política por omisión durante el periodo de renovación y para manejar las condiciones de error que pueden producirse al renovar la base de datos de políticas.
CONFIG, feature policy, add, user
CONFIG, feature policy, change, user **Nota:** La clave precompartida definida para el usuario puede utilizarse inmediatamente sin reiniciar o volver a cargar el dispositivo. Si este usuario forma parte de un grupo asociado con el grupo de usuarios remoto de un perfil, se deberá restablecer la base de datos de políticas antes de que pueda realizarse esta asociación.

Utilización de Seguridad de IP

Este capítulo explica cómo utilizar la característica Seguridad de IP y contiene las secciones siguientes:

Visión general de Seguridad de IP

Esta sección proporciona una visión general de las posibilidades de seguridad de IP para IPv4 y IPv6.

Utilización de túneles de seguridad

Para proteger los paquetes IP que se envían a otro sistema principal, direccionador o cortafuegos, puede configurar un túnel de seguridad para cada ruta de IP que debe ser segura. Un túnel IPSec es una conexión lógica de doble sentido hacia el sistema principal remoto, direccionador o cortafuegos a través de la cual un direccionador local envía paquetes IP protegidos. Un túnel de seguridad se identifica mediante parámetros tales como las direcciones del sistema principal de origen y el sistema principal de destino, los números de puerto y el ID de túnel.

Con IPv4 puede definir un túnel negociado configurando una política de túnel en la base de datos de políticas o puede generar un túnel manual utilizando el mandato Talk 6 **add tunnel** tal como se muestra en "Configuración del túnel para el direccionador A" en la página 358. Con IPv6, utilice el mandato Talk 6 **add tunnel**.

Para establecer un túnel IPSec de seguridad, una política puede especificar la función Cabecera de autentificación (AH) de IP (consulte "Cabecera de autentificación de IP" en la página 326), que conecta cabeceras de autentificación especiales y la función Carga de seguridad de encapsulación (ESP) de IP (consulte "Carga de seguridad de encapsulación de IP" en la página 327), que cifra los datos. La política establece cuáles de las siguientes medidas de seguridad se implantan para los paquetes:

- Algoritmo de AH y claves de autentificación de AH (Consulte "Configuración de los algoritmos" en la página 348 o "Configuración de los algoritmos" en la página 361 según convenga.)
- Algoritmo de cifrado de ESP y claves de cifrado y descifrado de ESP (Consulte "Configuración de los algoritmos" en la página 348 o "Configuración de los algoritmos" en la página 361 según convenga.)
- Índices de parámetros de seguridad (SPI) (Consulte "Asociaciones de seguridad" en la página 328.)

Nota: Para cada túnel de seguridad, el emisor y el receptor deben seleccionar opciones idénticas.

Conceptos de seguridad de IP

Los paquetes que se envían utilizando Protocolo Internet (IP) se pueden proteger utilizando la característica Seguridad de IP del 2210.

La seguridad, tal como define la RFC 2401 - la Arquitectura de seguridad para el Protocolo Internet, consta de las funciones siguientes:

Autentificación
Comprobar que los datos recibidos son iguales que los datos que se envían y que el emisor alegado es el emisor real.

Integridad
Comprobar que los datos se transmiten desde el origen hasta el destino sin que se detecte ninguna modificación.

Confidencialidad
Comunicarse de modo que los receptores designados sepan qué se envía pero que las partes no designadas no puedan determinar qué se envía.

Sin-repudiación
Comunicarse de modo que el receptor pueda probar que el emisor ha enviado determinados datos aunque posteriormente el emisor pueda negar haberlos enviado.

Nota: En algunos países, no se proporciona el soporte de cifrado debido a las regulaciones de exportación de los EE.UU. y los parámetros de cifrado no se visualizan. Sin embargo, el algoritmo ESP-NULL siempre está disponible. Para obtener una definición del algoritmo ESP-NULL, consulte “Algoritmos de cifrado ESP” en la página 327.

Terminología de seguridad de IP

Los términos siguientes se utilizan cuando se describen temas de IPSec relacionados con IPv4:

Cabecera de autentificación (AH)
Área de datos que contiene información de cabecera de paquete, que proporciona autentificación de origen de datos e integridad de datos, y protección de reproducción.

Certificado
Elemento de datos de codificación ASN.1 (de acuerdo con los estándares ITU X.509) que enlaza el ID de una entidad final con su clave pública .(En este caso, la entidad final es la entidad de negociación ISAKMP.) La entidad final debe registrar su ID y clave pública con una autoridad certificadora (CA) emitiendo una petición de certificado. La CA verifica la petición, la firma y la emite a la entidad. ISAKMP utiliza el certificado de clave pública durante el proceso de la Fase 1 para autentificar los intercambios de los mensajes iniciales que constituyen el secreto principal (clave de cifrado) entre direccionadores.

Autoridad certificadora (CA)
Autoridad fiable que emite certificados digitales X.509 “firmados” que los usuarios de la red deben utilizar para intercambiar datos del usuario de manera segura utilizando ISAKMP. Para participar en intercambios de datos seguros con otras partes habilitadas para ISAKMP, un direccionador debe registrarse con una CA y obtener un certificado digital X.509 para utilizarlo en la autentificación.

Nota: Deberá comprobar de forma regular con la CA para asegurarse de que está utilizando una lista actual de partes habilitadas para ISAKMP. Consulte el mandato **load** de PKI Talk 6 en el apartado “Mandatos de configuración de Infraestructura de clave pública” en la página 345 para obtener detalles.

Firma digital
Elemento de datos que contiene el ID codificado de un usuario, que forma parte de un certificado digital X.509. Los usuarios intercambian certificados durante las negociaciones de la Fase 1 para autentificarse entre ellos. La firma se genera realizando una operación de clave pública en un área de datos de entrada que debe firmarse.

Carga de seguridad de encapsulación (ESP)
Función de IPSec que puede encapsular y cifrar un datagrama de modo que su contenido sólo lo puede determinar el receptor. Incluye integridad de los datos y protección de la reproducción. La ESP también proporciona autentificación del origen de los datos. Funciona en las modalidades siguientes: modalidad de transporte, que sólo cifra la carga útil del datagrama original y deja la información de direccionamiento visible para las partes no autorizadas, y la modalidad de túnel, en la que se cifra todo el datagrama original, incluyendo la cabecera. Así se oculta la información de dirección sensible.

Internet Key Exchange (IKE)
Protocolo derivado de los protocolos ISAKMP y Oakley, que se utiliza en la comunidad de Internet para intercambiar claves de cifrado y autentificar las partes que se comunican.

ISAKMP
Protocolo de asociaciones de seguridad en Internet y gestión de claves. Esta función establece automáticamente las asociaciones de seguridad y gestiona las claves de cifrado de los paquetes hasta el final de un intercambio de datos.

Base de información de gestión (MIB)
Bloque de datos enviado por un direccionador en respuesta a una consulta desde una autoridad central, fiable que ha solicitado información estadística sobre las operaciones del direccionador. La autoridad puede detectar problemas en la red y ponerse en contacto con una parte responsable para que lleve a cabo la acción de corrección.

Oakley
El protocolo de gestión de claves de cifrado utilizado por ISAKMP.

Secreto de reenvío perfecto (PFS)
El nivel de seguridad de datos obtenido si las negociaciones de la Fase 2 deriva nueva información de claves de cifrado nueva para cada negociación. El ISAKMP realiza esta característica de seguridad habilitando el intercambio de valores de Diffie Hellman públicos entre las distintas partes. Esta característica de seguridad impide que se pueda determinar una clave de cifrado a partir de una clave previamente comprometida.

Negociaciones de la Fase 1
La comunicación entre un emisor y un receptor que establece una asociación de seguridad de ISAKMP y claves de cifrado que protegerán los mensajes de ISAKMP que deben intercambiarse durante las negociaciones de la Fase 2. La Fase 1 exige un uso intensivo del procesador y, generalmente, se lleva a cabo con poca frecuencia, quizás tan solo una vez al día o a la semana.

Negociaciones de la Fase 2
El intercambio de mensajes de ISAKMP entre un emisor y un receptor durante el cual se negocian las asociaciones de seguridad y las claves de cifrado que protegerán los intercambios de datos del usuario. Estas negociaciones normalmente se producen con gran frecuencia, quizás cada dos o tres minutos, y se utilizan para renovar las claves de cifrado regularmente sin la intervención del usuario.

Proxy
Un direccionador que se asigna para operar en nombre de otro dispositivo de la red.

Infraestructura de clave pública (PKI)
La estructura que utiliza una CA para enlazar el ID del usuario con su clave pública y que distribuye la clave pública enlazada de modo que asegura su seguridad.

Modalidad rápida
Término utilizado para describir las negociaciones de la Fase 2 para asociaciones de seguridad que no son de ISAKMP.

Reproducción
La acción de capturar un datagrama e intentar determinar su contenido o realizar un ataque de denegación de servicio reenviándolo repetidamente.

Asociación de seguridad (SA)
Área de datos que une información sobre un paquete de datos, como por ejemplo su algoritmo de cifrado e información de clave, las identidades de sus partes participantes, etc.

Conversión
Conjunto con nombre de información sobre una configuración de selecciones de autentificación y cifrado.

Cabecera de autentificación de IP

La Cabecera de autentificación (AH) se describe en la RFC 2402 IP Authentication Header. Esta cabecera contiene datos de autentificación para el datagrama de IP.

Para que IPv4 utilice la IPSec negociada, la política asignada a un datagrama implanta una función de autentificación de cifrado que se basa en el protocolo Internet Key Exchange (IKE) y en un par de claves pública/privada. Para túneles manuales IPv4 y para IPv6, el emisor utiliza una función de cifrado que se basa en una clave de autentificación secreta. En los dos casos, la función de autentificación de cifrado se aplica al contenido del datagrama. Puede especificar la AH sola o con ESP. Consulte el apartado “Utilización de AH y ESP” en la página 328 para obtener información detallada.

Algoritmos de autentificación de AH

Un túnel de seguridad que utiliza la política de túnel de AH debe utilizar uno de los algoritmos de autentificación siguientes:

- Autentificación de IP HMAC-MD5 con prevención de reproducción
- Autentificación de IP HMAC-SHA-1 con prevención de reproducción

Estos algoritmos de AH combinan una función de autentificación de mensajes con clave utilizando hash de cifrado (código de autentificación de mensajes a los que se ha aplicado la función hash, abreviado como HMAC) con una función de pre-

vención de reproducción opcional. La prevención de reproducción utiliza un número de secuencia contenido en la AH para verificar que un paquete no se haya recibido previamente. La prevención de reproducción protege al receptor de ataques de denegación de servicio, en los que se envía repetidamente el mismo paquete y el direccionador está tan ocupado procesando los paquetes duplicados que no puede procesar el tráfico legítimo. El código de autentificación se aplica a una clave de cifrado secreta y a los datos, y, después, a la salida de la clave secreta y a la salida de la primera operación. Consulte la Figura 22 para obtener una ilustración sobre cómo funciona esta acción para HMAC-MD5.

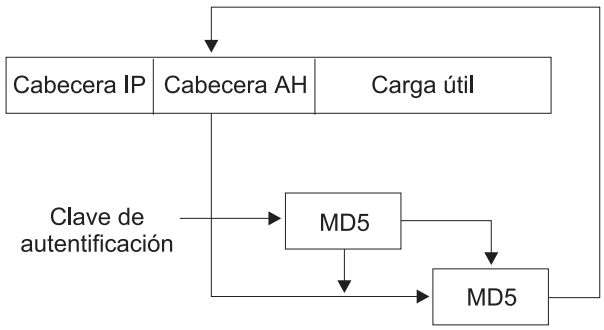


Figura 22. Creación de un Mensaje autentificado con HMAC MD5

Carga de seguridad de encapsulación de IP

La Carga de seguridad de encapsulación (ESP) de IP se describe en la RFC 2406 IP Encapsulating Security Payload. La ESP cifra una parte del paquete IP, o todo, para proporcionar confidencialidad además de autentificación (opcional) e integridad. Sin embargo, si selecciona el algoritmo ESP-NULL, la ESP sólo realiza comprobación de autentificación e integridad. Puede especificar la ESP sola o con AH. Consulte el apartado “Utilización de AH y ESP” en la página 328 para obtener información detallada.

Algoritmos de autentificación de ESP

Los algoritmos disponibles para la autentificación de ESP son los mismos que los de la AH, previamente mostrados en “Algoritmos de autentificación de AH” en la página 326.

Algoritmos de cifrado ESP

Un túnel de seguridad que utiliza la política de cifrado de ESP debe utilizar uno de los algoritmos de cifrado siguientes o el algoritmo ESP-NULL:

- Data Encryption Standard in Cipher Block Chaining Mode (DES-CBC)
- Commercial Data Masking Facility (CDMF)
- Triple DES (3DES)

Nota: Salvo para ESP-NULL, los algoritmos de cifrado ESP están sujetos a las leyes de exportación de los EE.UU. Si el 2210 no le permite utilizar alguno o ninguno de dichos algoritmos, es posible que la venta de estos algoritmos esté prohibida en su país. Consulte al representante de IBM para obtener más información.

El algoritmo ESP-NULL no cifra los datos de texto claro y está disponible en todos los países. Solamente habilita la comprobación de autentificación e integridad de

ESP, no el cifrado. Si utiliza ESP-NULL, ***debe*** utilizar uno de los algoritmos de autentificación de ESP.

Utilización de AH y ESP

Un túnel de seguridad debe utilizar una de las siguientes selecciones de autentificación/cifrado: AH, ESP, AH-ESP o ESP-AH. Si desea una combinación de AH y ESP, se aplican las siguientes declaraciones:

- La política AH-ESP especifica que para paquetes de salida, el cifrado se ejecuta antes que la autentificación. En este caso, en el direccionador de destino la función de autentificación de AH se ejecuta primero, comprobando los paquetes de entrada, y solamente los paquetes que pasan la autentificación se reenvían a ESP para ser descifrados.
- La política ESP-AH especifica que para paquetes de salida, la autentificación se ejecuta antes que el cifrado. En este caso, en el direccionador de destino la función de ESP primero descifra los paquetes de entrada, y sólo los paquetes que se descifran satisfactoriamente se reenvían a la autentificación de AH.

Asociaciones de seguridad

Una Asociación de seguridad (SA) es una “conexión” simplex (en un solo sentido) que proporciona servicios de seguridad al tráfico que transporta. Los servicios de seguridad se proporcionan a una SA mediante la utilización de AH o ESP, pero no ambos. Si se aplica protección de AH y ESP a la corriente de tráfico, se crean dos (o más) SA para proporcionar protección a la corriente de tráfico. Para que la comunicación bidireccional típica sea segura entre dos sistemas principales o entre dos pasarelas de seguridad, se necesitan dos SA (una en cada dirección).

Modalidad de túnel y modalidad de transporte

La modalidad operativa (túnel o transporte) determina cómo IPSec maneja paquetes IP. La modalidad de túnel es el valor por omisión y es necesaria si el direccionador actúa como pasarela de seguridad. Protege los datos de un único segmento de una ruta a través de una red. La modalidad de transporte sólo se permite cuando el direccionador actúa como sistema principal, y protege los datos de extremo a extremo, a lo largo de una ruta completa.

AH y modalidades operativas

En modalidad de túnel, la AH se sitúa delante del paquete IP y se crea una nueva cabecera IP que se sitúa delante de la AH. La cabecera IP del paquete para el que se utiliza un túnel (cabecera interior) contiene las direcciones de origen y de destino finales del paquete. La nueva cabecera IP (cabecera exterior) puede contener las direcciones de pasarelas de seguridad, que son los puntos finales del túnel. La AH protege todo el paquete nuevo, tanto la cabecera IP nueva como el paquete IP para el que se utiliza un túnel, salvo los campos variables de la cabecera IP nueva.

En modalidad de transporte, la AH se inserta después de la cabecera IP y antes que la cabecera de un protocolo de capa superior, como por ejemplo TCP o UDP. En esta modalidad, la AH autentifica la cabecera de protocolo de capa superior y el contenido del paquete IP, salvo los campos variables de la cabecera IP (como por ejemplo duración [TTL], suma de comprobación, distintivo de fragmento, desplazamiento de fragmento y tipo de servicio [TOS]).

La Figura 23 en la página 329 muestra el formato de los datagramas protegidos mediante AH.

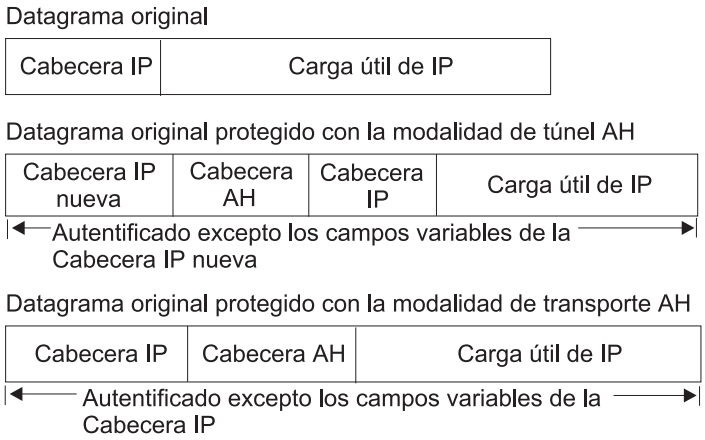


Figura 23. Formato de datagrama protegido mediante AH

ESP y modalidades operativas

En modalidad de túnel, los datos de carga útil contienen el paquete IP completo y se crea una cabecera IP nueva que se sitúa delante de la cabecera ESP. La cabecera IP del paquete para el que se utiliza un túnel (cabecera interior) contiene las direcciones de origen y de destino finales del paquete, mientras que la cabecera IP nueva (cabecera exterior) contiene las direcciones de las pasarelas de seguridad. La ESP cifra el paquete IP para el que se utiliza un túnel. Si utiliza autentificación de ESP, se autentifica la cabecera ESP, el paquete IP para el que se utiliza un túnel y la cola de ESP.

En modalidad de transporte, los datos de carga útil contienen datos cifrados de protocolo de capa superior, como por ejemplo datos TCP o UDP. Si utiliza autentificación, se autentifica la cabecera ESP, los datos del protocolo de capa superior y la cola de ESP.

La Figura 24 en la página 330 muestra el formato de los datagramas protegidos mediante ESP.

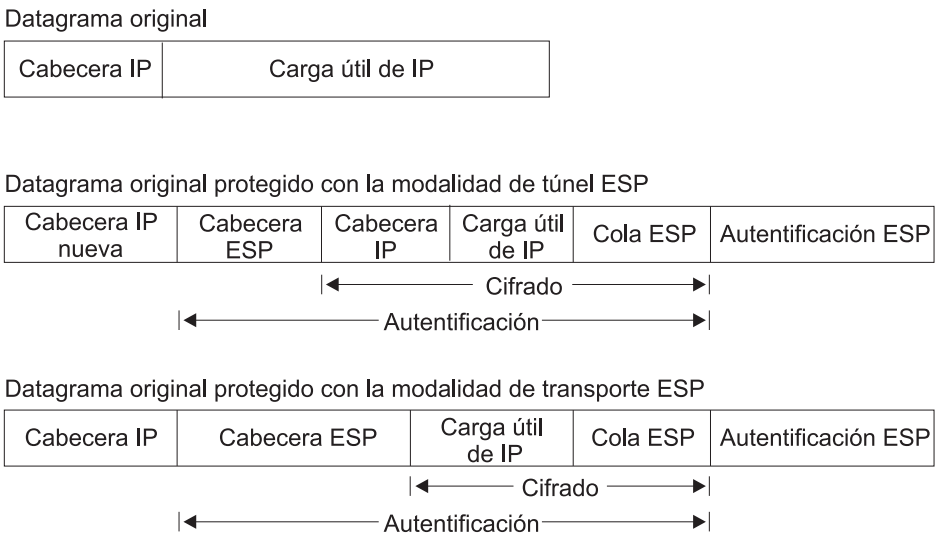


Figura 24. Formato de datagrama protegido mediante ESP

Jerarquización de AH y ESP

Puede jerarquizar un protocolo dentro de otra instancia de sí mismo o del otro protocolo. La Figura 25 muestra los efectos de la jerarquización de un datagrama protegido mediante ESP dentro de un túnel de AH.

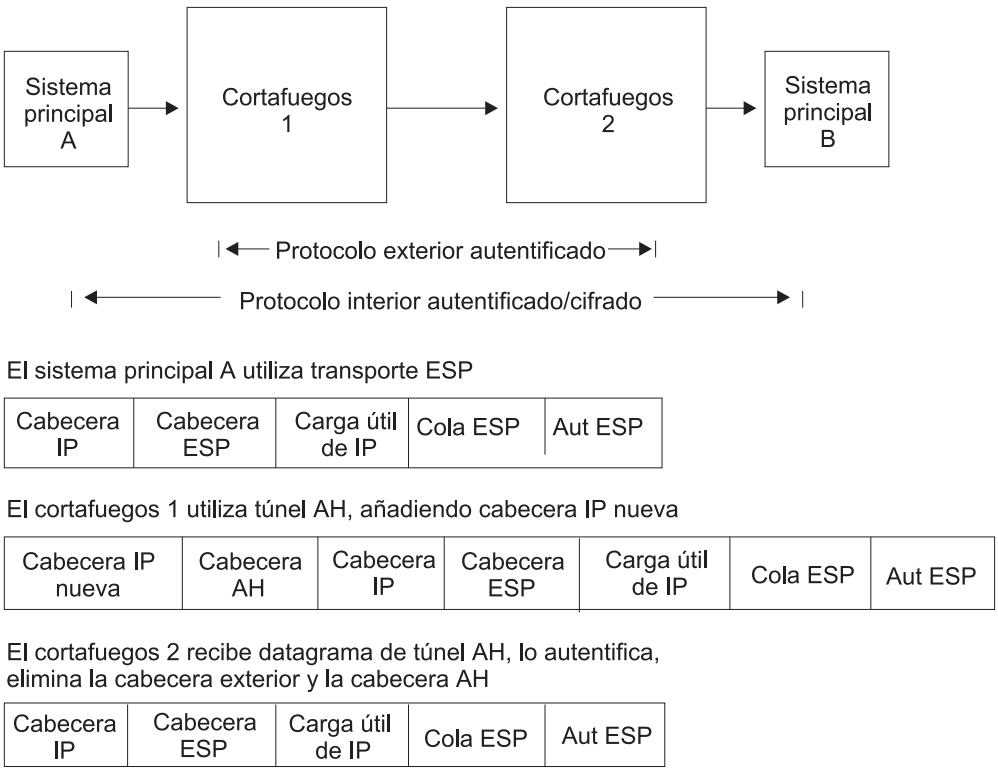


Figura 25. Jerarquización de ESP dentro de un túnel de AH

Utilización de Seguridad de IP con paquetes L2TP

Con IPv4 también puede utilizar IPSec para proteger paquetes L2TP. Después de crear un túnel L2TP encapsulando una trama L2TP dentro de un paquete UDP, puede encapsular el paquete UDP dentro de un paquete IP cuyas direcciones de origen y de destino definen los puntos finales del túnel. A continuación, puede aplicar protocolos de AH, ESP, e ISAKMP al paquete IP. La Figura 26 muestra un paquete L2TP encapsulado con IP que incluye PPP y su protocolo de carga útil para la transmisión a través de Internet.

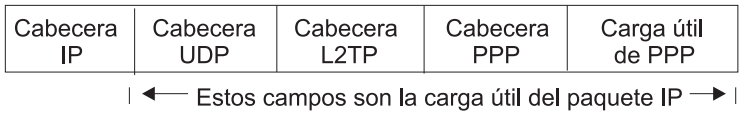


Figura 26. Paquete L2TP protegido mediante IPSec

Modalidad de túnel en túnel

Para una mayor seguridad, además de las características de seguridad que ya se han descrito, puede encapsular los paquetes de una corriente de tráfico dos veces y transmitirlos primero a través de un túnel IPSec y, después, a través de otro (túnel en túnel).

Nota: La utilización del cifrado múltiple (utilización de la modalidad de túnel en túnel cuando el cifrado se realiza para ambos túneles) dentro del direccionador está limitada por las regulaciones de exportación del Gobierno de los EE.UU. Sólo está soportado en cargas de software que están bajo un control de exportación estricto (las cargas de software que soportan RC4 con claves de 128 bits y Triple DES).

Con IPv4, una norma de la base de datos de políticas designa un paquete para encapsulación (interior) para el primer túnel y antes de que se envíe el paquete, la norma hace que el paquete se someta a un segundo túnel para una segunda encapsulación (exterior). Con IPv6, una norma de control de acceso de filtro de paquetes identifica a un paquete para encapsulación (interior) para el primer túnel y antes de que se envíe el paquete, una segunda norma hace que el paquete se someta a un segundo túnel para una segunda encapsulación (exterior).

Los dos túneles de IPSec se originan en el mismo direccionador y los extremos remotos de los túneles están en la misma ubicación física, pero en máquinas distintas. El extremo remoto del primer túnel puede ser una pasarela de seguridad o un sistema principal; el extremo remoto del segundo túnel *debe* ser un direccionador de pasarela de seguridad. Puesto que los túneles tienen destinos diferentes, deben tener direcciones IP remotas diferentes. Los dos túneles utilizados para túnel en túnel deben estar configurados para modalidad de túnel y no se permite relleno adicional en el segundo túnel.

Cuando se ha encapsulado dos veces, el paquete se transmite a través del segundo túnel (exterior). Al final de este túnel, se elimina la encapsulación exterior y el paquete se reenvía al primer túnel (interior), basándose en la información de la cabecera creada mediante la encapsulación del primer túnel. Al final de este túnel, la encapsulación interna se elimina y el paquete se reenvía a su destino final.

Determinación de la Unidad máxima de transmisión de la ruta

Tanto para IPv4 como IPv6, IPSec soporta Determinación de Unidad máxima de transmisión de ruta (PMTU) si el 2210 actúa como pasarela de seguridad. El soporte de Determinación de PMTU es importante si el paquete no se puede fragmentar. Con IPv4, un paquete no se puede fragmentar si está establecido el bit de Don't Fragment (No Fragmentar) (DF). Con IPv6, un paquete no lo puede fragmentar ningún direccionador intermedio. En estas situaciones, si el paquete no cabe en un enlace de la ruta de un extremo al otro del túnel de seguridad, se envía un mensaje de error de ICMP "packet too big" (paquete demasiado grande) al originador del paquete.

Dado que el direccionador actúa como pasarela de seguridad, el paquete erróneo se devuelve al direccionador originador en lugar de devolverlo al verdadero originador del paquete. El direccionador de recepción debe devolver la MTU informada al originador verdadero, el cual puede reducir el tamaño del paquete para que pueda llegar a su destino final. El soporte para Determinación de PMTU se describe en la RFC 2401 - Security Architecture for the Internet Protocol.

IPv4 proporciona las opciones siguientes para el valor del bit de DF en la cabecera exterior del paquete para el que se utiliza el túnel:

1. Copiar desde la cabecera interior
2. Establecer siempre
3. Borrar siempre

Estas opciones están disponibles cuando se configura la modalidad túnel en túnel de seguridad, por ejemplo, utilizando el mandato **add ipsec-manual-tunn** (IPv4) o Talk 6 **add tunnel** (IPv6) de la característica de política. El bit de DF se maneja de acuerdo con la opción seleccionada salvo bajo las condiciones siguientes:

- La MTU del túnel es igual que la MTU mínima.
- El tamaño del paquete de entrada es menor o igual que la MTU mínima.
- El tamaño del paquete encapsulado debe ser mayor que la MTU mínima.

En estas circunstancias, para IPv4, el bit de DF bit no se establece, independientemente de la configuración, y el paquete protegido se puede fragmentar tanto como sea necesario en la ruta hacia el receptor. Para IPv6, el paquete se fragmenta tanto como es necesario cuando sale de la pasarela de seguridad para que se ajuste a la PMTU para el túnel. Esta acción especial es necesaria puesto que el paquete de entrada ya es menor o igual que la MTU mínima, por lo que el sistema principal de origen no disminuirá más el tamaño. Si no estuviera permitida la fragmentación, este paquete nunca llegaría a su destino final.

Dado que los cambios en la topología o configuración de la red pueden cambiar la PMTU, el valor de PMTU debe caducar periódicamente y restablecerlo en el máximo. El valor del temporizador de caducidad es por omisión 10 minutos y se puede configurar con el mandato Talk 6 **set path**. El establecimiento del parámetro caducidad en 0 inhabilita la duración des PMTU.

Diagrama de una red con un túnel de seguridad de IP

La Figura 27 muestra un ejemplo de una red con dos túneles de IPSec que conectan el direccionador A (con IPSec) con el direccionador B (con IPSec y Conversión de direcciones de red para IPv4).

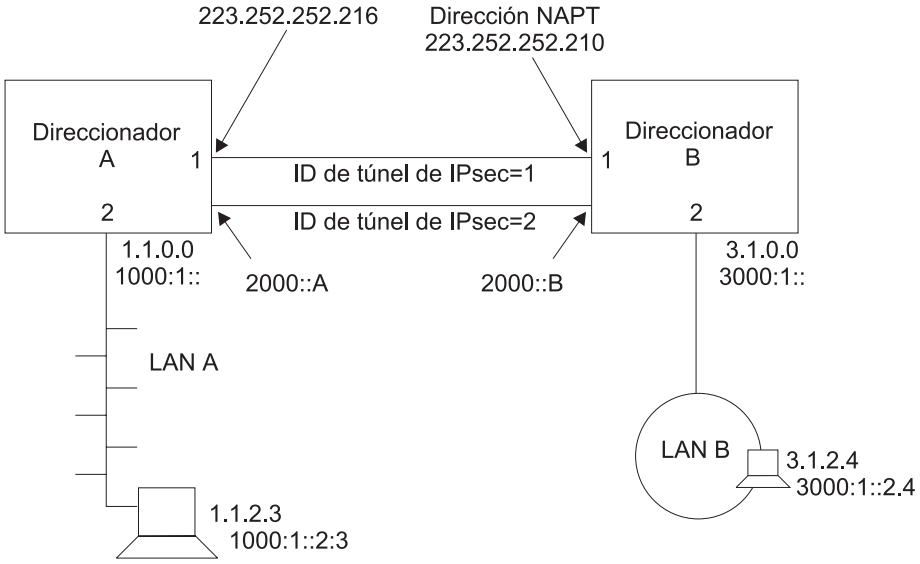


Figura 27. Red con IPSec y NAT

En esta red, un túnel IPSec con el ID de túnel IPSec 1 se ha configurado desde la dirección IPv4 223.252.252.216 del direccionador A a la dirección IPv4 223.252.252.210 en el direccionador B. El direccionador A se configura para IPSec. El direccionador B se configura para IPSec y NAT.

Además en esta red, un túnel IPSec con el ID de túnel IPSec 2 se ha configurado desde la dirección IPv6 2000::A del direccionador A a la dirección IPv6 2000::B del direccionador B.

Con IPv4, para configurar esta red para IKE, siga los pasos empezando desde “Configuración de Internet Key Exchange (IPv4)” en la página 343. Para IPv4 con IPSec manual, siga los pasos empezando desde “Configuración de un túnel manual (IPv4)” en la página 358. Para IPv6, siga los pasos empezando desde “Configuración de un túnel manual (IPv6)” en la página 362.

Nota: Incluso si no tiene intención de utilizar NAT en la red, la descripción de la configuración del direccionador B puede ayudarle a comprender con mayor claridad las relaciones entre los parámetros de cada extremo del túnel IPSec.

Utilización de Internet Key Exchange

Esta sección explica cómo puede utilizar Internet Key Exchange (IKE) para automatizar la definición y la creación de asociaciones de seguridad (SA) de IPSec. IKE es un estándar soportado por el IETF (RFC 2409), que proporciona un modo estándar para que los productos con IPSec habilitado del mismo proveedor o de diferentes proveedores se comuniquen sus requisitos de seguridad.

IKE proporciona una estructura mediante la cual se cumplen los requisitos de seguridad siguientes:

Autentificación de la entidad negociadora remota (similar IKE) Mediante la utilización de una clave previamente compartida o de un certificado digital, IKE autentifica la entidad con la que se está comunicando haciendo que la entidad demuestre que es quien afirma ser.

Creación de material de clave idéntica en ambos similares Utilizando el mecanismo de clave pública/clave privada de Diffie-Hellman, IKE proporciona el intercambio del componente de clave pública y la generación independiente de claves idénticas por parte de cada similar.

Protección para la negociación de asociaciones de seguridad de IPSec Mediante un proceso de dos fases que se describe en el tema siguiente, IKE proporciona la creación de asociaciones de seguridad que se utilizan únicamente para proteger la negociación de *túneles* de IPSec, así como la negociación y creación real de *asociaciones de seguridad* que IPSec utiliza para proteger los datos del usuario.

Fases de Internet Key Exchange

IKE define dos intercambios de negociación diferentes: La Fase 1 y la Fase 2. La Fase 1 configura un túnel de seguridad entre los dos similares IKE, el cual proporcionará protección para las negociaciones de túnel IPSec posteriores. Las acciones siguientes se producen durante la Fase 1 en el orden mostrado:

1. Las características de la asociación de seguridad de la Fase 1 las negocian y acuerdan los similares IKE. Estas características incluyen el algoritmo de cifrado que se utilizará para cifrar *las comunicaciones de IKE*, el algoritmo hash que debe utilizarse, el método de autentificación y el grupo Diffie-Hellman que debe utilizarse cuando se generen claves.
2. Se generan claves de Diffie-Hellman y las partes públicas se intercambian con el similar IKE. Estas claves se utilizan para generar claves que cifrarán las negociaciones de la Fase 1 y también permitirán la generación de claves que serán utilizadas por túneles de IPSec.
3. El similar IKE se autentifica utilizando uno de los dos métodos soportados—modalidad de clave previamente compartida y modalidad de firma.

   En la modalidad de clave previamente compartida, ambos similares IKE, por medio de un proceso de fuera de línea previo, han intercambiado una clave que se utiliza durante la Fase 1 para autentificar al similar. Configure la clave previamente compartida utilizando el mandato **add user** de la característica de política.

   En la modalidad de firma, se utiliza un certificado digital X.509 firmado para proporcionar las claves que se utilizan para cifrar y descifrar las cargas útiles de los mensajes de la Fase 1. Una firma y verificación satisfactorias incluyen la autentificación del similar. Para obtener una descripción detallada de la modalidad de firma y la utilización de certificados digitales X.509, consulte “Utilización de la infraestructura de clave pública” en la página 336.

Las negociaciones de la Fase 1 pueden tener lugar utilizando cualquiera de las dos modalidades de intercambio siguientes:

- La modalidad principal utiliza seis mensajes para efectuar las negociaciones de la Fase 1 y cifra las identidades de los similares negociadores.

- La modalidad agresiva utiliza tres mensajes para efectuar las negociaciones de la Fase 1. Los similares intercambian identidades no protegidas en los dos primeros mensajes.

Negociación de un túnel de seguridad de IP

El proceso tratado en este tema se produce cuando un direccionador se prepara para enviar un paquete cuyos atributos coinciden con los definidos en una norma de una base de datos de políticas. La negociación de un túnel se produce en dos fases. Durante la Fase 1, el direccionador que envía inicia la comunicación transmitiendo el primer mensaje de un intercambio de seis mensajes, el cual establece las opciones de seguridad que deben utilizarse durante la Fase 2. El receptor responde y las dos partes negocian las características de asociación de seguridad (SA) de ISAKMP, los algoritmos de autentificación y de cifrado que deben utilizarse, y cada una de ellas autentifica la identidad de la otra. Durante la Fase 2, las partes intercambian un total de tres mensajes para negociar las SA y las claves que deben utilizarse para proteger los datagramas IP que se envían entre las dos partes. La Fase 1 procede del modo siguiente:

1. Mensaje 1: El emisor propone cómo va a tener lugar la actividad de comunicación—el método de autentificación (por ejemplo, firmas digitales), el algoritmo de autentificación (por ejemplo, HMAC-MD5) y el algoritmo de cifrado (por ejemplo, DES-CBC) que deben utilizarse.
2. Mensaje 2: El receptor indica al emisor cuál de las opciones de seguridad , si existe alguna, va a soportar.
3. Mensaje 3: El emisor transmite su valor público de Diffie Hellman y un valor aleatorio a partir de los cuales se van a crear las claves de cifrado.
4. Mensaje 4: El receptor transmite su propio valor público de Diffie Hellman y un valor al azar a partir de los cuales se van a crear las claves de cifrado. En este punto, ambas partes crean claves públicas y claves privadas, y la información relacionada con las claves que debe utilizarse en los intercambios de mensajes de ISAKMP.
5. Mensaje 5: El emisor transmite una firma digital y puede incluir un certificado digital X.509 firmado por una autoridad certificadora (CA) fiable. Si el emisor no incluye ningún certificado válido, el receptor debe utilizar el protocolo LDAP para obtener un certificado de una CA fiable, de un servidor DNS de seguridad, de una antememoria local de seguridad que correlacione los certificados previamente utilizados con sus respectivos valores de ID o puede solicitar un certificado desde el emisor, el cual debe enviarlo inmediatamente.
6. Mensaje 6: Después de verificar la firma digital del emisor, el receptor transmite al emisor el mismo tipo de información de identificación sobre sí mismo.

En este punto, ambas partes se han autentificado a sí mismas ante la otra parte, se han puesto de acuerdo sobre las características de la SA y han deducido sus claves y la información relacionada con las claves para manejar las SA de ISAKMP. A continuación, las partes inician la Fase 2 para negociar las SA y claves que no sean de ISAKMP, que se utilizarán para proteger los datagramas IP que intercambian entre ellas. La Fase 2 procede del modo siguiente:

1. Mensaje 1: El emisor propone una SA no ISAKMP transmitiendo una selección de algoritmo AH o ESP y también incluye otra información relacionada con la seguridad.

2. Mensaje 2: El receptor indica al emisor qué propuesta ha seleccionado y también incluye información relacionada con la seguridad.
3. Mensaje 3: El emisor transmite un registro hash de varios elementos para indicar al receptor que está preparado para continuar utilizando los protocolos de seguridad negociados. Cuando el receptor verifica la información, el enlace se completa y las partes pueden empezar a intercambiar corrientes de datos protegidos.

Utilización de la infraestructura de clave pública

Esta sección explica cómo utilizar la infraestructura de clave pública (PKI). Mediante PKI, IKE soporta la modalidad de firma de clave pública para autentificar entidades de IKE. Aunque este release soporta la modalidad de clave previamente compartida, que no requiere soporte de PKI, esta modalidad contiene una desventaja inherente. Para la autentificación necesita que se configure cada entidad de IKE con la clave previamente compartida de cada uno de sus similares. Esto limita mucho la escalabilidad de las operaciones de IKE. La firma basada en la clave pública o la modalidad de cifrado público proporcionan una mejor escalabilidad. En este release, el certificado digital X.509 se utiliza en las negociaciones de la Fase 1 de IKE en modalidad de firma para autentificar entidades de IKE.

Asigne una identidad a cada entidad de IKE que desee que participe en las negociaciones de IKE especificando un valor exclusivo en el campo de ID de ISAKMP cuando configure su perfil de política de usuario. Cada entidad de IKE autentifica su identidad con sus similares.

PKI se está definiendo y desarrollando actualmente para que soporte operación con claves públicas. En PKI, un certificado digital X.509 enlaza una clave pública de una entidad con la identidad alegada. Una entidad de IKE puede extraer la clave pública contenida en un certificado. A continuación puede realizar una operación de clave pública para autentificar la identidad de un similar que participa en una negociación de IKE. Se utiliza una clave pública para la modalidad de firma de IKE. En esta modalidad, el firmante utiliza su clave privada para firmar la firma digital. El receptor extrae la clave pública del firmante del certificado y la utiliza para verificar la firma. La función de certificado digital proporciona un modo escalable para que una entidad de IKE autentifique la identidad de otra entidad de IKE.

Configuración de PKI

Este release supone que las dos entidades de IKE que participan en una negociación utilizan la misma CA. Antes de empezar las negociaciones de IKE utilizando la firma, debe configurar PKI para el direccionador. También debe generar la clave privada del direccionador y el certificado del direccionador y bajar el certificado de la CA raíz. Los pasos siguientes explican cómo configurar PKI:

1. Genere el par de claves y solicite el certificado.

   Debido a que la operación de la clave pública implica un par de claves (la modalidad de firma utiliza la clave privada para firmar y la clave pública para verificar), debe generar un par de claves para el direccionador. Para una petición de certificado, debe enviar la clave pública generada a la CA para colocarla en un certificado digital X.509. A continuación, cada similar de IKE potencial puede extraer esta clave pública del certificado emitido por la CA. La clave privada reside en el direccionador y se mantiene en secreto, solamente la conoce el direccionador.

En esta versión, puede emitir un mandato **certificate request**, que realiza lo siguiente:

a. Genera un par de claves, cuya longitud de clave puede especificarse como 512, 768 ó 1024 bits. La clave privada generada permanece en la antememoria.

b. Solicita que entre información para incluirla en la petición de certificado (por ejemplo, el ID de direccionador en la forma de dirección IP, el nombre de dominio o el nombre de email.

c. Crea una petición de certificado (en formato PKCS#10) que contiene la clave pública generada y la información que ha entrado.

d. Utiliza TFTP para la petición de certificado a un sistema principal.

2. Emita el certificado (fuera del direccionador)

   La CA recibe la petición de certificado PKCS#10. La CA puede verificar manualmente la petición y emitir un certificado. El certificado contiene la clave pública del direccionador y la información que ha entrado. La CA firma el certificado utilizando su clave privada, convirtiéndose de este modo en información digital fiable siempre y cuando la CA que firma sea fiable. Ahora el certificado está preparado para utilizarlo en negociaciones de IKE. (Este proceso está fuera del alcance de la operación del direccionador y no se describe adicionalmente en este manual.)

3. Baje el certificado del direccionador

   Una vez la CA ha emitido el certificado, PKI puede bajarlo al direccionador. Según cómo la CA publica el certificado, PKI puede utilizar TFTP o LDAP para llevar a cabo la bajada.

   Tenga en cuenta que la clave privada y la clave pública del certificado del direccionador deben coincidir para poder realizar una operación de clave pública, como por ejemplo una firma digital. Cuando PKI baja el certificado al direccionador, la clave privada que se ha generado con la clave pública debe estar en la antememoria de claves del direccionador. El certificado bajado es inservible si pierde su clave privada coincidente. Esto significa que desde el momento en que emite la petición de certificado hasta el momento en que se baja el certificado, **no debe** reiniciar ni volver a cargar el direccionador, borrar la antememoria ni emitir una nueva petición de certificado. Cualquiera de estas operaciones destruye la clave privada en la antememoria del direccionador que se utiliza.

4. Baje el certificado de la CA

   Para verificar el certificado del similar de IKE debe obtener el certificado de CA raíz del similar. Este release soporta operación de CA de un solo nivel, lo que significa que las entidades de IKE deben asignarse a la misma CA. Cada entidad de IKE (en este caso, cada direccionador) debe bajar el certificado de la CA (utilizando TFPT o LDAP) para verificar que el certificado recibido desde el similar sea válido.

5. Guarde y vuelva a cargar el certificado

   Cuando el direccionador ha obtenido el certificado, su clave privada coincidente y el certificado de la CA, puede iniciar la negociación de IKE. Puesto que un certificado generalmente es válido durante meses o años, puede que desee guardar el certificado y la clave privada en la SRAM para no tener que emitir una petición de certificado y bajarlo cada vez que vuelva a cargar o a

iniciar el direccionador. Esta versión proporciona los mandatos **cert save** y **cert load** para guardar o recuperar el certificado y la clave privada en la SRAM.

Tenga en cuenta que el certificado y la clave privada del direccionador deben procesarse como un par (por ejemplo, siempre se guardan o se recuperan juntos de la SRAM).

Utilice los mandatos Talk 6 para configurar y listar información de servidor de TFTP y LDAP tal como se muestra en los ejemplos siguientes:

Ejemplo: Add Server (T6)

```
Config>f ipsec
IP Security feature user configuration
IPsec config>pki
PKI config>add server
Name ? (max 65 chars) []? test
Enter server IP Address []? 8.8.8.8
Transport type (Choices: TFTP/LDAP)  [TFTP]?
PKI config>
```

Ejemplo: List Server Configuration (T6)

```
PKI config>li server

1)  Name: SERVER1
    Type: TFTP
    IP addr: 8.8.8.8


2)  Name: TEST
    Type: TFTP
    IP addr: 8.8.8.8
```

Ejemplo: List Root Certificate (T6)

```
PKI config>li cert

Root CA  certificate:
       SRAM    Name:   R1
       Subject Name:   /c=US/o=ibm/ou=nhd
       Issuer  Name:   /c=US/o=ibm/ou=nhd
           Validity:   1998/12/19 -- 2018/12/19
  Default Root Cert:   No

       SRAM    Name:   R2
      Subject  Name:   /c=US/o=ibm/ou=nhd
      Issuer   Name:   /c=US/o=ibm/ou=nhd
           Validity:   1998/12/19 -- 2018/12/19
  Default Root Cert:   Yes
```

```
Router   Certificate:
       SRAM    Name:   B1
      Subject  Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
      Issuer   Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA
   Subject alt Name:   1.1.1.1
         Key Usuage:   Sign & Encipherment
           Validity:   1998/10/29 -- 2001/10/29
       Default Cert:   No

       SRAM    Name:   B2
      Subject  Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
      Issuer   Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA
   Subject alt Name:   1.1.1.1
         Key Usuage:   Sign & Encipherment
           Validity:   1998/10/29 -- 2001/10/29
       Default Cert:   Yes

       SRAM    Name:   B3
      Subject  Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
      Issuer   Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA
   Subject alt Name:   1.1.1.1
         Key Usuage:   Sign & Encipherment
           Validity:   1998/10/29 -- 2001/10/29
       Default Cert:   No

       SRAM    Name:   YYY
      Subject  Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
      Issuer   Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA
   Subject alt Name:   1.1.1.1
         Key Usuage:   Sign & Encipherment
           Validity:   1998/10/29 -- 2001/10/29
       Default Cert:   No
```

Ejemplo: Certificate Request (T5)

```
PKI Console>cert-req
Enter the following part for the subject name
   Country Name(Max 16 characters) []? us
   Organization Name(Max 32 characters) []? IBM
   Organization Unit Name(Max 32 characters) []? NHD
   Common Name(Max 32 characters) []? router1
Key modulus size
 [512]?
Certificate subject-alt-name type:
   1--IPv4 Address
   2--User FQDN
   3--FQDN
Select choice [1]?
Enter an IPv4 addr) []? 12.1.1.1
Generating a key pair. This may take some time. Please wait ...
PKCS10 message successfully generated
Enter tftp server IP Address []? 8.8.8.8
Remote file name (max 63 chars) [/tmp/tftp_pkcs10_file]?
Memory transfer starting.
.Memory transfer completed - successfully.
Certificate request TFTP to remote host successfully.
Private Key Alias [ROUTER_KEY]? local
Generated private key LOCAL stored into cache
```

Ejemplo: List Router Certificate (T5)

```
PKI Console>li cert
Router   certificate
      Serial Number:   909343811
      Subject  Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
      Issuer   Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA
   Subject alt Name:   1.1.1.1
         Key Usuage:   Sign & Encipherment
           Validity:   1998/10/29 -- 2001/10/29

Root CA  certificate
      Serial Number:   914034740
      Subject  Name:   /c=US/o=ibm/ou=nhd
      Issuer   Name:   /c=US/o=ibm/ou=nhd
           Validity:   1998/12/19 -- 2018/12/19
```

Ejemplo: Cert Save (T5)

```
PKI Console>cert-save
Enter type of certificate to be stored into SRAM:
     1)Root certificate;
     2)Box  certificate with private key;
Select the certificate type (1-2) [2]?
SRAM Name for certificate and private key []? yyy
Load as default router certificate at initialization?? [No]:
Private key YYY written into SRAM
Both Certificate and private key saved into SRAM successfully
PKI Console>
```

Ejemplo: Cert Load (T5)

```
PKI Console>cert-load
Enter type of certificate to be stored into SRAM:
     1)Root certificate;
     2)Box  certificate with private key;
Select the certificate type (1-2) [2]?
Name []? yyy
Box certificate and private key saved into cache successfully
PKI Console>
```

Utilización de Seguridad de IP (IPv4) manual

La característica de seguridad de IP contenida en IPv4 para el 2210, junto con la característica de política y otros procesos relacionados con IPSec, proporcionan autentificación, integridad, confidencialidad y sin-repudiación. Para implantar IPSec manualmente, debe configurar previamente una política que contenga un subconjunto de opciones de IPSec en una base de datos de políticas para definir el perfil y el período de validez del túnel manual. También puede configurar previamente el conjunto completo de opciones de IPSec (política) en la base de datos de modo que cuando un direccionador con política habilitada se prepare para enviar un paquete IPSec, negocie dinámicamente y establezca opciones de IPSec con el direccionador de destino, basándose en el contenido de la política. Para definir un túnel manual, consulte “Configuración de Seguridad de IP (IPv4) manual” en la página 348. Para obtener una explicación de las opciones de política, consulte “Utilización de la característica de política” en la página 243.

Utilización de Seguridad de IP (IPv6) manual

La característica de seguridad de IP contenida en IPv6 para el 2210 proporciona autentificación, integridad y confidencialidad. Para definir un túnel manual, consulte “Configuración de la seguridad de IP manual (IPv6)” en la página 360.

Configuración y supervisión de la seguridad de IP

Este capítulo describe cómo configurar y supervisar la seguridad de IP, y cómo utilizar los mandatos de supervisión de seguridad de IP. Para IPv4, “Utilización de la característica de política” en la página 243 y “Configuración y supervisión de la característica de política” en la página 287 proporcionan información adicional sobre cómo configurar y supervisar políticas de seguridad de IP. Este capítulo contiene las secciones siguientes:

Nota: Si crea un túnel de IPSec para transportar tráfico TN3270, APPN®-ISR o APPN-HPR y tiene la intención de dar prioridad al tráfico que utiliza el BRS, necesitará utilizar la característica de establecimiento de bit de prioridad de IPv4 del BRS. Consulte el apartado “Utilización del proceso de bits de prioridad de IP Versión 4 para el tráfico SNA en túneles seguros y fragmentos secundarios de IP” en la página 10 para obtener información.

Configuración de Internet Key Exchange (IPv4)

Este tema explica cómo configurar Internet Key Exchange (IKE).

Antes de establecer un túnel de IPSec, debe:

1. Configurar los atributos de los paquetes que utilizarán el túnel y las acciones resultantes que deben realizarse (la política).
2. Configure las opciones de cifrado y autentificación que desee.

Para obtener detalles sobre cómo realizar estas tarea, consulte “Utilización de la característica de política” en la página 243, “Configuración y supervisión de la característica de política” en la página 287 y “Configuración de la Infraestructura de clave pública (IPv4)” en la página 344.

Configuración de la Infraestructura de clave pública (IPv4)

Este tema explica cómo configurar la Infraestructura de clave pública (PKI) con IPv4.

Antes de establecer un túnel de IPSec, debe:

1. Crear un par de claves criptográficas pública/privada y obtener un certificado digital de una Autorización de certificado (CA) fiable. Consulte el apartado "Obtención de un certificado" para obtener información detallada.
2. Decida qué algoritmos, SA y otras opciones de IPSec desea utilizar para los direccionadores para los cuales configura su política. Consulte "Negociación de un túnel de seguridad de IP" en la página 335 y los temas siguientes para obtener más detalles.
3. Configure IKE y la base de datos de políticas. Consulte "Configuración de Internet Key Exchange (IPv4)" en la página 343, "Utilización de la característica de política" en la página 243 y "Configuración y supervisión de la característica de política" en la página 287 para obtener más detalles.

Obtención de un certificado

Antes de establecer un túnel de IPSec, debe seleccionar y registrarse con una Autorización de certificado (CA) fiable, tal como se describe en "Utilización de la infraestructura de clave pública" en la página 336. La CA devuelve un certificado digital X.509 firmado, que le permite identificarse y autentificarse ante otras partes de la red. El certificado consta de un ID digital codificado (firma) y de un par de claves criptográficas pública/privada. Haga lo siguiente:

1. Identifique una CA y obtenga su dirección de servidor.
2. Configure las opciones de recuperación de depósito de certificados utilizando el mandato PKI Talk 6 **add ldapserver** o **add tftpserver** tal como se describe en "Mandatos de configuración de Infraestructura de clave pública" en la página 345.
3. Cree un par de claves pública/privada utilizando el mandato PKI Talk 5 **certificate request** tal como se describe en "Mandatos de supervisión de Infraestructura de clave pública" en la página 369. Puede hacerlo en el direccionador o remotamente, por ejemplo, actuando como administrador de Red privada virtual (VPN), en cuyo caso debe cifrar y transferir de modo seguro el par de claves al direccionador.
4. Someta una petición de certificado inicial a la CA utilizando el mandato PKI Talk 5 **certificate request** tal como se describe en "Mandatos de supervisión de Infraestructura de clave pública" en la página 369. La petición se envía en un mensaje PKCS#10 a través de email o FTP. La CA enlaza el par de claves en el certificado, lo firma con la clave privada de la CA y lo almacena en un depósito (LDAP o FTP) central o se lo devuelve en un mensaje PKCS#7. Generalmente, un certificado es válido durante varios meses o más y después se renueva. Esto identifica qué partes de una red todavía son fiables.
5. Guarde el certificado en la SRAM del direccionador utilizando el mandato PKI Talk 5 **certificate save** tal como se describe en "Mandatos de supervisión de Infraestructura de clave pública" en la página 369.

Notas:

1. Para visualizar una lista de registros de certificado de la SRAM, utilice el mandato PKI Talk 6 **list certificate** tal como se describe en “Mandatos de configuración de Infraestructura de clave pública” en la página 345.
2. Para suprimir registros de certificado de la SRAM, utilice el mandato PKI Talk 6 **delete certificate** tal como se describe en “Mandatos de configuración de Infraestructura de clave pública” en la página 345.
3. Para eliminar la necesidad de volver a someter una petición de certificado durante las negociaciones de IPSec futuras, utilice el mandato PKI Talk 5 **certificate load** tal como se describe en “Mandatos de supervisión de Infraestructura de clave pública” en la página 369 para cargar el certificado recibido en la antememoria.

Mandatos de configuración de Infraestructura de clave pública

Add

Utilice el mandato PKI Talk 6 **add** para configurar el servidor de depósito de certificados y su ubicación.

Sintaxis:

a**dd** server

server Especifica que la operación de add es para un servidor.

Ejemplo 1: Añadir un servidor

```
PKI config>add server
Name ? (max 65 chars) []? myldap
Enter server IP Address []? 8.8.8.9
Transport type (Choices: TFTP/LDAP)  [TFTP]? ldap
LDAP search timeout value [3]?
LDAP retry interval (mins) [1]?
LDAP server port number [389]?
LDAP version [2]?
Bind to the server anonymously? [No]:
Enter your bind DN: []? c=us o=ibm
Enter your bind PW: []? testldap
```

Change

Utilice el mandato PKI Talk 6 **change** para cambiar el servidor de depósito de certificados y su ubicación.

Sintaxis:

c**hange**
server

server Especifica que la operación de add es para un servidor.

Ejemplo 1: Cambiar un servidor

```
PKI config>change server
Name []? myldap
Enter server IP Address []? 8.8.8.7
Server type will continue to be LDAP
LDAP search timeout value [3]?
LDAP retry interval (mins) [1]?
LDAP server port number [389]?
LDAP version [2]?
Enter your bind DN: [c=us o=ibm]?
Enter your bind PW: [testldap]?
```

Delete

Utilice el mandato Talk 6 **delete** de PKI para suprimir un registro de certificado o un registro de clave privada de la SRAM de un direccionador o para suprimir un servidor.

Sintaxis:

delete
certificate
private-key
server

certificate
Especifica que la operación de delete es para uno o más registros de certificado.

all Especifica que deben suprimirse todos los registros de certificado.

id Especifica el ID del registro de certificado que debe suprimirse.

Ejemplo 1: suprimir un certificado

```
PKI config>delete certificate
Cert Name []? test
Enter the type of the certificate:
Choices:  1-Root CA Cert, 2-Router Cert
Enter (1-2): [2]?
Box Certificate [TEST] deleted successfully
Corresponding private Key [TEST] deleted successfully
```

Ejemplo 2: Suprimir claves privadas

```
PKI config>delete private-keys
Private Key Name []? test
Private Key [TEST] deleted successfully
Corresponding box certificate [TEST] deleted successfully
```

Ejemplo 3: Suprimir registros de servidor

```
PKI config>delete server
Name []? myldap
Server MYLDAP deleted successfully
```

private-key
Especifica que la operación de delete es para uno o más registros de clave privada.

server Especifica que la operación de delete es para un servidor.

List

Utilice el mandato PKI Talk 6 **list** para listar registros de certificado o de clave de la SRAM de un direccionador o para visualizar la lista de revocación de certificados (CRL — lista de partes habilitadas para ISAKMP cuyos certificados se han revocado). Para obtener la CRL actual, utilice el mandato PKI Talk 6 **load**.

Sintaxis:

list certificates
crl
private-keys
servers

certificates
Especifica que la operación de list es para los registros de certificado.

crl Especifica que la operación de list es para la lista de revocaciones de certificado.

private-keys
Especifica que la operación de list es para los registros de clave privada.

servers Especifica que la operación de list es para los registros de servidor.

Ejemplo: Listar certificados

```
PKI config>list certificates

Root CA  certificate:
       SRAM    Name:   B
       Subject Name:   /c=US/o=ibm/ou=nhd
       Issuer  Name:   /c=US/o=ibm/ou=nhd
          Validity:   1998/12/19 2:2:21 -- 2018/12/19 2:32:21
  Default Root Cert:   Yes



Router   Certificate:
       SRAM    Name:   W
       Subject Name:   /c=US/o=ibm/ou=nhd/cn=testip
       Issuer  Name:   /c=US/o=ibm/ou=nhd
   Subject alt Name:   1.1.1.1
         Key Usuage:   Sign & Encipherment
           Validity:   1999/1/19 23:24:27 -- 2002/1/19 23:54:27
       Default Cert:   No
```

Ejemplo: Listar crl

```
PKI config>list crl
```

Ejemplo: Listar claves privadas

```
PKI config>list private-keys
Private Keys In SRAM:

1) Name W
```

Ejemplo: Listar registros de servidor

```
PKI config>list servers
1)  Name: SERVER1
    Type: LDAP
    IP addr: 1.1.1.2
        LDAP search timeout (secs): 10
        LDAP retry interval (mins): 3
        LDAP server port number: 390
        LDAP version: 2
        Anonymous bind ?: y


2)  Name: TEST
    Type: TFTP
    IP addr: 8.8.8.8
```

Load

Utilice el mandato PKI Talk 6 **load** para recuperar la lista de revocaciones de certificados (CRL) más actual del CA. Deberá realizar dicha acción con regularidad y frecuencia para asegurarse de la validez de la copia de la lista. Durante la autentificación, la característica IPSec valida el certificado basándose en el contenido de la CRL.

Sintaxis:

load crl

Configuración de Seguridad de IP (IPv4) manual

Esta sección describe las opciones de configuración disponibles para IPSec manual con IPv4. Todas las funciones de IPSec se aplican a IPv4.

Realice los pasos siguientes para configurar un túnel manual de IPSec:

1. Cree el túnel de IPSec.
2. Restablezca IPSec.
3. Configure la política para el túnel manual (perfil, validez, política)
4. Restablezca la Política.

Configuración de los algoritmos

Puede configurar políticas de túnel con los algoritmos que se muestran en la Tabla 42 en la página 349.

Tabla 42. Algoritmos configurados con varias políticas de túnel	
Política de túnel	**Algoritmos**
AH, AH-ESP o ESP-AH	• Algoritmo de autentificación de AH—Necesario • Algoritmo de autentificación de AH remota—Opcional
ESP, AH-ESP o ESP-AH	• Algoritmo de cifrado local—Necesario • Algoritmo de cifrado remoto—Opcional • Algoritmo de autentificación de ESP local—Opcional • Algoritmo de autentificación de ESP remota—Opcional **Nota:** Si la carga de software no incluye cifrado, no se verían los parámetros relacionados con el cifrado.

Una política de túnel utiliza un algoritmo local en paquetes de salida y un algoritmo remoto en paquetes de entrada. El algoritmo local para el direccionador en el extremo cercano de un túnel debe coincidir con el algoritmo remoto para el direccionador en el extremo lejano del túnel. Los valores para los algoritmos remotos son opcionales y, por omisión, toman el valor de los algoritmos locales correspondientes. El algoritmo de autentificación de ESP local es opcional puesto que la autentificación de ESP es opcional.

Configuración de claves de cifrado

Para cada algoritmo local que configure, también debe configurar una clave que sea idéntica a la clave para el algoritmo correspondiente en el sistema principal remoto. Consulte la descripción de las claves para el mandato **add tunnel** en “Mandatos de configuración de seguridad de IP manual”.

Acceso al entorno de configuración de seguridad de IP

Para acceder al entorno de configuración de Seguridad de IP, entre **t 6** en el indicador de mandatos OPCON (*) y, a continuación, entre la secuencia siguiente de mandatos en el indicador de mandatos `Config>`:

```
   Config> feature ipsec
IP Security feature user configuration
   IPsec config>ipv4
   IPV4-IPsec config>
```

Mandatos de configuración de seguridad de IP manual

Esta sección describe los mandatos de configuración de seguridad de IP. Entre estos mandatos en el indicador de mandatos `IPV4-IPsec config>`.

Tabla 43. Resumen de mandatos de configuración de seguridad de IP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Add tunnel	Añade un túnel de seguridad.
Change tunnel	Cambia valores de un parámetro de configuración de túnel de seguridad.
Delete tunnel	Suprime un túnel de seguridad.
Disable	Inhabilita todo el proceso de Seguridad de IP de un modo seguro (los paquetes que coinciden con los filtros del paquete se excluyen), inhabilita todo el proceso de Seguridad de IP de un modo no seguro (los paquetes que coinciden con los filtros del paquete se aceptan) o inhabilita un túnel manual.
Enable	Habilita todo el proceso de Seguridad de IP o habilita un túnel de seguridad.
List	Lista información sobre información de Seguridad de IP global o información sobre túneles definidos.
Set	Establece varias opciones de IPSec.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Add Tunnel

Utilice el mandato **add tunnel** para añadir los parámetros para definir un túnel de IPSec.

Sintaxis:

add tunnel...

nombre-túnel

Parámetro opcional para etiquetar el túnel. Debe ser exclusivo dentro del 2210.

Valores válidos: un máximo de 15 caracteres; el primer carácter debe ser una letra; no se pueden utilizar blancos.

Valor por omisión: ninguno

duración

Tiempo en minutos que el túnel puede estar activo. El valor 0 indica que la duración del túnel no caduca nunca.

Valores válidos: 0 - 525600 (0 = sin caducidad; 525600 = 365 días)

Valor por omisión: 46080 (32 días)

modalidad-encapsulación

La manera de encapsular el paquete de IP. En modalidad de túnel, se encapsula todo el paquete de IP y se crea una nueva cabecera de IP; en modalidad de transporte, no se encapsula la cabecera de IP. Si un extremo del túnel de seguridad es un direccionador, ***debe*** utilizarse la modalidad de túnel, según el borrador de la arquitectura de seguridad Internet Engineering Task Force (IETF).

Valores válidos: túnel (*TUNN*) o conversión (*TRANS*)

Valor por omisión: túnel (*TUNN*)

política-túnel
Una de las cuatro opciones que define la política de túnel: Cabecera de autentificación (AH) de IP, Carga de seguridad de encapsulación (ESP) de IP o combinaciones de estos protocolos (AH-ESP y ESP-AH). En AH-ESP, el cifrado de ESP se ejecuta primero en los paquetes de salida; en ESP-AH, la autentificación de AH se ejecuta primero en los paquetes de salida. Algunos parámetros son exclusivos para ESP o AH. Los parámetros de cifrado sólo se configuran si se selecciona ESP, AH-ESP o ESP-AH; los parámetros de autentificación sólo se configuran si se selecciona AH, AH-ESP o ESP con autentificación.

Valores válidos: AH, ESP, AH-ESP, ESP-AH

Valor por omisión: AH-ESP

dirección-IP-local
Dirección IP para este extremo del túnel.

Valores válidos: una dirección IP válida que se ha configurado para una interfaz o como la dirección interna del 2210.

Valor por omisión: una de las direcciones IP configuradas para el direccionador

spi-local
Una asociación de seguridad es una conexión de seguridad en un único sentido que utiliza AH o ESP para proteger el tráfico de conexión. El índice de parámetros de seguridad (SPI) es un valor de 32 bits arbitrario que identifica exclusivamente una de las dos asociaciones de seguridad (entrada o salida) asociadas con este túnel de seguridad. Este parámetro, que es necesario, identifica el SPI que se espera en este túnel para los paquetes de entrada recibidos en el extremo local del túnel. Este valor no puede coincidir con el SPI local de otro túnel con la misma dirección IP local. Independientemente de la política de túnel (ESP, AH, AH-ESP o ESP-AH), sólo se configura un SPI local para el tráfico de entrada para un túnel de seguridad de IP.

Valores válidos: cualquier valor de 32 bits mayor que 255

Valor por omisión: 256

algoritmo-cifrado-local
El algoritmo de cifrado que se utiliza para ESP en los paquetes de salida que se envían desde el direccionador local, necesario cuando se configura ESP. En algunos países, alguno de estos algoritmos, o todos, puede que no estén disponibles debido a las normas de exportación de los EE.UU. Este algoritmo de cifrado debe coincidir con el algoritmo de cifrado remoto.

El algoritmo ESP-NULL impide que ESP realice el cifrado. Este algoritmo está disponible en todos los países. Si se ha seleccionado ESP-NULL, debe activarse ESP para la autentificación seleccionando uno de los algoritmos de autentificación HMAC-MD5 o HMAC-SHA-1.

Valores válidos: DES-CBC, CDMF, 3DES o ESP-NULL

Valor por omisión: DES-CBC

clave-cifrado-local

La clave o las claves utilizadas con el algoritmo de cifrado ESP local. Deben coincidir con las claves correspondientes que se configuran en el extremo opuesto del túnel de seguridad. Esta clave no se configura cuando se selecciona el algoritmo de cifrado ESP-NULL.

Valores válidos:

- Para DES-CBC: 16 caracteres hex (0 - 9, a - f, A - F)
- Para CDMF: 16 caracteres hex (0 - 9, a - f, A - F)
- Para 3DES: tres claves separadas, ninguna de las cuales es igual, cada una de 16 caracteres hex (0 - 9, a - f, A - F)

Valor por omisión: ninguno

relleno-para-cifrado-local

Tamaño en bytes del relleno adicional que se añade a los paquetes de ESP de salida. El relleno adicional se puede utilizar para enmascara el tamaño de los paquetes de IP que se cifran cuando el algoritmo de cifrado da como resultado un paquete de cifrado del mismo tamaño que el paquete original. Los valores de relleno de ESP deben ser un múltiplo de 8. Si se configura un valor que no sea divisible entre 8, dicho valor se redondea hasta el valor siguiente que sea divisible entre 8.

Cuando el algoritmo de cifrado es ESP-NULL, el relleno no es necesario puesto que el algoritmo ESP-NULL añade un byte al tamaño del paquete original. Si se configura relleno para el cifrado local, el valor se ignora.

Valores válidos: 0 - 120

Valor por omisión: 0

autentificación-ESP-local

Selecciona autentificación de ESP local, si se desea. La autentificación es necesaria si el algoritmo de cifrado es ESP-NULL.

Valores válidos: Sí o No

Valor por omisión: Sí

algoritmo-autentificación-local

El algoritmo de autentificación se utiliza en paquetes de salida. Es un parámetro opcional para ESP y no es necesario a menos que seleccione autentificación de ESP. Parar AH , AH-ESP o ESP-AH, este parámetro es necesario. El algoritmo de autentificación utilizado debe coincidir con el algoritmo de autentificación remoto que se utiliza en el extremo alejado del túnel de IPSec.

Valores válidos: HMAC-MD5 o HMAC-SHA

Valor por omisión: HMAC-MD5

clave-autentificación-local

Clave que se utiliza con el algoritmo de autentificación local. Debe coincidir con la clave equivalente que se configura en el extremo opuesto del túnel de IPSec. Es necesario si la política es AH, AH-ESP o ESP-AH, o si la política es ESP y se ha configurado el algoritmo de autentificación de ESP local.

Valores válidos:

- para HMAC-MD5: 32 caracteres hex (0 - 9, a - f, A - F)
- para HMAC-SHA: 40 caracteres hex (0 - 9, a -f, A - F)

Valor por omisión: ninguno

dirección-IP-remota
Dirección IP para el extremo remoto del túnel. Es un parámetro necesario.

Valores válidos: una dirección IP válida

Valor por omisión: ninguno

spi-remoto
Una asociación de seguridad es una conexión de seguridad en un único sentido que utiliza AH o ESP para proteger el tráfico de conexión. El índice de parámetros de seguridad (SPI) es un valor de 32 bits arbitrario que identifica exclusivamente una de las dos asociaciones de seguridad (entrada o salida) asociadas con este túnel de seguridad. Este parámetro, que es necesario, identifica el SPI que se espera en ESP o AH para los paquetes de salida destinados al sistema principal remoto. Este valor no puede coincidir con el SPI remoto de otro túnel con la misma dirección IP remota. Independientemente de la política de túnel (ESP, AH, AH-ESP o ESP-AH), sólo se configura un SPI local para el tráfico de salida para un túnel de IPSec.

Valores válidos: cualquier valor de 32 bits mayor que 255

Valor por omisión: 256

algoritmo-cifrado-remoto
Algoritmo de descifrado que se utiliza en los paquetes de entrada recibidos desde el sistema principal. Debe coincidir con el algoritmo de cifrado local.

El algoritmo ESP-NULL impide que ESP realice el cifrado. Si se ha seleccionado ESP-NULL, debe activarse ESP para la autentificación seleccionando uno de los algoritmos de autentificación HMAC-MD5 o HMAC-SHA-1.

Valores válidos: DES-CBC, CDMF, 3DES o ESP-NULL

Valor por omisión: valor del algoritmo de cifrado local

clave-cifrado-remoto
La clave o las claves que se utilizan con el algoritmo de cifrado ESP. Deben coincidir con las claves equivalentes que se configuran en el extremo opuesto del túnel de seguridad. Esta clave no se configura cuando se selecciona el algoritmo de cifrado ESP-NULL.

Valores válidos:

- Para DES-CBC: 16 caracteres hex (0 - 9, a - f, A - F)
- Para CDMF: 16 caracteres hex (0 - 9, a - f, A - F)
- Para 3DES: tres claves separadas, ninguna de las cuales coincide, cada una de 16 caracteres hex (0 - 9, a - f, A - F)

Valor por omisión: ninguno

verificación-de-relleno-cifrado-remoto
Determina si se ha verificado el tamaño del relleno de cifrado en los paquetes recibidos.

Valores válidos: Sí o No

Valor por omisión: No

relleno-para-cifrado-remoto
Tamaño en bytes de relleno adicional que se espera en los paquetes de ESP recibidos. Este parámetro es necesario y sólo es válido si el valor de *verificación-de-relleno-cifrado-remoto* es Sí. Los valores de relleno de ESP

deben ser un múltiplo de 8. Si se configura un valor que no sea divisible entre 8, dicho valor se redondea hasta el valor siguiente que sea divisible entre 8.

Valores válidos: 0 - 120

Valor por omisión: 0

autentificación-ESP-remota
Selecciona autentificación de ESP remota para paquetes de entrada, si se desea.

Valores válidos: Sí o No

Valor por omisión: Sí

algoritmo-autentificación-remoto
Algoritmo de autentificación utilizado para los paquetes de entrada. Es un parámetro opcional para ESP y no es necesario a menos que seleccione autentificación de ESP. Para AH o combinaciones de AH y ESP (AH-ESP o ESP-AH), este parámetro es necesario. El algoritmo de autentificación utilizado debe coincidir con el algoritmo de autentificación local que se utiliza en el extremo alejado del túnel de IPSec.

Valores válidos: HMAC-MD5 o HMAC-SHA

Valor por omisión: HMAC-MD5

clave-autentificación-remota
Clave que se utiliza con el algoritmo de autentificación remota. Debe coincidir con la clave equivalente que se configura en el extremo opuesto del túnel de seguridad. Es necesario en AH, AH-ESP y ESP-AH, y en ESP si se ha configurado el algoritmo de autentificación ESP remota.

Valores válidos:

- para HMAC-MD5: 32 caracteres hex (0 - 9, a - f, A - F)
- para HMAC-SHA: 40 caracteres hex (0 - 9, a -f, A - F)

Valor por omisión: ninguno

habilitar-prevención-reproducción
Especifica si está habilitada la prevención de reproducción. Si está habilitada la prevención de reproducción, se supervisan los números de secuencia de las cabeceras de seguridad de IP para evitar que el receptor del túnel procese paquetes duplicados. La utilización de la prevención de reproducción no se recomienda puesto que debe desactivarse la asociación de seguridad cuando un contador de número de secuencia del emisor llega a su límite. Cuando esto sucede, es necesaria una intervención manual para reiniciar la asociación de seguridad existente o crear una nueva.

Además, si está habilitada la prevención de reproducción y restablece IPSec utilizando el mandato **reset ipsec**, debe asegurarse de que IPSec también esté restablecido en el direccionador situado en el otro extremo del túnel de IPSec. Esto es necesario para reinicializar el número de secuencia en ambos extremos del túnel. Si IPSec se restablece en un extremo del túnel y no en el otro, es posible que los direccionadores de cada extremo del túnel excluyan paquetes debido a una no coincidencia de número de secuencia.

Valores válidos: Sí o No

Valor por omisión: No

Bit-DF

Especifica el manejo del bit de Don't Fragment (No Fragmentar) (DF) en la cabecera exterior para los túneles de seguridad de modalidad de túnel. Este bit se puede establecer en cabeceras IPv4 para especificar que el paquete no se puede fragmentar. El parámetro Bit-DF indica al 2210 cómo debe manejar el bit de DF en paquetes de entrada - si debe copiarse el valor del Bit-DF de la cabecera interior en la cabecera exterior o si debe establecerse o borrarse el bit en la cabecera exterior.

Si el bit de DF está establecido y el paquete no se puede fragmentar, IPSec utiliza la función Determinación de la MTU de la ruta (PMTU). Consulte el apartado "Determinación de la Unidad máxima de transmisión de la ruta" en la página 332 para obtener información.

Valores válidos: Copiar, Establecer, Borrar

Valor por omisión: Copiar

habilitar-túnel

Especifica si este túnel está habilitado. El túnel habilitado no filtrará paquetes hasta que se haya definido un filtro de paquete para definir la interfaz a través de la cual operará el túnel de IPSec y se haya restablecido o reiniciado IP en el 2210. Puede utilizar el mandato **reset ip** para restablecer IP.

Valores válidos: Sí o No

Valor por omisión: Sí

Change Tunnel

Utilice el mandato **change tunnel** para cambiar un parámetro de túnel de IPSec previamente configurado mediante el mandato **add tunnel**.

Sintaxis:

c**hange** t**unnel ...**

Consulte el mandato **add tunnel** para obtener una lista de los parámetros que se pueden cambiar.

Delete Tunnel

Utilice el mandato Talk 6 **delete tunnel** para suprimir un túnel de IPSec.

Sintaxis:

de**lete** t**unnel**
id-túnel
nombre-túnel
all

id-túnel Especifica el identificador del túnel de IPSec que debe suprimirse.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre-túnel

Especifica el nombre del túnel de IPSec que debe suprimirse.

Valores válidos: cualquier nombre de túnel configurado

Valor por omisión: ninguno

all Especifica que deben suprimirse todos los túneles de IPSec de esta interfaz.

Disable

Utilice el mandato **disable** para inhabilitar el túnel de IPSec o para inhabilitar todos los túneles de IPSec de un modo seguro (los paquetes que coinciden con los filtros de IPSec se excluyen) o de una manera no segura (los paquetes que coinciden con los filtros de IPSec se aceptan).

Sintaxis:

d**isable**
i**p**sec **d**rop
i**p**sec **p**ass
tunnel ...

ipsec drop
Inhabilita la seguridad de IP en el direccionador de una manera segura. Se inhabilitarán todos los túneles de IPSec, pero la información de túnel de seguridad de las normas de filtro de paquete se utiliza para identificar los paquetes que coinciden con los filtros de paquete de túnel de IPSec. Los paquetes que coinciden se excluyen.

ipsec pass
Inhabilita la seguridad de IP en el direccionador de una manera no segura. Se inhabilitarán todos los túneles de IPSec. Los paquetes que coinciden con los filtros de paquete de túnel de IPSec se reenvían como tráfico normal.

tunnel *id-túnel nombre-túnel* **all**
Inhabilita la seguridad de IP en un túnel especificado o en todos los túneles.

id-túnel
Especifica el identificador del túnel de seguridad que debe inhabilitarse.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre-túnel
Especifica el nombre del túnel de seguridad que debe inhabilitarse.

Valores válidos: cualquier nombre de túnel configurado

Valor por omisión: ninguno

all Todos los túneles.

Enable

Utilice el mandato **enable** para habilitar el protocolo de Seguridad de IP en todas las interfaces o en un único túnel. Debe habilitar IPSec globalmente en el direccionador para que se activen los túneles de IPSec habilitados individualmente.

Sintaxis:

e**nable**
i**p**sec
tunnel ...

ipsec
Habilita la seguridad de IP en el direccionador.

tunnel *id-túnel nombre-túnel* **all**

Habilita la seguridad de IP en un túnel especificado o en todos los túneles.

id-túnel

Especifica el identificador del túnel de seguridad que debe habilitarse.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre-túnel

Especifica el nombre del túnel de seguridad que debe habilitarse.

Valores válidos: cualquier nombre de túnel configurado

Valor por omisión: ninguno

all Todos los túneles.

List

Utilice el mandato **list** para visualizar la configuración de Seguridad de IP actual. Los túneles globales incluyen todos los túneles del direccionador, tanto los activos como los definidos. En todos los túneles se incluyen todos los túneles configurados en esta interfaz, tanto los activos como los definidos. Los túneles activos son los que están actualmente activos; los túneles definidos están definidos pero no están activos. Para IPv4, también se listan los certificados seleccionados de la SRAM de un direccionador.

Sintaxis:

list ...
- all
- status
- tunnel
  - active *id-túnel nombre-túnel* all
  - defined *id-túnel nombre-túnel* all

Ejemplo 1: Listado de todos los túneles de IPSec

```
IPsec config>list all

IPsec is ENABLED

IPsec Path MTU Aging Timer is 20 minutes

Defined Manual Tunnels:

   ID         Name         Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------
      1  test                    1.1.1.1          2.1.1.1  TUNN   Enabled
      2  test2                   1.1.1.1          1.1.1.3  TRANS  Enabled

Tunnel Cache:

 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  ---------------  ---------------  -----  ------  ------------------
    2          1.1.1.1          1.1.1.3  TRANS  ESP     ****************
    1          1.1.1.1          2.1.1.1  TUNN   AH      ****************
```

Ejemplo 2: Listado de un túnel de IPSec con la política ESP y el algoritmo ESP-NULL

```
IPsec config>li tun 1000

Tunnel  Name            Mode   Policy   Life   Replay  Rcv  IPsec  State
ID                                              Prev    Win  Vers
------  --------------  -----  ------  ------  ------  ---  -----  --------
1000    t1000           TUNN   ESP      46080    No    ---   V2    Enabled

Handling of DF bit in outer header:  COPY

Local Information:

      IP Address: 10.11.12.10
  Authentication:  SPI: -----    Algorithm: ----------
      Encryption:  SPI:  1234    Encryption Algorithm: NULL
                                 Extra Pad:   0
                                 ESP Authentication Algorithm: HMAC-MD5
Remote Information:

      IP Address: 10.11.12.11
  Authentication:  SPI: -----    Algorithm: ----------
      Encryption:  SPI:  1234    Encryption Algorithm: NULL
                                 Verify Pad?:  No
                                 ESP Authentication Algorithm: HMAC-MD5
```

Set

Utilice el mandato **set** para controlar el valor de PMTU del túnel.

Sintaxis:

set path-mtu-age-timer

path-mtu-age-timer
Especifica el tiempo (en minutos) que transcurrirá antes de que el 2210 restablezca el valor de PMTU de túnel al máximo.

Valor por omisión: 10 (0 significa inhabilitado)

Configuración de un túnel manual (IPv4)

Este tema proporciona información sobre cómo configurar un túnel manual IPv4 para la red que se muestra en la Figura 27 en la página 333.

Configuración del túnel para el direccionador A

El ejemplo siguiente muestra cómo configurar un túnel manual de IPSec para el direccionador A en la red que se muestra en la Figura 27 en la página 333 utilizando IPv4.

```
Config> feature ipsec
IP Security feature user configuration
IPsec config>ipv4
IPV4-IPsec config>add tunnel
Adding tunnel 1
Tunnel Name (optional)? tunnelone
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH, ESP, AH-ESP, ESP-AH) [AH-ESP]? AH
Local IP Address [1.1.1.1]? 223.252.252.216
Local Authentication SPI (256-65535)[256]?
Local Authentication Algorithm (HMAC-MD5, HMAC-SHA)[HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0.0.0.0]? 223.252.252.210
Remote Authentication SPI (1-65535) [256]?
Remote Authentication Algorithm (HMAC-MD5, HMAC-SHA)[HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Copy, set, or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
IPV4-Ipsec config>
```

Como puede ver en este ejemplo, se le solicitan los parámetros que debe proporcionar. La configuración de un túnel de seguridad ESP, AH-ESP o ESP-AH necesita parámetros similares.

Nota: Los valores de las claves no se visualizan cuando se entran. Por lo tanto, no se pueden ver en este ejemplo. Si las claves para la autentificación HMAC-MD5 son visibles, verá 32 caracteres hexadecimales. Por ejemplo, una clave puede tener el valor: X'1234567890ABCDEF1234567890ABCDEF'.

Configuración del túnel para el direccionador B

Dentro del direccionador B, debe configurar el mismo túnel manual de IPSec que se ha configurado para el direccionador A, túnel 1 de IPSec. La dirección IP local de este túnel en el direccionador B es 223.252.252.210 y la dirección IP remota es 223.252.252.216. Todos los otros parámetros del túnel de IPSec deben coincidir con los parámetros que se han configurado para el direccionador A.

Ejemplo: configurar manualmente un túnel de seguridad de IP con ESP

Tenga en cuenta que se le socilitará que establezca el bit de DF cuando el túnel esté en modalidad de túnel y la política de túnel sea ESP. Este ejemplo sólo muestra la configuración del túnel de IPSec, no de todos los filtros de paquete.

```
IPV4-IPsec config>add tunnel
Adding tunnel 2
Tunnel Name (optional)? tunneltwo
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]? ESP
Local IP Address [1.1.1.1]?
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES, NULL) [DES-CBC]?
Do you wish to change the Local Encryption Key? [No]:
Additional Padding for Local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [Yes]:
Remote IP Address [0.0.0.0]?
Remote Encryption SPI (1-65535) [256]?
Remote Encryption Algorithm (DES-CBC,CDMF) [DES-CBC]?
Do you wish to change the Remote Encryption Key? [No]:
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No]:
Copy, set or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
IPV4-IPsec config>
```

Ejemplo: configurar manualmente un túnel de seguridad de IP con ESP y ESP-NULL

Tenga en cuenta que es necesaria la autentificación.

```
IPV4-IPsec config>add tunnel
Adding tunnel 3
Tunnel Name (optional)? tunnel3
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]? ESP
Local IP Address [1.1.1.1]?
Local Encryption SPI (256-65535) [256]? 1234
Local Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [DES-CBC]? null
Additional Padding for Local Encryption (0-120) [0]?
Local ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0.0.0.0]? 10.11.12.11
Remote Encryption SPI (1-65535) [1234]?
Remote Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [NULL]?
Do you wish to perform verification of remote encryption padding? [No]:
Remote ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Copy, set or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
IPV4-IPsec config>
```

Configuración de la seguridad de IP manual (IPv6)

Esta sección describe las opciones de configuración disponibles para IPSec manual con IPv6. Todas las funciones de IPSec se aplican a IPv6. Observe los cambios siguientes en las preguntas de la configuración de IPSec cuando se configura IPSec para IPv6:

- Debe entrar las direcciones en formato de dirección IPv6 (por ejemplo, 8:0:9:8::1).
- No se le solicita el establecimiento del bit de DF.

Realice los pasos siguientes para configurar un túnel manual de IPSec:

1. Cree el túnel de IPSec.
2. Restablezca IPSec.
3. Configure normas de filtro.
4. Restablezca IPV6.

Configuración de los algoritmos

Puede configurar políticas de túnel con los algoritmos que se muestran en la Tabla 44.

Tabla 44. Algoritmos configurados con varias políticas de túnel

Política de túnel	Algoritmos
AH, AH-ESP o ESP-AH	• Algoritmo de autentificación de AH—Necesario • Algoritmo de autentificación de AH remota—Opcional
ESP, AH-ESP o ESP-AH	• Algoritmo de cifrado local—Necesario • Algoritmo de cifrado remoto—Opcional • Algoritmo de autentificación de ESP local—Opcional • Algoritmo de autentificación de ESP remota—Opcional **Nota:** Si la carga de software no incluye cifrado, no se verían los parámetros relacionados con el cifrado.

Una política de túnel utiliza un algoritmo local en paquetes de salida y un algoritmo remoto en paquetes de entrada. El algoritmo local para el direccionador en el extremo cercano de un túnel debe coincidir con el algoritmo remoto para el direccionador en el extremo lejano del túnel. Los valores para los algoritmos remotos son opcionales y, por omisión, toman el valor de los algoritmos locales correspondientes. El algoritmo de autentificación de ESP local es opcional puesto que la autentificación de ESP es opcional.

Configuración de claves de cifrado

Para cada algoritmo que configure, también debe configurar una clave que sea igual que la clave para el algoritmo correspondiente en el sistema principal remoto. Consulte la descripción de las claves para el mandato **add tunnel** en “Mandatos de configuración de seguridad de IP manual” en la página 349.

Acceso al entorno de configuración de seguridad de IP

Para acceder al entorno de configuración de Seguridad de IP, entre **t 6** en el indicador de mandatos OPCON (*) y, a continuación, entre la secuencia siguiente de mandatos en el indicador de mandatos `Config>`:

```
   Config> feature ipsec
IP Security feature user configuration
IPsec config> ipv6
IPV6-IPsec config>
```

Mandatos de configuración de seguridad de IP manual

Consulte “Mandatos de configuración de seguridad de IP manual” en la página 349 para obtener una descripción de los mandatos de configuración de Seguridad de IP disponibles para IPv6. Los mandatos para IPv6 son los mismos que se utilizan para IPv4 a menos que se indique lo contrario. Entre los mandatos en el indicador de mandatos `IPV6-IPsec config>`.

Configuración de un túnel manual (IPv6)

Consulte la red de ejemplo de la Figura 27 en la página 333 cuando lea este tema. El túnel 1 de IPSec tiene un punto final en la interfaz 1 del direccionador A. El direccionador A se configurará para IPSec. Realice los pasos siguientes para configurar el direccionador A manualmente:

1. Cree el túnel de IPSec.
2. Cree un filtro de paquete de salida en la interfaz del direccionador, que es el punto final del túnel de IPSec.
3. Cree normas de control de acceso para los filtros de paquete.
4. Restablezca IPSec.
5. Restablezca IPv6.

Creación del túnel de seguridad de IP para el direccionador A

El ejemplo siguiente muestra cómo crear el túnel 1 de IPSec para el direccionador A.

```
Config> feature ipsec
IP Security feature user configuration
IPsec config> ipv6
IPV6-IPsec config> add tunnel
IPsec Tunnel ID (1 - 65535) [1]
Tunnel Name (optional)? tunnelone
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH, ESP, AH-ESP, ESP-AH) [AH-ESP]? AH
Local IP Address [1000:1::1]? 2000::A
Local Authentication SPI (256-65535)[256]?
Local Authentication Algorithm (HMAC-MD5, HMAC-SHA)[HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0::0]? 2000::B
Remote Authentication SPI (1-65535) [256]?
Remote Authentication Algorithm (HMAC-MD5, HMAC-SHA)[HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Do you wish to enable this tunnel? [Yes]:
IPV6-IPsec config>
```

Como puede ver en este ejemplo, se le solicitan los parámetros que debe proporcionar. La configuración de un túnel de seguridad ESP, AH-ESP o ESP-AH necesita parámetros similares.

Nota: Los valores de las claves no se visualizan cuando se entran. Por lo tanto, no se pueden ver en este ejemplo. Si las claves para la autentificación HMAC-MD5 son visibles, verá 32 caracteres hexadecimales. Por ejemplo, una clave puede tener el valor X'1234567890ABCDEF1234567890ABCDEF'.

Configuración de filtros de paquete para el direccionador A

Después de crear el túnel de IPSec para el direccionador A, debe configurar un filtro de paquete de IP. La creación del filtro de paquete *direccionador-A-salida* se muestra en el ejemplo siguiente. Consulte las secciones Filtrado de IPv6 y Control de acceso en el capítulo Utilización de IPv6 de la publicación *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener más información sobre cómo configurar filtros de paquete y normas de control de acceso de IPv6.

```
*talk 6
Config> Protocol IPv6
Internet protocol user configuration
IPv6 Config> set access-control on
IPv6 Config> add packet-filter
Packet-filter name [ ]? out-router-A
Filter incoming or outgoing traffic? [IN]? OUT
Which interface is this filter for [0]? 1
IPv6 Config> update packet-filter
Packet-filter name [ ]? out-router-A
Packet-filter 'out-router-A' Config>
```

Configuración de normas de control de acceso de filtro de paquete para el direccionador A

El paso siguiente consiste en configurar las normas de control de acceso de filtro de paquete. Cree dos normas de control de acceso en el filtro de paquete de salida *direccionador-A-salida*.

Las normas de control de acceso del filtro de paquete de salida llevan a cabo estas funciones:

- Una norma de control de acceso define el rango de las direcciones de origen y de destino de los paquetes que deben pasarse al túnel de IPSec.
- La otra norma de control de acceso permite que el tráfico de IPSec pase a través del filtro de paquete.

Configure la primera norma de control de acceso para el filtro de paquete *direccionador-A-salida*. Esta norma de control de acceso pasa paquetes desde la red 1000:1:: a la red de destino 3000:1:: conectada al Direccionador B.

```
IPv6 Config> update packet-filter
Packet-filter name [ ]? out-router-A
Packet-filter 'out-router-A' Config> add access
Enter type [E]? IS
Internet source [0::0]? 1000:1::
Prefix Length [64]? 64
Internet destination [0::0]? 3000:1::
Prefix Length [64]? 64
Enter IPsec Tunnel ID [1]? 2
Packet-filter 'out-router-A' Config>
```

La segunda norma de control de acceso para *direccionador-A-salida* permite que los paquetes protegidos pasen entre los dos extremos del túnel de IPSec.

```
Packet-filter 'out-router-A' Config> add access
Enter type [E]? I
Internet source [0::0]? 2000::A
Prefix Length [64]? 64
Internet destination [0::0]? 2000::B
Prefix Length [64]? 64
Packet-filter 'out-router-A' Config>
```

Al igual que en los otros filtros de paquete, puede que desee configurar una norma de control de acceso comodín para *direccionador-A-salida* para pasar tráfico que no coincida con ninguna norma de control de acceso.

Restablecimiento de la seguridad de IP y de IP en el direccionador de A

Después de configurar la política, utilice el mandato Talk 5 **reset ipsec** para volver a cargar la SRAM con la nueva configuración de IPSec. El mandato **reset ipsec** no afecta a ninguna configuración de IP. A continuación, utilice el mandato Talk 5 **reset ipv6** para restablecer dinámicamente IPv6 dentro del direccionador. Alternativamente, para restablecer cada componente, puede reiniciar el direccionador. Debe restablecer IPSec e IPv6 o reiniciar el direccionador para asegurar que se vuelvan a cargar las normas de filtro. De lo contrario, puede que la configuración no esté soportada correctamente en la interfaz. Consulte “Configuración y supervisión de la seguridad de IP” en la página 343 y el mandato **reset ipv6** en la publicación *Consulta de configuración y supervisión de protocolos Volumen 2* para obtener más información.

Como se muestra en la Figura 27 en la página 333, el túnel 2 de IPSec tiene un punto final en la interfaz 1 del direccionador B. Lleve a cabo los pasos siguientes para configurar el direccionador B manualmente.

1. Cree el túnel de IPSec.
2. Cree un filtro de salida en la interfaz del direccionador que sea el punto final del túnel de IPSec.
3. Cree normas de control de acceso para los filtros de paquete.
4. Restablezca IPSec.
5. Restablezca IPv6.

Creación del túnel de seguridad de IP para el direccionador B

Dentro del direccionador B, se ha creado el mismo túnel de IPSec para el direccionador A, debe crearse el túnel 2 de IPSec. La dirección IP local de este túnel en el direccionador B es 2000::B y la dirección IP remota es 2000::A. Todos los demás parámetros de túnel de IPSec deben coincidir con los parámetros que se han especificado para el direccionador A.

Configuración de filtros de paquete para el direccionador B

Igual que para el direccionador A, configure un filtro de paquete de salida (*direccionador-B-salida*) en la interfaz 1, que es la interfaz en el direccionador B que es el punto final del túnel 1 de IPSec.

Configuración de normas de control de acceso de filtro de paquete para el direccionador B

Configure una norma de control de acceso en *direccionador-B-salida* para pasar paquetes de salida desde la red 3000:1:: a IPSec para su proceso y transmisión a través del túnel 2 de IPSec 2. Esta norma de control de acceso es de tipo I y S.

```
Packet-filter name [ ]? out-router-B
Packet-filter 'out-router-B' Config> add access
Enter type [E]? IS
Internet source [0::0]? 3000:1::
Prefix Length [64]? 64
Internet destination [0::0]? 1000:1::
Prefix Length [64]? 64
Enter IPsec Tunnel ID [1]? 2
Packet-filter 'out-router-B' Config>
```

Ahora, para *direccionador-B-salida*, cree una norma de control de acceso inclusiva para permitir que los paquetes que haya procesado IPSec pasen a través del túnel 2 de IPSec 2.

```
Packet-filter 'out-router-B' Config> add access
Enter type [E]? I
Internet source [0::0]? 2000::B
Prefix Length [64]? 64
Internet destination [0::0]? 2000::A
Prefix Length [64]? 64
Packet-filter 'out-router-B' Config>
```

Para *direccionador-B-salida*, cree una norma de control de acceso comodín inclusiva si desea que se acepten en lugar de excluirse los paquetes que no coinciden con ninguna de las dos normas de control de acceso, como por ejemplo, tráfico no destinado al túnel 2 de IPSec.

Restablecimiento de la seguridad de IP y de IPv6 en el direccionador B

Para que la función de IPSec funcione y se activen los filtros, primero debe restablecer IPSec e IPv6. Utilice el mandato talk 5 **reset IPSec** para restablecer IPSec e IPv6. Consulte “Restablecimiento de la seguridad de IP y de IP en el direccionador de A” en la página 364 para obtener información sobre cómo restablecer IPSec. Después de restablecer IPSec, utilice el mandato talk 5 **reset IPv6** para restablecer IPv6. Alternativamente, para restablecer cada componente, puede reiniciar el direccionador.

Ejemplo: Configuración de un túnel de seguridad de IP con ESP

Tenga en cuenta que este ejemplo sólo muestra la configuración del túnel de IPSec, no de los filtros de paquete.

```
IPV6-IPsec config>add tun
Tunnel ID or Tunnel Name [ ]? 2
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [ESP]?
Local IP Address [0::0]? 2000::A
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES, NULL) [DES-CBC]?
Do you wish to change the Local Encryption Key? (Yes or [No]):
Additional Padding for Local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [Yes]:
Remote IP Address [0::0]? 2000::B
Remote Encryption SPI (1-65535) [256]?
Remote Encryption Algorithm (DES-CBC,CDMF) [DES-CBC]?
Do you wish to change the Remote Encryption Key? (Yes or [No]):
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No][No]:
Do you wish to enable this tunnel? [Yes]:
IPV6-IPsec config>
```

Ejemplo: Configuración de un túnel de seguridad de IP con ESP y ESP-NULL

Tenga en cuenta que es necesaria la autentificación.

```
IPV6-IPsec config>add tun
Tunnel ID or Tunnel Name [ ]? 2
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [ESP]?
Local IP Address [0::0]? 2000::A
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [DES-CBC]? null
Additional Padding for Local Encryption (0-120) [0]?
Local ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0::0]? 2000::B
Remote Encryption SPI (1-65535) [1234]?
Remote Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [NULL]?
Do you wish to perform verification of remote encryption padding? [No]:
Remote ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Do you wish to enable this tunnel? [Yes]:
IPV6-IPsec config>
```

Supervisión de la seguridad de IP manual (IPv4)

Esta sección explica cómo supervisar IPSec manual con IPv4. Describe cómo acceder al entorno Internet Key Exchange y los mandatos disponibles.

Acceso al entorno Internet Key Exchange

Esta sección explica cómo utilizar el Internet Key Protocol (IKE) con IPv4.

Para acceder al entorno de supervisión de IKE de seguridad de IP, entre la secuencia de mandatos siguiente en el indicador de mandatos +:

```
+ feature ipsec
IPSP>ike
IKE>
```

Mandatos de supervisión de Internet Key Exchange

Esta sección describe los mandatos de supervisión de IKE.

Tabla 45. Resumen de los mandatos de supervisión de IKE

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Delete	Suprime dinámicamente las SA de la Fase 1 de ISAKMP de un túnel específico o todas las SA de la Fase 1.
List	Lista información sobre las SA de la Fase 1 de un túnel específico o sobre todas las SA de la Fase 1.
Stats	Visualiza estadísticas para un túnel.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Delete

Utilice el mandato **delete** de IKE para suprimir dinámicamente una SA de la Fase 1 para un túnel o todas las SA de la Fase 1.

Sintaxis:

delete
- tunnel
- all

tunnel Especifica que debe suprimirse una SA de la Fase 1 para un túnel específico.

all Especifica que deben suprimirse todas las SA de la Fase 1.

Ejemplo: Supresión de un túnel

```
PKI config>delete tunnel
Peer address [10.0.0.3]?
```

List

Utilice el mandato **list** de IKE para visualizar información sobre las SA de la Fase 1 de un túnel específico o todas las SA.

Sintaxis:

list
- tunnel
- all

tunnel Especifica que debe visualizarse información para las SA de un túnel específico.

all Especifica que debe visualizarse información para todas las SA.

Ejemplo: Listado de información para todas las SA

```
IKE>list all

Phase 1 ISAKMP Tunnels for IPv4:
-------------------------------------------------------
 Peer Address    I/R  Mode  Auto    State         Auth
---------------  ---  ----  ----  ----------  ------------
       10.0.0.3   R   Aggr   N    QM_IDLE       pre-shared


IKE>list tunnel 10.0.0.3

                    Peer IKE address: 10.0.0.3
                   Local IKE address: 10.0.0.1
                               Role: Responder
                           Exchange: Aggr
                          Autostart: No
                       Oakley State: QM_IDLE
                Authentication Method: Pre-shared Key
                 Encryption algorithm: des3
                        Hash function: md5
                 Diffie-Hellman group: 1
                    Refresh threshold: 85
                      Lifetime (secs): 15000
```

Stats

Utilice el mandato **stats** de IKE para visualizar estadísticas de túnel.

Sintaxis:

stats
túnel

túnel Visualiza información estadística sobre los SA de un túnel.

Valores válidos: cualquier nombre-túnel o id-túnel configurado.

Ejemplo: Visualización de estadísticas de SA de un túnel

```
IKE>stats

Peer address [10.0.0.3]?

    Peer IP address......:        10.0.0.3
    Active time (secs)...:             187

                                       In              Out
                                       ---             ---
    Octets..............:            1229             1248
    Packets.............:              14               16
    Drop pkts...........:               0                1
    Notifys.............:               6                0
    Deletes.............:               0                0
    Phase 2 Proposals....:              16               18
    Invalid Proposals....:               0
    Rejected Proposals...:               0                0
```

Acceso al entorno de Infraestructura de clave pública (IPv4)

Esta sección explica cómo utilizar la Infraestructura de clave pública (PKI) con IPv4.

Para acceder al entorno de supervisión de PKI de seguridad de IP, entre la secuencia de mandatos siguiente en el indicador de mandatos +:

```
+ feature ipsec
IPSP>pki
PKI>
```

Mandatos de supervisión de Infraestructura de clave pública

Esta sección describe los mandatos de supervisión de Infraestructura de clave pública (PKI).

Tabla 46. Resumen de los mandatos de supervisión de PKI

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Cert-load	Carga un certificado en la SRAM de un direccionador.
Cert-req	Somete una petición de certificado a una CA.
Cert-save	Guarda un certificado en la antememoria para una posible utilización futura.
List certificate	Lista información sobre un certificado.
List configured-servers	Visualiza información sobre los servidores configurados.
Load certificate	Carga un registro que contiene el certificado de la SRAM a la antememoria de tiempo de ejecución.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Cert-load

Utilice el mandato **cert-load** de PKI para cargar un registro que contenga el certificado y la clave privada de la SRAM a la antememoria de certificado de tiempo de ejecución.

Sintaxis:

cert-load

Ejemplo: Carga de un registro de certificado de la SRAM a la antememoria

```
Enter type of certificate to be stored into SRAM:
     1)Root certificate;
     2)Box  certificate with private key;
Select the certificate type (1-2) [2]?
Name []? test
mystr=1.1.1.1
Box certificate and private key saved into cache successfully
```

Cert-req

Utilice el mandato **cert-req** de PKI para solicitar un certificado de una CA.

Sintaxis:

cert-req

Ejemplo: Solicitud de un certificado de una CA

```
Enter the following part for the subject name
   Country Name(Max 16 characters) []? us
   Organization Name(Max 32 characters) []? ibm
   Organization Unit Name(Max 32 characters) []? nhd
   Common Name(Max 32 characters) []?
Key modulus size (512|768|1024)
 [512]?
Certificate subject-alt-name type:
   1--IPv4 Address
   2--User FQDN
   3--FQDN
Select choice [1]?
Enter an IPv4 addr) []? 1.1.1.1
Generating a key pair. This may take some time. Please wait ...
PKCS10 message successfully generated
Enter tftp server IP Address []? test
Bad address, try again
Enter tftp server IP Address []? 8.8.8.8
Remote file name (max 63 chars) [/tmp/tftp_pkcs10_file]?
Certificate request TFTP to remote host successfully.
```

Cert-save

Utilice el mandato **cert-save** de PKI para guardar un registro que contenga el certificado y la clave privada en la SRAM.

Sintaxis:

cert-save

Ejemplo: Guardar un registro de certificado en la SRAM

```
Enter type of certificate to be stored into SRAM:
     1)Root certificate;
     2)Box  certificate with private key;
Select the certificate type (1-2) [2]?
SRAM Name for certificate and private key []? test
Load as default router certificate at initialization? [No]:
Private key TEST written into SRAM
Both Certificate and private key saved into SRAM successfully
```

List Certificate

Utilice el mandato **list certificate** de PKI para visualizar información sobre un certificado digital X.509.

Sintaxis:

list certificate

Ejemplo: Listado de información de certificado

```
Router   certificate
      Serial Number:   914034877
      Subject  Name:   /c=US/o=ibm/ou=nhd/cn=testip
      Issuer   Name:   /c=US/o=ibm/ou=nhd
   Subject alt Name:   1.1.1.1
         Key Usuage:   Sign & Encipherment
           Validity:   1999/1/19 23:24:27 -- 2002/1/19 23:54:27
```

List Configured-servers

Utilice el mandato **list configured-servers** de PKI para visualizar información sobre los servidores configurados.

Sintaxis:

list configured-servers

Ejemplo: Listado de información sobre servidores configurados

```
1)  Name: SERVER1
    Type: LDAP
    IP addr: 0.0.0.0
        LDAP search timeout (secs): 0
        LDAP retry interval (mins): 0
        LDAP server port number: 0
        LDAP version: 0
        LDAP version: 0
        Anonymous bind ?: y


2)  Name: TEST
    Type: TFTP
    IP addr: 9.9.9.9


3)  Name: TFTP
    Type: TFTP
    IP addr: 2.2.2.2
```

Load Certificate

Utilice el mandato **load certificate** de PKI para cargar un certificado de la SRAM a la antememoria de tiempo de ejecución.

Sintaxis:

load certificate

Ejemplo: Carga de un certificado en antememoria

```
Enter the type of the certificate:
Choices:  1-Root CA Cert, 2-Router Cert
Enter (1-2): [2]?
Encoding format:
Choices: 1-DER 2-PEM
Enter (1-2): [1]?
Server info name []? test
Remote file name on tftp server (max 63 chars) [/tmp/default_file]? /tmp/test.cert

Attempting to load certificate file. Please wait ...
Router Certificate  loaded into run-time cache
```

Acceso al entorno de supervisión de seguridad de IP (IPv4)

Para acceder al entorno de supervisión de seguridad de IP de IPv4, escriba **t 5** en el indicador de mandatos OPCON (*):

```
* t 5
```

A continuación, entre la secuencia de mandatos siguiente en el indicador de mandatos +:

```
+ feature ipsec
IPSP>ipv4
IPV4-IPsec>
```

Mandatos de supervisión de Seguridad de IP (IPv4)

Esta sección describe los mandatos de supervisión de Seguridad de IP.

Tabla 47. Resumen de mandatos de supervisión de Seguridad de IP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Change tunnel	Cambia dinámicamente los valores de un parámetro de configuración de túnel de seguridad.
Delete tunnel	Suprime dinámicamente un túnel de seguridad.
Disable	De manera dinámica inhabilita todo el proceso de Seguridad de IP de una manera segura (los paquetes que coinciden se excluyen), inhabilita todo el proceso de Seguridad de IP de una manera no segura (los paquetes que coinciden se reenvían) o inhabilita un túnel de seguridad determinado.
Enable	De manera dinámica habilita todo el proceso de Seguridad de IP o habilita un túnel de seguridad.
Itp	Ping de túnel de seguridad de IP. Determina si se puede establecer el contacto con la parte que está en el extremo más lejano de un túnel IPSec.
List	Lista información global sobre Seguridad de IP, sobre los túneles activos y definidos.
Reset	Restablece la Seguridad de IP o restablece un túnel de seguridad. Este mandato vuelve a cargar la configuración que se ha creado en Talk 6. Con este restablecimiento, los valores de los parámetros configurados utilizando Talk 5 prevalecen sobre los valores de los parámetros configurados utilizando Talk 6.
Set	Establece dinámicamente el temporizador de período de MTU de la ruta (PMTU).
Stats	Visualiza estadísticas para todos los túneles o para un túnel activo.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Change Tunnel

Cambia dinámicamente un túnel de seguridad.

Sintaxis:

change tunnel ...

Vea la descripción del mandato **add tunnel** bajo “Mandatos de configuración de seguridad de IP manual” en la página 349 para obtener una descripción de los parámetros.

Delete Tunnel

Utilice el mandato **delete** para suprimir dinámicamente un túnel de seguridad o todos los túneles de seguridad.

Sintaxis:

delete **tunnel**

id-túnel
nombre-túnel
all

id-túnel Especifica el identificador del túnel de IPSec que debe suprimirse.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre-túnel
Especifica el nombre del túnel de IPSec que debe suprimirse.

Valores válidos: cualquier nombre de túnel configurado

Valor por omisión: ninguno

all Especifica que deben suprimirse todos los túneles de IPSec de esta interfaz.

Disable

Utilice el mandato **disable** para inhabilitar dinámicamente el protocolo de Seguridad de IP en todas las interfaces o en un único túnel.

Sintaxis:

disable
ipsec drop
ipsec pass
tunnel ...

ipsec drop
Inhabilita la seguridad de IP en el direccionador de una manera segura. Se inhabilitarán todos los túneles de IPSec, pero la información de túnel de seguridad de las normas de filtro de paquete se utiliza para identificar los paquetes que coinciden con los filtros de paquete de túnel de IPSec. Los paquetes que coinciden se excluyen.

ipsec pass
Inhabilita la seguridad de IP en el direccionador de una manera no segura. Se inhabilitarán todos los túneles de IPSec. Los paquetes que coinciden con los filtros de paquete de túnel de IPSec se reenvían como tráfico normal.

tunnel *id-túnel* **all**
Inhabilita la seguridad de IP en un túnel especificado o en todos los túneles.

id-túnel
Especifica el identificador del túnel de seguridad que debe inhabilitarse.

Valores válidos: 1 - 65535

Valor por omisión: 1

all Todos los túneles.

Enable

Utilice el mandato **enable** para habilitar dinámicamente el protocolo de Seguridad de IP en todas las interfaces o en un único túnel. Debe habilitar IPSec globalmente en el direccionador para que se activen los túneles de IPSec habilitados individualmente.

Nota: IPSec no se puede habilitar dinámicamente si se ha reiniciado el redireccionador con IPSec inhabilitado.

Sintaxis:

e**nable**
ipsec
tunnel ...

ipsec
Habilita la seguridad de IP en el direccionador.

tunnel *id-túnel* **| all**

id-túnel
Especifica el identificador del túnel de seguridad que debe habilitarse.

Valores válidos: 1 - 65535

Valor por omisión: 1

all Todos los túneles.

Itp

Utilice el mandato **itp** (ping de túnel IPSec) para crear y enviar un paquete IP especial por un túnel IPSec, que verifica si el direccionador del extremo más lejano del túnel puede responder mediante la devolución del paquete. El paquete se envía repetidamente con la frecuencia especificada por el argumento de cadencia hasta que se termina el mandato pulsando **Intro**. Al pulsar **Intro**, itp imprime su estado para todos los paquetes que ha enviado.

Nota: El mandato **itp** sólo funciona para túneles que están operando en modalidad de túnel. Asimismo, el otro direccionador debe tener la posibilidad de reenvío IP y debe estar habilitado.

Sintaxis:

itp tunnel-id
size
rate

tunnel-id
Necesario. Valor entero de 2 bytes asignado a un túnel específico.

size Opcional. Tamaño de la carga útil de datos del paquete de ping. Este valor debe ser mayor que el tamaño mínimo creado por itp y menor que el valor MTU del túnel.

rate Opcional. Frecuencia (en segundos) con la que se transmite el paquete de datos de ping.

Valor por omisión: 1

List

Utilice el mandato **list** para visualizar la configuración de Seguridad de IP actual. Los túneles globales incluyen todos los túneles del direccionador, tanto los activos como los definidos. En todos los túneles se incluyen todos los túneles configurados en esta interfaz, tanto los activos como los definidos. Los túneles activos son los que están actualmente activos; los túneles definidos están definidos pero no están activos.

Sintaxis:

list ...
all
global
tunnel
active *id-túnel nombre-túnel* all
defined *id-túnel nombre-túnel* all

Ejemplo: Listado de todos los túneles definidos

```
IPV4-IPsec>LIST TUNNEL DEFINED
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]?

Defined Tunnels for IPv4:
------------------------------------------------------------------------------
   ID     Type    Local IP Addr   Remote IP Addr   Mode    State
 ------  ------  ---------------  ---------------  -----  --------
      3  ISAKMP       211.0.1.17        211.0.5.2  TUNN   Enabled
      4  ISAKMP       211.0.1.17        211.0.5.3  TUNN   Enabled
      5  ISAKMP       211.0.1.17        211.0.5.4  TUNN   Enabled


Defined Manual Tunnels for IPv6:
------------------------------------------------------------------------------
   IPV4-IPsec>
```

Ejemplo: Listado de un túnel definido

```
IPV4-IPsec>LIST TUNNEL DEFINED
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 1

Tunnel    Type     Mode   Policy    Life    Replay     State
  ID                                                              Prev
------    ------  -----   ------   -----   -------     ---------     -----------
     1    ISAKMP   TUNN      ESP       0        No     Enabled


Tunnel Name: ---------------

Local (Outbound) Information:
      IP Address: 211.0.1.17
  Authentication:  SPI: ----------          Algorithm: --------
      Encryption:  SPI: 2305164930    Encryption Algorithm: DES-CBC
                                                Extra Pad:   0
                               ESP Authentication Algorithm: HMAC-MD5

Remote (Inbound) Information:
      IP Address: 211.0.5.3
  Authentication:  SPI: ----------          Algorithm: --------
      Encryption:  SPI: 2661613010    Encryption Algorithm: DES-CBC
                                             Verify Pad?:  No
                               ESP Authentication Algorithm: HMAC-MD5
IPV4-IPsec>
```

Ejemplo: Listado de todos los túneles activos

```
IPV4-IPsec>LIST TUNNEL ACTIVE
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]?

Tunnel Cache for IPv4:
-------------------------------------------------------------------------------
 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
----   -------------   --------------   ----   --------    ------------------
  1       211.0.1.17      211.0.5.214   TUNN        ESP                 none
  2       211.0.1.17      211.0.5.215   TUNN        ESP                 none
  3       211.0.1.17       211.0.5.41   TUNN        ESP                 none


Tunnel Cache for IPv6:
-------------------------------------------------------------------------------
   IPV4-IPsec>
```

Ejemplo: Listado de un túnel activo

```
IPV4-IPsec>LIST TUNNEL ACTIVE 1
                                Tunnel ID: 1
                           Tunnel Name: ---------------
                                       Type: ISAKMP
                                       Mode: TUNN
                                     Policy: ESP
                           Replay Prevention: No
                             Tunnel LifeTime: 0 secs
                           Tunnel Expiration: None
                                       PMTU: n/a
                                Tunnel State: Enabled
                             DF bit handling: COPY
                                   SA State: Working
                                SA LifeTime: 360 secs
                                SA LifeSize: 50000 KBytes
                               SA Threshold: 85 percent
Local (Outbound) Information:
        IP Address: 211.0.1.17
    Authentication:  SPI: ----------              Algorithm: --------
        Encryption:  SPI: 2861614221   Encryption Algorithm: DES-CBC
                                Extra Pad:   0
                                ESP Authentication Algorithm: HMAC-MD5

Remote (Inbound) Information:
        IP Address: 211.0.5.41
    Authentication:  SPI: ----------              Algorithm: --------
        Encryption:  SPI: 2266666369   Encryption Algorithm: DES-CBC
                                                 Verify Pad?:  No
                                ESP Authentication Algorithm: HMAC-MD5
IPV4-IPsec>
```

2 Es una dirección IPv6. Si la versión de IP es IPv4, se visualiza un mensaje que define el manejo del bit de DF: COPY, SET o CLEAR.

Reset

Utilice el mandato **reset** para restablecer dinámicamente la seguridad de IP en el direccionador o en un único túnel. Después de restablecer IPSec o los túneles, asegúrese de utilizar el mandato **reset IP** para restablecer la configuración de IP. Esto es necesario para volver a cargar la información de control de acceso, como por ejemplo filtros de paquete y sus normas de control de acceso. Si no restablece IP, puede ser que los filtros de paquete y las normas de control de acceso no soporten la nueva configuración de IPSec.

Rearrancar el direccionador es una alternativa a utilizar los mandatos **reset**. Sin embargo, el rearranque del direccionador lo retira de la red por un tiempo, mientras que los mandatos **reset** sólo interrumpen funciones de IP.

Sintaxis:

reset
    ipsec
    tunnel *id-túnel nombre-túnel* all

ipsec
    Restablece la seguridad de IP en el 2210. La seguridad de IP se inhabilita temporalmente y, a continuación, se reinicia. Mientras la seguridad de IP está inhabilitada, los paquetes que se manejan normalmente mediante túneles de IPSec se excluyen hasta que la restauración finaliza. El restablecimiento de la seguridad de IP no afecta a las otras funciones del 2210. Este mandato activa la configuración de seguridad de IP que se ha creado utilizando Talk 6.

La configuración de seguridad de IP de Talk 6 prevalece sobre la configuración de Talk 5.

tunnel
Restablece la seguridad de IP en un túnel especificado. Si el túnel está inhabilitado durante el restablecimiento, la configuración de túnel se vuelve a crear desde la configuración de la SRAM, pero el túnel permanece inhabilitado después del restablecimiento.

id-túnel
Especifica el identificador del túnel de seguridad que debe restablecerse.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre-túnel
Especifica el nombre del túnel de seguridad que debe restablecerse.

Valores válidos: cualquier nombre de túnel configurado

Valor por omisión: ninguno

all Todos los túneles.

Set

Establece dinámicamente el temporizador de período de MTU de la ruta (PMTU).

Sintaxis:

s**et** path

path
Este parámetro define el tiempo en minutos que transcurrirá hasta que el 2210 establezca la MTU del túnel en el máximo.

Valor por omisión: 10 (0 significa inhabilitado)

Stats

Utilice el mandato **stats** para visualizar estadísticas sobre un túnel específico o todos los túneles. Por ejemplo, el mandato **stats** muestra los paquetes enviados y recibidos.

Sintaxis:

s**tats**
id-túnel
nombre-túnel
all

id-túnel
Especifica el identificador del túnel de seguridad.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre-túnel
Especifica el nombre de un túnel de seguridad que se ha configurado.

Valores válidos: cualquier nombre de túnel configurado

Valor por omisión: ninguno

all Visualiza estadísticas sobre todos los túneles configurados en el 2210.

Ejemplo:

```
IPV6-IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? all

                          Global IPSec Statistics
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
           0            0             0             0            0            0

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
           0            0             0             0            0            0

Receive Packet Errors:
  total errs    AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   ----------   -----------
           0            0            0            0             0

Send Packet Errors:
  total errs    AH errors   ESP errors
  ----------   ----------   ----------
           0            0            0
```

Supervisión de Seguridad de IP manual (IPv6)

Esta sección explica cómo supervisar IPSec manual con IPv6. Describe cómo acceder al entorno de seguridad de IP y los mandatos disponibles.

Acceso al entorno de supervisión de Seguridad de IP

Para acceder al entorno de supervisión de Seguridad de IP, escriba **t 5** en el indicador de mandatos OPCON (*):

```
* t 5
```

A continuación, entre la secuencia de mandatos siguiente en el indicador de mandatos +:

```
+ feature ipsec
IPSP>ipv6
IPV6-IPsec>
```

Mandatos de supervisión de Seguridad de IP (IPv6)

Los mandatos de supervisión de Seguridad de IP para IPv6 son los mismos que se utilizan para IPv4, a menos que se indique lo contrario. Consulte “Mandatos de supervisión de Seguridad de IP (IPv4)” en la página 372 para obtener una descripción de los mandatos. Entre los mandatos en el indicador de mandatos `IPV6-IPsec>`.

Soporte de reconfiguración dinámica de seguridad de IP

Esta sección describe la reconfiguración dinámica (DR) en lo que afecta a los mandatos de Talk 6 y Talk 5.

Delete interface de CONFIG (Talk 6)

La Seguridad de IP (IPSec) no soporta el mandato de CONFIG (Talk 6) **delete interface**.

Activate interface de GWCON (Talk 5)

El mandato de GWCON (Talk 5) **activate interface** no es aplicable para IPSec. IPSec es independiente de una interfaz determinada.

Reset interface de GWCON (Talk 5)

El mandato de GWCON (Talk 5) **reset interface** no es aplicable para IPSec. IPSec es independiente de una interfaz determinada.

Mandatos reset de componente GWCON (Talk 5)

IPSec soporta los mandatos de GWCON (Talk 5) **reset** siguientes específicos de IPSec:

Mandato GWCON, feature IPSec, ipv4, reset IPSec

Descripción: Se volverá a inicializar IPSec.

Efecto en la red: Cuando se restablezca IPSec, todos los túneles desaparecerán. Se volverán a crear túneles manuales desde la SRAM. Los túneles negociados desaparecerán. Esto hará que el tráfico que utiliza estos túneles se detenga momentáneamente.

Limitaciones: Ninguna.

La tabla siguiente resume los cambios de configuración de la Característica de Seguridad de IP que se activan cuando se invoca el mandato **GWCON, feature IPSec, ipv4, reset IPSec**:

Mandatos cuyos cambios activa el mandato GWCON, feature ipsec, ipv4, reset ipsec
CONFIG, feature ipsec, ipv4, enable tunnel
CONFIG, feature ipsec, ipv4, disable tunnel
CONFIG, feature ipsec, ipv4, disable ipsec
CONFIG, feature ipsec, ipv4, add tunnel
CONFIG, feature ipsec, ipv4, delete tunnel
CONFIG, feature ipsec, ipv4, change tunnel

Mandato GWCON, feature IPSec, ipv4, reset tunnel

Descripción: Se volverá a inicializar el túnel o todos los túneles.

Efecto en la red: Se puede restablecer un túnel o todos los túneles. Se volverán a crear túneles manuales desde la SRAM. Los túneles negociados desaparecerán. Esto hará que el tráfico que utiliza estos túneles se detenga momentáneamente.

Limitaciones: Ninguna.

La tabla siguiente resume los cambios de configuración de la Característica de Seguridad de IP que se activan al invocar el mandato **GWCON, feature IPSec, ipv4, reset tunnel**:

Mandatos cuyos cambios activa el mandato GWCON, feature ipsec, ipv4, reset tunnel
CONFIG, feature ipsec, ipv4, add tunnel
CONFIG, feature ipsec, ipv4, delete tunnel
CONFIG, feature ipsec, ipv4, change tunnel
CONFIG, feature ipsec, ipv4, disable tunnel

Mandatos de cambio temporal de GWCON (Talk 5)

IPSec soporta los mandatos de GWCON siguientes que cambian temporalmente el estado operativo del dispositivo. Estos cambios se pierden siempre que se vuelve a cargar o se reinicia el dispositivo o se ejecuta cualquier mandato reconfigurable dinámicamente.

Mandatos
GWCON, feature ipsec, ipv4, change tunnel **Nota:** Se pueden cambiar los parámetros de un túnel en la memoria.
GWCON, feature ipsec, ipv4, disable tunnel **Nota:** Se puede inhabilitar un túnel o todos los túneles. Se detendrá el tráfico para estos túneles.
GWCON, feature ipsec, ipv4, disable IPSec pass **Nota:** Se inhabilita IPSec y se reenvía el tráfico sin seguridad.
GWCON, feature ipsec, ipv4, disable IPSec stop **Nota:** Se inhabilita IPSec y se elimina el tráfico.
GWCON, feature ipsec, ipv4, delete tunnel **Nota:** Suprime uno o todos los túneles. Se excluirá el tráfico para estos túneles.
GWCON, feature ipsec, ipv4, enable tunnel **Nota:** Habilita uno o todos los túneles. Se permitirá el tráfico para estos túneles.
GWCON, feature ipsec, ipv4, enable IPSec **Nota:** Habilita IPSec. IPSec puede procesar el tráfico.
GWCON, feature ipsec, ipv4, set path-MTU-age-timer **Nota:** Cambia el temporizador de antigüedad de MTU de ruta.

Mandatos no reconfigurables dinámicamente

La tabla siguiente describe los mandatos de configuración de la Característica de Seguridad de IP que no se pueden cambiar dinámicamente. Para activar estos mandatos, es necesario volver a cargar o reiniciar el dispositivo.

Mandatos
CONFIG, enable ipsec **Nota:** Cuando se habilita por primera vez IPSec después de que se haya inicializado el dispositivo, es necesario volver a cargar o reiniciar el dispositivo.

Utilización de la característica Servicios diferenciados

Este capítulo describe cómo utilizar la característica Servicios diferenciados (DiffServ) para que un direccionador pueda proporcionar un servicio preferente a los paquetes de datos de IP adecuados. Basándose en la información de la cabecera de IP, el direccionador clasifica los paquetes comparándolos con configuraciones predefinidas en la base de datos de políticas (creadas con la característica de política). Consulte el apartado “Utilización de la característica de política” en la página 243 para obtener información detallada. Como resultado de ello, algunos paquetes pueden recibir un servicio preferente. Este capítulo consta de las secciones siguientes:

- “Visión general de Servicios diferenciados”
- “Terminología de Servicios diferenciados” en la página 389
- “Configuración de Servicios diferenciados” en la página 390

Visión general de Servicios diferenciados

La mayoría de dispositivos de reenvío instalados en una red IP actual proporcionan servicio de mayor eficacia estándar a los paquetes, siguiendo la regla de primero en llegar, primero en recibir servicio. Este método de entrega es adecuado para la mayoría de tráfico, pero están saliendo aplicaciones nuevas que necesitan una transmisión más rápida y más temprana de algunos paquetes.

La característica Servicios diferenciados (DiffServ) proporciona diferentes niveles de servicio a los paquetes IP cuando un direccionador los procesa para transmitirlos. DiffServ proporciona servicio preferente a algunos paquetes reservando recursos del sistema (almacenamientos intermedios) y recursos de enlace (ancho de banda) para ellos. Una función de clasificador de DiffServ determina el tipo de servicio proporcionado a los paquetes IP examinando diversos campos de la cabecera IP, por ejemplo, los rangos de los números de puerto y las direcciones de origen y de destino de IP, el tipo de protocolo y el byte DS (TOS) de entrada. Para llevar a cabo esta función de un modo escalable, se añaden flujos individuales a corrientes. Las corrientes son entidades a través de las cuales DiffServ gestiona el acceso a los almacenamientos intermedios y al ancho de banda. La Figura 28 muestra cómo DiffServ procesa los paquetes de una corriente.

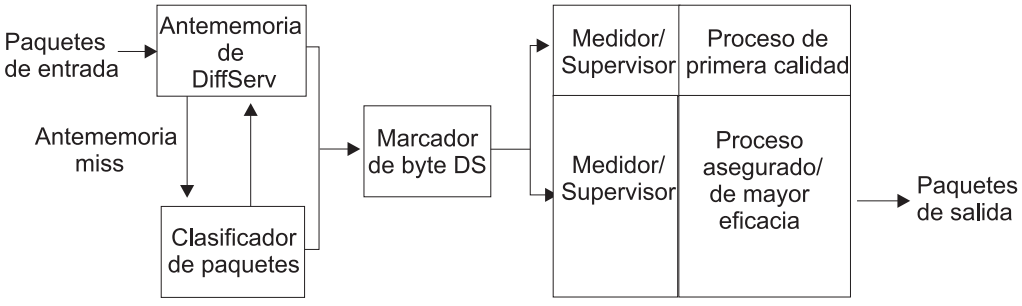


Figura 28. Ruta de paquetes de datos de DiffServ

Además del servicio de mayor eficacia tradicional, DiffServ proporciona los tipos de servicio siguientes:

Reenvío acelerado (EF) El servicio de reenvío acelerado representa la implantación de DiffServ del servicio de primera calidad y ambos términos se utilizan indistintamente en el texto siguiente. Este servicio garantiza una velocidad de transmisión específica y un retardo menor que el servicio de reenvío asegurado o de mayor eficacia. Si se produce un exceso de tráfico, DiffServ excluye el exceso de tráfico. La cola de primera calidad proporciona servicio de EF y se aparece en la Figura 29 en la página 385 como cola de EF.

Reenvío asegurado (AF) El servicio de reenvío asegurado representa la implementación de DiffServ del servicio asegurado y ambos términos (reenvío asegurado y servicio asegurado) se utilizan indistintamente en el texto siguiente. El servicio AF garantiza una velocidad de transmisión específica pero no garantiza el retardo. Si existen recursos desocupados, DiffServ puede envía el exceso de tráfico a una velocidad más alta.

El tráfico AF se mide y se supervisa opcionalmente por medio de la configuración de la política. Los tipos de supervisión soportados son el Marcador de tres colores (TCM) de una velocidad y de dos velocidades. El TCM permite que los paquetes se clasifiquen o se vuelvan a marcar basándose en las características del tráfico de entrada. Se proporcionan tres clasificaciones: Verde, Amarilla y Roja. La política proporciona la especificación de los umbrales para la clasificación de color. La cola de AF/BE proporciona servicio de AF y se muestra en la Figura 29 en la página 385.

Mayor eficacia (BE) Es el servicio de mayor eficacia estándar, que no proporciona garantías ni de servicio ni de retardo. Debe buscar un equilibrio entre reservar recursos para los servicios EF y AF y dejar suficientes recursos libres para que el tráfico de mayor eficacia reciba el servicio adecuado. La cola de AF/BE proporciona servicio de BE y se muestra en la Figura 29 en la página 385.

Los direccionadores locales crean y envían paquetes de control, por lo que también debe dejar suficientes recursos libres proporcionarles el servicio adecuado.

La medición, el marcado y la supervisión de DiffServ en un direccionador del borde permite al direccionador del centro, en redes habilitadas para DiffServ, clasificar los paquetes basándose en el elemento de código DS (TOS) y controlar la congestión excluyendo el tráfico que no se ajusta o disminuyendo su nivel de servicio. Por ejemplo, el direccionador del centro puede excluir todos los paquetes rojos, reenviar los paquetes amarillos como mayor eficacia y reenviar los paquetes verdes con una baja probabilidad de exclusión. Esto ayuda a obtener un mayor rendimiento y un retardo menor para el tráfico preferido en las redes habilitadas para DiffServ.

DiffServ se implementa actualmente en enlaces PPP, Multilink PPP y Frame Relay y puede ser utilizado por el subsistema RSVP. La Figura 28 en la página 383 muestra cómo se procesan los paquetes de una corriente. Cuando un direccionador recibe el primer paquete de un flujo (suponiendo que esté designado para el servicio de primera calidad), no existe ninguna indicación de su categoría de servicio en la antememoria de DiffServ, de modo que el paquete se procesa por la ruta lenta. DiffServ solicita una búsqueda en la base de datos de políticas para obtener el criterio de manejo de paquete (política). La acción definida por la política

se guarda en la antememoria de DiffServ. Cuando el direccionador recibe un paquete subsiguiente de este flujo, detecta que ya existe una entrada en la antememoria de DiffServ para el flujo, de modo que se aplica su acción definida por la política y el paquete toma la ruta rápida. De este modo, los paquetes siguientes de este flujo reciben servicio de primera calidad.

La Figura 29 muestra la relación entre el agente, la gestión de almacenamientos intermedios, las colas y el planificador—algunos de los componentes básicos que proporcionan calidades diferentes de los niveles de servicio.

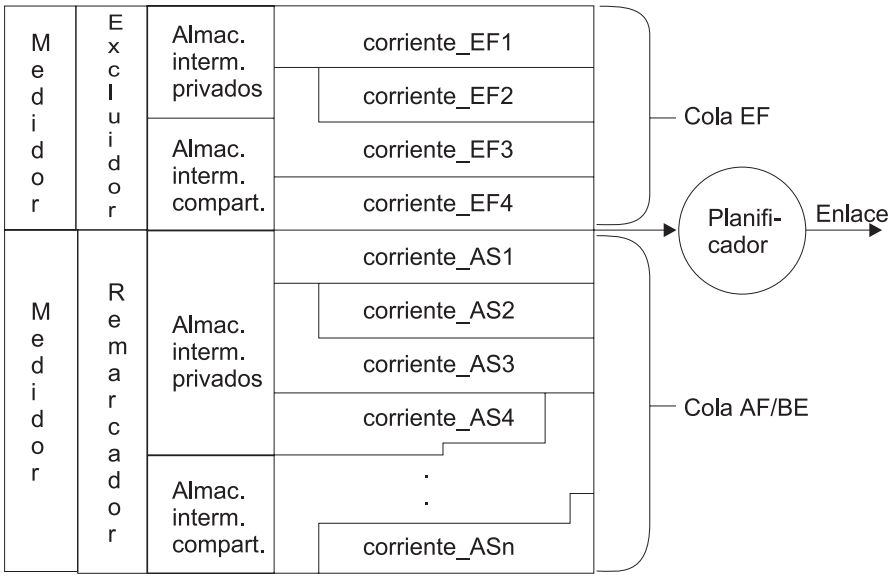


Figura 29. Relación entre el supervisor, los almacenamientos intermedios, las colas y el planificador

Los servicios de reenvío acelerado (EF) y reenvío asegurado (AF) tienen características diferentes, soportadas por tres funciones en el direccionador: (1) El medidor y supervisor, (2) la gestión de almacenamientos intermedios y colas y (3) el planificador. Estas funciones proporcionan un control del tráfico más sofisticado que el que está disponible en un dispositivo de direccionador de BE tradicional.

Después de utilizar la característica de política para configurar políticas apropiadas, el primer paso en la implementación de DiffServ es utilizar el mandato de DiffServ **enable ds** para habilitar la característica DiffServ y el mandato **set interface** para habilitar la interfaz de salida.

Es posible configurar opciones de DiffServ de forma que los recursos de red se comprometan en exceso o se agoten, es decir, los controles de acondicionador de tráfico se configuran como si existiera más ancho de banda o almacenamientos intermedios de los que están realmente disponibles. DiffServ no soporta compromisos en exceso.

Si una corriente de DiffServ queda desocupada (no se ha enviado ningún paquete a la corriente durante algún tiempo), el sistemas reclama los recursos para que otras corrientes puedan utilizarlos. Si la corriente se reactiva, se le devuelven los recursos. Si los recursos ya no están disponibles debido a excesivos compromisos, DiffServ intenta periódicamente volver a asignar los recursos.

Interpretación del elemento de código de DiffServ

DiffServ proporciona una cabecera de sustitución para el octeto IPv4 TOS definido en RFC791, que contiene un byte denominado el campo Diffserv (DS) (mostrado en la Figura 30. Los seis bits de orden superior del campo DS se utilizan como un elemento de código de DiffServ (DSCP) para determinar el comportamiento por salto (PHB). Los dos bits restantes se reservan para uso futuro. El ejemplo siguiente muestra el formato del campo DS:

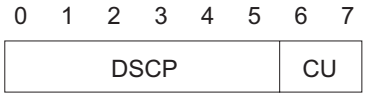


Figura 30. Formato de elemento de código de DiffServ para la cabecera del octeto IPv4 TOS

donde:

DSCP = elemento de código de servicios diferenciados
CU = utilizado actualmente

El elemento de código recomendado para el EF PHB es 101110xx.

La Figura 31 muestra el formato del campo DS para el AF PHB:

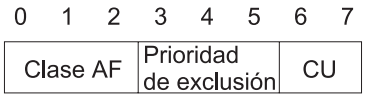


Figura 31. Formato de elemento de código de DiffServ para la cabecera AF PHB

donde:

Tres bits para el tipo de clase AF
- 001 - clase AF11
- 010 - clase AF21
- 011 - clase AF31
- 100 - clase AF41

Tres bits para prioridad de exclusión
- 010 - Prioridad de exclusión baja, significa color Verde en TCM
- 100 - Prioridad de exclusión media, significa color Amarillo en TCM
- 110 - Prioridad de exclusión alta, significa color Rojo en TCM

CU = utilizado actualmente

La lista siguiente muestra los valores de elementos de código AF recomendados con las clases AF y los valores de prioridad de exclusión:

Clase 1	Clase 2	Clase 3	Clase 4
AF11 = 001010xx	AF21 = 010010xx	AF31 = 011010xx	AF41 = 100010xx
AF12 = 001100xx	AF22 = 010100xx	AF32 = 011100xx	AF42 = 100100xx
AF13 = 001110xx	AF23 = 010110xx	AF33 = 011110xx	AF43 = 100110xx

Interpretación de los medidores y del supervisor

La medición y la supervisión se proporcionan para el tráfico EF y AF como se especifica en la política. El algoritmo EF mide el tráfico y excluye paquetes que están por encima del umbral especificado. El algoritmo AF mide el tráfico y posiblemente vuelve a marcar paquetes, pero no los excluye.

Reenvío acelerado (EF)

El tráfico EF tiene un valor por omisión, el supervisor basado en cubeta de señales, que elimina paquetes si éstos exceden la velocidad especificada durante la configuración de parámetros de ancho de banda de política. Puede especificar los parámetros Token Rate (Velocidad de señal) (TR) y Token Bucket Size (Tamaño de cubeta de señales) (TBS) para cambiar el funcionamiento por omisión del supervisor. El medidor determina si la cubeta contiene un número suficiente de señales para enviar un paquete. Si hay señales disponibles, se envía el paquete. De lo contrario, el supervisor excluye el paquete. La cubeta se vuelve a llenar de señales a la velocidad especificada en el parámetro Token Rate. La velocidad de señal se mide en bytes por segundo, es decir, incluye la cabecera IP, pero no las cabeceras específicas de enlace. La velocidad de señal se mide antes de la compresión de cabecera IP y del cifrado y compresión de datos de la Capa 2. Token Bucket Size se utiliza para manejar ráfagas temporales que están por encima del límite de velocidad sin penalización.

Reenvío asegurado (AF)

El tráfico AF tiene tres opciones de política: (1) Marcador de tres colores de una sola velocidad (srTCM), (2) Marcador de tres colores de dos velocidades (trTCM) y (3) ninguno (ninguna política). Estas opciones de política están disponibles para las clases AF1, AF2, AF3 y AF4 y se especifican durante la configuración de política.

El srTCM mide una corriente de tráfico basándose en un algoritmo de cubeta de señales con dos cubetas y una sola velocidad de relleno. Marca los paquetes como verde, amarillo o rojo de acuerdo con tres parámetros de tráfico: (1) Committed Information Rate (Velocidad de información comprometida (CIR), (2) Committed Burst Size (Tamaño de ráfaga comprometido) (CBS) y (3) Excess Burst Size (Tamaño de ráfaga excesivo) (EBS). Un paquete se marca de color verde si no excede el CBS, de color amarillo si excede el CBS pero no el EBS y de color rojo en el caso contrario. La CIR se mide en bytes de paquetes IP por segundo, es decir, incluye la cabecera IP, pero no las cabeceras específicas de enlace. La CIR se mide antes de la compresión de cabecera IP y del cifrado y compresión de los datos de la Capa 2. El CBS y el EBS se miden en bytes.

El medidor opera en modalidad sin distinción de color o en modalidad con distinción de color. En modalidad sin distinción de color, se supone que un paquete de entrada está marcado como verde, independientemente del valor de los bits de prioridad de exclusión de su elemento de código DS. El CBS representa el tamaño de la cubeta verde y EBS representa el tamaño de la cubeta amarilla. En primer lugar, se buscan señales disponibles en la cubeta verde. Si hay suficientes señales verdes, el paquete se marca como verde y se envía. Si no hay suficientes señales verdes, se busca en la cubeta amarilla. Si hay suficientes señales amarillas, el paquete se marca como amarillo y se envía. Si no hay suficientes señales amarillas, el paquete se marca como rojo. En modalidad con distinción de color, en primer lugar se comprueba el color del paquete de entrada y se comprueba la cubeta de señales correspondiente. Si hay señales disponibles, se envía como se ha recibido. De lo contrario, se reduce apropiadamente su valor de prioridad de

exclusión. La modalidad con distinción de color es útil si los paquetes de entrada ya están clasificados y marcados previamente con color.

El trTCM es también un algoritmo de cubeta de señales, similar a srTCM, excepto en que proporcionar velocidades de relleno independientes para las cubetas verde y amarilla. Los parámetros de configuración son: (1) Committed Information Rate (CIR), (2) Committed Burst Size (CBS), (3) Peak Information Rate (Velocidad de información máxima) (PIR) y (4) Peak Burst Size (Tamaño de ráfaga máximo) (PBS). El CBS representa el tamaño de la cubeta verde y el PBS representa el tamaño de la cubeta amarilla. El algoritmo es el mismo que para srTCM, excepto en que el valor de CIR determina la velocidad de relleno de la cubeta verde y el valor de PIR determina la velocidad de relleno de la cubeta amarilla. El trTCM es útil si es necesario imponer una velocidad máxima independientemente de una velocidad de información comprometida. Los paquetes que exceden la PIR se marcarán de color rojo (probabilidad más alta de exclusión).

Interpretación de la gestión de almacenamientos intermedios y colas

Si el tráfico es para EF o es tráfico AF o BE que el supervidor ha permitido, la función de *gestión de almacenamientos intermedios* basada en la velocidad lo procesa. Esta función asigna almacenamientos intermedios de una agrupación privada o de una agrupación compartida común para la interfaz de salida habilitada para DiffServ. Los almacenamientos intermedios para el tráfico EF sólo se asignan desde la agrupación privada.

Utilice el mandato de configuración de Talk 6 **set receive-buffers** (consulte la publicación *Guía del usuario de software* para obtener una descripción y conocer la sintaxis) para especificar la cantidad total de espacio de almacenamiento intermedio físico disponible para una interfaz. Utilice el mandato Talk 6 **set interface** de DiffServ para establecer el tamaño de almacenamiento intermedio de salida para las colas de primera calidad y asegurada. Éste es el espacio de almacenamiento intermedio que DiffServ gestiona.

DiffServ gestiona dos agrupaciones independientes— una para la cola de primera calidad (EF) y otra para la cola de reenvío asegurado (AF). Asegúrese de que el espacio de almacenamiento intermedio que especifica refleja la cantidad real de espacio de almacenamiento intermedio disponible en el sistema.

La gestión de almacenamientos intermedios determina si los almacenamientos intermedios de su agrupación privada de la interfaz están disponibles para el paquete. Si están disponibles, esta función acepta el paquete y lo pone en cola. Si no están disponibles, esta función intenta asignar espacio de almacenamientos intermedios de la agrupación compartida y, si puede, pone el paquete en cola. Si no hay espacio de almacenamientos intermedios compartido disponible, la gestión de almacenamientos intermedios excluye el paquete.

Interpretación del planificador

La función *planificador* examina las colas con regularidad, saca de la cola los paquetes que están en cola y los envía al adaptador de interfaz para su transmisión. Es un planificador de puesta en cola según reloj propio, que es una variación de puesta en cola según peso. Puede configurar los pesos del planificador y especificar la frecuencia con la que el planificador examina las colas.

Terminología de Servicios diferenciados

Se utilizan los términos siguientes para explicar DiffServ:

Committed Information Rate (Velocidad de información comprometida) (CIR)
Este parámetro especifica la velocidad máxima a la que se permite operar a una corriente de tráfico AF de un usuario antes de que se considere que está enviando de forma excesiva. Se mide en bytes de paquetes IP por segundo (incluyendo la cabecera IP pero no las cabeceras específicas de enlace). La utilizan las funciones TCM de una sola velocidad y de dos velocidades para las corrientes AF.

Committed Burst Size (Tamaño de ráfaga comprometido) (CBS)
Este parámetro especifica (en bytes de paquetes IP) el número máximo de bytes que se pueden enviar en una ráfaga, a una velocidad que excede la CIR. El CBS limita el tamaño de la cubeta de señales comprometida en las funciones TCM de una sola velocidad y TCM de dos velocidades.

Antememoria de DiffServ
Esta antememoria contiene el perfil del tráfico y servicio de los flujos de IP activos más recientes a los que proporciona servicio el direccionador.

Excess Burst Size (Tamaño de ráfaga excesivo) (EBS)
Este parámetro especifica (en bytes de paquetes IP) el número máximo de bytes que exceden el CBS que se pueden enviar en una ráfaga, a una velocidad que excede la CIR. Este parámetro lo utilizan las funciones TCM de una sola velocidad y limita el tamaño de la cubeta de señales excesivas.

Flujo
Secuencia de paquetes con la misma dirección y puerto de origen, protocolo de IP, y dirección y puerto de destino.

Token Rate (Velocidad de señal)
Este parámetro especifica la velocidad máxima a la que se permite operar a una corriente de tráfico EF de un usuario antes de que se considere que está enviando de forma excesiva. Se mide en bytes de paquetes IP por segundo (incluyendo la cabecera IP pero no las cabeceras específicas de enlace).

Token Bucket Size (Tamaño de cubeta de señales)
Este parámetro mide el número máximo de bytes de paquetes IP de una corriente de tráfico EF que se pueden enviar en una ráfaga a una velocidad que excede la velocidad de señal.

Peak Bucket Size (Tamaño de cubeta máximo) (PBS)
Este parámetro sólo lo utilizan las funciones TCM de dos velocidades. Especifica (en bytes de paquetes IP) el número máximo de bytes que se pueden enviar en una ráfaga a una velocidad que excede la PIR. Este parámetro limita el tamaño máximo de la cubeta de señales máxima.

Peak Information Rate (Velocidad de información máxima) (PIR)
Este parámetro sólo lo utilizan las funciones TCM de dos velocidades. Representa la velocidad máxima (en bytes de paquetes IP por segundo, incluyendo la cabecera IP pero no las cabeceras específicas de enlace) a la que el usuario puede enviar paquetes de corrientes AF, más allá de la cual la prioridad de exclusión del paquete se establece en el valor más alto.

Corriente
Un conjunto de flujos.

Interfaz virtual (VIF)
Para enlaces Frame Relay, cada conexión DLCI se considera una interfaz virtual.

Configuración de Servicios diferenciados

Los procedimientos siguientes proporcionan una descripción de alto nivel sobre cómo configurar DiffServ para proporcionar servicio preferente a paquetes seleccionados. En primer lugar, acceda a la característica DiffServ:

1. En el indicador de mandatos *, entre **talk 6**.
2. En el indicador de mandatos Config>, entre **feature ds**. Se visualizará el indicador de mandatos DS config> y se abrirá el diálogo de configuración.

```
* talk 6
Config>feature ds
DS config>
```

3. Habilite la característica DiffServ en un direccionador:

```
DS config>enable ds
DiffServ enabled
```

4. Habilite y establezca los parámetros de interfaz:

```
DS config>set interface
Enter Diffserv Interface number [0]? 2
Set Premium Queue Bandwidth (%) (1 - 99) [20]?
    Assured Queue Bandwidth (%) = 80
Configure Advanced setting (y/n)? [No]: no
Accept input (y/n)? [Yes]:
```

Nota: Si especifica no en el indicador Configure Advanced setting, se utilizarán los parámetros por omisión para Cola de primera calidad y Cola asegurada/BE.

```
Configure Advanced setting (y/n)? [No]: yes
Set Premium Queue Weight (%) (20 - 99) [90]?
    Assured Queue Weight (%) = 10
EGRESS BufSize for Premium Queue (in bytes) (550 - 27500) [5500]?
Max EGRESS QoS Allocation for Premium Queue (%) (1 - 99) [95]?
EGRESS BufSize for Assured/BE Queue (in bytes) (5500 - 140800) [27500]?
Max EGRESS QoS Allocation for Assured/BE Queue (%) (1 - 99) [80]?
```

En este ejemplo, el 20 por ciento del ancho de banda de línea y el 90 por ciento del peso del planificador se proporcionan a la cola de EF. El tamaño de almacenamiento intermedio de salida para la cola EF es de 5500 bytes (que corresponde a 10 paquetes con un promedio de tamaño de paquete de 550 bytes), del cual se puede asignar el 95 por ciento a las corrientes QoS. El tamaño de almacenamiento intermedio de salida para la cola AF/BE es de 27.500 bytes (que corresponde a 50 paquetes con un promedio de tamaño de paquete de 550 bytes), del cual se puede asignar el 80 por ciento a las corrientes QoS.

5. Cuando termine de habilitar DiffServ en los direccionadores y de establecer los parámetros de interfaz, entre **Control-P** para volver al indicador de mandatos *.

Después de habilitar DiffServ y de establecer los parámetros de interfaz, debe volver a iniciar o volver a cargar el dispositivo para activar DiffServ. Para obtener más detalles sobre cómo especificar mandatos de DiffServ, consulte “Configuración y supervisión de la característica Servicios diferenciados” en la página 393.

Configuración y supervisión de la característica Servicios diferenciados

Este capítulo describe los mandatos que proporciona la característica Servicios diferenciados (DiffServ) para configurar direccionadores e interfaces para proporcionar servicio preferente a paquetes de datos seleccionados. El capítulo incluye las secciones siguientes:

Acceso al indicador de mandatos de configuración de Servicios diferenciados

Para entrar mandatos de configuración de DiffServ:

1. Entre **talk 6** en el indicador de mandatos OPCON (*).
2. Entre **feature ds** en el indicador de mandatos `Config>`.

Se visualiza el indicador de mandatos `DS Config>`. Ahora puede entrar mandatos de configuración de DiffServ.

Mandatos de configuración de Servicios diferenciados

Estos mandatos le permiten configurar las opciones de DiffServ, que designan servicio preferente para los paquetes de datos seleccionados. La Tabla 48 resume los mandatos de configuración de DiffServ y el resto de esta sección los describe con detalle. Entre los mandatos en el indicador de mandatos `DS Config>`. Entre el mandato y las opciones en una línea o entre solamente el mandato y, después, responda a las solicitudes. Para ver una lista de las opciones de mandatos válidas, entre el mandato con un interrogante en lugar de opciones.

Tabla 48. Mandatos de configuración de DiffServ

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxx.
Delete	Suprime un registro de configuración de DiffServ la la SRAM de un direccionador.
Disable	Inhabilita DiffServ en un direccionador o en una interfaz de salida específica.
Enable	Habilita DiffServ en un direccionador o en una interfaz de salida específica.
List	Visualiza información sobre un sistema y los valores relacionados con la interfaz de DiffServ de un direccionador.
Set	Especifica los valores relacionados con DiffServ de un direccionador.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxi.

Delete

Utilice el mandato **delete** para suprimir un registro de configuración de sistema o un registro de configuración de interfaz de DiffServ de la SRAM de un direccionador.

Sintaxis: delete ds
interface

ds Suprime el registro de configuración de sistema de DiffServ del direccionador.

Ejemplo:

```
DS Config> delete ds
Diffserv system config record deleted
```

interface
Le solicita el número de interfaz que debe suprimirse.

Ejemplo:

```
DS Config> delete interface
Enter Diffserv Interface number to delete [0]? 3
Diffserv interface config record deleted
```

Disable

Utilice el mandato **disable** para inhabilitar la función de DiffServ en un direccionador o en una interfaz de salida específica.

Sintaxis: disable ds
interface

ds Inhabilita la función DiffServ del direccionador.

Ejemplo:

```
DS Config> disable ds
DiffServe feature disabled
```

interface
Le solicita el número de la interfaz que debe inhabilitarse.

Ejemplo:

```
DS Config> disable interface
Enter Interface number [0]? 2
DiffServe interface disabled
```

Enable

Utilice el mandato **enable** para habilitar la función DiffServ en un direccionador o en una interfaz de salida específica.

Sintaxis: enable ds
interface

ds Habilita la función DiffServ del direccionador.

Ejemplo:

```
DS Config> enable ds
DiffServe feature enabled
```

interface
Le solicita el número de la interfaz que debe habilitarse.

Ejemplo:

```
DS Config> enable interface
Enter Interface number [0]? 2
DiffServe interface enabled
```

Nota: DiffServ sólo se puede habilitar en enlaces PPP y Frame Relay.

List

Utilice el mandato **list** para visualizar información sobre un sistema y los valores relacionados con la interfaz de DiffServ de un direccionador.

Sintaxis: list all
ds
interface

all Visualiza información sobre configuraciones de DiffServ y la interfaz de un direccionador.

ds Visualiza la configuración de DiffServ de un direccionador.

Ejemplo:

```
DS Config> list ds

System Parameters:

        DiffServ:               ENABLED
        Packet_size:            550
        Min BE Alloc (%):       10
        Min CTL Alloc (%):      5
        Number_of_Q:            2
```

interface
Visualiza las interfaces de un direccionador, su estado DiffServ habilitado/inhabilitado y los parámetros para cada interfaz y cola.

Ejemplo:

```
DS Config> list interface
-------------------------------------------------------------------------------
                          ---------- Premium -------   --------- Assured --------
Net If     Status  NumQ Bwdth  Wght  OutBuf  MaxQos Bwdth  Wght  OutBuf  MaxQos
Num                       (%)   (%) (bytes)     (%)   (%)   (%) (bytes)     (%)
-------------------------------------------------------------------------------
2   PPP   Enabled     2    20    90    5500      95    80    10   27500      80
3   PPP   Enabled     2    20    90    5500      95    80    10   55000      80
```

Set

Utilice el mandato **set** para establecer un sistema y los parámetros relacionados con la interfaz de DiffServ de un direccionador.

Sintaxis: set
- be-alloc-min
- ctl-alloc-min
- interface
- pkt-size

be-alloc-min

Especifica el porcentaje mínimo de espacio total de almacenamiento intermedio de salida a asignar al servicio de mayor eficacia.

Valor por omisión: 10

Ejemplo:

```
DS Config> set be-alloc-min
Enter Minimum percent output BW allocated to BE service (10 - 50) [10]?
```

ctl-alloc-min

Especifica el porcentaje mínimo del espacio total de almacenamientos intermedios de salida para asignar al servicio de control de la red.

Valor por omisión: 5

Ejemplo:

```
DS Config> set ctl-alloc-min
Enter Minimum percent output BW allocated to CTL service (5 - 20) [5]?
```

interface

Especifica la interfaz que debe habilitarse para DiffServ y le solicita parámetros específicos de la interfaz.

Queue bandwidth

Especifica el porcentaje del enlace de salida que debe utilizarse para la cola de primera calidad. El resto del porcentaje se utiliza para el valor de cola asegurado.

Valor por omisión: 20

Queue weight

Especifica el porcentaje de tiempo que el planificador supervisa la cola de primera calidad. El resto del porcentaje se utiliza para el valor de cola asegurado. El peso de la cola es por omisión el 90 por ciento de modo que el planificador reacciona rápidamente para el tráfico de EF.

Valor por omisión: 90

Egress buffer size

Especifica la cantidad de datos (en bytes) que se pueden poner en cola en la cola de primera calidad y en la cola asegurada.

Para la cola de primera calidad, este parámetro controla la cantidad de datos (en bytes) que se pueden poner en cola en la cola de primera calidad. Un valor demasiado grande para este parámetro podría provocar un gran retardo en la puesta en cola para el tráfico de primera calidad. Por ejemplo, si se establece en 25 kilobytes y

la velocidad de enlace de salida es de 1,5 Mbps (velocidad T1), existe un retardo potencial de puesta en cola de 133 mseg (25.000 bytes * 8 bits/byte)/1.500.000 bps o 0,133 seg (133 milisegundos). Un valor demasiado pequeño para este parámetro podría hacer imposible poner en almacenamientos intermedios pequeñas subidas. Por ejemplo, si se establece en 2 kb, implica que no habrá suficiente almacenamiento intermedio para una ráfaga de 2 paquetes de paquetes de 1500 bytes (porque necesitan 3000 bytes de espacio de almacenamiento intermedio).

Como solución entre estos dos extremos, el valor por omisión es 5500 bytes, que es diez veces el tamaño del paquete por omisión de 550.

Valor por omisión: 5500 (cola de primera calidad)

Para la cola asegurada, este parámetro controla la cantidad de datos (en bytes) que se pueden poner en cola en la cola asegurada. Las consideraciones para el valor de este parámetro son las mismas que para la cola de primera calidad, salvo que para el tráfico de la cola asegurada no existen requisitos de retardo demasiado estrictos. En lugar de ello, lo más probable es que el tráfico de cola asegurada consistirá en flujos TCP, que experimentan subidas por naturaleza. Debido a esto, debe definirse suficiente espacio de almacenamiento intermedio para adaptarse a las subidas de varios flujos.

El tamaño por omisión es 27.500 bytes, que es cincuenta veces el tamaño de paquete por omisión de 550.

Valor por omisión: 27500 (cola asegurada)

Egress QoS allocation

Especifica la cantidad del valor de tamaño de almacenamiento intermedio de salida (como un porcentaje) que pueden reservar todas las corrientes de DiffServ. El resto del porcentaje se utiliza para el tamaño mínimo de la agrupación compartida.

Valor por omisión: 95 (cola de primera calidad)

Valor por omisión: 80 (cola asegurada)

Notas:

1. Para Multilink PPP, habilite DiffServ en la interfaz virtual del paquete. No se permite la habilitación de DiffServ en un enlace individual de la interfaz de paquete.
2. Para subinterfaces Frame Relay, habilite DiffServ en la red Frame Relay base. No se permite la habilitación de DiffServ en subinterfaces.

Ejemplo:

```
DS Config> set interface
Enter Diffserv Interface number [0]? 2

DiffServ Interface enabled

Set Premium Queue Bandwidth (%) (1 - 99) [20]?
    Assured Queue Bandwidth (%) = 80

Configure Advanced setting (y/n)? [No]: y

Set Premium Queue Weight (%) (20 - 99) [90]?
    Assured Queue Weight (%) = 10

EGRESS BufSize for Premium Queue (in bytes) (550 - 27500) [5500]?
Max EGRESS QoS Allocation for Premium Queue (%) (1 - 99) [95]?

EGRESS BufSize for Assured/BE Queue (in bytes) (5500 - 140800) [27500]?
Max EGRESS QoS Allocation for Assured/BE Queue (%) (1 - 99) [80]?

        DiffServ Interface: ENABLED
PREMIUM Queue Bandwidth (%) =                          20
PREMIUM Queue Weight (%) =                             80
PREMIUM Queue EGRESS BufSize in bytes =              5500
PREMIUM Queue Max EGRESS QoS allocation (%) =          95
ASSURED/BE Queue Bandwidth (%) =                       80
ASSURED/BE Queue Weight (%) =                          20
ASSURED/BE Queue EGRESS BufSize in bytes =          27500
ASSURED/BE Queue Max EGRESS QoS allocation (%) =       80
Accept input (y/n)? [Yes]:
```

pkt-size

Especifica el tamaño de paquete medio del flujo de tráfico (en bytes). Permite que DiffServ determine el espacio de direccionamiento intermedio disponible en las interfaces de entrada y de salida. Si se cambia, debe reiniciarse el direccionador y deben revisarse y cambiarse, si es necesario, los valores del mandato **set interface** de DiffServ.

Valor por omisión: 550

Ejemplo:

```
DS Config> set pkt-size
Average packet size (64 - 64000) [550]?
```

Acceso al entorno de supervisión de Servicios diferenciados

La parte de consola de la característica DiffServ le permite ver y gestionar valores relacionados con DiffServ. Para acceder al entorno de supervisión de DiffServ, entre **talk 5** en el indicador de mandatos OPCON (*):

```
* t 5
```

A continuación, entre el mandato siguiente en el indicador de mandatos **+**:

```
+ feature ds
DS Console>
```

Mandatos de supervisión de Servicios diferenciados

Estos mandatos le permiten ver valores relacionados con DiffServ. La Tabla 49 resume los mandatos de supervisión de DiffServ y el resto de esta sección los describe. Entre los mandatos en el indicador de mandatos `DS Console>`. Entre el mandato y las opciones en una línea o entre solamente el mandato y, después, responda a las solicitudes. Para ver una lista de las opciones de mandatos válidas, entre el mandato con un interrogante en lugar de opciones.

Tabla 49. Mandatos de supervisión de DiffServ

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Clear	Borra estadísticas para una corriente entre un par de interfaces de entrada y de salida específico.
DScache	Borra o visualiza información de la antememoria de DiffServ de un direccionador.
List	Visualiza información sobre un sistema y los valores relacionados con la interfaz de DiffServ de un direccionador.
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 borrar estadísticas para una corriente entre un par de interfaces de entrada y de salida específico.

Sintaxis: clear stream-stats

Ejemplo:

```
DS Console> clear stream-stats
Incoming Network number : 0
Outgoing Network number : 2
Net 0->2 stream stats cleared at sysclock 85327 Second.
```

DScache

Utilice el mandato **dscache** para borrar o visualizar información de la antememoria de DiffServ de un direccionador.

Sintaxis: dscache actions
clear
nexthop
order
stats

actions

Visualiza las acciones que deben llevarse a cabo para los paquetes enviados desde el origen de IP especificado hasta el destino de IP especificado, y el ID de corriente de DiffServ, si existe alguno.

Ejemplo:

```
DS Console> dscache actions
Source Address to list []?
Destination Address to list []?
Source          Destination     Pro ProtocolInf Net TosIn/Out Action StrmID
10.1.100.1      9.1.140.1         1 T:x08 C:x00   0 x00->x15  PASS   85
9.1.140.1       10.1.100.1        1 T:x00 C:x00   1 x00->x15  PASS   null
```

clear

Especifica el borrado de toda la antememoria de DiffServ.

nexthop

Visualiza la dirección IP del próximo salto.

Ejemplo:

```
DS Console> dscache nexthop
Source Address to list []? 5.0.13.248
Destination Address to list []? 5.0.11.249
Source          Destination     Pro ProtocolInf Net  Tos  NextHop
5.0.13.248      5.0.11.249       17  1031> 1031   0  x00  5.0.61.7      (PPP/1)
5.0.13.248      5.0.11.249       17  1032> 1032   0  x00  5.0.61.7      (PPP/1)
5.0.13.248      5.0.11.249       17  1033> 1033   0  x00  5.0.67.1      (PPP/1)
```

order

Visualiza el orden con el que han llegado los paquetes.

Ejemplo:

```
DS Console> dscache order
Order Source          Destination     Pro ProtocolInf Net  Tos
   1  5.0.16.246      5.0.13.248        1 T:x03 C:x03   2  x00
   2  5.0.13.248      5.0.16.246       17  4000> 5678   0  x00
   3  5.0.16.246      5.0.13.244        1 T:x03 C:x03   1  x00
   4  5.0.13.248      5.0.15.243       17   123>  123   0  x00
```

stats

Visualiza estadísticas para paquetes enviados desde el origen de IP especificado hasta el destino de IP especificado.

Ejemplo:

```
DS Console> dscache stats
Source Address to list []? 5.0.13.248
Destination Address to list []? 5.0.11.249
Source          Destination     Pro ProtocolInf Net  Tos    RxPkts    RxBytes
5.0.13.248      5.0.11.249       17  1031> 1031   0  x00       432     444096
5.0.13.248      5.0.11.249       17  1032> 1032   0  x00       432     444096
5.0.13.248      5.0.11.249       17  1033> 1033   0  x00       437     459516
```

List

Utilice el mandato **list** para visualizar información sobre un sistema y los valores relacionados con la interfaz de DiffServ de un direccionador.

Sintaxis: list
- interface
- queue
- stream
- vifs

interface

Lista las interfaces de un direccionador, sus estados DiffServ habilitado/inhabilitado, sus asignaciones de almacenamiento intermedio de entrada y otra información.

Net Visualiza el número de interfaz.

Status Visualiza el estado de DiffServ.

KB/s Visualiza la velocidad de enlace en kb por segundo.

VirtTime Visualiza el tiempo virtual utilizado por el planificador (indicas n/a (n/d) para enlaces que no sean de DiffServ, indica 0 si no hay ningún paquete en proceso).

InMax Visualiza el tamaño máximo de almacenamiento intermedio configurado para reenvío asegurado.

InCurr Visualiza la cantidad de espacio de almacenamiento intermedio que se utiliza actualmente para la corriente de entrada. Los almacenamientos intermedios contienen paquetes en proceso.

InShar Visualiza la cantidad de espacio de almacenamiento intermedio compartido para este interfaz de salida.

InMaxA Visualiza la cantidad máxima de espacio de almacenamiento intermedio que se puede asignar a todas las corrientes de QoS colectivamente.

InCurA Visualiza la cantidad de espacio de almacenamiento intermedio asignado para que lo utilice la corriente de entrada.

NumI Visualiza el número de corrientes de entrada.

NumO Visualiza el número de corrientes de salida.

Ejemplo:

```
DS Console> list interface
DiffServ interfaces:
Net Status   KB/s  VirtTime InMax  InCurr InShar InMaxA InCurA NumI NumO
--- -------- ----- -------- ------ ------ ------ ------ ------ ---- ----
  0 Disabled  1250      n/a  55000    550  49775  44000   5225   22  n/a
  1 Disabled  1250      n/a  27500      0  27500  22000      0   20  n/a
  2 Enabled    256        0  27500      0  27500  22000      0   20    3
  3 Enabled    256        0  55000      0  55000  44000      0   20    3
  4 Disabled     0      n/a 550000      0 550000 550000      0   20  n/a
  5 Disabled     0      n/a 550000      0 550000 550000      0   20  n/a
  6 Disabled     0      n/a 550000      0 550000 550000      0   20  n/a
  7 Disabled     0      n/a 550000      0 550000 550000      0   20  n/a
  8 Disabled  2000      n/a  27500      0  27500  22000      0   20  n/a
  9 Disabled     0      n/a 550000      0 550000 550000      0   20  n/a
```

queue

Visualiza los pesos asignados a las colas de salida de DiffServ y el estado de asignación de almacenamiento intermedio de las interfaces de salida.

Queued packets

Visualiza el número de paquetes que están actualmente en cola (0 indica que actualmente no hay ningún paquete en cola).

Svc Tag Visualiza la siguiente hora virtual en la que esta cola debe recibir servicio.

Weight Visualiza el peso de planificador configurado de esta cola.

out_max_alloc
Visualiza la cantidad máxima de espacio de almacenamiento intermedio que se puede asignar a una corriente de DiffServ.

out_curr_alloc
Visualiza la cantidad actual de espacio de almacenamiento intermedio asignado.

out_max_buff
Visualiza la cantidad máxima de espacio de almacenamiento intermedio para esta cola.

out_curr_buff
Visualiza la cantidad de espacio de almacenamiento intermedio asignado actualmente que se utiliza para paquetes.

out_share_buff
Visualiza la cantidad del espacio de almacenamiento intermedio que existe actualmente en la agrupación compartida.

Ejemplo:

```
DS Console> list queue
OUT Network number : 1

Premium Queue:
        Queued packets: 0
        Svc Tag:        4294967295
        Weight: 90
        out_max_alloc:  5225 (Bytes)
        out_curr_alloc: 0 (Bytes)
        out_max_buff:   5500 (Bytes)
        out_curr_buff:  0 (Bytes)
        out_share_buff: 5500 (Bytes)


Assured Queue:
        Queued packets: 0
        Svc Tag:        4294967295
        Weight: 10
        out_max_alloc:  22000 (Bytes)
        out_curr_alloc: 4125 (Bytes)
        out_max_buff:   27500 (Bytes)
        out_curr_buff:  0 (Bytes)
        out_share_buff: 23375 (Bytes)
```

stream meter-mark
Visualiza información acerca de la medición y el marcado para las corrientes AF.

Id Número de identificación de la corriente

t Tipo de corriente

- **D** Corriente de DiffServ
- **B** Corriente de mayor eficacia
- **C** Corriente de control de la red
- **R** Corriente de RSVP

I/o q Tipo de cola de interfaz de salida

- **q1** Cola de primera calidad
- **q2** Cola Asegurada/BE

pkt snt Número total de paquetes enviados por esta corriente.

buf drp Número de paquetes excluidos de esta corriente debido a que no hay espacio de almacenamiento intermedio disponible.

snt g Número de paquetes marcados de color verde enviados

snt y Número de paquetes marcados de color amarillo enviados.

snt r Número de paquetes marcados de color rojo enviados

g->y En modalidad con distinción de color, número de paquetes marcados de color verde enviados como si estuvieran marcados de color amarillo.

g->r En modalidad con distinción de color, número de paquetes marcados de color verde enviados como si estuvieran marcados de color rojo.

y->r En modalidad con distinción de color, número de paquetes marcados de color amarillo enviados como si estuvieran marcados de color rojo.

Ejemplo:

```
DS Console> list stream meter-mark 0 1
At interface 0, 4 in-streams; clock=25493 sec.
Streams from net 0 to net 1:
 Id   t I/o q  pkt snt  buf drp   mrk g    mrk y   mrk r   g->y    g->r    y->r
 ---- - -----  -------  -------  -------  ------  ------  ------  ------  ------
(af1)
 101  D   in     3615        0        0       0       0       0       0       0
         o-q2    3615        0     1223    1222    1770       0       0       0
```

stream packet-stats

Visualiza información acerca de los paquetes de las corrientes.

Id Número de identificación de la corriente

t Tipo de corriente

- **D** Corriente de DiffServ
- **B** Corriente de mayor eficacia
- **C** Corriente de control de la red
- **R** Corriente de RSVP

I/o q Tipo de cola de interfaz de salida

- **q1** Cola de primera calidad
- **q2** Cola Asegurada/BE

allo/cur(K) Espacio total de almacenamiento intermedio (en kilobytes) asignado y utilizado actualmente por esta corriente.

tot pkt Número total de paquetes recibidos por esta corriente para transmitirlos.

tot Kby Número total de kilobytes recibidos por esta corriente para transmitirlos.

pkt snt Número total de paquetes enviados por esta corriente.

Kby snt Número total de kilobytes enviados por esta corriente.

ovr snt Número de paquetes enviados utilizando almacenamientos intermedios compartidos.

buf drp Número de paquetes excluidos de esta corriente debido a que no hay espacio de almacenamiento intermedio disponible.

pol drop Número de paquetes excluidos por el agente en la cola de primera calidad.

Ejemplo:

```
DS Console> list stream packet-stats 0 1
At interface 0, 4 in-streams; clock=25496 sec.
Streams from net 0 to net 1:
 Id   t I/o q  allo/cur(K)  tot pkt  tot Kby  pkt snt  Kby snt  ovr snt  buf drp pol drp
 ---- - -----  -----------  -------  -------  -------  -------  -------  ------- -------
(af1)
 101  D    in   6.3/   0.0     3615     3730     3615     3730        0        0
         o-q2   6.3/   0.0                      3615     3730        0        0       0

(ef)
 100  D    in   5.2/   0.0     2393     2469     2393     2469        0        0
         o-q1   5.2/   0.0                      2393     2469        0        0     132

(-)
 40   B    in   0.0/   0.0        0        0        0        0        0        0       0
         o-q2   2.8/   0.0                         0        0        0        0       0

(-)   C    in   0.0/   0.0        0        0        0        0        0        0
         o-q2   1.4/   0.0                         0        0        0        0       0
```

stream police-para

Visualiza información acerca del parámetro de política configurado para corrientes EF y AF.

Id Número de identificación de la corriente

t Tipo de corriente

- **D** Corriente de DiffServ
- **B** Corriente de mayor eficacia
- **C** Corriente de control de la red
- **R** Corriente de RSVP

I/o q Tipo de cola de interfaz de salida

- **q1** Cola de primera calidad
- **q2** Cola Asegurada/BE

TR/CIR en B/s

Velocidad de señal o velocidad de información comprometida configurada en bytes por segundo.

TBS/CBS en bytes

Tamaño de cubeta de señales o tamaño de ráfaga comprometido configurado en bytes.

PIR en B/s

Velocidad de información máxima configurada en bytes por segundo.

EBS/PBS en bytes

Tamaño de cubeta excesivo o tamaño de ráfaga máximo configurado en bytes.

pol typ Tipo de acción de política.

None Ninguna política.

SRCB TCM sin distinción de color, de una sola velocidad.

SRCA TCM con distinción de color, de una sola velocidad.

TRCB TCM sin distinción de color, de dos velocidades.

TRCA TCM con distinción de color, de dos velocidades.

EF-DRP Supervisor EF con acción de exclusión por omisión.

Ejemplo:

```
DS Console> list stream police-para 0 1
At interface 0, 16 in-streams; clock=18429 sec.
Streams from net 0 to net 1:
 Id   t I/o q     TR/CIR    TBS/CBS    PIR      EBS/PBS  pol typ
                  in B/s   in bytes   in B/s   in bytes
 ---- - -----  ---------  ---------  -------  ---------  -------
(af1)
 101  D   in
         o-q2      25000       4000        0       4000  SRCB

(ef)
 100  D   in
         o-q1      48706       5225                      EF-DRP
```

vifs

Visualiza información sobre interfaces virtuales Frame Relay.

Ejemplo:

```
DS Console> list vifs 1

DiffServ virtual interface for dlci:  17
     Status: Inactive - no packets queued for transmission
     CIR: 64000 (bits/sec)
     Virtual Time: 0
     Service Tag:  0

DiffServ virtual interface for dlci:  16
     Status: Inactive - no packets queued for transmission
     CIR: 64000 (bits/sec)
     Virtual Time: 0
     Service Tag:  0
```

Soporte de reconfiguración dinámica de servicios diferenciados

Esta sección describe la reconfiguración dinámica (DR) en lo que afecta a los mandatos de Talk 6 y Talk 5.

Delete interface de CONFIG (Talk 6)

Los Servicios diferenciados (o DiffServ o DS) soportan el mandato de CONFIG (Talk 6) **delete interface** con la consideración siguiente:

Suprime el registro SRAM de interfaz de DiffServ correspondiente. Tiene que rearrancar el dispositivo para activar este cambio.

Activate interface de GWCON (Talk 5)

DiffServ soporta el mandato de GWCON (Talk 5) **activate interface** con la consideración siguiente:

DS seguirá la secuencia normal de activación de red/desactivación de red si se activa una interfaz configurada para DS.

Reset interface de GWCON (Talk 5)

DiffServ soporta el mandato de GWCON (Talk 5) **reset interface** con la consideración siguiente:

- Si se habilita DiffServ en esta interfaz, sucederá lo siguiente: **reset interface** borrará todas las corrientes creadas en/desde esta interfaz. También borrará la antememoria de diffserv. Si se habilita BRS, BRS tiene prioridad sobre DiffServ en esta interfaz. Para cualquier operación add/del/change en el registro SRAM de la interfaz de DiffServ, necesita rearrancar el dispositivo para activar el cambio.

Mandatos no reconfigurables dinámicamente

La tabla siguiente describe los mandatos de configuración de DiffServ que no se pueden cambiar dinámicamente. Para activar estos mandatos, es necesario volver a cargar o reiniciar el dispositivo.

Mandatos
CONFIG, feature DS, enable/disable/del ds
CONFIG, feature DS, enable/disable/del/set interface
CONFIG, feature DS, set be-alloc-min
CONFIG, feature DS, set ctl-alloc-min
CONFIG, feature DS, set pkt-size

Utilización de la característica Detección aleatoria temprana

Este capítulo describe cómo utilizar la característica Detección aleatoria temprana (Random Early Detection) (RED) para que un dispositivo de red, basándose en la probabilidad de exclusión configurada, marque paquetes de entrada aleatorios para excluirlos si se produce una congestión, evitando de este modo un desbordamiento. Esto beneficia al tráfico de comportamiento correcto como TCP, que responde a la indicación de congestión reduciendo el tamaño de la ventana de transmisión. La RED soporta enlaces PPP, Multilink PPP y Frame Relay. Este capítulo consta de la sección siguiente:

- "Utilización de la Detección aleatoria temprana"

Utilización de la Detección aleatoria temprana

La RED le permite evitar el desbordamiento si se produce una congestión. La RED calcula el promedio de la longitud de cola y, si está dentro de los límites especificados, se marca un paquete de entrada para su exclusión, basándose en la probabilidad de exclusión configurable. La utilización del *promedio* de la longitud de cola en lugar del tamaño de cola actual evita que una cola de tráfico por ráfagas afecte a la velocidad de desactivación.

Suponga que ha especificado los valores siguientes para los parámetros de RED:

```
1 Weight factor: 4
2 Exponential Maximum Packet Drop Probability: 9
3 Minimum Threshold Value: 70
4 Maximum threshold Value: 100
5 Initial Average Queue Size: 60
```

1 Este valor determina cuánta influencia tiene una cola actual sobre el cálculo del promedio de la longitud de cola.

El valor mínimo de este parámetro (1) designa menos peso y es un valor conservador. Con este valor, el promedio de la longitud de cola en un momento específico permanece más próximo al promedio anterior de la longitud de cola, de modo que el tráfico por ráfagas con una longitud de cola grande tiene poco efecto en el cálculo del nuevo promedio de la longitud de cola.

El valor máximo de este parámetro (8) designa un peso mayor y es un valor agresivo. Con este valor, el promedio de la longitud de cola es igual a la longitud de cola actual, de modo que el tráfico por ráfagas con una longitud de cola grande tiene un gran efecto sobre el cálculo del nuevo promedio de la longitud de cola.

2 Este valor es la probabilidad de exclusión de un paquete con un promedio máximo de longitud de cola.

Si el promedio de la longitud de cola es coherentemente igual al valor máximo de umbral, se marca uno de cada 2^9 (512) paquetes para su exclusión. La probabilidad de exclusión aumenta linealmente a medida que aumenta el promedio de longitud de cola del umbral mínimo al umbral máximo.

3 Este valor designa el requisito mínimo de cola para calcular la probabilidad de exclusión de un paquete y lo marca como corresponde.

Se expresa como un porcentaje del valor máximo de cola de dispositivo, que es un valor no configurable determinado por el protocolo de la capa 2. Por

ejemplo, si especifica un valor de 40 por ciento y el valor máximo de cola de dispositivo es 16, el valor de umbral mínimo se establece en 6 (0,4*16).

4 Este valor designa el requisito máximo de cola para calcular la probabilidad de exclusión de un paquete y marcarlo como corresponde.

Se expresa como un porcentaje del valor máximo de cola de dispositivo, que es un valor no configurable determinado por el protocolo de la capa 2. Por ejemplo, si especifica un valor de 100 por cien y el valor máximo de cola de dispositivo es 16, el valor de umbral máximo se establece en 16 (1,0*16).

5 Este valor designa el valor inicial utilizado para calcular la probabilidad de exclusión de paquete.

Se expresa como un porcentaje del valor máximo de cola de dispositivo, que es un valor no configurable determinado por el protocolo de la capa 2. Impide que el tráfico por ráfagas aumente el peso en el cálculo de promedio de longitud de cola antes de que el propio tráfico establezca un valor de promedio de cola. (Cuando se inicializa el dispositivo, la longitud de cola es cero y no existe ninguna indicación de promedio de longitud de cola anterior). Deberá especificar un valor relativamente bajo como se muestra en el ejemplo anterior.

Después de habilitar la RED y de establecer los parámetros de interfaz, deberá reiniciar o volver a cargar el dispositivo para activar la RED. Para obtener detalles sobre cómo especificar mandatos de RED, consulte el apartado “Configuración y supervisión de la característica Detección aleatoria temprana” en la página 409.

Configuración y supervisión de la característica Detección aleatoria temprana

Este capítulo describe los mandatos proporcionados por la característica RED (Detección aleatoria temprana) para configurar interfaces para excluir paquetes de forma aleatoria durante condiciones de congestión. El capítulo incluye las secciones siguientes:

- "Acceso al indicador de mandatos de configuración de Detección aleatoria temprana"
- "Mandatos de configuración de Detección aleatoria temprana"
- "Acceso al entorno de supervisión de Detección aleatoria temprana" en la página 412
- "Mandatos de supervisión de Detección aleatoria temprana" en la página 412

Acceso al indicador de mandatos de configuración de Detección aleatoria temprana

Para entrar mandatos de configuración de RED:

1. Entre **talk 6** en el indicador de mandatos de OPCON (*).
2. Entre **feature red** en el indicador de mandatos `Config>`.

Se visualiza el indicador de mandatos `RED Config>`. Ahora puede entrar mandatos de configuración de RED.

Mandatos de configuración de Detección aleatoria temprana

Estos mandatos le permiten configurar las opciones de RED, que determinan cómo se excluyen paquetes durante los periodos de congestión de tráfico. Esto puede evitar el desbordamiento y la resincronización global. La Tabla 50 en la página 410 resume los mandatos de configuración de RED y el resto de este tema los describe detalladamente. Entre los mandatos en el indicador de mandatos `RED Config>`. Entre el mandato y las opciones en una línea o entre solamente el mandato y, a continuación, responda a las solicitudes. Para ver una lista de las opciones de mandatos válidas, entre el mandato con un interrogante en lugar de las opciones.

Tabla 50. Mandatos de configuración de Detección aleatoria temprana	
Mandato	**Función**
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Delete	Suprime un registro de interfaz o un registro de configuración de RED de la SRAM de un dispositivo de red.
Disable	Inhabilita RED en un dispositivo de red o en una interfaz de salida específica.
Enable	Habilita RED en un dispositivo de red o en una interfaz de salida específica.
List	Visualiza información acerca del estado RED de un dispositivo de red y de los valores relacionados con la interfaz.
Set	Especifica valores de RED para una interfaz específica de un dispositivo de red.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Delete

Utilice el mandato **delete** para suprimir un registro de configuración de RED para una interfaz de la SRAM de un dispositivo de red.

Sintaxis: delete interface

interface
Le solicita el número de interfaz que debe suprimirse.

Ejemplo:

```
RED Config> delete interface
Enter RED Interface number to delete [0]? 3
RED interface config record deleted
```

Disable

Utilice el mandato **disable** para inhabilitar RED para un dispositivo de red o en una interfaz de salida específica.

Sintaxis: disable red
interface

red
Inhabilita RED para un dispositivo de red.

Ejemplo:

```
RED Config> disable red
RED disabled
```

interface
Inhabilita RED en una interfaz de salida específica.

Ejemplo:

```
RED Config> disable interface
Enter RED Interface number [0]? 2
RED interface disabled
```

Enable

Utilice el mandato **enable** para habilitar RED para un dispositivo de red o en una interfaz de salida específica.

Sintaxis: enable red
interface

red

Habilita RED para un dispositivo de red.

Ejemplo:

```
RED Config> enable red
RED enabled
```

interface

Habilita RED en una interfaz de salida específica.

Ejemplo:

```
RED Config> enable interface
Enter RED Interface number [0]? 2
RED interface enabled
```

Nota: RED sólo se puede habilitar en enlaces PPP, Multilink PPP y Frame Relay.

List

Utilice el mandato **list** para visualizar información acerca del estado RED de un dispositivo de red y de los valores relacionados con la interfaz.

Sintaxis: list all

all Visualiza el estado RED de un dispositivo de red.

Ejemplo:

```
RED Config>list all

        RED Status: Enabled

-------------------------------------------------
Status  Net If   qW   maxP   minT   maxT    initAvgQ
                             ------ %ofdevQ --------
-------------------------------------------------
Enable  6   PPP  4    1/512  70     100     60


Abbreviation:

qW = Queue Weight
minT = Minimum Threshold, maxT = Maximum Threshold
maxP = Maximum Drop Probability: 1 drop in 512 pkts
%ofdevQ = A percentage of the Maximum Device Queue
```

Set

Utilice el mandato **set** para especificar valores de RED para una interfaz específica de un dispositivo de red.

Sintaxis: set interface

interface *número*

Especifica el número de la interfaz para la que se deben establecer las opciones de RED.

Valor por omisión: ninguno

Ejemplo:

```
RED config>set interface
Enter RED Interface number [0]? [6]
RED Interface enabled
Exponential Maximum Packet Drop Probability (9 for 1/2e9) (5 - 10) [9]?
Advanced Setting (y/n)? [Yes]: yes

Maximum Device Queue = 5
Weight Factor (1 - 8) [4]?
Minimum Threshold value (% of the max device queue) (0 - 100) [70]?
Maximum Threshold value (% of the max device queue) (0 - 100) [100]?
Initial Average Queue Size (% of the max device queue) (0 - 100) [60]?
Accept input (y/n)? [Yes]: yes
```

Acceso al entorno de supervisión de Detección aleatoria temprana

La parte de consola de la característica Detección aleatoria temprana le permite ver y gestionar valores relacionados con RED. Para acceder al entorno de supervisión de RED entre **talk 5** en el indicador de mandatos de OPCON (*):

```
* t 5
```

A continuación, entre el mandato siguiente en el indicador de mandatos **+**:

```
+ feature red
RED Console>
```

Mandatos de supervisión de Detección aleatoria temprana

Estos mandatos le permiten ver valores relacionados con RED. La Tabla 51 resume los mandatos de supervisión de RED y el resto de esta sección los describe. Entre los mandatos en el indicador de mandatos `RED Console>`. Entre el mandato y las opciones en una línea o entre solamente el mandato y, después, responda a las solicitudes. Para ver una lista de las opciones de mandatos válidas, entre el mandato con un interrogante en lugar de las opciones.

Tabla 51. Mandatos de supervisión de RED

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Clear	Restablece los valores de parámetros de RED de una interfaz.
List	Visualiza los valores de interfaz de dispositivo de red habilitado para RED.
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 restablecer los valores de parámetros de RED de una interfaz. El ejemplo de la descripción del mandato **list** ilustra los resultados del mandato **clear**.

Sintaxis: clear *número-interfaz*

List

Utilice el mandato **list** para visualizar información acerca de los valores de interfaz de dispositivo de red habilitado para RED.

Sintaxis: list *número-interfaz*

número-interfaz
Lista los valores de RED para la interfaz especificada de un dispositivo de red.

Ejemplo:

```
RED Console>list 6
-------------------------------------------------------------------------------------
Status  If    maxQ   avgQ   minT   maxT qW   maxP   pktCnt    pdpDepth  passCnt drpCnt
                            (dvQ)  (dvQ)     (pkt)   til drp     count     pkt    pkt
-------------------------------------------------------------------------------------
Enable   6       5      3      3      5  4  1/512    1:3787        285     4283      1


Abbreviations:

maxQ = Maximum Queue Length, avgQ = Average Queue Size
minT = Minimum Threshold, maxT = Maximum Threshold
dvQ = Device Queue, qW = Queue Weight
maxP = Maximum Drop Probability: 1 drop in 512 pkts
pktCnt til drp = Packet Count before a drop occurs
pdpDepth = Probability Drop Depth: 1 drop in 2048 depth count

RED Console>clear 6

RED Console>list 6
-------------------------------------------------------------------------------------
Status  If   maxQ   avgQ   minT   maxT  qW   maxP  pktCnt    pdpDepth  passCnt  drpCnt
                           (dvQ)  (dvQ)      (pkt)  til drp     count     pkt     pkt
-------------------------------------------------------------------------------------
Enable   6      5      3      3      5   4  1/512   1:3530   0         0        0


Abbreviations:

maxQ = Maximum Queue Length, avgQ = Average Queue Size
minT = Minimum Threshold, maxT = Maximum Threshold
dvQ = Device Queue, qW = Queue Weight
maxP = Maximum Drop Probability: 1 drop in 512 pkts
pdkCnt til drp = Packet Count before a drop occurs
pdpDepth = Probability drop Depth: 1 drop in 2048 depth count
```

Utilización de Función de túnel de la capa 2 (L2TP, PPTP, L2F)

Este capítulo describe la Función de túnel de la capa 2. Consta de las secciones siguientes:

La Función de túnel de la capa 2 (L2T) consta de los protocolos de función de túnel L2TP, L2F y PPTP.

El Layer 2 Tunneling Protocol (L2TP) es un protocolo de seguimiento de estándares IETF para la función de túnel de PPP a través de una red como por ejemplo UDP/IP. L2TP está orientado a la conexión.

Layer 2 Forwarding (L2F) y Point to Point Tunneling Protocol (PPTP) son protocolos informativos de IETF para la función de túnel de PPP a través de una red IP.

Nota: La Función de túnel de la capa 2 no está soportada en el 2210 Modelos 1S4 y 1U4.

Visión general de L2TP

L2TP permite que muchos dominios de protocolo separados y autónomos compartan una infraestructura de acceso común que incluye módems, servidores de acceso y direccionadores RDSI. L2TP permite la función de túnel de la capa de enlace PPP, por ejemplo, HDLC y HDLC asíncrono. Utilizando estos túneles, es posible disociar la ubicación del servidor de marcación contactado de la ubicación que proporciona acceso a la red.

Tradicionalmente, el servicio de red de marcación de Internet solamente se proporciona para direcciones IP registradas. L2TP define una nueva clase de aplicación de marcación virtual que permite múltiples protocolos y direcciones IP sin registrar en la Internet. Esta clase de aplicación de red es útil para soportar marcaciones de IP, IPX y AppleTalk direccionadas de forma privada a través de una infraestructura existente en Internet.

El soporte de estas aplicaciones de marcación virtual multiprotocolo es ventajosa para los usuarios, empresas y proveedores de servicios de Internet puesto que permite el compartimiento de inversiones importantes en acceso y e infraestructuras de núcleo, y permite que los usuarios finales utilicen llamadas locales cuando acceden a los servicios.

L2TP también permite una utilización segura de inversiones existentes en aplicaciones de que no sean del protocolo IP dentro de la infraestructura existente en Internet.

La Figura 32 en la página 417 muestra un ejemplo de red L2TP que utiliza ISDN. La red puede utilizar cualquier tipo de medio entre el Concentrador del acceso de red a L2TP (LAC) y el Servidor de red L2TP (LNS). El ejemplo utiliza el modelo de túnel obligatorio. Este capítulo también describe la configuración del modelo de túnel voluntario.

Términos de L2TP

Los términos siguientes se utilizan cuando se describe L2TP:

Par de valores de atributo (AVP)
Método uniforme para codificar tipos y cuerpos de mensajes. Este método maximiza la extensibilidad a la vez que permite interoperabilidad L2TP.

Concentrador de acceso a L2TP (LAC)
Dispositivo conectado a una o más líneas de red telefónica de servicios públicos (PSTN) o RDSI capaces de manejar operación de PPP y el protocolo L2TP. El LAC implanta el medio a través del cual opera L2TP. L2TP pasa el tráfico a uno o más Servidores de red L2TP (LNS). L2TP puede aplicar un túnel a cualquier protocolo incluido en la red PPP.

Servidor de red L2TP (LNS)
Un LNS opera en cualquier plataforma que pueda ser una estación final PPP. El LNS maneja la parte del servidor del protocolo L2TP. Puesto que L2TP se basa en el único medio a través del cual llegan los túneles de L2TP, el LNS sólo puede tener una única interfaz de LAN o WAN, pero puede finalizar las llamadas que llegan de cualquier interfaz PPP soportada por un LAC.

Servidor de acceso de red (NAS)
Dispositivo que proporciona acceso de red a petición, temporal, a los usuarios. Este acceso es punto a punto y utiliza líneas PSTN o RDSI.

Sesión (Llamada)
L2TP crea una sesión cuando se intenta una conexión PPP de final a final entre un usuario de Dial y el LNS. Los datagramas para la sesión se envían a través del túnel entre el LAC y el LNS. El LNS y el LAC mantienen la información de estado para cada usuario conectado a un LAC.

Túnel
Un túnel se define mediante un par LNS-LAC. El túnel transporta datagramas entre el LAC y el LNS. Un único túnel puede multiplexar varias sesiones. Una conexión de control que funciona a través del mismo túnel controla el establecimiento, liberación y mantenimiento de todas las sesiones y del mismo túnel.

Características soportadas

L2TP se ejecuta a través de UDP/IP y soporta las funciones siguientes:

- Función de túnel de clientes de marcación de entrada de único usuario.
- Función de túnel de direccionadores pequeños, como por ejemplo un direccionador con una única ruta estática a configurar basándose en un perfil de usuario autentificado.
- Se pueden iniciar llamadas desde el LAC al LNS (de entrada), desde el LNS al LAC (salida) desde cualquier similar (ambos). Las llamadas de salida pueden

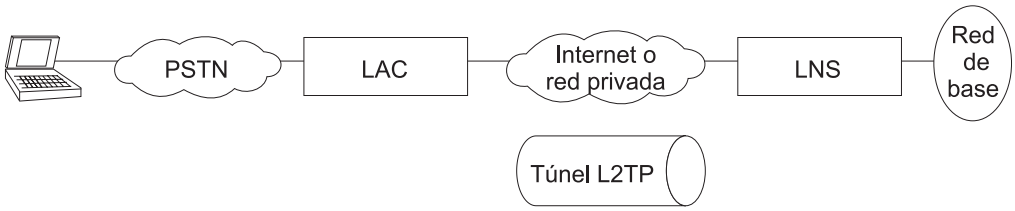


Figura 32. Red L2TP de ejemplo

iniciar una sesión *fija* (siempre activa) o una sesión de función de túnel L2 a petición.

- Múltiples llamadas por túnel.
- Autentificación Proxy para PAP, CHAP y MS-CHAP.
- LCP Proxy.
- Reinicio de LCP si no se utiliza LCP Proxy en el LAC.
- Autentificación de punto final de túnel.
- AVP oculto para transmitir una contraseña PAP proxy.
- Función de túnel utilizando una tabla de búsqueda rhelm local (es decir, usuario@rhelm).
- Función de túnel utilizando búsqueda de nombre de usuario PPP en el subsistema AAA.
- Gestión de túneles L2TP utilizando SNMP. Consulte “Gestión de SNMP” en la publicación *Consulta de configuración y supervisión de protocolos Volumen 1*.

Nota: La función de túnel rhelm necesita nombres de usuario en formato *nombre@rhelm*. Este modo de función de túnel necesita que el software busque en dos tablas para determinar el destino al cual se dirige el túnel para el usuario de marcación de entrada. La ventaja de utilizar este método de función de túnel es que tan solo debe definir el rhelm y los nombres de usuario que coincidan con el rhelm tendrán un túnel al mismo destino.

La función de túnel basada en el usuario se resuelve en una única tabla. Permite la granularidad de aplicar el túnel a cada usuario a un destino exclusivo.

- BRS para un LNS (como punto final PPP).
- La capacidad de utilizar el mandato **delete interface** para suprimir dispositivos L2TP.
- La capacidad de volver a configurar dinámicamente dispositivos L2TP.
- El establecimiento de una secuencia, puesta en cola, retransmisión y canal de control de flujo. L2TP también realiza la secuencia en el canal de datos.
- La capacidad de fijar el puerto UDP L2TP (1701) para que pueda establecer filtros de Seguridad de IP basados en el puerto UDP.
- Un cliente de direccionador de L2TP. Un cliente de direccionador de L2TP es un modelo de “cliente iniciado” (también conocido como función de túnel voluntaria). Esta función proporciona servicios de Red privada virtual (VPN) multiprotocolo, de túnel, seguros sin tener en cuenta la topología del proveedor del servicio. Esta función une el cliente y el LAC en una parte física del hardware.

- Conexión de una llamada de entrada con la interfaz apropiada basándose en una coincidencia de nombre de sistema principal remoto. Si el nombre de sistema principal remoto no coincide con ninguna de las interfaces configuradas para la comparación de nombre de sistema principal, la llamada se completa en una interfaz de entrada que no utiliza comparación de nombre de sistema principal remoto.

  Nota: Si ha configurado múltiples comparaciones de red entre el mismo par de LAC y LNS, asegúrese de que sólo exista un túnel para cada comparación.

- Configuración de puente IP, IPX, automática de redes de entrada que no utilizan comparación de nombre de sistema principal remoto. Debe configurar manualmente las redes de salida y las redes de entrada que utilizan comparación de nombre de sistema principal remoto.

Otros protocolos de Función de túnel de la capa 2 soportados incluyen:

- Están soportadas las funciones L2F de NAS y de pasarela.
- Están soportados Cliente de direccionador PPTP, PAC (Concentrador de acceso PPTP) y PNS (Servidor de red PPTP).

L2F proporciona Función de túnel de la capa 2 interoperable al conectarse a dispositivos de red que no soportan L2TP.

PPTP proporciona Función de túnel de la capa 2 interoperable al conectarse a dispositivos de red que no soportan L2TP. Específicamente se puede utilizar PPTP para servicios VPN de Microsoft Windows 95 (DUN 1.2 y superior), Windows 98 y Windows NT en direccionadores IBM.

Nota: Tanto L2F como PPTP están configurados en la característica Función de túnel de la capa 2.

Consideraciones sobre el tiempo

La naturaleza de la función de túnel de los paquetes PPP a través de redes direccionadas tiene algunas consecuencias de tiempo que deben considerarse. L2TP supone que la conexión entre el LAC y el LNS no tiene ningún retardo que sea tan largo que los similares con túnel excedan el tiempo de espera. Si el estado latente del similar alcanza o excede el tiempo de espera de la máquina de estado PPP (generalmente 3 segundos), la conectividad puede verse afectada negativamente. ' Tenga en cuenta que si el estado de latencia entre el LAC y el LNS es tan pobre, la conectividad en general será tan pobre que la conexión no será aconsejable incluso si las máquinas de estado PPP se mantienen activas artificialmente. Si ambos extremos poseen esta capacidad, el tiempo de espera de PPP puede ampliarse para conseguir la conectividad a través de una conexión muy pobre.

Además del estado de latencia, una no coincidencia de ancho de banda entre el par LAC/LNS y el par LAC/Cliente puede causar problemas. Por ejemplo, si el ancho de reserva real entre el LAC y LNS es significativamente menor que el ancho de banda del cliente PPP, el LAC puede perder un tiempo considerable intentando enviar paquetes al LNS. Por otro lado, si la conexión entre el LNS y un sistema principal en la red inicial LNS es excepcionalmente rápida comparada con

el cliente de marcación de entrada, es posible que el LNS esté intentando enviar datos en exceso a LAC.

Consideraciones sobre LCP

Cuando se utiliza LCP Proxy, el LAC negocia LCP y PPP continúa procesándose en el LNS. El LAC reenvía opciones de LCP al LNS de modo que el LNS sabe lo que se ha negociado. El LNS debe permanecer flexible para los parámetros negociados por el cliente y LAC. Si existe algún parámetro que no sea aceptable para el LNS, L2TP intenta volver a negociar el LCP enviando una *Petición de configuración de LCP* al cliente a través del túnel.

El requisito para que el LNS permanezca flexible es particularmente importante con respecto a la MRU. En el LNS de IBM, la MRU configurada es la máxima permitida para LCP Proxy. Si el valor del mensaje de LCP Proxy desde una LAC es mayor que la MRU configurada en el LNS, L2TP intentará volver a negociar el LCP con una MRU igual que la MRU configurada sin cambiar otras opciones de LCP del LAC.

Configuración de Función de túnel de la capa 2

Para configurar L2T:

1. Acceda a la característica Función de túnel de la capa 2 utilizando el mandato **feature**.

```
Config> feature layer-2-tunneling
Layer-2-Tunneling config>
```

2. Habilite L2TP, L2F y PPTP, según sea necesario.

```
Layer-2-Tunneling config> enable L2TP

Layer-2-Tunneling config> enable L2F

Layer-2-Tunneling config> enable pptp
```

3. Añada tantas redes L2T como sea necesario. Si debe ser estrictamente un LAC, L2F NAS, o PPTP PAC, no es necesario que añada ninguna red L2T. Debe definir una red L2T para cada conexión PPP de túnel simultánea.

```
Layer-2-Tunneling Config>ADD L2-NETS
Additional L2 nets:  [0]? 10
Add unnumbered IP addresses for each L2 net? [Yes]: yes
Adding device as interface 31
Defaulting Data-link protocol to PPP
Adding device as interface 32
Defaulting Data-link protocol to PPP
Adding device as interface 33
Defaulting Data-link protocol to PPP
Adding device as interface 34
Defaulting Data-link protocol to PPP
Adding device as interface 35
Defaulting Data-link protocol to PPP
Adding device as interface 36
Defaulting Data-link protocol to PPP
Adding device as interface 37
Defaulting Data-link protocol to PPP
Adding device as interface 38
Defaulting Data-link protocol to PPP
Adding device as interface 39
Defaulting Data-link protocol to PPP
Adding device as interface 40
Defaulting Data-link protocol to PPP
```

   a. Configure los túneles L2TP, L2F o PPTP.

      Para configurar un túnel L2TP utilizando una lista local AAA:

```
Config> add tunnel-profile
     Enter name:  []? lns.org
Tunneling Protocol? (PPTP, L2F, L2TP): L2TP
     Enter local hostname: []? lac.org
     set shared secret? (Yes, No): [No] Y
     Shared secret for tunnel authentication:
     Enter again to verify:
 Tunnel-Server endpoint address: [0.0.0.0]? 11.0.0.1

      PPP user name: lns.org
      Tunnel Server: 11.0.0.1
               Hostname: lac.org

     User 'lns.org' has been added
     Config>
```

Puede utilizar el ejemplo anterior para configurar autorización de túnel en el LAC así como la función de túnel “rhelm” con el formato “usuario@lns.org.”

Puede establecer autentificación y autorización de túnel para que se lleve a cabo en un servidor RADIUS particular. Consulte “Using Authentication, Authorization, and Accounting (AAA) Security” en la publicación *Utilización y configuración de las características*.

Si está configurando un LNS y la autentificación de túnel está inhabilitada en el LAC y en el LNS, no es necesario configurar ningún perfil de túnel.

Para aplicar la función de túnel por nombre de usuario PPP en un LAC que utiliza lista local AAA o RADIUS:

```
Config>add ppp-user
 Enter name:  []? peter
 Password:
     Enter again to verify:
Allow inbound access for user? (Yes, No):[Yes]
 Will 'peter' be tunneled? (Yes, No): [No] Y
Tunneling Protocol (PPTP, L2F, L2TP): [L2TP] L2TP
     Enter local hostname: []? lac.org
 Tunnel-Server endpoint address: [0.0.0.0]? 11.0.0.1

      PPP user name: peter
      Tunnel Server: 11.0.0.1
               Hostname: lac.org

 Is information correct? (Yes, No, Quit): [Yes]

 User 'peter' has been added
     Config>
```

b. Configure la comparación con nombre de sistema principal remoto para los túneles de entrada, si es necesario.

   Tenga en cuenta que para escenarios de marcación de entrada, este paso no suele ser necesario. Utilice esta opción cuando una conexión deba utilizar una red específica.

   Suponiendo que la configuración anterior se ha utilizado para la red 10:

   ```
   Config> net 10
   L2TP 10> set remote-hostname
   Remote Tunnel Hostname: [] ibm.com
   ```

   Nota: Para desactivar la comparación de nombre de sistema principal remoto, utilice los mandatos siguientes:

   ```
   Config> net 10
   L2TP 10> set any-remote-hostname
   ```

4. Configure las llamadas de salida de L2TP. El ejemplo siguiente muestra un LAX con una dirección IP 1.1.1.1 y un LNS con una dirección IP 1.1.1.2. El LNS se configura para establecer una llamada RDSI Dial-on-demand a 5552160 desde el LAC.

Configuración de LNS:

```
Config> add tunnel-profile
     Enter name:  []? lac.org
Tunneling Protocol? (PPTP, L2F, L2TP): [L2TP]
     Enter local hostname: []? lns.org
     set shared secret? (Yes, No): [No] Y
     Shared secret for tunnel authentication:
     Enter again to verify:
     Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.1

            Tunnel name: lac.org
               TunnType: L2TP
               Endpoint: 1.1.1.1
               Hostname: lns.org

     User 'lac.org' has been added
     Config>
     Config> add dev layer-2-tunneling
     Config> net 10
     L2TP 10> set connection-direction outbound
     L2TP 10> set idle 30
     L2TP 10> set remote-hostname lac.org
     L2TP 10> enable outbound-call-from-lac
        Outbound Call Type (ISDN, V34)? [ISDN]
        Outbound calling address: 5552160
        Outbound calling subaddress:
     L2TP 10>
     L2TP 10> encapsulator
     PPP 10> set name vickie  a
     L2TP 10>
     L2TP 10> exit
     Config> add ppp-user larry  b
```

Notas:

a. Establezca el nombre de autentificación en el caso de que el dispositivo de LNS esté autentificado. Existen indicadores de mandatos adicionales que no aparecen en este ejemplo. Para obtener más detalles, consulte “Configuración de la autentificación de PPP” en el capítulo “Utilización de interfaces de Point-to-Point Protocol” de la publicación *Guía del usuario de software*.

b. Añada usuarios que deban autentificarse en el LNS. Existen indicadores de mandatos adicionales que no aparecen en este ejemplo. Consulte el mandato Add en el capítulo “The CONFIG Process (CONFIG - Talk 6) and Commands” en la publicación *Guía del usuario de software* para obtener una descripción de la sintaxis y opciones del mandato.

Configuración de LAC:

```
Config> add tunnel-profile
     Enter name:  []? lns.org
Tunneling Protocol? (PPTP, L2F, L2TP): [L2TP]
     Enter local hostname: []? lac.org
     set shared secret? (Yes, No): [No] Y
     Shared secret for tunnel authentication:
     Enter again to verify:
     Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.2

            Tunnel name: lns.org
               TunnType: L2TP
               Endpoint: 1.1.1.1
               Hostname: lac.org

     User 'lns.org' has been added
     Config>
     Config> add dev dial-in  a
```

Nota: Se utiliza para establecer una llamada física.

5. Configure los clientes de direccionador de L2T. El ejemplo siguiente muestra una conexión de caja a caja de L2TP utilizando la función de cliente de direccionador de L2TP. Esta conexión se establece en una dirección y se lleva a cabo a petición.

Configuración de cliente:

```
Config> add tunnel-profile
     Enter name:  []? lns.org
Tunnel Protocol? (PPTP, L2T, L2TP): [L2TP]
     Enter local hostname: []? client.org
     set shared secret? (Yes, No): [No] Y
     Shared secret for tunnel authentication:
     Enter again to verify:
     Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.1

            Tunnel name: lns.org
               TunnType: L2TP
               Endpoint: 1.1.1.1
               Hostname: client.org

     User 'lns.org' has been added
     Config>
     Config> add dev layer-2-tunneling
     Config> net 10
     L2TP 10> set connection-direction outbound
     L2TP 10> set idle 30
     L2TP 10> set remote-hostname lns.org
     L2TP 10> encapsulator
     PPP 10> set name donald  a
     PPP 10> exit
     L2TP 10> exit
     Config>
```

Nota: Establezca el nombre de autentificación en el caso de que se autentifique el dispositivo de cliente. Existen indicadores de mandatos adicionales que no aparecen en este ejemplo. Para obtener detalles, consulte “Configuración de la autentificación de PPP” en la publicación *Guía del usuario de software*.

.

Configuración de LNS:

```
Config> add tunnel-profile
     Enter name:  []? client.org
Tunneling Protocol? (PPTP, L2F, L2TP): [L2TP]
     Enter local hostname: []? lns.org
     set shared secret? (Yes, No): [No] Y
     Shared secret for tunnel authentication:
     Enter again to verify:
     Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.2

            Tunnel name: client.org
               TunnType: L2TP
               Endpoint: 1.1.1.2
               Hostname: lns.org

     User 'client.org' has been added
     Config>
     Config> add dev layer-2-tunneling
     Config> net 10
     L2TP 10> set connection-direction inbound
     L2TP 10> set remote-hostname client.org
     Config>
     Config> add ppp-user donald  b
     Config>
```

Nota: **b**— Añada usuarios que deban autentificarse en el LNS. Existen indicadores de mandatos adicionales que no aparecen en este ejemplo. Para obtener más detalles, consulte “**add** Config command” en la publicación *Guía del usuario de software* .

6. Configure los distintos parámetros de L2T de la característica utilizando los mandatos **set** y **enable**, si lo desea.

```
Layer-2-Tunneling Config>set ?
Layer-2-Tunneling Config>enable ?
```

7. Configure los parámetros de PPP para todas las redes L2 que estén establecidas para entrada y *cualquier* nombre de sistema principal de túnel de entrada utilizando el mandato encapsulator, si lo desea.

```
Layer-2-Tunneling Config>encapsulator
PPP-L2TP Config>
```

   Cuando finalice la configuración de PPP, entre **exit** para volver al entorno de configuración de la característica L2T.

Configuración y supervisión de protocolos de Función de túnel de la capa 2

Este capítulo describe la configuración de la Función de túnel de la capa 2 (L2T) y los mandatos operativos. L2T incluye Layer 2 Tunneling Protocol (L2TP), Layer 2 Forwarding Protocol (L2F) y Point-to-Point Tunneling Protocol (PPTP). Este capítulo contiene las secciones siguientes:

Acceso al indicador de mandatos de configuración de interfaz L2T

Para acceder al indicador de mandatos de configuración de la interfaz de L2T:

1. Entre **talk 6** en el indicador de mandatos OPCON (*).
2. Entre **add dev layer-2-tunneling** en el indicador de mandatos `Config>` (o utilice el mandato **add l2–nets**). Consulte "Add" en la página 428).
3. Entre **n** *número-interfaz* en el indicador de mandatos `Config>`.

```
Config> add device layer-2-tunneling
Enter the number of Layer-2-Tunneling interfaces [1]
Adding device as interface 8
Defaulting Data-link protocol to PPP
Config> n 8
Session configuration
L2T config:   8>
```

Mandatos de configuración de interfaz de Función de túnel de L2

La Tabla 52 en la página 426 resume los mandatos de configuración de interfaz L2T. Entre estos mandatos en el indicador de mandatos `L2T Config n>` (donde *n* es el número de red).

Tabla 52. Mandatos de configuración de interfaz de Función de túnel de L2

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Disable	Inhabilita las llamadas de salida.
Enable	Habilita las llamadas de salida.
Encapsulator	Le permite configurar parámetros de PPP para la interfaz L2T. **Nota:** La opción encapsulador sólo está disponible si una interfaz tiene configurado un nombre de sistema principal remoto.
List	Visualiza información sobre la interfaz L2T.
Set	Le permite establecer varios parámetros de interfaz L2T.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Disable

Utilice el mandato **disable** para inhabilitar llamadas de salida desde el concentrador del acceso a L2TP (LAC).

Sintaxis:

disable outbound-calls-from-lac

outbound-calls-from-lac
Impide que el LNS inicie una señal de marcación desde el LAC a través de un túnel L2TP.

Enable

Utilice el mandato **enable** para habilitar llamadas de salida desde el concentrador del acceso a L2TP (LAC). Este mandato sólo debe utilizarse con L2TP.

Sintaxis:

enable outbound-calls-from-lac

outbound-calls-from-lac
Permite que el LNS inicie una señal de marcación desde el LAC a través de un túnel L2TP.

Ejemplo:

```
L2T 10> enable outbound-call-from-lac
        Outbound Call Type (ISDN, V34)? [ISDN]
        Outbound calling address: 1234
        Outbound calling subaddress:
L2T 10>
```

Encapsulator

Utilice el mandato **encapsulator** para configurar los parámetros de PPP para la interfaz L2T.

Sintaxis:

encapsulator

Este mandato sólo está disponible cuando se ha configurado un nombre de sistema principal remoto. Para obtener una lista de los mandatos disponibles en el

indicador de mandatos `ppp-L2tp config>`, consulte “Encapsulator” en la página 431.

List

Utilice el mandato **list** para visualizar el estado de varios parámetros de configuración de interfaz L2T.

Sintaxis:

list

```
Layer-2-Tunneling Config>list
CONNECTION TYPE
---------- -----
  Connection Direction            INBOUND
  Remote Tunnel Hostname           *ANY*
```

Set

Utilice el mandato set para configurar los parámetros operativos de interfaz L2T.

Sintaxis:

set any-remote-hostname
connection-direction
idle
remote-hostname

any-remote-hostname
Borra el nombre de sistema principal remoto de salida e inhabilita la correspondencia de nombre de sistema principal remoto de entrada en la red.

connection-direction [inbound] o [outbound] o [both]
Especifica si puede iniciar la conexión el similar (entrada), el dispositivo local (salida) o el similar o el dispositivo local (ambos) en esta red. Si especifica ambos, no puede especificar cero para el tiempo de desocupado.

Valor por omisión: entrada

idle-time *segundos*
Especifica el número de segundos de inactividad después del cual la función de túnel de L2 desconectará la sesión de túnel en esta red. Un valor de cero indica que el túnel es fijo y no debe desconectarse.

Rango válido: 0 a 1024

Valor por omisión: 0

remote-hostname *nombre-sispral*
Especifica el nombre de sistema principal de túnel del similar.

Para un túnel de salida, el nombre de sistema principal especifica un perfil de túnel configurado en un subsistema AAA. Debe ser el nombre de sistema principal de túnel que utiliza el similar para identificarse a sí mismo.

Para un túnel de entrada, sólo los similares de túnel que se identifican a sí mismos mediante este nombre de sistema principal pueden conectarse a esta interfaz.

Valores válidos: Cualquier nombre de 1 a 64 caracteres ASCII

Valor por omisión: *Nombre*

Acceso al indicador de mandatos de configuración de la Función de túnel de L2

Para acceder al indicador de mandatos de configuración de la característica Función de túnel L2:

1. Entre **talk 6** en el indicador de mandatos OPCON (*).
2. Entre **feature layer-2-tunneling** en el indicador de mandatos `Config>`.

Mandatos de configuración de la característica Función de túnel de L2

La Tabla 53 resume los mandatos de configuración de la característica función de túnel de L2 y el resto de esta sección explica los mandatos. Entre estos mandatos en el indicador de mandatos `Layer-2-Tunneling Config>`.

Tabla 53. Mandatos de configuración de la característica Función de túnel de L2

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Add	Añade redes y similares de función de túnel de L2.
Disable	Inhabilita funciones de túnel de L2.
Enable	Habilita funciones de túnel de L2.
Encapsulator	Le permite configurar parámetros PPP para todas las redes de función de túnel de L2 que no están configurados con un nombre de sistema principal remoto (ANY).
List	Visualiza información sobre la configuración de función de túnel de L2.
Set	Le permite establecer almacenamientos intermedios, la ventana de recepción de llamadas y otros parámetros de función de túnel de L2.
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 Redes L2. Hace falta una Red L2 para cada sesión PPP simultánea que finaliza en este direccionador. El final de una sesión PPP de túnel es el punto final de LNS del túnel.

Sintaxis:

`add` L2-nets

L2-nets

Nota: Este mandato puede entrarse totalmente en minúsculas. El carácter inicial aparece en mayúsculas para una mayor claridad.

Añade Redes L2 a la configuración de función de túnel de L2. Hace falta una Red L2 para cada sesión PPP simultánea que debe finalizaren este direccionador. Si este direccionador debe utilizarse exclusivamente como un LAC, no son necesarias Redes L2 no virtuales. Cuando entre este mandato, se le solicitará el número de redes adicionales y si deben añadirse direcciones IP para cada red L2.

El número de redes adicionales hace referencia a cuántas redes se añaden automáticamente en este momento. Estas redes son además de las Redes L2 que ya existen.

La adición de direcciones IP sin numerar para cada Red L2 añade automáticamente entradas de IP sin numerar a la tabla de direccionamiento de IP para cada una de las Redes L2. Las direcciones IP sin numerar son la modalidad preferida de operación. Si necesita direcciones numeradas para las Redes L2, puede modificarlas en el entorno de configuración de protocolo IP (hace referencia al capítulo titulado “Configuración de IP” en la publicación *Consulta de configuración y supervisión de protocolos Volumen 1*).

Disable

Utilice el mandato **disable** para inhabilitar funciones de túnel de L2.

Sintaxis:

disable	fixed-ip-source-address
	fixed-udp-source-port
	force-chap-challenge
	hiding-for-pap-attributes
	L2f
	L2tp
	pptp
	proxy-auth
	proxy-lcp
	sequencing
	tunnel-auth

fixed-ip-source-address
Hace que el direccionador inhabilite la dirección de origen especificada.

fixed-udp-source-port
Borra la utilización de un puerto UDP fijo. La inhabilitación de este parámetro le obliga a configurar filtros de Seguridad de IP entre el LAC y el LNS por dirección IP.

force-chap-challenge
Inhabilita la recomprobación CHAP de LNS de un cliente. Puede que necesite inhabilitar la recomprobación CHAP si el cliente PPP tiene dificultad con las reconfrontaciones CHAP.

hiding-for-pap-attributes
Inhabilita el cifrado de información PAP Proxy entre el LAC y el LNS.

L2f Inhabilita el protocolo L2F en este direccionador.

L2tp
Inhabilita el protocolo L2TP en este direccionador.

pptp
Inhabilita el protocolo PPTP en este direccionador.

proxy-auth
Inhabilita el envío de autentificación proxy de PPP del LAC al LNS.

proxy-lcp
Inhabilita el envío de información de LCP del LAC al LNS.

sequencing
Inhabilita la secuencia en el canal de datos.

tunnel-auth
Inhabilita la autentificación de similar de túnel basada en un secreto compartido para este direccionador.

Enable

Utilice el mandato **enable** para habilitar funciones de túnel de L2.

Sintaxis:

enable
- fixed-ip-source-address
- fixed-udp-source-port
- force-chap-challenge
- hiding-for-pap-attributes
- L2f
- L2tp
- pptp
- proxy-auth
- proxy-lcp
- sequencing
- tunnel-auth

fixed-ip-source-address
Hace que el direccionador responda con una dirección de origen igual que la dirección de destino de entrada.

fixed-udp-source-port
La habilitación de este parámetro le permite configurar filtros de Seguridad de IP por puerto UDP para función de túnel de L2 de modo que puede cifrar o autentificar fácilmente tráfico de función de túnel de L2. Establece el puerto UDP en 1701 para L2TP.

force-chap-challenge
Habilita la recomprobación CHAP de LNS de un cliente incluso si el LNS recibe un CHAP proxy. Esto es preferible desde el punto de vista de la seguridad, si se sabe que el cliente puede manejar dicha recomprobación sin problemas.

hiding-for-pap-attributes
Habilita el cifrado de información PAP Proxy entre el LAC y el LNS.

L2f Habilita L2F en este direccionador.

L2tp
Habilita L2TP en este direccionador.

pptp
Habilita PPTP en este direccionador.

proxy-auth
Habilita el envío de autentificación proxy de PPP del LAC al LNS.

proxy-lcp
Habilita el envío de información de LCP del LAC al LNS.

sequencing
Habilita la secuencia en el canal de datos.

tunnel-auth
Habilita autentificación de similar de túnel basada en un secreto compartido para este direccionador.

Encapsulator

Utilice el mandato **encapsulator** para acceder al indicador de mandatos `ppp-L2tp config>` para configurar los parámetros de PPP para todas las interfaces de Función de túnel de Capa 2 que están configuradas como entrada y *cualquier* nombre de sistema principal remoto.

Sintaxis:

e**ncapsulator**

List

Utilice el mandato **list** para visualizar el estado de los distintos parámetros de configuración de función de túnel de L2.

Sintaxis:

list

```
Layer-2-Tunneling Config>list
GENERAL ADMINISTRATION
------- --------------
  L2TP                                = Enabled
  L2F                                 = Disabled
  PPTP                                = Disabled
  Maximum number of tunnels           = 20
  Maximum number of calls (total)     = 50
  Buffers Requested                   = 300

CONTROL CHANNEL SETTINGS
------- ------- --------
  Tunnel Auth                         = Enabled
  Tunnel Rcv Window                   = 4
  Retransmit Retries                  = 6
  Local Hostname                      = Host6

DATA CHANNEL SETTINGS
---- ------- --------
  Force CHAP Challenge (extra security)= Disabled
  Hiding for PAP Attributes           = Disabled
  Hardware Error Polling Period (Sec)  = 120
  Sequencing                          = Enabled

MISCELLANEOUS
-------------
  SEND PROXY-LCP FROM LAC             = Enabled
  SEND PROXY-AUTH FROM LAC            = Enabled
  Fixed UDP Source Port (1701)        = Enabled
  Fixed Source IP Address             = Enabled
```

Set

Utilice el mandato set para configurar los parámetros operativos de la función de túnel de L2.

Sintaxis:

s**et** b**uffers**
e**rror-check-direction**
h**ost-lookup-password**

local-hostname
max-calls
max-tunnels
transmit-retries
tunnel-rcv-window

buffers
Especifica el número de almacenamientos intermedios de función de túnel de L2. Si no existe suficiente memoria para cumplir la petición, sólo una parte de los almacenamientos intermedios estará disponible en el rearranque. Para confirmar la cantidad de memoria mientras L2T está activa, utilice el mandato **memory** (consulte “Memory” en la página 437).

Rango válido: 1 a 4000

Valor por omisión: Depende del modelo:

Modelo	Valor por omisión
x2x, xSx, 1Ux	30
x4x	100

error-check-period [seconds]
Especifica el período de sondeo de errores de hardware del LAC. Cada período de sondeo dará como resultado un mensaje de Notificación de error de WAN que se transmitirá desde el LAC al LNS. El rango es de 60 a 65.000 segundos.

Valor por omisión: 120 segundos.

host-lookup-password
Especifica el secreto compartido para la autorización de túnel RADIUS. Debe coincidir con el secreto configurado en el servidor.

Valor por omisión: Ninguno.

local-hostname
Especifica la serie de caracteres del nombre de sistema principal que identifica al direccionador local que se envía a los mensajes de configuración de túnel.

Valor por omisión: IBM

max-calls
Especifica el número máximo de llamadas a través de túneles que se pueden activar en un momento determinado como LAC o LNS.

Rango válido: Depende del modelo:

Modelo	Rango
x2x, xSx, 1Ux	1 a 30
x4x	1 a 200

Valor por omisión: Depende del modelo:

Modelo	Valor por omisión
x2x, xSx, 1Ux	10
x4x	30

max-tunnels
Especifica el número máximo de túneles que pueden estar activos en un momento determinado como LAC o LNS.

Rango válido: Depende del modelo:

Modelo	Rango
x2x, xSx, 1Ux	1 a 30
x4x	1 a 200

Valor por omisión: Depende del modelo:

Modelo	Valor por omisión
x2x, xSx, 1Ux	10
x4x	30

transmit-retries
Especifica el número de veces que se retransmite un paquete de L2TP en el canal de control antes de que la sesión o el túnel se declaren inactivos y se cierren.

Rango válido: 2 a 100

Valor por omisión: 6

tunnel-rcv-window
Especifica el tamaño de la ventana de recepción de L2TP para el transporte de conexiones de control fiables. Este transporte transmite y recibe los mensajes necesarios para la configuración, eliminación y mantenimiento del túnel o de la sesión.

Rango válido: 1 a 100

Valor por omisión: 4

Acceso al indicador de mandatos de supervisión de Función de túnel de L2

Para acceder al indicador de mandatos de supervisión de función de túnel de L2 :

1. Entre **talk 5** en el indicador de mandatos OPCON (*).
2. Entre **feature layer-2-tunneling** en el indicador de mandatos GWCON (+).

Mandatos de supervisión de Función de túnel de L2

Esta sección resume y, a continuación, describe los mandatos de supervisión de función de túnel de L2. Entre los mandatos en el indicador de mandatos `Layer-2-Tunneling Console>`.

La Tabla 54 en la página 434 resume los mandatos de supervisión de función de túnel de L2.

Tabla 54. Mandatos de supervisión de Función de túnel de L2

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Call	Visualiza estadísticas e información sobre cada llamada en proceso.
Kill	Finaliza un túnel inmediatamente.
Memory	Visualiza la asignación y utilización del almacenamiento intermedio de función de túnel de L2.
Start	Inicia un túnel con otro similar.
Stop	Detiene un túnel y permite que cada similar realice la administración necesaria.
Tunnel	Visualiza estadísticas e información sobre cada túnel existente.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Call

Utilice el mandato **call** para visualizar estadísticas e información sobre llamadas.

Sintaxis:

call errors
physical-errors
queue
state
statistics

errors

Visualiza los errores de transmisión generales que se han producido en las llamadas.

Ejemplo:

```
Layer-2-Tunneling Console> call errors
CallID │ Serial # │ ACK-timeout │ Dropped pkts
 56744 │        1 │           0 │         0
```

CallID

El identificador local asociado con esta llamada.

Serial #

El número utilizado para registrar esta llamada.

ACK-timeout

El número de veces que una notificación de tiempo de espera excedido se ha recibido desde el similar.

Dropped pkts

El número de paquetes que se han declarado perdidos para esta llamada. Estos paquetes deberían haberse recibido, pero el similar los han señalado como perdidos.

physical-errors

Visualiza los errores en los datos que se han producido en las llamadas.

Ejemplo:

```
Layer-2-Tunneling Console> call physical-errors
CallID │ Serial# │ CRC    │framing│   HW    │ buffer│timeout│ align-│ time since
       │         │ Errors│ Errors│overrun│overrun│ Errors│ ment  │ updated
 56744 │       1 │     0 │     0 │     0 │     0 │     0 │     0 │
```

CallID
El identificador local asociado con esta llamada.

Serial #
El número utilizado para registrar esta llamada.

CRC Errors
El número de paquetes en los que el CRC no ha coincidido.

framing errors
El número de paquetes con un error de trama.

HW overrun
El número de veces que se ha producido un desbordamiento de hardware.

buffer overrun
El número de veces que se ha producido un desbordamiento de almacenamiento intermedio.

timeout errors
El número de veces que una interfaz ha excedido el tiempo de espera.

alignment
El número de veces que se ha producido un error de alineación.

time since updated
El tiempo transcurrido desde el último sondeo de errores.

queue
Visualiza información sobre la cola para cada llamada.

Ejemplo:

```
Layer-2-Tunneling Console> call queue
CallID | Serial # |Tx Win|Rx Win|   Ns   |   Nr   |Rx Q|Tx Q|priority| out Q
 56744 |       1  |    4 |    4 |    100 |   200  |  0 |  0 |     0  |    0
```

CallID
El identificador local asociado con esta llamada.

Serial #
El número utilizado para registrar esta llamada.

Tx Win
La ventana de recepción máxima del similar para los datos.

Rx Win
La ventana de transmisión máxima local.

Ns El número de secuencia del paquete siguiente que debe enviarse a esta llamada.

Nr El número de secuencia del paquete siguiente que se espera recibir para esta llamada.

Rx Q
El número actual de paquetes en la cola de recepción.

Tx Q
El número actual de paquetes en la cola de transmisión.

priority
El número de paquetes PPP de prioridad en espera de ser transmitidos por L2TP.

out Q
El número de paquetes PPP corrientes en espera de ser transmitidos por L2TP.

state
Visualiza el estado actual de cada llamada.

Ejemplo:

```
Layer-2-Tunneling Console> call state
CallID | Serial # | Net #  |    State    | Time Since Chg | PeerID | TunnelID
 56744 |       1  |     2  | Established |   00:00:00     |  345   | 45678
```

CallID
El identificador local asociado con esta llamada.

Serial #
El número utilizado para registrar esta llamada.

Net #
El número de dispositivo asociado con esta llamada. Para una llamada de LNS, es la Red L2. Para una llamada de LAC, es el dispositivo PPP que ha recibido la llamada inicial.

State
El estado de llamada actual. Los estados de llamada válidos son:

Established
Preparada para tráfico de red de túnel.

Idle
La llamada está desocupada.

Wait Cs Answer
En espera de que se abra el enlace de comunicaciones.

Wait Reply
En espera de una respuesta desde el similar.

Wait Tunnel
En espera del establecimiento de túnel.

Time since chg
El tiempo transcurrido desde el último cambio de estado.

PeerID
El ID de llamada del similar.

TunnelID
El túnel local asociado con esta llamada.

statistics
Visualiza estadísticas sobre la transmisión de datos para cada llamada.

Ejemplo:

```
Layer-2-Tunneling Console> call statistics
CallID | Serial # | Tx Pkts | Tx Bytes | Rx Pkts | Rx Bytes |  RTT  | ATO
 56744 |       1  |     34  |    1056  |     45  |    1567  |   10  | 34
```

CallID
El identificador local asociado con esta llamada.

Serial #
El número utilizado para registrar esta llamada.

Tx Pkts
El número de paquetes transmitidos para esta llamada.

Tx Bytes
El número de bytes transmitidos para esta llamada.

Rx Pkts
El número de paquetes recibidos para esta llamada.

Rx Bytes
El número de bytes recibidos para esta llamada.

RTT
El tiempo de ida y vuelta actualmente calculado para esta llamada.

ATO
El tiempo de adaptación actualmente calculado para esta llamada.

Kill

Utilice el mandato **kill** para finalizar inmediatamente un túnel. Este mandato libera todos los recursos locales para un túnel, forzando de este modo el final de la conexión. No se envía ninguna notificación del final del túnel al similar.

Nota: Utilice este mandato solamente si el mandato **stop** no puede detener un túnel.

Sintaxis:

kill tunnel *id-túnel*

tunnel *id-túnel*
Especifica el túnel que debe finalizarse.

Memory

Utilice el mandato **memory** para visualizar la utilización de memoria actual de L2TP.

Sintaxis:

m**emory**

Ejemplo:

```
Layer-2-Tunneling Console> mem
Number of layer-2-tunneling buffers: Requested = 2000, Total = 1200, Free = 1000
```

En este ejemplo, se han configurado 2000 almacenamientos intermedios pero sólo se han podido asignar 1200. Actualmente, 200 almacenamientos intermedios están en uso y quedan 1000 libres.

Start

Utilice el mandato **start** para iniciar un túnel con otro similar.

Sintaxis:

start **tunnel** *nombre-sispral*

(si no se especifica ningún parámetro se le solicita el nombre de sistema principal)

tunnel*nombre-sispral*
El nombre del sistema principal con el cual L2T establece el túnel.

Stop

Utilice el mandato **stop** para detener un túnel. Cualquier borrado necesario se completa antes de finalizar el túnel.

Sintaxis:

stop tunnel *id-túnel*

tunnel *id-túnel*
Especifica el túnel que debe finalizarse.

Tunnel

Utilice el mandato **tunnel** para visualizar estadísticas e información sobre todos los túneles.

Sintaxis:

tunnel
- call
- errors
- peer
- queue
- state
- statistics
- transport

calls
Visualiza todos los túneles y el estado de llamada para cada llamada dentro de cada túnel.

errors
Visualiza los errores que se han producido en un túnel.

Ejemplo:

```
Layer-2-Tunneling Console> tunnel errors
Tunnel ID | Type |ACK-timeouts
 96785    | L2TP |    0
 43690    | PPTP |    2
 96785    | L2F  |    0
```

Tunnel ID
El identificador local asociado con un túnel.

Type
El tipo de protocolo de túnel que se utiliza.

ACK-timeouts
El número de veces que una notificación de tiempo de espera excedido se ha recibido desde el similar.

peer
Visualiza los túneles y los similares asociados con los túneles.

Ejemplo:

```
Layer-2-Tunneling Console> tunnel peer
Tunnel ID | Type | Peer ID | Peer Hostname
 96785    | L2TP |   89777 | peer1
 11264    | L2F  |   46538 | peer2
 34653    | L2F  |   11209 | peer3
 87511    | PPTP |   55377 | peer4
```

Tunnel ID
El identificador local asociado con un túnel.

Type
El tipo de protocolo de túnel que se utiliza.

Peer ID
El identificador de túnel del similar asignado a este túnel.

Peer Hostname
El nombre de sistema principal del similar tal como aparece en la base de datos local.

queue
Visualiza información sobre la cola para cada túnel.

Ejemplo:

```
Layer-2-Tunneling Console> tunnel queue
Tunnel ID │ Type │ Rx Win │ Tx Win │   Ns   │   Nr   │ Rx Q │ Tx Q
 96785    │ L2TP │      4 │      4 │      5 │      6 │    0 │    0
 76488    │ L2F  │      4 │      4 │      5 │      6 │    0 │    0
 22209    │ PPTP │      4 │      4 │      5 │      6 │    0 │    0
```

Tunnel ID
El identificador local asociado con un túnel.

Type
El tipo de protocolo de túnel que se utiliza.

Rx Win
El número máximo local de paquetes que constituyen la ventana de recepción.

Tx Win
El número máximo de paquetes del similar que constituyen la ventana de recepción.

Ns El número de secuencia del siguiente paquete que debe enviarse.

Nr El número de secuencia del siguiente paquete que debe recibirse.

Rx Q
El número de paquetes que existen actualmente en la cola de recepción.

Tx Q
El número de paquetes que existen actualmente en la cola de transmisión.

state
Visualiza el estado actual de todos los túneles.

Ejemplo:

```
Layer-2-Tunneling Console> tunnel state
Tunnel ID │ Type │ Peer ID │    State    │ Time Since Chg │ # Calls │ Flags
 17404    │ PPTP │  0      │ Established │   00:00:00     │      1  │  0
 96785    │ L2TP │  0      │ Established │   00:02:05     │      2  │  0
 38237    │ L2F  │  0      │ Established │   00:00:00     │      1  │  0
```

Tunnel ID
El identificador local asociado con un túnel.

Type
El tipo de protocolo de túnel que se utiliza.

Peer ID
El identificador de túnel del similar asignado a este túnel.

State
El estado del túnel actual. Los estados de túnel válidos son:

Established
El túnel está establecido.

Idle
El túnel está desocupado.

Wait Ctrl Reply
El sistema principal espera una respuesta desde el similar.

Wait Ctrl Conn
El sistema principal espera una indicación de conexión.

Time since chg
El tiempo transcurrido desde el último cambio de estado.

 # Calls
El número de llamadas activas en este túnel.

Flags
Los distintivos utilizados para controlar los mensajes de conexión en este túnel.

statistics
Visualiza las estadísticas asociadas con los túneles.

Ejemplo:

```
Layer-2-Tunneling Console> tunnel statistics
Tunnel ID │ Type │ Tx Pkts │ Tx Bytes │ Rx Pkts │ Rx Bytes │  RTT  │ ATO
 96785    │ L2TP │       4 │       78 │       5 │       89 │    10 │ 31
 96366    │ L2F  │    9344 │    34578 │     305 │     4300 │    10 │ 31
 12344    │ PPTP │      24 │      478 │     115 │     2745 │    10 │ 31
```

Tunnel ID
El identificador local asociado con un túnel.

Type
El tipo de protocolo de túnel que se utiliza.

Tx Pkts
El número de paquetes transmitidos.

Tx Bytes
El número de bytes transmitidos.

Rx Pkts
El número de paquetes recibidos.

Rx Bytes
El número de bytes recibidos.

RTT
El tiempo de ida y vuelta actualmente calculado para los mensajes de conexión de control de túnel.

ATO
El tiempo de espera excedido de adaptación calculado actualmente para los mensajes de conexión de control de túnel.

transport
Visualiza información de UDP sobre los túneles.

Ejemplo:

```
Layer-2-Tunneling Console> tunnel transport
Tunnel ID | Type | Peer IP Address | UDP Src | UDP Dest
 96785    | L2TP |  11.0.0.102     |  1056   |   1089
 30000    | L2F  |  11.0.0.104     |  1058   |   1090
 45772    | PPTP |  11.4.4.027     |  1345   |   1020
```

Tunnel ID
El identificador local asociado con un túnel.

Type
El tipo de protocolo de túnel que se utiliza.

Peer IP address
La dirección IP del similar para este túnel.

UDP Src
El puerto de origen UDP para este túnel.

UDP Dest
El puerto de destino UDP para este túnel.

Soporte de reconfiguración dinámica de la función de túnel de L2

Esta sección describe la reconfiguración dinámica (DR) en lo que afecta a los mandatos de Talk 6 y Talk 5.

Delete interface de CONFIG (Talk 6)

La Función de túnel de la capa 2 soporta el mandato de CONFIG (Talk 6) **delete interface** sin restricciones.

Activate interface de GWCON (Talk 5)

La Función de túnel de la capa 2 soporta el mandato de GWCON (Talk 5) **activate interface** con la consideración siguiente:

No existen limitaciones adicionales en otras interfaces PPP.

Todos los cambios de configuración de la Función de túnel de la capa 2 se activan automáticamente excepto en los casos siguientes:

Mandatos cuyos cambios no activa el mandato de GWCON (Talk 5) activate interface
CONFIG, net, enable ccp **Nota:** La compresión no se habilitará si ésta es la primera red PPP con CCP habilitado.
CONFIG, net, set lcp options (opción mru) **Nota:** MRU no se establecerá en un valor mayor que el tamaño de almacenamiento intermedio asignado para el direccionador en el rearranque.

Reset interface de GWCON (Talk 5)

La Función de túnel de la capa 2 soporta el mandato de GWCON (Talk 5) **reset interface** con la consideración siguiente:

No existen limitaciones adicionales en otras interfaces PPP.

Todos los cambios de configuración de la Función de túnel de la capa 2 se activan automáticamente excepto en los casos siguientes:

Mandatos cuyos cambios no activa el mandato de GWCON (Talk 5) reset interface
CONFIG, net, enable ccp **Nota:** La compresión no se habilitará si ésta es la primera red PPP con CCP habilitado.
CONFIG, net, set lcp options (opción mru) **Nota:** MRU no se establecerá en un valor mayor que el tamaño de almacenamiento intermedio asignado para la interfaz PPP en el rearranque.

Mandatos de cambio inmediato de CONFIG (Talk 6)

La Función de túnel de la capa 2 soporta los mandatos de CONFIG siguientes que cambian inmediatamente el estado operativo del dispositivo. Estos cambios se guardan y se conservan si se vuelve a cargar o se reinicia el dispositivo o si se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
CONFIG, feature layer-2-tunneling, disable fixed-ip-source-address
CONFIG, feature layer-2-tunneling, disable fixed-udp-source-port
CONFIG, feature layer-2-tunneling, disable force-chap-challenge
CONFIG, feature layer-2-tunneling, disable hiding-for-pap-attributes
CONFIG, feature layer-2-tunneling, disable proxy-auth
CONFIG, feature layer-2-tunneling, disable proxy-lcp
CONFIG, feature layer-2-tunneling, disable sequencing
CONFIG, feature layer-2-tunneling, disable tunnel-auth
CONFIG, feature layer-2-tunneling, enable fixed-ip-source-address
CONFIG, feature layer-2-tunneling, enable fixed-udp-source-port
CONFIG, feature layer-2-tunneling, enable force-chap-challenge
CONFIG, feature layer-2-tunneling, enable hiding-for-pap-attributes
CONFIG, feature layer-2-tunneling, enable proxy-auth
CONFIG, feature layer-2-tunneling, enable proxy-lcp
CONFIG, feature layer-2-tunneling, enable sequencing
CONFIG, feature layer-2-tunneling, enable tunnel-auth
CONFIG, feature layer-2-tunneling, set error-check-period
CONFIG, feature layer-2-tunneling, set host-lookup-password
CONFIG, feature layer-2-tunneling, set local-hostname
CONFIG, feature layer-2-tunneling, set transmit-retries
CONFIG, feature layer-2-tunneling, set tunnel-rcv-window
CONFIG, add tunnel-profile

Mandatos no reconfigurables dinámicamente

La tabla siguiente describe los mandatos de configuración de la Función de túnel de la capa 2 que no se pueden cambiar dinámicamente. Para activar estos mandatos, es necesario volver a cargar o reiniciar el dispositivo.

Mandatos
CONFIG, feature layer-2-tunneling, enable l2f
CONFIG, feature layer-2-tunneling, enable l2tp
CONFIG, feature layer-2-tunneling, enable pptp
CONFIG, feature layer-2-tunneling, disable l2f
CONFIG, feature layer-2-tunneling, disable l2tp
CONFIG, feature layer-2-tunneling, disable pptp
CONFIG, feature layer-2-tunneling, set buffers
CONFIG, feature layer-2-tunneling, set max-calls
CONFIG, feature layer-2-tunneling, set max-tunnels

Utilización del Conversor de direcciones de red

El Conversor de direcciones de red (NAT) y su extensión Conversor de puertos y direcciones de red (NAPT) pueden ampliar el número de direcciones IP disponibles para una organización y pueden evitar que los usuarios de una red pública conozcan algunas de las direcciones de la red privada. El NAT funciona utilizando direcciones IP públicas para representar direcciones IP privadas.

Las direcciones IP públicas son las direcciones válidas de los sistemas principales de la red pública de IP y deben ser exclusivas dentro de la red pública. Si la red pública es Internet, las direcciones IP públicas deben ser direcciones de Internet proporcionadas por el Centro de información de la red (NIC).

Las direcciones privadas las conoce el direccionador, pero no la red pública. Las direcciones dentro de cada red privada deben ser exclusivas; sin embargo, la misma dirección puede estar duplicada en dos redes privadas diferentes. Las direcciones privadas se asignan a sistemas principales dentro de redes de apéndice. Las redes de apéndice son redes que tienen acceso a la red pública únicamente a través de un direccionador.

El NAT amplía el número de direcciones IP disponibles de varias maneras:

- Permite que cada dirección pública represente varias direcciones privadas efectuando una utilización rotativa de las direcciones públicas.
- Permite la duplicación de las direcciones siempre y cuando cada dirección duplicada se utilice en una red privada diferente.
- Permite que el administrador de la red utilice cualquier dirección IP en las redes privadas, en lugar de direcciones de NIC que se están convirtiendo en recursos limitados.

La utilización de direcciones privadas también oculta estas direcciones del mundo exterior. Esta característica de NAT hace que sea útil como un tipo de cortafuegos para hacer que las direcciones privadas no se conozcan.

Importante: Tal como se afirma en la sección 5.4 del Borrador de Internet que define el NAT, “cualquier aplicación que contiene (y utiliza) la dirección IP (y puerto TCP/UDP, en el caso de NAPT) dentro de la aplicación no funcionará a través de NAT...”. Debe tenerse en cuenta que DLSw y XTP toman decisiones basándose en las direcciones IP de punto final — específicamente qué asociado tiene la dirección más alta. Puesto que la aplicación (como por ejemplo DLSw o XTP) que se ejecuta a través del NAT cree que esta dirección es la dirección privada, pero la aplicación asociada en el otro direccionador cree que la dirección de la aplicación es la dirección pública, se pueden tomar decisiones incorrectas.

Consulte la Figura 33 en la página 446 para ver un dibujo de una estación de trabajo en una red de apéndice. En este ejemplo, la red de apéndice consiste en una subred IP que tiene la dirección IP 10.33.96.0 con la máscara de red 255.255.255.0.

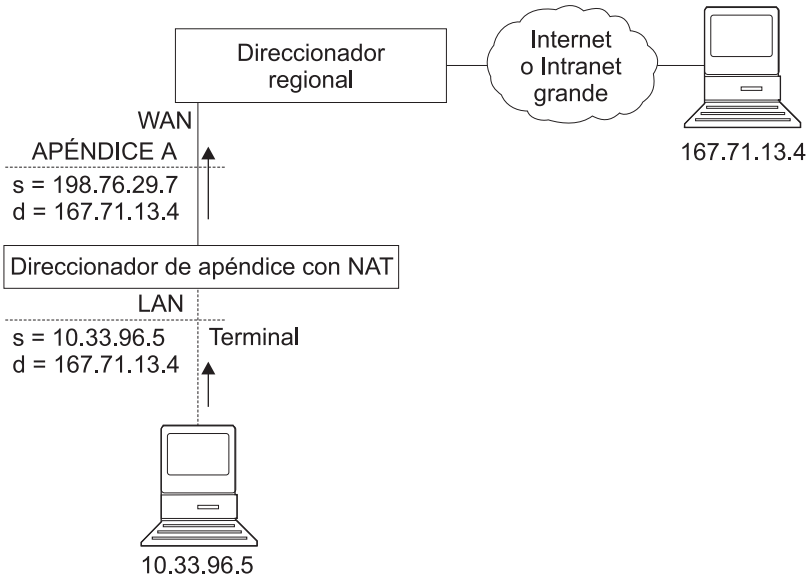


Figura 33. Red que ejecuta el NAT

Para utilizar el NAT, el administrador de la red asigna una o más direcciones IP públicas a una agrupación de direcciones públicas del 2210 y asigna una dirección IP privada a cada estación de trabajo de la red de apéndice. Las direcciones IP públicas se asignan a una *agrupación de reserva* y las direcciones IP privadas se asignan al *rango de conversión*.

La función NAT primero enlaza la dirección privada de una estación en la red privada con una de las direcciones públicas. Enlazar significa que cada paquete con la dirección privada se convierte en la dirección IP pública cuando el paquete va a salir. Los paquetes de entrada tienen la dirección IP pública como destino. El NAT reconoce la dirección pública, la convierte en la dirección IP privada y reenvía el paquete. Cuando el tráfico se detiene, el enlace se mantiene hasta que un temporizador que se puede establecer excede el tiempo de espera. En este punto, el NAT finaliza el enlace y hace que la dirección pública esté disponible para ser reutilizada.

En este ejemplo, un paquete se transmite desde la dirección de origen privada de envío 10.33.96.5 a una dirección de destino en la Internet, 167.71.13.4. El NAT en el 2210 convierte la dirección privada 10.33.96.5 en la dirección pública 198.76.29.7. Esta conversión oculta la dirección privada 10.33.96.5 a la red pública, de modo que ningún paquete de entrada se dirige directamente a la dirección privada 10.33.96.5. En lugar de ello, los paquetes de entrada de 167.71.13.4 se dirigen a la dirección pública 198.76.29.7. Cuando el direccionador del NAT recibe paquetes dirigidos a 198.76.29.7, el NAT convierte la dirección pública de destino en la dirección privada 10.33.96.5 y reenvía los paquetes.

Conversor de puertos y direcciones de red

La NAPT sólo se puede utilizar para tráfico TCP y UDP. En NAPT, varias direcciones privadas pueden utilizar una sola dirección pública simultáneamente. Mientras que el NAT correlaciona una dirección pública con una dirección privada, la NAPT correlaciona la dirección pública ***y*** el número de puerto público de NAPT con

una dirección privada y número de puerto privado. Sólo se puede configurar una dirección de NAPT para cada agrupación de direcciones públicas.

La NAPT se configura simplemente especificando una dirección pública o una interfaz de Dirección dinámica (que utiliza PPP/IPCP para recuperar una dirección pública) que se utilizará para el tráfico de NAPT. La ventaja de NAPT es que puede habilitar una dirección de la agrupación de direcciones IP públicas para dar soporte a varias direcciones IP privadas simultáneamente.

Correlaciones de direcciones estáticas

Puede que alguna vez desee configurar una estación o un servidor en la red privada al que se pueda acceder directamente desde la red pública. En este caso, debe crear una correlación estática de la dirección privada de la estación con una dirección pública particular. Todos los mensajes de salida de la dirección privada se convierten en la dirección pública designada y todos los mensajes de entrada para la dirección pública designada se reenvían automáticamente a la dirección privada asociada. Existen dos tipos de correlaciones de direcciones estáticas: NAT y NAPT.

Correlación de direcciones estáticas de NAT

En una correlación de NAT, todos los protocolos IP pueden acceder al sistema principal. A continuación se proporciona un ejemplo de la configuración de una correlación de NAT:

Dirección privada	10.1.1.2
Puerto privado	0
Dirección de NAT pública	9.67.1.1
Puerto público	0

Correlación de direcciones estáticas de NAPT

Para especificar una aplicación TCP o UDP, tiene la opción de especificar una correlación de NAPT que incluya un puerto conocido privado. Para una correlación de direcciones estáticas de NAPT, debe configurarse una dirección pública de NAPT. Por ejemplo, para configurar un sistema principal Telnet en la dirección privada 10.1.1.1 para que utilice la dirección pública de NAPT 9.67.1.2, la correlación estática podría configurarse del modo siguiente:

Dirección privada	10.1.1.1
Puerto privado	23
Dirección de NAPT pública	9.67.1.2
Puerto público	23

Los puertos privados y públicos se correlacionan con el puerto 23, que es el puerto conocido públicamente para Telnet. Ahora bien, si el administrador también tiene un servidor FTP (dirección conocida públicamente 21) en la misma dirección privada 10.1.1.1 para correlacionar con la dirección pública de NAPT 9.67.1.2, esta correlación podría ser similar a la siguiente:

Dirección privada	10.1.1.1
Puerto privado	21
Dirección de NAPT pública	9.67.1.2
Puerto público	21

El servidor en la dirección 10.1.1.1 tiene la misma dirección pública de NAPT (9.67.1.2) para ambas aplicaciones, pero la NAPT puede diferenciar entre las dos utilizando números de puerto diferentes (23 y 21). Sin embargo, la NAPT no puede diferenciar entre dos servidores que utilicen la misma dirección pública de NAPT y que tengan la misma aplicación y número de puerto. Por ejemplo, si la dirección pública de NAPT y el puerto conocido públicamente son los mismos para 10.1.1.3 puerto 21 y para 10.1.1.1 puerto 21, la NAPT no puede decidir si debe enviar el tráfico de FTP de entrada al servidor 10.1.1.3 o al servidor 10.1.1.1. Para configurar más de un servidor con la misma dirección y aplicación de NAPT, debe utilizar un puerto que no sea el puerto conocido públicamente en el servidor (por ejemplo, puede iniciar el daemon FTP en el puerto 200).

Establecimiento de filtros de paquete y normas de control de acceso para NAT

Además de identificar el rango de direcciones privadas que deberá convertir NAT o NAPT, el administrador debe establecer filtros de paquete y normas de control de acceso para IP en el 2210. Para la configuración de NAT debe configurar un filtro de paquete de entrada y otro de paquete de salida en la interfaz que está conectada a la red pública. Debe configurar una o más normas de control de acceso para el filtro de paquete de entrada y una o más normas de control de acceso para el filtro de paquete de salida. Las normas de control de acceso de filtro de entrada pasan a NAT los paquetes de entrada con las direcciones públicas definidas apropiadas. Las normas de control de acceso de filtro de salida pasan a NAT los paquetes de salida con las direcciones privadas definidas apropiadas.

Las normas de control de acceso que se aplican para NAT tienen los tipos de norma de control de acceso ***I*** y ***N*** para inclusiva y NAT. Consulte la publicación *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener información sobre cómo configurar los controles de acceso de IP.

Nota: El NAT también se puede configurar junto con un túnel de IPsec. Puede verse un ejemplo de esta configuración en “Configuración de normas de control de acceso de filtro de paquete para el direccionador A” en la página 363.

Ejemplo: Configuración de NAT con filtros de IP y normas de control de acceso

Este ejemplo muestra cómo configurar el NAT para el direccionador de apéndice en la red ilustrada en la Figura 34 en la página 449. Consulte “Configuración y supervisión del Conversor de direcciones de red” en la página 453 para obtener las descripciones de los mandatos.

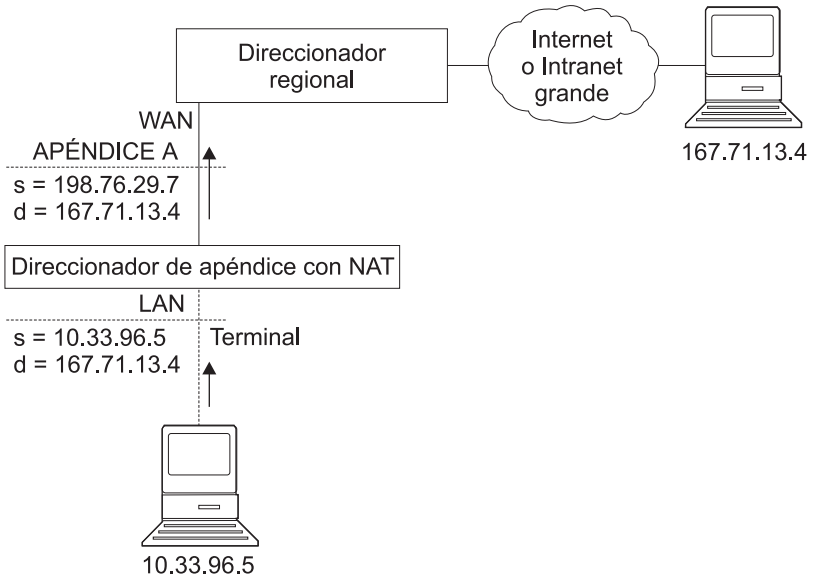


Figura 34. Red que ejecuta el NAT

Siga este procedimiento:

1. Configure agrupaciones de direcciones públicas para que las utilicen el NAT y la NAPT. Para ello, utilice el mandato **reserve**.

   ```
   NAT config> reserve No 198.76.29.7 255.255.255.0 6 pool1 198.76.29.7
   NAT config> reserve No 198.76.29.15 255.255.255.0 3 pool1 0.0.0.0
   ```

   En este ejemplo, se establece una agrupación llamada *pool1*. La dirección de NAPT en la agrupación es 198.76.29.7. Las direcciones 198.76.29.13 y 198.76.29.14 no están disponibles, por lo que la agrupación se configura para excluirlas. Los parámetros entrados son: *dirección-pública, máscara, número-en-grupo, nombre y dirección-napt*. El valor 0.0.0.0 para la dirección de NAPT indica que ninguna de las direcciones de este grupo es la dirección de NAPT. Utilice 0.0.0.0 para la dirección de NAPT en todos los grupos si no configura NAPT para la agrupación.

2. Utilice el mandato **translate** para establecer los rangos de direcciones privadas que deben convertirse mediante las direcciones públicas de pool1. Los parámetros entrados son: *dirección-privada, máscara y nombre*.

   ```
   NAT config> translate 10.33.96.0 255.255.255.0 pool1
   ```

3. Establezca correlaciones estáticas para estaciones dentro de la red privada que deban correlacionarse de modo permanente con una de las direcciones públicas. Los mandatos siguientes identifican a una máquina (10.33.96.5) que recibirá cualquier tipo de tráfico desde la red pública. Una segunda máquina (10.33.96.4) es a la vez un servidor Telnet y HTTP. Los parámetros son *dirección-privada, número-puerto-privado, dirección-pública y numero-puerto-público*. Tenga en cuenta que la dirección de NAPT para pool1 se utiliza como la dirección pública para el sistema principal que se configura con dos números de puerto.

   ```
   NAT config> map 10.33.96.5 0 198.76.29.8 0
   NAT config> map 10.33.96.4 23 198.76.29.7 23
   NAT config> map 10.33.96.4 80 198.76.29.7 80
   ```

4. Habilite el NAT.

   ```
   NAT config> enable NAT
   ```

5. Cree dos filtros de paquete de IP de modo que IP pase paquetes a NAT. Son filtros de paquete de entrada y de paquete de salida para la interfaz 0, que es la interfaz conectada a la red pública.

```
IP Config> add packet-filter outbound out-0 0
IP Config> add packet-filter inbound in-0 0
```

6. Utilice el mandato **update** para llegar al indicador de mandatos `packet-filter 'nombre-filtro' Config>`. Añada una norma de control de acceso para NAT para el filtro de entrada. Los paquetes que se reciben a través de la interfaz pública (red 0) que están destinados a una dirección de la agrupación de direcciones públicas reservadas de el NATP deben pasarse al NAT. El NAT sustituirá la dirección pública (y el puerto público si el paquete está destinado a la dirección de NAPT) por la dirección privada correcta (y el puerto privado si el paquete está destinado a la dirección de NAPT). La dirección 0.0.0.0 y la máscara para el origen de Internet indican que cualquier dirección de origen de la red pública se pasará al NAT.

```
IP Config>update packet-filter
Packet-filter name [ ]? in-0
Packet-filter 'in-0' Config> add access
Enter type [E]? IN
Internet source [0.0.0.0]?
Source mask [255.255.255.255]? 0.0.0.0
Internet destination [0.0.0.0]? 198.76.29.0
Destination mask [255.255.255.255]?255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enable logging? (Yes or [No]):
Packet-filter 'in-0' Config>
```

   El rango de direcciones de la norma de control de acceso es mayor que el rango de direcciones definido en pool1. Si la dirección del paquete que se pasa al NAT está dentro del rango definido en la norma de control de acceso pero no es uno de los de la agrupación de direcciones públicas, el NAT devuelve el paquete a IP sin modificarlo.

7. Si desea que el direccionador acepte los paquetes que no coinciden con la norma de control de acceso, en lugar de excluirlos, puede crear una norma de control de acceso comodín. El ejemplo siguiente muestra una norma de control de acceso de este tipo:

```
Packet-filter 'in-0' Config> add access
Enter type [E]? I
Internet source [0.0.0.0]? 0.0.0.0
Source mask [255.255.255.255]? 0.0.0.0
Internet destination [0.0.0.0]? 0.0.0.0
Destination mask [255.255.255.255]?0.0.0.0
Enter starting protocol number ([0] for all protocols) [0]?
Enable logging? (Yes or [No]):
Packet-filter 'in-0' Config>
```

8. Añada una norma de control de acceso para NAT para el filtro de paquete de salida. Los paquetes que deben reenviarse desde la interfaz de red 0 que tienen una dirección de origen en la red privada se identifican de modo que IP puede pasarlos al NAT. El NAT sustituye la dirección privada por una de las direcciones públicas de pool1.

```
Packet-filter 'out-0' Config> add access
Enter type [E]? IN
Internet source [0.0.0.0]? 10.33.96.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]?
Destination mask [255.255.255.255]?0.0.0.0
Enter starting protocol number ([0] for all protocols) [0]?
Enable logging? (Yes or [No]):
Packet-filter 'out-0' Config>
```

Con este filtro de paquete, al igual que con el filtro *en-0*, puede añadir una norma de control de acceso inclusiva comodín como última norma de control de acceso si tiene intención de reenviar paquetes que no coincidan con la norma de control de acceso.

9. Puede utilizar el mandato **list packet-filter** *nombre-filtro* desde el indicador de mandatos `IP Config>` para comprobar la exactitud y secuencia de las normas de control de acceso en cada filtro de paquete.
10. Habilite los controles de acceso para IP.

    ```
    IP Config> set access-control on
    ```

11. Establezca IP y NAT utilizando talk 5. Hasta ahora, ha efectuado cambios en la configuración del direccionador, pero estos cambios no han afectado al direccionador. Los mandatos reset para IP y NAT hacen que el direccionador lea la nueva configuración y ejecute las normas definidas en la configuración.

    ```
    NAT> reset NAT
    IP> reset IP
    ```

Configuración y supervisión del Conversor de direcciones de red

Este capítulo describe los mandatos de configuración y supervisión del Conversor de direcciones de red (NAT) e incluye las secciones siguientes:

- "Acceso al entorno de configuración del Conversor de direcciones de red"
- "Mandatos de configuración del Conversor de direcciones de red"
- "Acceso al entorno de supervisión del Conversor de direcciones red" en la página 460
- "Mandatos de supervisión del Conversor de direcciones de red" en la página 460
- "Soporte de reconfiguración dinámica del NAT" en la página 462

Acceso al entorno de configuración del Conversor de direcciones de red

Para acceder al entorno de configuración de NAT, entre el mandato siguiente en el indicador de mandatos `Config>`:

```
Config> feature nat
Network Address Protocol user configuration
NAT config>
```

Mandatos de configuración del Conversor de direcciones de red

Esta sección explica los mandatos de configuración del Conversor de direcciones de red (NAT). Para configurar el NAT, entre estos mandatos en el indicador de mandatos `NAT config>`.

Tabla 55. Mandatos de configuración de NAT

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxx.
Change	Cambia agrupaciones de reserva de direcciones IP públicas, rangos de conversión de direcciones privadas y correlaciones estáticas.
Delete	Suprime agrupaciones de reserva de direcciones IP públicas, rangos de conversión de direcciones privadas y correlaciones estáticas.
Disable	Inhabilita el NAT.
Enable	Habilita el NAT.
List	Lista información sobre la configuración de NAT.
Map	Crea un enlace de NAT o NAPT estático para una estación o servidor.
Reserve	Crea una agrupación de direcciones IP públicas y añade direcciones a dicha agrupación.
Reset	Hace que el direccionador lea la configuración de NAT y que se ejecute de acuerdo con las normas de NAT que se han configurado.
Set	Establece tiempos de espera excedidos.
Translate	Identifica las direcciones IP privadas que debe convertir la agrupación de direcciones públicas de NAT.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxi.

Change

Utilice el mandato **change** para cambiar agrupaciones de reserva de direcciones IP públicas, rangos de conversión de direcciones IP privadas y correlaciones estáticas.

Sintaxis:

change reserve
translate
mappings

reserve *agrupaciones*
Proporciona indicadores de mandatos que le permiten cambiar las características de cualquier agrupación de reserva de direcciones IP públicas (como por ejemplo direcciones y máscaras de IP).

Valores válidos: Un número de índice para identificar la agrupación configurada. Este número se visualiza cuando entra el mandato **list reserve pools**.

Valor por omisión: ninguno

translate *rangos*
Proporciona indicadores de mandatos que le permiten cambiar las características de cualquier rango de conversión de direcciones IP privadas (como por ejemplo direcciones y máscaras de IP).

Valores válidos: Un número de índice para identificar el rango de conversión configurado. Este número se visualiza cuando entra el mandato **list translate**.

Valor por omisión: ninguno

mappings
Proporciona indicadores que le permiten cambiar las características de cualquier correlación de direcciones estáticas (como por ejemplo direcciones y puertos de IP).

Valores válidos: Un número de índice para identificar la correlación configurada. Este número se visualiza cuando entra el mandato **list mappings**.

Valor por omisión: ninguno

Delete

Utilice el mandato **delete** para suprimir agrupaciones de reserva de direcciones IP públicas, rangos de conversión de direcciones IP privadas y correlaciones.

Sintaxis:

delete reserve
translate
mappings

reserve *agrupaciones*
Proporciona indicadores de mandatos que le permiten suprimir cualquier agrupación de reserva de direcciones IP públicas.

Valores válidos: Un número de índice para identificar la agrupación configurada. Este número se visualiza cuando entra el mandato **list reserve pools**.

Valor por omisión: ninguno

translate *rangos*
Proporciona indicadores de mandatos que le permiten suprimir cualquier rango de conversión de direcciones IP privadas.

Valores válidos: Un número de índice para identificar el rango de conversión configurado. Este número se visualiza cuando entra el mandato **list translate**.

Valor por omisión: ninguno

mappings
Proporciona indicadores de mandatos que le permiten suprimir cualquier correlación de direcciones estáticas.

Valores válidos: Un número de índice para identificar la correlación configurada. Este número se visualiza cuando entra el mandato **list mappings**.

Valor por omisión: ninguno

Disable

Utilice el mandato **disable** para inhabilitar el NAT. Puede inhabilitar el NAT para que excluya los paquetes que necesitan conversión o puede inhabilitar el NAT para que acepte paquetes que necesitan conversión.

Sintaxis:

disable nat

drop

pass

drop
Inhabilita el NAT de modo que excluye los paquetes que necesitan conversión.

pass
Habilita el NAT de modo que acepta los paquetes que necesitan conversión.

Enable

Utilice el mandato **enable** para habilitar el NAT. La habilitación del NAT hace que esté preparada para ejecutarse, pero no funcionará hasta que utilice el mandato **reset** o reinicie el direccionador.

Sintaxis:

enable nat

List

Utilice el mandato **list** para listar las agrupaciones de reserva de direcciones IP públicas, los rangos de conversión de direcciones IP privadas, las correlaciones, los valores globales o toda la información del NAT.

Sintaxis:

list reserve

addresses

pools

translate

mappings

global

all

En el ejemplo siguiente, los tiempos se visualizan como horas, minutos y segundos. El período de entrada es el tiempo que transcurre desde que la entrada se ha utilizado por última vez. Un enlace significa que el tráfico circula entre las dos direcciones. Los tiempos de espera excedidos determinan cuánto tiempo transcurrirá después de la última comunicación antes de que se excluya un enlace. Consulte el mandato **set** para obtener más información sobre tiempos excedidos.

Ejemplo:

```
NAT config>list all
NAT Globals:
NAT is ENABLED
Tcp Timeout....:   24:00:00
Non-Tcp Timeout:    0:01:00
NAT Reserved Address Pool(s):
Index First Address    Mask             Count NAPT Address     Pool Name
1     9.8.7.1          255.255.255.0    3     0.0.0.0          pool1
2     9.8.7.6          255.255.255.0    12    9.8.7.9          pool1
NAT Translate Range(s):
Index IP Address       IP Mask          Associated Pool Name
1     7.1.1.0          255.255.255.0    pool1
2     10.0.0.0         255.0.0.0        pool1
NAT Static Mapping(s):
Index Private Address:Port    Public Address.:Port
1     10.1.2.3        0       9.8.7.1        0
2     7.1.1.1         21      9.8.7.9        21
```

Map

Utilice el mandato **map** para enlazar estadísticamente un sistema principal o servidor de la red privada con una dirección pública. Este mandato, que se puede utilizar para configurar servidores en la red privada, establece una asociación en el arranque de NAT que no cambia nunca.

Las correlaciones estáticas con el número de puerto público y privado 0 son correlaciones de NAT; las que tienen otros valores para los números de puerto son correlaciones de NAPT.

Sintaxis:

map *dirección-privada número-puerto-privado dirección-pública número-puerto-público*

dirección-privada

La dirección privada de la estación de trabajo.

Valores válidos: una dirección del sistema principal de Internet en formato IP válido. Debe ser la dirección que se asigna a una estación de la red de apéndice que necesita acceso permanente desde la red pública, como por ejemplo un servidor.

Valor por omisión: ninguno

número-puerto-privado
El número de puerto TCP/UDP de la aplicación que se ejecuta en el dispositivo con la dirección privada. Si se entra **0** se crea un enlace de NAT y si se entra otro valor se crea un enlace de NAPT. Los valores de puerto común para NAPT son 23 para Telnet, 21 para FTP y 80 parar HTTP.

Valores válidos: 0 - 65535

Valor por omisión: 0

dirección-pública
La dirección IP pública con la que debe correlacionarse esta dirección privada. Debe ser una dirección de NAPT para una correlación de NAPT y una dirección de NAT para una correlación de NAT.

Valores válidos: una dirección IP válida exclusiva en la red pública. La red pública puede ser Internet o una intranet, según el diseño de la red.

Valor por omisión: ninguno

número-puerto-público
El número de puerto de los paquetes que deben convertirse en la dirección pública. El valor 0 representa todos los puertos. Los valores comunes son 23 para Telnet, 21 para FTP y 80 para HTTP.

Valores válidos: 0 - 65535

Valor por omisión: 0

En este ejemplo, el servidor con la dirección IP privada 10.11.12.200 acepta todo el tráfico desde Internet; el servidor con la dirección privada 10.11.12.199 es un servidor Telnet y un servidor FTP.

Ejemplo:

```
map 10.11.12.200 0 9.8.7.2 0
map 10.11.12.199 23 9.8.7.9 23
map 10.11.12.199 21 9.8.7.9 21
```

Reserve

Utilice el mandato **reserve** para crear y añadir un rango de direcciones IP a una agrupación de direcciones públicas. Adicionalmente, puede utilizarse para añadir una interfaz de IP dinámica a la agrupación de direcciones públicas.

Sintaxis:

reserve *dinámica [interfaz][dirección-pública][máscara][número-en-grupo] nombre [dirección-napt]*

Nota: Los valores que aparecen entre corchetes se visualizan opcionalmente.

- Dinámica - Especifica si esta entrada es para un grupo de direcciones públicas o para una interfaz de Dirección dinámica que recuperará su dirección IP de una conexión PPP que utilice IPCP. Los valores válidos son *sí* o *no*. El valor por omisión es *no*. Si Dinámica=*sí*, tan solo debe especificar la interfaz y el nombre. Si Dinámica=*no*, no debe especificar la interfaz, pero debe especificar todos los demás valores.

- Interfaz - Especifica la interfaz de Dirección dinámica tal como está configurada en IP. Puede especificarse cualquier número de interfaz. El valor por omisión es cero.

dirección-pública
La primera dirección IP pública de la secuencia de direcciones que forman este rango o grupo en la agrupación. Por ejemplo, si este grupo de la agrupación incluye las 12 direcciones en la secuencia de 9.8.7.6 a 9.8.7.17, este valor es 9.8.7.6.

Nota: Para añadir otro rango de direcciones a la agrupación de direcciones públicas, utilice el mandato **reserve** de modo separado para cada grupo, relacionando un grupo con otro, utilizando el mismo nombre de agrupación. Por ejemplo, las direcciones de 9.8.7.6 a 9.8.7.17 se pueden configurar en un grupo dentro de pool1 y las direcciones de 9.8.7.1 a 9.8.7.3 se pueden configurar en otro grupo dentro de la misma agrupación. Por lo tanto, dicha agrupación no configura ni utiliza las direcciones 9.8.7.4 y 9.8.7.5.

Valores válidos: una dirección IP válida que es exclusiva en la red pública

Valor por omisión: ninguno

máscara
Una máscara para seleccionar bits de la dirección IP. La máscara, como una dirección de Internet, tiene 32 bits de longitud. Los 1 de la máscara seleccionan parte de red o subred de la dirección. Los 0 seleccionan la parte de sistema principal. Por ejemplo, la dirección 9.8.7.6 y la máscara 255.255.0.0 incluye el rango de todas las direcciones cuyos dos primeros bytes son 9.8 (es decir, de 9.8.0.0 a 9.8.255.255).

Valores válidos: cualquier máscara de IP válida

Valor por omisión: ninguno

número-en-grupo
Especifica cuántas direcciones secuenciales, empezando desde la *dirección-pública*, se incluyen en el grupo. Para las direcciones de 9.8.7.6 a 9.8.7.17, este valor es 12.

Valores válidos: 1 - el valor que puede definir la máscara de IP

Valor por omisión: ninguno

nombre
El nombre de la agrupación de reserva de direcciones públicas. Esta serie debe coincidir con el nombre de agrupación en el mandato **translate** correspondiente.

Valores válidos: cualquier nombre, que utilice un máximo de 16 caracteres imprimibles; los blancos iniciales y de cola se ignoran.

Valor por omisión: ninguno

dirección-napt
La dirección IP de la agrupación de direcciones públicas que se utilizará en la Conversión de puertos y direcciones de red (NAPT). Esta dirección se utiliza para el tráfico TCP y UDP para correlacionar varias direcciones privadas con una dirección de NAPT de acuerdo con el numero de puerto del protocolo. La utilización de NAPT es opcional. Si se utiliza, sólo puede existir una dirección de NAPT por agrupación de direcciones públicas. Si no existe ninguna direc-

ción de NAPT para una agrupación o grupo, entre el valor **0.0.0.0**. Sólo debe entrar la dirección de NAPT una vez para la agrupación.

Valores válidos: una de las direcciones IP públicas. No es necesario que se incluya en el rango de valores definidos en la agrupación de direcciones públicas, pero debe estar en la misma subred.

Valor por omisión: 0.0.0.0 (indicando sin NAPT)

Ejemplo:

```
reserve no 9.8.7.1 255.255.255.0 3  pool1 0.0.0.0
reserve no 9.8.7.6 255.255.255.0 12 pool1 9.8.7.9
reserve yes 2 dynamic_ip_pool
```

Reset

Utilice el mandato **reset** para restablecer el NAT. Este mandato suprime todos los enlaces, libera toda la memoria utilizada por el NAT y reinicia el NAT basándose en la configuración de Talk 6 actual. El restablecimiento del NAT no interrumpe ningún otro componente del 2210.

Sintaxis:

reset n**at**

Tenga en cuenta que si el NAT encuentra una configuración no válida, verá un mensaje sobre ello. Revise los mensajes del ELS de NAT para ver por qué ha fallado la inicialización del NAT.

Set

Utilice el mandato **set** para establecer tiempos de espera TCP y no TCP.

Sintaxis:

s**et** t**cp**

n**ontcp**

tcp *tiempo-espera*
El tiempo que el NAT mantiene un enlace TCP después de que pase el último mensaje entre las dos estaciones de trabajo enlazadas. Un enlace es el mantenimiento de la relación entre una dirección privada y una de las direcciones IP públicas.

Valores válidos: 0 - 65535 minutos (de 0 minutos a aproximadamente 45 días)

Valor por omisión: 1440 minutos (24 horas)

nontcp *tiempo-espera*
El tiempo que el NAT mantiene un enlace que no es TCP después de que pase el último mensaje entre las dos estaciones de trabajo enlazadas. Un enlace es el mantenimiento de la relación entre una dirección privada y una de las direcciones IP públicas.

Valores válidos: 0 - 65535 minutos (de 0 minutos a aproximadamente 45 días)

Valor por omisión: 1 minuto

Translate

Utilice el mandato **translate** para añadir una subred a la lista de direcciones que el NAT va a convertir. Cada subred es un rango de conversión. Este mandato debe entrarse una vez para cada rango de conversión que debe conocer el NAT. Cualquier número de rangos de conversión pueden utilizar una única agrupación de reserva de direcciones públicas.

Sintaxis:

t**ranslate** *dirección-privada máscara nombre*

dirección-privada
Cualquier dirección de sistema principal IP o subred que deba convertirse.

Valores válidos: una dirección en formato de IP decimal con puntos válido. Cuando se aplica AND entre esta dirección y su máscara de subred, esta dirección identifica todas las direcciones de una subred de apéndice. Una subred de apéndice es una subred que accede a la red pública solamente a través del direccionador.

Valor por omisión: ninguno

máscara
Valores válidos: La red o máscara de subred asociada con la red de apéndice que debe convertirse.

Valor por omisión: máscara de clase de la dirección privada

nombre
El nombre de la agrupación de direcciones públicas que debe utilizar el NAT para este rango de direcciones privadas.

Valores válidos: cualquier nombre, que utilice un máximo de 16 caracteres imprimibles. Debe coincidir con un nombre de agrupación de direcciones públicas creado mediante el mandato **reserve**.

Valor por omisión: ninguno

Acceso al entorno de supervisión del Conversor de direcciones red

para acceder al entorno de supervisión del NAT, escriba

```
* t 5
```

Después, entre el mandato siguiente en el indicador de mandatos **+**:

```
+ feature NAT
NAT>
```

Aparecerá el indicador de mandatos NAT>.

Mandatos de supervisión del Conversor de direcciones de red

Esta sección describe los mandatos de supervisión de Seguridad de IP. Entre estos mandatos en el indicador de mandatos NAT>.

Tabla 56. Mandatos de supervisión de NAT

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
List	Lista información sobre el NAT.
Reset	Hace que el direccionador lea la configuración de NAT y que se ejecute de acuerdo con las normas de acceso del NAT que se han configurado. El NAT no afecta a la ejecución del direccionador hasta que entra el mandato **reset NAT**.
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 visualizar información sobre la configuración de NAT.

Sintaxis:

list
- all
- binding
- fragment
- global
- reserve
  - pools
  - addresses
- statistics
- translate

En el ejemplo siguiente, los tiempos se visualizan como horas, minutos y segundos. El período de entrada es el tiempo que transcurre desde que la entrada se ha utilizado por última vez. Un enlace significa que hay establecida una sesión entre las dos direcciones. Los tiempos de espera excedidos determinan cuánto tiempo transcurrirá después de la última comunicación antes de que se excluya un enlace. Consulte el mandato **set** en Talk 6 para más información sobre tiempos excedidos.

Ejemplo:

```
NAT>list all
NAT Globals:
Current State    Tcp Timeout    Non-Tcp Timeout    Memory Usage (in bytes)
ENABLED             24:00:00            0:01:00           408

NAT Statistics:
Requests :     Passes      Drops      Holds
       0 :          0          0          0

NAT Address Binding(s):
Private Address//Port  Public Address//Port  Bind Type  Entry Age
        7.1.1.1    21         9.1.1.1    21  STATIC       0:00:13
       10.1.2.3     0         9.1.1.2     0  STATIC       0:00:13

NAT TCP Session Information:
Private Address//Port  Public Address//Port  Tcp State  Data Delta  Entry Age
        7.1.1.1    21         9.1.1.1    21  ESTAB'ED      0        0:00:56

NAT Translate Range(s):
Base Ip Address        Range Mask      Associated Reserve Pool
       7.1.1.0         255.255.255.0   carol
      10.0.0.0         255.0.0.0       carol

NAT Reserve Pool(s):
Reserve Pool     Pool Size    NAPT Address   1st Available Address
carol                21           9.1.1.1          9.1.1.12
-------------------------------------------------------------
Number of Reserve Pools using NAPT.....:     1
Number of configured Reserved Addresses:    21

NAT Fragment Information:
Number of Entries    Number of Saved Fragments
           0                          0
```

Reset

Utilice el mandato **reset** para restablecer el NAT. Este mandato suprime todos los enlaces, libera toda la memoria utilizada por el NAT y reinicia el NAT basándose en la configuración de Talk 6 actual. El restablecimiento del NAT no interrumpe ningún otro componente del 2210.

Sintaxis:

reset n**at**

Soporte de reconfiguración dinámica del NAT

Esta sección describe la reconfiguración dinámica (DR) en lo que afecta a los mandatos de Talk 6 y Talk 5.

Delete interface de CONFIG (Talk 6)

El NAT no soporta el mandato de CONFIG (Talk 6) **delete interface**.

Activate interface de GWCON (Talk 5)

El mandato de GWCON (Talk 5) **activate interface** no es aplicable para el NAT. El NAT no tiene registros SRAM asociados con una interfaz.

Reset interface de GWCON (Talk 5)

El mandato de GWCON (Talk 5) **reset interface** no es aplicable para el NAT. El NAT no tiene registros SRAM asociados con una interfaz.

Mandatos reset de componente GWCON (Talk 5)

El NAT soporta los mandatos de GWCON (Talk 5) **reset** siguientes específicos del NAT:

Mandato GWCON, feature NAT, reset NAT

Descripción: Reset detiene todos los temporizadores del NAT, establece en estado de NAT en inhabilitado y libera toda la memoria utilizada por el NAT. Se borran todas las correlaciones de conversión, los fragmentos de paquetes y la información de sesión TCP. La rutina de inicialización del NAT leerá el estado del NAT en los registros de configuración. Si se habilita el NAT, todas las agrupaciones de direcciones públicas, los rangos de direcciones privadas, las tablas de correlación, las tablas de reensamblaje de fragmentos, los tiempos de espera y los temporizadores se inicializan desde los registros de configuración. En este punto, el NAT está preparado de nuevo para los paquetes que le presentan los filtros de paquetes IP.

Efecto en la red: Si el NAT se había habilitado anteriormente, todas las sesiones TCP excederán el tiempo de espera y se informará a la aplicación. Las correlaciones de UDP y datagrama se perderán y los paquetes de dichas corrientes de datos se excluirán. Una vez que se ha vuelto a inicializar el NAT, se pueden volver a establecer sesiones TCP así como UDP y otras corrientes de paquetes de datagramas.

Limitación: Los Filtros de paquetes IP debe configurarse correctamente para que IP pase paquetes al NAT.

El mandato **GWCON, feature nat, reset nat** soporta todos los mandatos del NAT.

Mandatos de cambio inmediato de CONFIG (Talk 6)

El NAT soporta los mandatos de CONFIG siguientes que cambian inmediatamente el estado operativo del dispositivo. Estos cambios se guardan y se conservan si se vuelve a cargar o se reinicia el dispositivo o si se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
CONFIG, feature nat, reset nat

Utilización de un Servidor de Acceso de marcación de entrada a las LAN (DIAL)

Un Servidor DIAL permite que los usuarios se conecten a una LAN y accedan a los recursos de la LAN del mismo modo que si estuvieran conectados localmente con un adaptador de la LAN. De modo similar, el Servidor DIAL también permite que los usuarios conectados a la LAN se conecten a recursos de una WAN (como por ejemplo tablones de anuncios, máquinas de FAX, Proveedores de servicios de Internet (ISP) y otros servicios en línea) eliminando la necesidad de una línea telefónica analógica y módem en su estación de trabajo.

El Servidor DIAL se puede configurar para usuarios de marcación de entrada y de marcación de salida simultáneamente. El Cliente de marcación de entrada de IBM DIAL se ejecuta en la estación de trabajo remota y proporciona la función Marcación de entrada. La Figura 35 muestra un ejemplo de un dispositivo utilizado como Servidor DIAL que soporta la función Marcación de entrada.

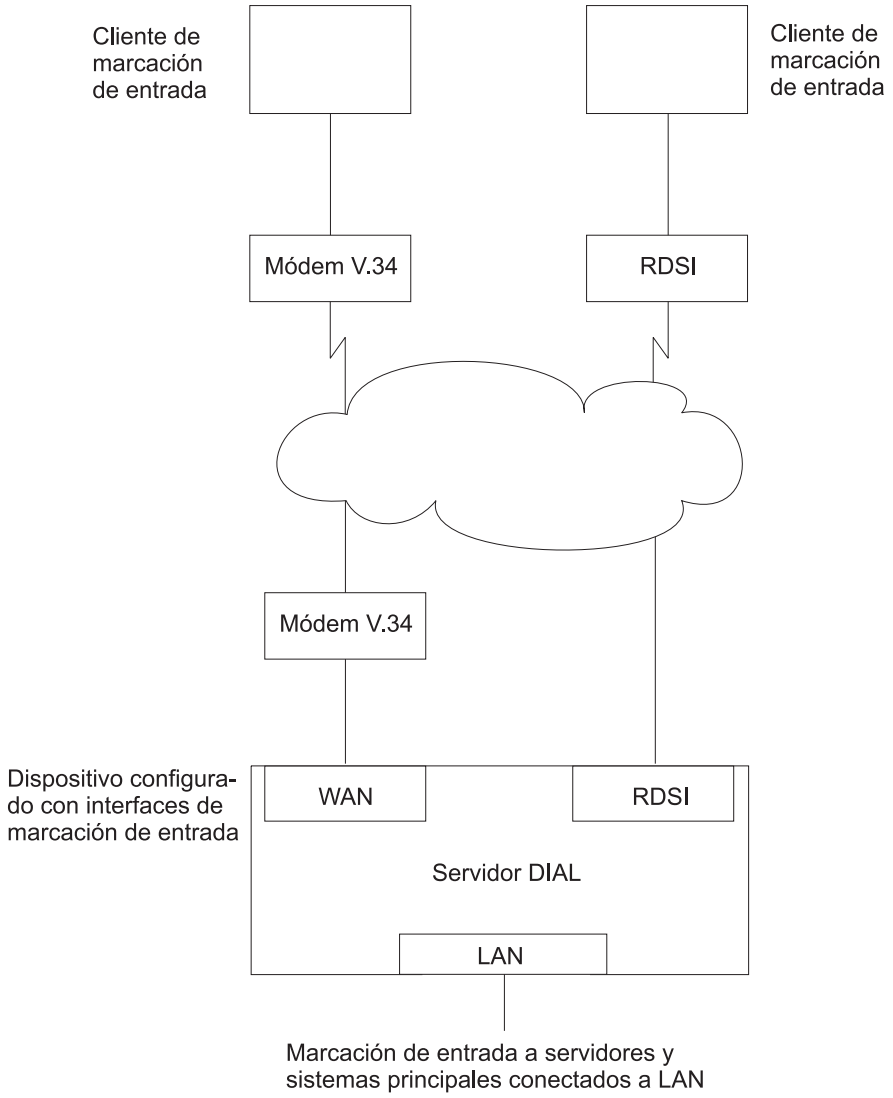


Figura 35. Ejemplo de un Servidor DIAL que soporta Marcación de entrada

El Cliente Marcación de salida de IBM DIAL se ejecuta en una estación de trabajo conectada a la red y proporciona la función Marcación de salida. La Figura 36 en la página 466 muestra un ejemplo de un 2210 que se utiliza como un Servidor DIAL que soporta la función Marcación de salida.

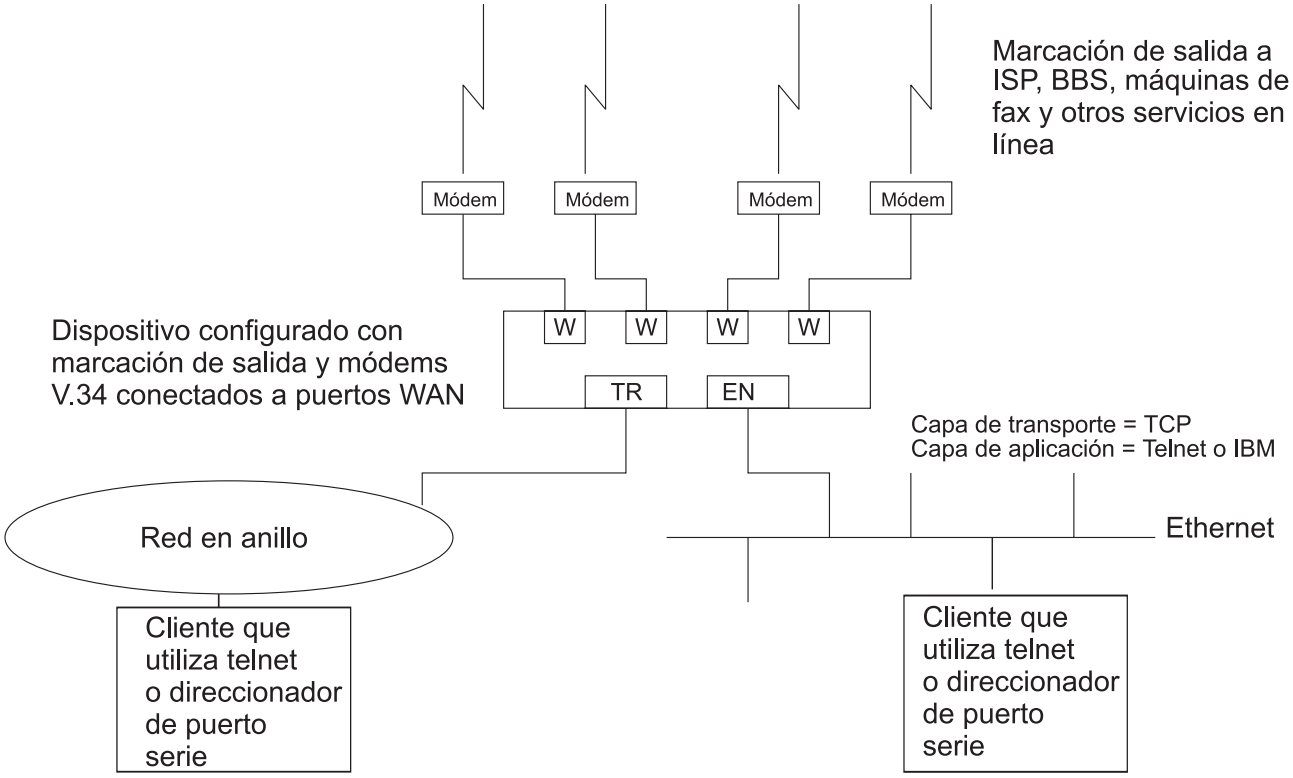


Figura 36. Ejemplo de un Servidor DIAL que soporta Marcación de salida

Antes de utilizar Acceso de marcación de entrada

Antes de utilizar Acceso de marcación de entrada, necesita:

- Una estación de trabajo que ejecute el Cliente de marcación de entrada de IBM DIAL u otro cliente de marcación de entrada PPP (a los cuales se hace referencia como ***cliente de marcación de entrada*** o ***cliente de marcación de entrada PPP*** en las secciones siguientes).
- Complete las configuraciones de protocolo en la máquina cliente.
- Interfaces RDSI , interfaces de módem integrado, una interfaz de módem nulo o módems V.34 externos conectados a los puertos de la WAN del 2210 que desea utilizar para la marcación de entrada de un único usuario.
- Un Servidor DIAL completamente configurado en la LAN.

Configuración de Acceso de marcación de entrada

Esta sección describe cómo configurar Marcación de entrada y Marcación de salida en el Servidor DIAL. La configuración de un cliente para utilizar Acceso de marcación de entrada se describe en la documentación asociada con el cliente que utiliza la estación de trabajo.

Configuración de interfaces de marcación de entrada

Las interfaces de marcación de entrada en el 2210 son un tipo especial de circuito de marcación. Puesto que la mayoría de valores para un circuito de marcación típico no son apropiados para aplicaciones de marcación de entrada de un único usuario, se puede añadir un nuevo tipo de dispositivo llamado ***Marcación de entrada*** que establezca los valores por omisión apropiados para el circuito de marcación. La adición de un dispositivo de marcación de entrada también configura los valores por omisión de la configuración del encapsulador PPP que funcionan con la mayoría de clientes de marcación de entrada PPP, incluyendo el cliente de marcación de entrada de IBM DIAL. Estos valores por omisión se describen en "Valores por omisión de los parámetros de circuito de marcación para interfaces de marcación de entrada" y "Parámetros de encapsulador PPP de circuito de marcación para circuitos de marcación de entrada" en la página 468.

Nota: La función DIAL sólo puede habilitarse en circuitos de marcación de entrada. Los circuitos de marcación de entrada sólo están soportados cuando la red base es V.34 o una red RDSI.

Valores por omisión de los parámetros de circuito de marcación para interfaces de marcación de entrada

Notas:

1. No altere temporalmente los parámetros que se describen en esta sección. Si lo hace impedirá que la función Marcación de entrada funcione correctamente.
2. Es posible que algunos parámetros no puedan visualizarse o no sean configurables. Para obtener una descripción completa de los parámetros, consulte "Configuración y supervisión de circuitos de marcación" en la publicación *Guía del usuario de software*.

Se establecen los valores por omisión siguientes al añadir una interfaz de marcación de entrada:

- ***Tiempo desocupado*** está establecido en 0. Tenga en cuenta que un circuito estándar se define como un circuito en el que el temporizador de desocupado no tiene ningún significado. No será un circuito fijo para conectarse automáticamente. La única vez que el circuito se conectará es si se ha negociado una devolución de llamada PPP o si está habilitado Multienlace PPP en este circuito. Consulte "Shiva Password Authentication Protocol (SPAP)" y "Using the Multilink PPP Protocol" en la publicación *Guía del usuario de software* .
- ***Llamadas de entrada***, están permitidas. Se configuran entradas porque los clientes de marcación de entrada PPP no utilizan el intercambio de LID implantado por los circuitos de marcación de Nways.
- ***Llamadas de salida***, están permitidas.

  Nota: "Salida" para un circuito de marcación de entrada no es lo mismo que un circuito de marcación de salida. Consulte "Antes de configurar interfaces de marcación de salida" en la página 469.
- Existe una dirección de destino por omisión para "default_address". Esta dirección se añade a la lista de direcciones V.34 o de direcciones RDSI. Puesto que estas llamadas son de entrada y las únicas llamadas de salida son las que resultan de una devolución de llamada o de un intercambio de multienlace PPP, la dirección de destino no es significativa. Sin embargo, la dirección es

necesaria para los parámetros del circuito. No suprima esta dirección o los circuitos se inhabilitarán.

Parámetros de encapsulador PPP de circuito de marcación para circuitos de marcación de entrada

Nota: Para obtener una descripción completa de los parámetros siguientes, consulte "Utilización de interfaces de Point-to-Point Protocol" en la publicación *Guía del usuario de software*.

Cuando añade una interfaz de marcación de entrada están establecidos los valores por omisión siguientes:

- La autentificación está habilitada para SPAP, CHAP y PAP.
- La MRU PPP está establecida en 1522. Este tamaño de MRU es necesario para versiones Windows 3.1, OS/2 y DOS de los clientes de marcación de entrada de IBM DIAL. No cambie este valor a menos que sepa que no va a utilizar estos clientes.
- Se habilita automáticamente DIAL en el encapsulador PPP. Con ello se activan algunas de las características importantes para los usuarios de Acceso de marcación de entrada a las LAN, como por ejemplo protocolo NetBIOS Control, protocolo NetBIOS Frame Control, tiempo restante, autentificación de SPAP, devolución de llamada, identificación de LCP, y adición y supresión automática de rutas estáticas de IP al cliente. Consulte "Utilización de interfaces de Point-to-Point Protocol" en la publicación *Guía del usuario de software* para obtener más información sobre las características de DIAL.

Adición de una interfaz de marcación de entrada

Para añadir una interfaz de marcación de entrada:

1. Configure una red base V.34 o RDSI en una de las interfaces de la WAN disponibles del 2210. Consulte "Using the V.34 Network Interface" y "Utilización de la interfaz RDSI" en la publicación *Guía del usuario de software* para obtener detalles sobre la configuración.
2. Entre **talk 6** para acceder al indicador de mandatos `Config >`.
3. Entre **add device dial-in** en el indicador de mandatos `Config >` para añadir la interfaz de marcación de entrada. Se le solicitará cuántos circuitos de marcación de entrada desea añadir. Este mandato creará las nuevas redes, informará de sus números de red, solicitará el número de red base y solicitará que se habilite el Multienlace PPP.

   Ejemplo: Suponga que la red máxima actual es 3 y que desea añadir una red de marcación de entrada 1 a la red base 2.

La Figura 37 es un ejemplo de definición de una interfaz de marcación de entrada.

Figura 37. Adición de una interfaz de marcación de entrada

```
Config>add dev dial-in
Adding device as interface 4
Defaulting Data-link protocol to PPP
Use "net 4" command to configure circuit parameters
Base net for this circuit [0]? 2

Enable as a Multilink PPP link? [no]

Disabled as a Multilink PPP link.

Use "set data-link" command to change the data-link  protocol
Use "net " command to configure dial circuit parameters.
Config>li dev
Ifc 0     Ethernet              CSR  81600, CSR2  80C00, vector 94
Ifc 1     V.34 Base Net         CSR  81620, CSR2  80D00, vector 93
Ifc 2     V.34 Base Net         CSR  81640, CSR2  80E00, vector 92
Ifc 3     PPP Dial-in Circuit
Ifc 4     PPP Dial-in Circuit
```

Antes de configurar interfaces de marcación de salida

Antes de configurar y utilizar interfaces de marcación de salida en el 2210, necesita:

- Software de IBM Nways con el soporte de DIAL cargado en un 2210.
- Un módem V.34 externo, un módem integrado o un módem nulo, , o una interfaz RDSI si se conecta a un puerto de WAN disponible en el 2210. Consulte “Using the V.34 Network Interface” en la publicación *Guía del usuario de software* para obtener información sobre la configuración.
- Una estación de trabajo conectada a la LAN que tiene acceso al Servidor DIAL de 2210.
- Software en el cliente, por ejemplo Telnet, un direccionador Telnet o clientes de marcación de salida de IBM DIAL. IP debe estar configurado correctamente en el cliente para que el cliente de marcación de salida funcione.

Utilización de módem nulo

Cuando utilice un módem nulo, utilice el protocolo de conexión completa D25NM-3:

Correlación de patillas:

1 con 1	**1 con 1**
2 con 3	**3 con 2**
4 con 5	**5 con 4**
6 con 8, 20	**8, 20 con 6**
7 con 7	**7 con 7**

Configuración de interfaces de marcación de salida

Los pasos siguientes describen cómo configurar una interfaz de marcación de salida en el dispositivo.

1. Conecte un módem V.34 al puerto de WAN que va a utilizar como interfaz de marcación de salida.
2. Conéctese a la consola del Servidor DIAL de 2210.
3. Entre **talk 6** en el indicador de mandatos *.

4. Configure una interfaz V.34. Consulte “Using the V.34 Network Interface” en la publicación *Guía del usuario de software* para obtener más detalles.
5. Añada una interfaz de marcación de salida utilizando el mandato **add device dial-out**. Cuando se le solicite la interfaz, utilice un número de interfaz V.34 disponible.

   Notas:

   a. Se pueden configurar varios circuitos además de una red base V.34. Sin embargo, sólo puede haber un circuito activo en cada momento.

   b. El software define una dirección V.34 llamada ***default_address***. No suprima esta dirección ya que es necesaria para la marcación de salida y la marcación de salida no funcionará sin ella.
6. Configure el servidor de autentificación PPP, si utiliza el cliente de marcación de salida DIAL de IBM y añada usuarios PPP tal como se describe en “PPP Authentication Protocols” en la publicación *Guía del usuario de software*. Los usuarios PPP añadidos deben tener la marcación de salida habilitada. La marcación de salida utilizando Telnet no necesita autentificación, por consiguiente no configure autentificación para sesiones Telnet.
7. Configure los parámetros globales de la marcación de salida utilizando el mandato **feature dials**. Consulte el mandato **feature** en la publicación *Guía del usuario de software*.

   En este entorno puede configurar el temporizador de inactividad de marcación de salida, el nombre de servidor de la marcación de salida, agrupaciones de módems y otros parámetros.
8. Para que el cliente de marcación de salida de IBM DIAL funcione correctamente, se deberá habilitar SNMP en el 2210 y se deberá definir una comunidad SNMP llamada *public* en el 2210 con acceso de lectura. Esto es necesario para que la aplicación elector de marcación de salida pueda encontrar servidores de marcación de salida en la red. Consulte el apartado “Gestión de SNMP” de la publicación *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener información sobre cómo habilitar SNMP y cómo configurar una comunidad SNMP.
9. Reinicie el dispositivo.

Configuración de agrupaciones de módems

Las agrupaciones de módems se definen como un grupo de módems que aparecen ante el usuario como un módem. Cuando el usuario debe efectuar una conexión de salida, se utiliza el primer módem disponible de esta agrupación. Las agrupaciones de módems se crean en el Servidor DIAL de 2210 definiendo grupos de interfaces de marcación de salida con el mismo nombre de puerto. Por omisión, todas las interfaces de marcación de salida se denominan “ALL_PORTS”, lo que crea una agrupación de módems. La denominación de las interfaces de marcación de salida individualmente permite que un usuario seleccione un módem determinado para la marcación de salida.

Para configurar una agrupación de módems:

1. Entre **talk 6** en el indicador de mandatos *.
2. Entre **net *n***, donde ***n*** es el número de la interfaz de marcación de salida tal como se define en “Utilización de la interfaz de red V.34” en la publicación

Guía del usuario de software. Esta acción le conduce al entorno de configuración para la interfaz.

3. Entre **encapsulator** (consulte “Configuración y supervisión de circuitos de marcación” en la publicación *Guía del usuario de software*) en el indicador de mandatos `Circuit Config>`. Esta acción le conduce al entorno de configuración de la marcación de salida.
4. Entre **set portname** en el indicador de mandatos `Dial-out Config>`. Esta acción le solicitará el nombre del puerto (un máximo de 30 caracteres). Si especifica un nombre de puerto existente, el módem se añade a la agrupación con dicho nombre.
5. Reinicie el 2210.

Antes de configurar los parámetros globales de DIAL

Esta sección describe los parámetros globales del Servidor DIAL.

Direcciones IP proporcionadas por el servidor

El direccionador se puede configurar para proporcionar una dirección IP para un cliente de marcación de entrada para utilizarla mientras dure su conexión. La dirección que el direccionador asignará al cliente puede recuperarse mediante 4 métodos diferentes. Estos métodos se listan a continuación por orden de prioridad:

1. ID de usuario

   Se puede almacenar una dirección IP en el perfil de usuario PPP para cada cliente. Cuando un cliente se conecta y solicita una dirección IP, el direccionador recupera la dirección configurada en el perfil de usuario PPP de dicho usuario. Esto permite que el usuario obtenga la misma dirección IP cada vez, pero necesita una dirección IP para cada usuario.

   Utilice el mandato `Config>` **add ppp-user** para configurar una dirección IP en el perfil de usuario PPP.

2. Interfaz

   Se puede almacenar una dirección IP en la configuración de interfaz de marcación de entrada. Cuando un cliente se conecta y solicita una dirección IP, el direccionador recupera la dirección de la interfaz a través de la cual se ha efectuado la conexión. Este método requiere una dirección IP exclusiva para cada interfaz de marcación de entrada.

   Para establecer la dirección IP de la interfaz:

   - Utilice el mandato `Config>` **list devices** para visualizar el número de interfaz asignado a la interfaz de hardware.
   - Utilice el mandato `Config>` **net 'x'**, donde 'x' es el número de interfaz configurado, para acceder al indicador de mandatos para la interfaz.
   - Utilice el mandato `PPP Config>` **set ipcp** para establecer la dirección IP de la interfaz.

3. Agrupación

   Es posible almacenar bloques de direcciones IP en una agrupación de direcciones IP. Cuando un cliente se conecta y solicita una dirección, el direccionador recupera una dirección de la agrupación. Cuando el cliente se

desconecta, la dirección se devuelve a la agrupación. Este método proporciona una única ubicación para configurar la dirección IP del cliente de marcación de entrada sin necesidad de un servidor de direcciones.

Utilice el mandato `DIALs config>` **add ip-pool** para añadir una agrupación de direcciones IP.

4. Proxy DHCP

   Una dirección IP puede alquilarse a un servidor DHCP. Cuando un cliente se conecta y solicita una dirección, el direccionador solicita una dirección del servidor DHCP en nombre del cliente. Este método requiere que exista un servidor DHCP en la LAN o que esté configurado en el direccionador. Un servidor DHCP puede proporcionar direcciones para clientes en múltiples direccionadores. Consulte el apartado “Dynamic Host Configuration Protocol (DHCP)” para obtener información.

   Utilice el mandato `DIALs config>` **add dhcp-server** para añadir un servidor DHCP.

Métodos de asignación de direcciones IP

La dirección IP que utiliza un cliente de marcación de entrada mientras dura la conexión puede proceder de 5 fuentes diferentes. Estas fuentes se listan por orden de precedencia:

1. cliente proporcionado
2. id de usuario asignado
3. interfaz asignada
4. agrupación de direcciones
5. servidor DHCP

Cuando un cliente de marcación de entrada se conecta, el direccionador busca en estos orígenes hasta que encuentra una dirección o agota todas las fuentes. Si no encuentra ninguna dirección IP, la negociación de IPCP falla. Se puede utilizar cualquier combinación de métodos.

La configuración por omisión es:

```
Client     :  Enabled
UserID     :  Enabled
Interface  :  Enabled
Pool       :  Enabled
DHCP Proxy :  Disabled
```

Nota: No hay ninguna dirección configurada por omisión en el perfil de usuario PPP, la interfaz o la agrupación de direcciones IP.

Dynamic Host Configuration Protocol (DHCP)

El Dynamic Host Configuration Protocol (DHCP) se ha desarrollado para proporcionar parámetros de configuración a los sistemas principales de una red. Entre otros parámetros de configuración, DHCP tiene un mecanismo para asignar direcciones de red a sistemas principales.

La característica Proxy DHCP actúa como un cliente *en nombre* de un usuario PPP de marcación de entrada. Esto permite que el dispositivo obtenga un alquiler de dirección IP para el tiempo que dura la sesión de marcación de entrada o hasta

que caduca el alquiler. La dirección IP que se asigna desde el servidor DHCP se comunica al cliente de marcación de entrada a través de PPP IPCP (consulte “Protocolo de control de IP” en la publicación *Guía del usuario de software* para obtener una descripción de IPCP). El software de cliente de marcación de entrada no sabe que se ha utilizado DHCP para asignar una dirección IP y, en consecuencia, no se requiere ningún tipo de activación de DHCP.

Proxy DHCP requiere que esté configurado como mínimo un servidor DHCP y que sea accesible desde el direccionador.

Proxy DHCP requiere que las direcciones que se asignan a los usuarios de la marcación de entrada estén dentro de la misma subred de una LAN conectada directamente. En una configuración típica, para ello se necesita direccionamiento de subred ARP proxy para permitir que el direccionador responda a las peticiones de ARP a sistemas principales de la red local en nombre de los clientes de marcación de entrada.

Configuración básica de DHCP

La configuración más básica necesita un único servidor DHCP en la misma red que el direccionador, con direcciones de marcación de entrada que deben alquilarse dentro de la misma subred que esta LAN.

Cuando el cliente se conecta, se obtiene el alquiler de una dirección IP del servidor DHCP y se utiliza en la negociación de IPCP con el cliente.

1. Conecte 2210 y DHCP a la misma LAN.
2. Configure e inicie el servidor DHCP (consulte la documentación del servidor DHCP para obtener información sobre cómo configurar el servidor para que alquile direcciones IP). Recuerde que las direcciones IP que deben alquilarse DEBEN estar dentro de una subred de una LAN conectada directamente y ARP proxy debe estar habilitado en el 2210).
3. La configuración típica para Proxy DHCP inhabilita las opciones Cliente especificado, ID de usuario y Negociación de Interfaz y de dirección IP de agrupación:

   ```
   Dials Config>list ip
   DIALs client IP address specification:
   Client : disabled
   UserID : disabled
   Interface : disabled
   DHCP Proxy : enabled
   ```

4. Añada el servidor DHCP (`Dials Config>` **add dhcp 10.0.0.111**)
5. Establezca el software de cliente de marcación de entrada en *Servidor asignado*.

   Notas:

   a. La configuración de *Servidor asignado* varía entre las diferentes implantaciones de cliente de marcación de entrada.

   b. El software de cliente no debe configurarse para obtener su dirección de DHCP. El cliente debe obtener su dirección enviando una dirección 0.0.0.0 a IPCP en la petición de configuración inicial.
6. Para esta configuración, deje el valor por omisión de DHCP GATEWAY ADDRESS en 0.0.0.0.

Múltiples saltos al Servidor DHCP

El servidor o servidores DHCP configurados deben ser direcciones IP asequibles desde el direccionador conectado. Siempre debe poder sondear el servidor desde la caja de acceso remoto.

Cuando el servidor DHCP está situado a varios saltos, el servidor debe conocer una dirección a la que responder y debe indicar de qué agrupación debe asignarse una dirección IP. La agrupación de la que debe asignarse una dirección IP es importante puesto que el servidor DHCP puede utilizarse para proporcionar direcciones a varias subredes y debe existir alguna indicación sobre de qué agrupación de direcciones debe seleccionarse. Para ello se utiliza la dirección de pasarela DHCP (*giaddr*) (la terminología se basa en la definición proporcionada en la RFC 2131). La *giaddr* debe ser una dirección local para el 2210, como el puerto de LAN Red en Anillo o Ethernet. Además, dado que *giaddr* es la dirección que el servidor DHCP utilizará para responder, asegúrese de que se pueda sondear esta dirección desde el mismo servidor DHCP.

Red de múltiples servidores DHCP

Puede configurar múltiples servidores DHCP para redundancia. Cuando configura múltiples servidores, el cliente Proxy DHCP solicita a todos los servidores una dirección y acepta la primera respuesta recibida. Si algunos de los servidores DHCP están a más de un salto, o están conectados a una subred que no está asociada con las direcciones de esta agrupación, debe configurarse *giaddr*. Consulte “Múltiples saltos al Servidor DHCP”.

Mientras que puede existir más de un servidor DHCP que proporcione direcciones, es importante no permitir que la agrupación de direcciones configurada en cada servidor se solape. Además, dado que sólo existe una *giaddr* para el servidor DHCP a la que responder y con la que realizar una búsqueda, cada agrupación de direcciones debe estar en la misma subred que las demás.

Servidor de nombres de dominio dinámico (DDNS)

Un Servidor de nombres de dominio (DNS) correlaciona direcciones IP con nombres de sistema principal y generalmente suele ser de naturaleza estática. DNS dinámico es una característica que, utilizada con un servidor DHCP DDNS y un servidor DNS, habilita DHCP para que actualice dinámicamente el servidor DNS con una correlación de direcciones IP y nombres de sistema principal. Esta característica sólo debe utilizarse junto con Proxy DHCP.

Cuando habilita el DNS dinámico en el 2210 y configura un nombre de sistema principal en el perfil de usuario (consulte “PPP Authentication Protocols” en la publicación *Guía del usuario de software*), este nombre de sistema principal se pasa como opción 81 (DDNS) al DHCP SERVER. Si ha configurado el servidor DHCP correctamente para DDNS, el servidor DHCP actualiza el servidor DDNS con la dirección IP que ha alquilado al direccionador y el nombre de sistema principal que el direccionador le ha enviado. Esto permite que otros usuarios accedan al cliente de marcación de entrada mediante el nombre de sistema principal en lugar de exigir al cliente que conozca la dirección IP elegida dinámicamente.

Configuración de DIAL

Este capítulo describe la configuración y los mandatos operativos de DIAL. El capítulo incluye las secciones siguientes:

Acceso al entorno de configuración global de DIAL

Utilice el procedimiento siguiente para acceder al proceso de configuración global.

1. En el indicador de mandatos OPCON, entre **talk 6**. (Para obtener más detalles sobre este mandato, consulte *The OPCON Process and Commands* en la publicación Guía del usuario de software.) Por ejemplo:

   ```
   * talk 6
   Config>
   ```

   Después de entrar el mandato **talk 6**, se visualiza el indicador de mandatos (`Config>`) en el terminal. Si el indicador de mandatos no aparece cuando inicia la configuración, pulse **Retorno** de nuevo.

2. En el indicador de mandatos CONFIG, entre el mandato **feature dials** para llegar al indicador de mandatos `DIALs Config>` y acceder al entorno de configuración de parámetros globales de DIAL.

Mandatos de configuración global de DIAL

Tabla 57. Mandatos de configuración global de DIAL

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Add	Añade un servidor DHCP (Dynamic Host Configuration Protocol) a la lista de servidores DHCP o añade una agrupación de direcciones IP.
Delete	Suprime un servidor DHCP de la lista o elimina un bloque de direcciones de una agrupación de direcciones IP
Disable	Inhabilita métodos de asignación de direcciones IP, protocolos de marcación de salida, MP multichasis, Titular de SPAP y DNS dinámico.
Enable	Habilita varios métodos de asignaciones de direcciones IP, protocolos de marcación de salida, MP multichasis, Titular de SPAP y DNS dinámico.
List	Lista los parámetros globales de DIAL y sus valores.
Set	Establece el tiempo permitido, la dirección de pasarela dhcp, las direcciones de Servidor de nombres de NetBIOS, las direcciones MAC asignadas localmente, las Conexiones Virtuales (VC) las direcciones de Servidor de nombres dinámico, el temporizador de inactividad de marcación de salida y el nombre de servidor de marcación de salida.
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 nuevo servidor Proxy DHCP a una lista de servidores o para añadir una agrupación de direcciones IP.

La lista de servidores DHCP contiene las direcciones IP de los servidores DHCP que, a su vez, alquilarán direcciones IP a clientes de marcación de entrada. Se pueden añadir múltiples servidores para redundancia. El número máximo de servidores es 20.

La característica de agrupación de direcciones IP proporciona un método mediante el cual el direccionador puede recuperar una dirección IP de una agrupación de direcciones definida localmente para un cliente de marcación de entrada. El cliente puede utilizar esta dirección mientras dura la conexión al direccionador. Una agrupación consta de uno o más bloques de direcciones IP. El número máximo de bloques es 20. Cada uno de estos bloques se define mediante una dirección IP base y el número de direcciones en el bloque. Las direcciones de cada bloque son ascendentes y contiguas, empezando desde la dirección base.

Sintaxis:

a**dd** d**hcp-server** *dirección-ip*

i**p-pool** *dirección-base número-direcciones*

dhcp-server *dirección-ip*

Añade un servidor dhcp con la dirección IP especificada.

Ejemplo:

```
DIALs Config> add dhcp-server
DIALs Proxy DHCP server address [0.0.0.0]? 10.0.0.1
```

ip-pool *dirección-base número-direcciones*
Añade un bloque de direcciones a la agrupación de IP.

Ejemplo:

```
DIALs Config> add ip-pool
Base address []? 192.1.100.18
Number of addresses [1]? 57
DIALs config>add ip-pool
Base address []? 192.2.200.1
Number of addresses [1]? 250
DIALs config>list ip-pools
Configured IP address pools:
     Base Address      Last Address        Number
          ------------      ------------        ------
          192.1.100.18      192.1.100.74            57
           192.2.200.1     192.2.200.250           250
```

Delete

Utilice el mandato **delete** para suprimir un servidor Proxy DHCP existente de la lista de servidores o para eliminar un bloque de direcciones de la agrupación de direcciones IP.

Sintaxis:

de**lete** dhcp-server *dirección-ip*

ip-pool *dirección-base número-direcciones*

dhcp-server *dirección-ip*
Elimina un servidor dhcp con la dirección IP especificada.

Ejemplo:

```
DIALs Config> delete dhcp-server
Enter the address to be deleted [0.0.0.0]? 10.0.0.1
```

ip-pool *dirección-base número-direcciones*
Elimina un bloque de direcciones de la agrupación de IP.

Ejemplo:

```
DIALs Config> delete ip-pool
Base IP address of the block to be removed []? 192.2.200.1
```

Disable

Utilice el mandato **disable** para inhabilitar un método de asignación de direcciones IP, protocolos de marcación de salida, Titular SPAP y DNS dinámico.

Sintaxis:

di**sable** dynamic-dns

dial-out

ip-address-assignment *tipo*

spap-banner

dial-out ***tipo***
Inhabilita el uso de la marcación de salida con clientes de marcación de salida IBM DIAL o Telnet. Puede especificar:

dials Inhabilita todos los clientes de marcación de salida IBM DIAL

telnet Inhabilita todos los clientes Telnet.

Para inhabilitar ambos tipos de clientes debe entrar el mandato disable dial-out para cada tipo. La inhabilitación de ambos tipos inhabilita la marcación de salida en el 2210.

dynamic-dns
Inhabilita el envío de la opción 81 de DHCP para el nombre de sistema principal del usuario. Consulte el apartado “Servidor de nombres de dominio dinámico (DDNS)” en la página 474 para obtener información.

IP-address-assignment *tipo*
Inhabilita varias técnicas de asignación de direcciones IPCP. Puede que desee especificar lo siguiente:

- Client – Impide la asignación de direcciones IP asignadas por el cliente.
- Userid – Impide que se utilice el perfil de usuario autentificado para una dirección IP.
- Interface – Impide que el direccionador utilice los valores de IPCP para la interfaz.
- Pool – Impide que el direccionador utilice la agrupación de direcciones IP para asignar direcciones a clientes.
- DHCP-proxy – Impide que el direccionador alquile una dirección del servidor DHCP.

Consulte “Direcciones IP proporcionadas por el servidor” en la página 471 para obtener información adicional sobre técnicas de asignación.

spap-banner
Inhabilita el envío de un titular SPAP a un usuario remoto autentificado con SPAP.

Nota: Si se entra \n se fuerza un carácter de línea nueva en el titular visualizado en el cliente.

Enable

Utilice el mandato **enable** para habilitar la asignación de direcciones IP, protocolos de marcación de salida, Titular SPAP y DNS dinámico.

Sintaxis:

enable dynamic-dns
ip-address-assignment . . .
spap-banner

dial-out *tipo*
Habilita el uso de la marcación de salida con clientes de marcación de salida IBM DIAL o Telnet. Por omisión, están habilitados ambos tipos de clientes. Puede especificar:

dials Habilita todos los clientes de marcación de salida IBM DIAL

telnet Habilita todos los clientes Telnet.

dynamic-dns

Habilita el envío de la opción 81 de DHCP para el nombre de sistema principal del usuario. Consulte el apartado “Servidor de nombres de dominio dinámico (DDNS)” en la página 474 para obtener información.

IP-address-assignment *tipo*

Habilita varias técnicas de asignación de direcciones IPCP. El direccionador intentará cada método habilitado en el orden listado. Puede que desee especificar lo siguiente:

- Client – Permite que el cliente especifique la dirección que desea utilizar.
- Userid – El direccionador buscará en el perfil de usuario PPP autentificado para obtener una dirección IP. Si la dirección es distinta de cero, se ofrecerá al cliente.
- Interface – El direccionador buscará la dirección IP configurada para la interfaz. Si la dirección es distinta de cero, se ofrecerá al cliente.
- Pool – El direccionador solicitará una dirección de la agrupación de direcciones IP. Si hay disponible una dirección, se ofrecerá al cliente.
- DHCP-proxy – El direccionador intentará alquilar una dirección de DHCP. Si la acción es satisfactoria, la dirección se ofrecerá al cliente.

Consulte “Direcciones IP proporcionadas por el servidor” en la página 471 para obtener información adicional sobre técnicas de asignación.

spap-banner

Habilita el envío de un titular SPAP a un usuario remoto autentificado con SPAP. Utilice el mandato **set spap-banner** que se describe en “Set” en la página 481 para entrar el texto del titular SPAP. Consulte “Shiva Password Authentication Protocol (SPAP)” en la publicación *Guía del usuario de software* para obtener más información.

List

Utilice el mandato **list** para visualizar la configuración actual. El estado y tiempos de alquiler de DHCP se pueden supervisar para cada red desde la consola Punto a punto. Consulte el mandato **listipcp** en la publicación *Guía del usuario de software* para obtener un ejemplo.

Sintaxis:

list all

dhcp-servers

dial out

dynamic-dns

ip-address-assignment

ip-pools

name-servers

spap-banner

time-allowed

vc-parameters

Ejemplo:

```
DIALs config>li all
 DIALs client IP address assignment:
Client     :  Enabled
UserID     :  Enabled
Interface  :  Enabled
Pool       :  Enabled
DHCP Proxy :  Disabled


Configured IP address pools:
     Base Address      Last Address        Number
     ------------      ------------        ------
       11.0.0.100        11.0.0.129            30
       11.0.0.210        11.0.0.229            20

Configured DHCP servers:           11.0.0.2         11.0.0.50
Proxy DHCP is currently disabled
DHCP gateway address (giaddr): 11.0.0.10

Dynamic DNS: Enabled

Primary Domain Name Server     (DNS): 11.0.0.2
Secondary Domain Name Server   (DNS): None
Primary NetBIOS Name Server   (NBNS): 11.0.0.2
Secondary NetBIOS Name Server (NBNS): None

Time allowed for connections: Unlimited

SPAP banner  :Enabled
Bienvenido a la red...

Box-level dial-out settings
Inactive timer:                                      15
LAN Protocols enabled for dial-out:         TELNET DIALs
Server name:                                   DIALOUT_SERVER

Number of Mac Addresses defined = 0
Base MAC Address: 000000000000

VC: Maximum Virtual Connections = 50
VC: Maximum suspend time (hours) (0 is unlimited) = 12
VC: Idle timeout period (seconds) = 30

Multi-chassis MP: Endpoint discriminator (0 means use box s/n) = 0

DIALs config>
```

El ejemplo muestra lo siguiente:

DIALs client IP address specification
: Visualiza las técnicas de asignación de direcciones IP y si están habilitadas. Debería recibir esta sección de la pantalla y la sección que contiene valores de marcación de salida de nivel de recuadro en respuesta al mandato **list ip-address-assignment**.

IP address pools
: Visualiza las agrupaciones de direcciones IP configuradas. Recibirá esta sección de la pantalla en respuesta al mandato **list ip-pool**.

Configured DHCP servers
: Visualiza la lista de direcciones IP configuradas actualmente como servidores DHCP. Esta sección también lista la interfaz que se utiliza para

la pasarela DHCP. Recibirá esta sección de la pantalla en respuesta al mandato **list dhcp-servers**.

Dynamic Name Servers
Visualiza si el DNS dinámico está habilitado. Recibirá esta sección de la pantalla en respuesta al mandato **list dynamic-dns**.

primary domain server (dns)
Esta línea y las líneas siguientes visualizan los servidores de nombres primario y secundario configurados. Recibirá esta sección de la pantalla en respuesta al mandato **list name-servers**.

time allowed
Visualiza la cantidad máxima de tiempo (en minutos) para los usuarios de Dial. Recibirá esta sección de la pantalla en respuesta al mandato **list time-allowed**.

spap banner
Visualiza el contenido del titular spap. Recibirá esta sección de la pantalla en respuesta al mandato **list spap-banner**.

vc connections
Visualiza información sobre las conexiones virtuales configuradas.

multi-chassis mp
Visualiza el discriminador de punto final configurado.

Set

Utilice el mandato **set** para establecer el tiempo-permitido, dirección de pasarela dhcp, direcciones de Servidor de nombres de NetBIOS, direcciones de Servidor de nombres dinámico y temporizador de inactividad de marcación de salida, y nombre-servidor de marcación de salida.

Sintaxis:

set dhcp-gateway-address
dial-out . . .
dns . . .
laa
multi-chassis-mp
nbns . . .
spap-banner . . .
time-allowed
vc-parameters

dhcp-gateway-address ***número-interfaz dirección-ip***
Establece la dirección IP asociada con la pasarela DHCP. DHCP utiliza la dirección como:

1. Una dirección a la que DHCP responde
2. Una indicación de la agrupación de direcciones de la cual DHCP asigna una dirección IP

Si el servidor DHCP no está en una interfaz de LAN conectada directamente, debe configurar esta dirección como la dirección de una de las

interfaces de LAN que tiene conectividad de IP con el servidor DHCP. Consulte “Dynamic Host Configuration Protocol (DHCP)” en la página 472 y la definición de “giaddr” en la RFC 1541 para obtener más información.

dial-out ***parámetro***

Establece el temporizador de inactividad o el nombre de servidores para redes de marcación de salida. ***Parámetro*** puede ser:

inactivity-timer

Establece el temporizador de inactividad de marcación de salida para redes de marcación de salida. Se define como la cantidad de tiempo, en minutos, que un usuario puede estar conectado sin tráfico de datos a través de la conexión. Por ejemplo, si el temporizador de inactividad se establece en 5 minutos y durante cualquier intervalo de 5 minutos no se reciben ni se transmiten datos, se desactivará la conexión y el módem quedará disponible. El valor por omisión es 0, lo que significa que el temporizador de inactividad está inhabilitado y que la conexión se mantendrá indefinidamente.

servername

Establece el nombre del servidor de marcación de salida. Puede ser cualquier serie con un máximo de 30 caracteres de longitud. El valor por omisión es “2210_DIALS_SERVER”. Es el nombre que ven los clientes de marcación de salida de IBM DIAL cuando utilizan la aplicación “Chooser” para encontrar servidores de marcación de salida. Este parámetro no tiene ningún significado para los clientes de marcación de salida Telnet.

dns ***tipo dirección-ip***

Configura los servidores de nombres de dominio (DNS) primarios y secundarios. ***Tipo*** puede ser:

primary

Establece la dirección IP del servidor DNS primario para que lo utilice el cliente de marcación de entrada. Este valor se negocia durante IPCP para algunos clientes de marcación (especialmente Windows® 95).

secondary

Establece la dirección IP del servidor DNS secundario para que lo utilice el cliente de marcación de entrada. El valor se negocia durante IPCP para algunos clientes de marcación (particularmente Windows 95).

laa *número-direcciones_MAC dirección_MAC_base*

Establece el número de direcciones MAC y la dirección base para la tabla Direcciones administradas localmente (LAA). Sólo las redes de Función de túnel de la capa 2 utilizarán direcciones de LAA.

número-direcciones_MAC

Especifica el número de direcciones Mac que deben añadirse a la tabla LAA, empezando por la *Dirección_MAC_base*.

Valores válidos: de 0 a 256

Valor por omisión: 0

Dirección_MAC_base

Especifica la dirección MAC base de la tabla LAA.

Valores válidos: Cualquier dirección MAC válida

Valor por omisión: 000000000000

Ejemplo:

```
DIALs config>set laa
    Number of Mac Addresses:  [0]? 20
    Locally Administered Mac Address Base (hex) [000000000000]? 002210aaaaaa
DIALs Config>
```

multi-chassis-mp

Establece el discriminador de punto final que debe utilizarse. Todos los enlaces que deben unirse al mismo paquete deben tener el mismo discriminador de punto final.

Ejemplo:

```
DIALs Config> set multi-chassis-mp
   Enter Endpoint Discriminator to use from stacked group (0 for box S/N): 2345
```

nbns *tipo dirección-ip*

Configura los servidores de nombres de NetBIOS primario y secundario. ***Tipo*** puede ser:

primary Establece la dirección IP del servidor de nombres de NetBIOS primario.

secondary

Establece la dirección IP del servidor de nombres de NetBIOS secundario.

spap-banner

Permite la configuración de un mensaje que se envía a todos los clientes que completan satisfactoriamente la autentificación de SPAP.

Ejemplo:

```
DIALs config>set spap-banner
SPAP banner  :Disabled

Enter Banner: Bienvenido a la red...
```

time-allowed

Establece el tiempo permitido para usuarios de marcación de entrada PPP y usuarios de marcación de salida. Este parámetro define la cantidad máxima de tiempo (en minutos) que un usuario puede estar conectado. El valor por omisión es 0, lo que significa que el usuario puede estar conectado durante una cantidad de tiempo ilimitada.

vc-parameters

Utilice este parámetro para establecer los atributos globales de conexión virtual por omisión. El sistema le solicitará el número máximo de conexiones, el tiempo máximo de suspendido y el valor de tiempo de espera de inactividad.

Ejemplo:

```
Config> feature DIALs
DIALs Config> set vc-parameters
Maximum Virtual Connections [50]? 40
Maximum suspended time (hours) (0 is unlimited) [10]? 18
Inactivity Timeout (seconds) [30]? 60
DIALs Config>
```

Maximum Virtual Connections El número máximo de conexiones virtuales que pueden estar activas o suspendidas. Cuando utilice VC con MP, configure este valor para que sea mayor en 1 que el número de conexiones físicas.

Valores válidos: de 0 a 255

Valor por omisión: 50

Maximum suspended time La cantidad máxima de tiempo, en horas, que una conexión virtual puede estar suspendida antes de que el sistema finalice la conexión. La especificación de 0 para este parámetro permite suspender una conexión virtual indefinidamente.

Valores válidos: de 0 a 48

Valor por omisión: 12

Inactivity Timeout El número de segundos que una conexión virtual puede estar inactiva antes de ser suspendida.

Valores válidos: de 10 a 1024

Valor por omisión: 30

Acceso al entorno de supervisión global de DIAL

Utilice el siguiente procedimiento para acceder a los mandatos de supervisión de DIAL.

1. En el indicador de mandatos OPCON, entre **talk 5**. (Para obtener detalles sobre este mandato, consulte el capítulo “The OPCON Process and Commands” en la publicación *Guía del usuario de software*.) Por ejemplo:

   ```
   * talk 5
   +
   ```

   Después de entrar el mandato **talk 5**, el indicador de mandatos GWCON (+) se visualiza en el terminal. Si el indicador de mandatos no aparece cuando inicia la configuración, pulse **Retorno** de nuevo.

2. En el indicador de mandatos +, entre el mandato **feature dials** para llegar al indicador de mandatos `DIALS Console>` y acceder al entorno de supervisión global.

   Ejemplo:

   ```
   + feature dials
   DIALS Console>
   ```

Mandatos de supervisión global de DIAL

Tabla 58. Mandatos de supervisión global de DIAL

Mandato	Función
Clear	Borra una conexión virtual suspendida específica.
List	Visualiza el estado de varias conexiones virtuales o de todas las conexiones virtuales.
Reset	Activa dinámicamente los parámetros de DIALS.
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 eliminar conexiones virtuales suspendidas específicas.

Sintaxis:

c**lear** vc *id_conexión*

vc *id_conexión*
Especifica la conexión virtual suspendida que está finalizando. Para obtener el *id_conexión*, entre el mandato **list all-vc** o **list suspended-vcs**.

List

Utilice el mandato **list** para visualizar todas las conexiones virtuales, conexiones virtuales activas, conexiones virtuales suspendidas o los valores de los parámetros de vc.

Sintaxis:

list all

active-vcs

all-vcs

dhcp-servers

ip-address-assignment

ip-pool

suspended-vcs

active-vcs
Visualiza los atributos de todas las conexiones virtuales activas. Vea la descripción del parámetro **all-vcs** para obtener una explicación de los atributos.

all-vcs Visualiza los atributos de todas las conexiones virtuales activas y suspendidas. Esta visualización es una combinación de las visualizaciones para los mandatos **list active-vcs** y **list suspended-vcs**.

Ejemplo:

```
+ feature dials
DIALS console> list all
 DIALs client IP address assignment:
Client     :  Enabled
UserID     :  Enabled
Interface  :  Enabled
Pool       :  Enabled
DHCP Proxy :  Disabled


Current IP address pools:
     Base Address      Last Address         Total          Free
     ------------      ------------         -----          ----
*      11.0.0.100        11.0.0.129           30            30
       11.0.0.210        11.0.0.229           20            19

Current DHCP servers:           11.0.0.2         11.0.0.50
Proxy DHCP is currently disabled
DHCP gateway address (giaddr): 11.0.0.10


Active VCs:
Conn ID    Interface Idle-Timeout Connected Username
========== ========= ============ HHH:MM:SS ================
1656494850         8           30   0:26:15 don
7293521502         9           30   1:41:57 jane


Suspended VCs:
           Hrs.Max
Conn ID    Suspend Suspended Username
========== =======  HH:MM:SS ======================
9256166098      12   0: 4:13 joe
```

Los atributos para las VC activas y suspendidas son:

Conn ID El ID de conexión de la conexión virtual. El sistema asigna el ID cuando establece la conexión.

Username

El usuario AAA. RADIUS o de lista-local que establece la conexión virtual.

Para las VC activos:

Interface La interfaz de red que gestiona la conexión virtual.

Nota: No asigne direcciones IP a clientes de marcación que utilicen asignación de interfaz para evitar problemas causados por otros usuarios que utilizan esta interfaz con la VC suspendida.

Idle Timeout

La cantidad de tiempo inactivo, en segundos, después del cual el sistema suspenderá la VC. Corresponde al valor del temporizador de inactividad en el mandato **set**.

Connected HHH:MM:SS

La cantidad de tiempo total en horas, minutos y segundos, que la VC ha estado conectada a una interfaz.

Para VC suspendidos:

Hrs. Max Suspended

El número máximo de horas que una VC puede estar en estado de suspendida antes de que el sistema finalice la conexión. Corresponde al valor de tiempo máximo suspendido en el mandato **set**.

Suspended HH:MM:SS
La cantidad de tiempo total en horas, minutos y segundos, que la VC ha estado suspendida.

dhcp-servers
Visualiza la información configurada sobre los servidores DHCP y sus direcciones IP.

ip-address-assignment
Visualiza los métodos mediante los cuales las direcciones IP pueden asignarse a clientes.

ip-pool Visualiza la utilización actual de la agrupación.

Ejemplo:

```
DIALs Console> list ip-pool
Current IP address pools:
     Base Address      Last Address         Total          Free
     ------------      ------------         -----          ----
*    192.1.100.18      192.1.100.74            57            57
      192.2.200.1     192.2.200.250           250           250

Note: The * indicates from which block the next address will be retrieved.
```

suspended-vcs
Visualiza los atributos de todas las conexiones virtuales suspendidas. Vea la descripción del parámetro **all-vcs** para obtener una explicación de los atributos.

vc-parameters
Visualiza los valores de parámetros de conexión virtual (vc-parameters) que se han establecido utilizando el mandato **set vc-parameters**.

Reset

Utilice el mandato **reset** para activar dinámicamente los cambios de configuración efectuados en la interfaz DIAL en `talk 6`.

Sintaxis:

reset all

dhcp-parameters

ip-address-assignment

ip-pool

vc-parameters

all Activa dinámicamente el DHCP, la asignación de direcciones IP y los cambios de configuración de la agrupación de IP.

dhcp-parameters
Activa dinámicamente la configuración de DHCP.

ip-address-assignment
Activa dinámicamente la configuración del método de asignación de direcciones IP.

ip-pool Activa dinámicamente la configuración de la agrupación de direcciones IP.

vc-parameters

Actualiza dinámicamente los cambios efectuados en la configuración de la VC.

Mandatos de configuración de interfaz de marcación de salida

Para acceder al entorno de parámetros de interfaz de marcación de salida:

1. Entre **talk 6** en el indicador de mandatos `*`.
2. Entre **net *n*** en el indicador de mandatos `Config >`.
3. Entre **encapsulator** en el indicador de mandatos `Circuit config: n>`.

La Tabla 59 lista los mandatos disponibles desde el indicador de mandatos `dial-out config>`.

Tabla 59. Mandatos de configuración de interfaz de marcación de salida

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Set	Define el nombre de puerto asociado a un módem.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Set

Utilice el mandato **set** para definir el nombre de puerto para un módem.

Sintaxis:

set portname *nombre*

portname

Define el nombre del puerto asociado con un módem. Utilice este nombre para definir ***agrupaciones de módems.*** El nombre puede tener un máximo de 30 caracteres de longitud.

Valor por omisión: ALL_PORTS

Ejemplo: `dial-out config>`**set portname llamadas-locales**

Supervisión de interfaces de marcación de entrada

La supervisión de interfaces de marcación de entrada es igual que la supervisión de otros circuitos de marcación PPP. Para obtener más detalles, consulte “Configuring and Monitoring Point-to-Point Protocol Interfaces” en la publicación *Guía del usuario de software* .

Supervisión de interfaces de marcación de salida

La Tabla 60 en la página 489 lista los mandatos disponibles cuando se supervisan interfaces de marcación de salida.

Tabla 60. Mandatos de supervisión de interfaces de marcación de salida	
Mandato	**Función**
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Clear	Restablece las estadísticas para la interfaz de marcación de salida.
List	Lista el estado actual de la interfaz de marcación de salida, el número de bytes transmitidos y recibidos en esta interfaz y los parámetros actuales del cliente.
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 colocar a cero las estadísticas sobre el número de octetos recibidos y transmitidos por esta interfaz.

Sintaxis:

c**lear**

Ejemplo:

```
clear
Statistics reset.
```

List

Utilice el mandato **list** para visualizar el estado actual de la interfaz de marcación de salida. El mandato **list** siempre visualiza el estado actual de la red de marcación de salida, el tiempo desde el cambio de estado y el número de bytes recibidos y transmitidos.

Sintaxis:

l**ist**

Ejemplo para interfaz inactiva:

```
list
Dial-out Settings for current session:

Dial-out state is DOWN
Time since change           = 52 minutes and 34 seconds

Dial-out Octets transmitted = 0
Dial-out Octets received    = 0

Session down, no valid settings
```

Nota: Cuando un cliente se conecta a un puerto de marcación de salida utilizando Telnet, no existe ningún nombre de usuario porque el servidor no ha efectuado ninguna autentificación.

Ejemplo para interfaz activa:

```
list
Dial-out Settings for current session:

Dial-out state is UP
Time since change           = 3 seconds

Dial-out Octets transmitted = 14
Dial-out Octets received    = 765

Current user                = not available
Time allowed for user       = unlimited
Inactivity timer for port   = 10 minutes
Line speed                  = 57600
Current DTR state           = DTR ON
Current dial-out protocol   = TELNET
Options negotiated:
        Will Suppress Go Ahead
        Wont' Echo characters
```

Ejemplo para un cliente de marcación de salida IBM DIAL activo:

```
list
Dial-out Settings for current session:

Dial-out state is UP
Time since change           = 12 seconds

Dial-out Octets transmitted = 11
Dial-out Octets received    = 756

Current user                = ebooth
Time allowed for user       = unlimited
Inactivity timer for port   = 10 minutes
Line speed                  = 57600
Current DTR state           = DTR ON
Current dial-out protocol   = DIALs
```

Soporte de reconfiguración dinámica de servidor DIAL

Esta sección describe la reconfiguración dinámica (DR) en lo que afecta a los mandatos de Talk 6 y Talk 5.

Delete interface de CONFIG (Talk 6)

El servidor DIAL (Dial-In Access to LANs) (Acceso de marcación de entrada a LAN) no soporta el mandato de CONFIG (Talk 6) **delete interface**.

Activate interface de GWCON (Talk 5)

El servidor DIAL (Dial-In Access to LANs) soporta el mandato de GWCON (Talk 5) **activate interface** sin restricciones.

La tabla siguiente resume los cambios de configuración del Servidor DIAL (Dial-In Access to LANs) que se activan cuando se invoca el mandato de GWCON (Talk 5) **activate interface**:

Mandatos cuyos cambios activa el mandato de GWCON (Talk 5) activate interface
CONFIG, feature dials, disable spap-banner
CONFIG, feature dials, enable spap-banner
CONFIG, feature dials, set dial-out inactivity-timer
CONFIG, feature dials, set spap-banner

Reset interface de GWCON (Talk 5)

El servidor DIAL soporta el mandato de GWCON (Talk 5) **reset interface** sin restricciones.

La tabla siguiente resume los cambios de configuración del Servidor DIAL que se activan cuando se invoca el mandato de GWCON (Talk 5) **reset interface**:

Mandatos cuyos cambios activa el mandato de GWCON (Talk 5) reset interface
CONFIG, feature dials, disable spap-banner
CONFIG, feature dials, enable spap-banner
CONFIG, feature dials, set dial-out inactivity-timer
CONFIG, feature dials, set spap-banner

Mandatos reset de componente GWCON (Talk 5)

El Servidor DIAL soporta los mandatos de GWCON (Talk 5) **reset** siguientes específicos del Servidor DIAL:

Mandato GWCON, feature dials, reset DHCP-parameters

Descripción: Este mandato restablece los parámetros de DIAL que están asociados con la función de proxy DHCP.

Efecto en la red: Ninguna.

Limitaciones: Ninguna.

La tabla siguiente resume los cambios de configuración del Servidor DIAL que se activan cuando se invoca el mandato **GWCON, feature dials, reset dhcp-parameters**:

Mandatos cuyos cambios activa el mandato GWCON, feature dials, reset dhcp-parameters
CONFIG, feature dials, add dhcp-server
CONFIG, feature dials, delete dhcp-server
CONFIG, feature dials, set dhcp-gateway-address

Mandato GWCON, feature dials, reset IP-address-assignment

Descripción: Este mandato se utiliza para activar cambios en los métodos de asignación de dirección IP. Esto no cambiará las direcciones asignadas actualmente, sino que especifica cómo se pueden asignar las direcciones IP en conexiones futuras. El cambio de configuración DNS dinámica también se activa con este mandato.

Efecto en la red: Ninguna.

Limitaciones: Ninguna.

La tabla siguiente resume los cambios de configuración del Servidor DIAL que se activan cuando se invoca el mandato **GWCON, feature dials, reset ip-address-assignment**:

Mandatos cuyos cambios activa el mandato GWCON, feature dials, reset ip-address-assignment
CONFIG, feature dials, enable dynamic-dns
CONFIG, feature dials, enable ip-address-assignment
CONFIG, feature dials, disable dynamic-dns
CONFIG, feature dials, disable ip-address-assignment

Mandato GWCON, feature dials, reset IP-pools

Descripción: Este mandato restablece la definición de agrupación de direcciones IP (direcciones añadidas o eliminadas) sin interrumpir las conexiones de red. Si una definición de agrupación de direcciones IP nueva no incluye direcciones que estaban anteriormente en la agrupación y que se están utilizando actualmente, las direcciones seguirán utilizándose después del restablecimiento. Cuando la interfaz libere dichas direcciones, éstas no volverán a la agrupación de direcciones IP y no se asignarán de nuevo.

Efecto en la red: Ninguna.

Limitaciones: Ninguna.

La tabla siguiente resume los cambios de configuración del Servidor DIAL que se activan cuando se invoca el mandato **GWCON, feature dials, reset ip-pools**:

Mandatos cuyos cambios activa el mandato GWCON, feature dials, reset ip-pools
CONFIG, feature dials, add ip-pool
CONFIG, feature dials, delete ip-pool

Mandato GWCON, feature dials, reset VC-parameters

Descripción: Este mandato restablece los parámetros de Conexión Virtual y el tamaño de tabla.

Efecto en la red: Si se reduce el tamaño de tabla, puede que algunos circuitos virtuales finalicen.

Limitaciones: Ninguna.

La tabla siguiente resume los cambios de configuración del Servidor DIAL que se activan cuando se invoca el mandato **GWCON, feature dials, reset vc-parameters**:

Mandatos cuyos cambios activa el mandato GWCON, feature dials, reset vc-parameters
CONFIG, feature dials, set vc-parameters

Mandato GWCON, feature dials, reset all

Descripción: Este mandato restablece todos los parámetros que se pueden restablecer mediante los mandatos reset de DIAL.

Efecto en la red: Consulte los mandatos reset individuales.

Limitaciones: Ninguna.

La tabla siguiente resume los cambios de configuración del Servidor DIAL (Dial-In Access to LANs) que se activan cuando se invoca el mandato **GWCON, feature dials, reset all**:

Mandatos cuyos cambios activa el mandato GWCON, feature dials, reset all
CONFIG, feature dials, add dhcp-server
CONFIG, feature dials, add ip-pool
CONFIG, feature dials, delete dhcp-server
CONFIG, feature dials, delete ip-pool
CONFIG, feature dials, enable dynamic-dns
CONFIG, feature dials, enable ip-address-assignment
CONFIG, feature dials, disable dynamic-dns
CONFIG, feature dials, disable ip-address-assignment
CONFIG, feature dials, set dhcp-gateway-address
CONFIG, feature dials, set ip-pools
CONFIG, feature dials, set vc-parameters

Mandatos de cambio inmediato de CONFIG (Talk 6)

El Servidor DIAL soporta los siguientes mandatos de CONFIG que cambian inmediatamente el estado operativo del dispositivo. Estos cambios se guardan y se conservan si se vuelve a cargar o se reinicia el dispositivo o si se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
CONFIG, feature dials, set dns
CONFIG, feature dials, set nbns
CONFIG, feature dials, set time-allowed

Mandatos no reconfigurables dinámicamente

La tabla siguiente describe los mandatos de configuración del Servidor DIAL que no se pueden cambiar dinámicamente. Para activar estos mandatos, es necesario volver a cargar o reiniciar el dispositivo.

Mandatos
CONFIG, feature dials, set dial-out servername
CONFIG, feature dials, set laa
CONFIG, feature dials, set multi-chassis-mp
CONFIG, feature dials, disable dial-out dials
CONFIG, feature dials, disable dial-out Telnet
CONFIG, feature dials, enable dial-out dials
CONFIG, feature dials, enable dial-out Telnet

Soporte de reconfiguración dinámica de marcación de salida

Esta sección describe la reconfiguración dinámica (DR) en lo que afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

La marcación de salida soporta el mandato de CONFIG (Talk 6) **delete interface** sin restricciones.

Mandato activate interface de GWCON (Talk 5)

La marcación de salida soporta el mandato de GWCON (Talk 5) **activate interface** con las consideraciones siguientes:

- No puede activar una red de marcación de salida a no ser que la red base ya esté activa.
- No puede activar una red de marcación de salida a no ser que el tipo de red base sea V34

El mandato de GWCON (Talk 5) **activate interface** soporta todos los mandatos de marcación de salida específicos de interfaz.

Mandato reset interface de GWCON (Talk 5)

La marcación de salida soporta el mandato de GWCON (Talk 5) **reset interface** con la consideración siguiente:

No puede restablecer una red de marcación de salida si la red base ha cambiado

El mandato de GWCON (Talk 5) **reset interface** soporta todos los mandatos de marcación de salida específicos de interfaz.

Utilización del servidor DHCP

Este capítulo describe cómo utilizar el Servidor DHCP. El capítulo incluye las secciones siguientes:

Introducción a DHCP

El Dynamic Host Configuration Protocol (DHCP) es un protocolo cliente/servidor basado en el Bootstrap Protocol (BOOTP). El servidor DHCP proporciona direcciones IP reutilizables controlables centralmente y otra información de configuración de TCP/IP para clientes DHCP. Su funcionalidad puede aligerar la carga que tienen los Gestores de la red al distribuir información de configuración a los usuarios nuevos y existentes. Esta característica cumple la RFC 2131 pero da soporte a muchas características adicionales que se incluyen en dicho documento. También existe soporte para clientes BOOTP tal como define la RFC 951.

Con DHCP, los clientes con soporte pueden enviar mensajes DISCOVER de difusión general para encontrar servidores DHCP en su red y posteriormente RECIBIR sus datos de configuración dinámicamente a través de la red. DHCP utiliza los puertos UDP BOOTP conocidos públicamente (68 para el servidor y 67 para el cliente) para comunicar peticiones y respuestas. Los clientes y servidores DHCP pueden utilizar agentes de retransmisión BOOTP existentes para ampliar su rango de servicios. DHCP ofrece muchas ventajas sobre las redes configuradas estáticamente, incluyendo la capacidad de soportar redes que cambian. Los clientes tan sólo alquilan sus direcciones IP y, por lo tanto, cuando ya no necesitan una dirección o se trasladan a otra red, la dirección de puede LIBERAR y hacer que esté disponible para que la utilicen otros clientes.

Operación de DHCP

DHCP permite que los clientes obtengan información de configuración de red IP, incluyendo una dirección IP, desde un servidor DHCP central. Los servidores DHCP controlan si las direcciones que proporcionan a los clientes se asignan permanentemente o se alquilan durante un período de tiempo específico. Cuando un cliente recibe una dirección alquilada, debe solicitar periódicamente que el servidor revalide la dirección y renueve el alquiler.

Los procesos de asignación de dirección, alquiler y renovación de alquiler los manejan los programas cliente y servidor DHCP y son transparentes para los usuarios finales. Los clientes utilizan mensajes con arquitectura RFC para aceptar y utilizar las opciones que les ofrece el servidor DHCP. Por ejemplo:

1. El cliente emite un mensaje de difusión general (que contiene su ID de cliente) que anuncia su presencia y solicita una dirección IP (mensaje DHCPDISCOVER) y las opciones que desea como, por ejemplo, máscara de subred, servidor de nombres de dominio, nombre de dominio y ruta estática.

2. Opcionalmente, si hay direccionadores en la red configurados para reenviar mensajes DHCP y BOOTP (utilizando Retransmisión BOOTP), el mensaje de difusión general se reenvía a los servidores DHCP en las redes conectadas.
3. Cada servidor DHCP que recibe el mensaje DHCPDISCOVER del cliente envía un mensaje DHCPOFFER al cliente ofreciéndole una dirección IP. El servidor DHCP comprueba si existen direcciones IP duplicadas en la red antes de emitir una oferta. El servidor comprueba el archivo de configuración para ver si debe asignar una dirección estática o dinámica a este cliente. En el caso de una dirección dinámica, el servidor selecciona una dirección de la agrupación de direcciones y elige la dirección menos utilizada recientemente. Una agrupación de direcciones es un rango de direcciones IP que se pueden alquilar a los clientes. En el caso de una dirección estática, el servidor utiliza una sentencia Client de la configuración del servidor DHCP para asignar opciones a los clientes. Cuando efectúa la oferta, el servidor DHCP reserva la dirección ofrecida.
4. El cliente recibe el(los) mensaje(s) ofrecido(s) y selecciona el servidor que desea utilizar. Cuando un cliente DHCP recibe una oferta, tiene en cuenta cuántas de las opciones solicitadas se incluyen en la oferta. El cliente DHCP continúa recibiendo ofertas de los servidores DHCP durante un período de 4 segundos después de recibir la primera oferta, teniendo en cuenta cuántas de las opciones solicitadas se incluyen en cada oferta. Al final de dicho tiempo, el cliente DHCP compara todas las ofertas y selecciona la que se ajusta a su criterio.
5. El cliente emite un mensaje de difusión general para indicar el servidor que ha seleccionado y solicita la utilización de la dirección IP ofrecida por dicho servidor (mensaje DHCPREQUEST).
6. Si un servidor recibe un mensaje DHCPREQUEST indicando que el cliente ha aceptado la oferta del servidor, el servidor marca dicha dirección como alquilada. Si el servidor recibe un mensaje DHCPREQUEST indicando que el cliente ha aceptado una oferta de un servidor diferente, el servidor devuelve la dirección a la agrupación disponible. Si no se recibe ningún mensaje dentro de un tiempo especificado, el servidor devuelve la dirección a la agrupación disponible. El servidor seleccionado envía al cliente un acuse de recibo que contiene información de configuraciones adicionales (mensaje DHCPACK).
7. El cliente determina si la información de configuración es válida. Cuando recibe un mensaje DHCPACK, el cliente DHCP envía una petición de Address Resolution Protocol (ARP) a la dirección IP proporcionada para ver si todavía está en uso. Si recibe una respuesta para la petición de ARP, el cliente rechaza (mensaje DHCPDECLINE) la oferta e inicia el proceso de nuevo. De lo contrario, el cliente acepta la información de configuración.
8. Al aceptar un alquiler válido, el cliente entra en un estado de BINDING (Enlace) con el servidor DHCP y pasa a utilizar la dirección y opciones de IP. Si el cliente DHCP es un cliente de Dirección dinámica, el DHCP notifica al Servidor de nombres de dominio dinámico su correlación entre nombre de sistema principal y dirección IP.

Para clientes DHCP que solicitan opciones, el servidor DHCP generalmente proporciona opciones que incluyen máscara de subred, servidor de nombres de dominio, nombre de dominio, ruta estática, identificador de clase (que indica un proveedor particular) y clase de usuario.

Sin embargo, un cliente DHCP puede solicitar su propio conjunto exclusivo de opciones. Por ejemplo, los clientes DHCP de Windows NT 3.5.1 deben solicitar las opciones. El conjunto por omisión de opciones DHCP solicitadas por el cliente que proporciona IBM incluye la máscara de subred, el servidor de nombres de dominio, el nombre de dominio y la ruta estática. Para ver las descripciones de las opciones, vea “Opciones de DHCP” en la página 503.

Renovaciones de alquiler

El cliente DHCP realiza un seguimiento de cuánto tiempo queda de alquiler. En un determinado momento antes de que caduque el alquiler, generalmente cuando ha transcurrido la mitad del tiempo de alquiler, el cliente envía una petición de renovación, que contiene su información de dirección y configuración de IP actuales, al servidor del alquiler. Si el servidor responde con una oferta de alquiler, el alquiler del cliente DHCP se renueva.

Si el servidor DHCP rechaza explícitamente la petición, el cliente DHCP puede continuar utilizando la dirección IP hasta que caduque el tiempo de alquiler y, a continuación, iniciar el proceso de petición de dirección, incluyendo la emisión de un mensaje de difusión general para la petición de dirección. Si el servidor no es asequible, el cliente puede seguir utilizando la dirección asignada hasta que caduque el alquiler.

Traslado del cliente

Una ventaja de DHCP es la libertad que proporciona a un sistema principal cliente para trasladarse de una subred a otra sin necesidad de tener de antemano información sobre qué configuración de IP necesita en la nueva subred. Siempre y cuando las subredes a las que un sistema principal se traslada tengan acceso a un servidor DHCP, un cliente DHCP se configurará automáticamente a sí mismo correctamente para acceder a dichas subredes.

Para que los clientes DHCP puedan reconfigurarse para acceder a una nueva subred, el sistema principal cliente debe volverse a arrancar. Cuando un sistema principal se reinicia en una nueva subred, el cliente DHCP intenta renovar su alquiler antiguo con el servidor DHCP que le ha asignado originalmente la dirección. El servidor rechaza renovar la petición puesto que la dirección no es válida en la nueva subred. Si no recibe ninguna respuesta o instrucciones por parte del servidor DHCP, el cliente inicia el proceso de petición de dirección IP para obtener una nueva dirección IP y acceder a la red.

Cambio de las opciones del servidor

Con DHCP, se pueden efectuar cambios en el servidor, reinicializar el servidor y distribuir los cambios a todos los clientes apropiados. Un cliente DHCP retiene los valores de las opciones de DHCP asignados por el servidor DHCP mientras dura el alquiler. Si se implantan cambios de configuración en el servidor mientras un cliente ya está configurado y en ejecución, el cliente DHCP no procesa estos cambios hasta que el cliente intenta renovar su alquiler o hasta que se reinicia.

Nota: Si el servidor no contiene una tarjeta de Disco fijo o de almacenamiento Flash y se reinicializa (utilizando el mandato `t 5` **reset dhcp**), la información de tiempo de alquiler visualizada por el direccionador se perderá hasta que los clientes DHCP renueven su alquiler.

Número de servidores DHCP

El número de servidores necesarios dependerá en gran medida del número de subredes de que se disponga, del número de clientes DHCP a los que tiene intención de dar soporte, de si se utiliza Retransmisión BOOTP y del tiempo de alquiler que se elija. Tenga en cuenta que el protocolo DHCP actualmente no define comunicación de servidor a servidor. Por este motivo, no pueden compartir información, ni un servidor DHCP puede actuar como “de reserva” en el caso de que el otro falle. Los clientes DHCP envían mensajes de difusión general. Debido a su diseño, los mensajes de difusión general no cruzan subredes. Para permitir que los mensajes del cliente se reenvíen fuera de su subred, deben configurarse direccionadores adicionales para reenviar peticiones de DHCP utilizando el agente Retransmisión BOOTP. De lo contrario, deberá configurar un servidor DHCP en cada subred.

Un único servidor DHCP

Si elige utilizar un único servidor DHCP para servir a sistemas principales en una subred, considere las consecuencias que puede tener una anomalía del único servidor. Generalmente, la anomalía de un servidor sólo afectará a los clientes DHCP que intenten entrar en la red. Por lo general, los clientes DHCP que ya están en la red seguirán funcionando sin verse afectados hasta que caduque su alquiler. Sin embargo, los clientes con un tiempo de alquiler corto pueden perder su acceso a la red antes de poder restablecer el servidor. Para minimizar el impacto del tiempo de inactividad del servidor si sólo tiene un servidor DHCP en una subred, debe elegir un tiempo de alquiler suficientemente largo para dejar tiempo para responder al servidor DHCP que ha fallado o reiniciarlo.

Múltiples servidores DHCP

Para evitar un único punto de anomalía, puede configurar dos o más servidores DHCP para servir en la misma subred. Si falla un servidor, el otro puede continuar sirviendo en la subred. Cada uno de los servidores DHCP debe ser accesible mediante conexión directa a la subred o utilizando un agente de Retransmisión BOOTP.

Puesto que dos servidores DHCP no pueden servir las mismas direcciones, las agrupaciones de direcciones definidas para una subred deben ser exclusivas entre servidores DHCP. Por lo tanto, cuando se utilizan dos o más servidores DHCP para servir en una subred particular, la lista completa de direcciones para dicha subred debe dividirse entre los servidores. Por ejemplo, puede configurar un servidor con una agrupación de direcciones consistente en el 70% de las direcciones disponibles para la subred y el otro servidor con una agrupación de direcciones que consista en el 30% restante de las direcciones disponibles.

La utilización de varios servidores DHCP disminuye la probabilidad de tener una anomalía de acceso a la red relacionada con DHCP, pero no garantiza que no pueda producirse. Si un servidor DHCP para un subred particular falla, el otro servidor DHCP puede que no sea capaz de servir todas las peticiones de los clientes nuevos que, por ejemplo, agotan la agrupación limitada de direcciones disponibles del servidor.

Sin embargo, puede prever qué servidor DHCP agotará primero su agrupación de direcciones. Los clientes DHCP tienden a seleccionar el servidor DHCP que ofrece más opciones. Para inclinar el servicio hacia el servidor DHCP con el 70% de

direcciones disponibles, ofrezca menos opciones DHCP desde el servidor que tiene un 30% de las direcciones disponibles para la subred.

Servidores BOOTP

Si ya tiene clientes y servidores BOOTP en la red, puede que desee considerar la sustitución de los servidores BOOTP por servidores DHCP. Los servidores DHCP pueden servir opcionalmente a clientes BOOTP la misma información de configuración de IP que los servidores BOOTP actuales. Si no puede sustituir los servidores BOOTP por servidores DHCP y desea que ambos sirvan en la red, se recomienda tener en cuenta las siguientes precauciones:

- Desactive el soporte de BOOTP en el servidor DHCP.
- Asegúrese de que los servidores BOOTP y los servidores DHCP no proporcionen las mismas direcciones.
- Configure el soporte de Retransmisión BOOTP en los direccionadores para reenviar mensajes de difusión general de BOOTP a los servidores BOOTP y DHCP apropiados.

Un servidor DHCP asigna una dirección IP permanente a un cliente BOOTP. En el caso de que las subredes se renumeren de modo que una dirección asignada por BOOTP no se pueda utilizar, el cliente BOOTP debe reiniciarse y obtener una nueva dirección IP.

Clientes DHCP especiales

Puede tener clientes DHCP o Servidores de red que tengan necesidades administrativas individuales o especiales, como por ejemplo:

- Un alquiler permanente:

  Puede asignar alquileres permanentes a sistemas principales designados especificando un tiempo de alquiler infinito. El servidor DHCP también asignará un alquiler permanente a clientes BOOTP que lo soliciten explícitamente siempre y cuando esté habilitado el soporte para clientes BOOTP. El servidor DHCP también asignará un alquiler permanente a sistemas principales DHCP que lo soliciten explícitamente.

- Una dirección IP específica:

  Puede reservar una dirección específica y parámetros de configuración para un sistema principal cliente DHCP o BOOTP en una determinada subred.

- Parámetros de configuración específicos:

  Puede asignar información de configuración específica a un cliente independientemente de cuál sea su subred.

- Estaciones de trabajo definidas manualmente:

  Debe excluir explícitamente las direcciones de subredes DHCP para los sistemas principales existentes que no utilizan DHCP o BOOTP para configurar su acceso a la red IP. Aunque los servidores y clientes DHCP comprueban automáticamente si hay una dirección IP en uso antes de asignarla o de utilizarla, no podrán detectar las direcciones de sistemas principales definidos manualmente que estén desactivados o temporalmente fuera de la red. En este caso, pueden producirse problemas de direcciones duplicadas cuando un sistema principal definido manualmente vuelve a acceder a la red, a menos que su dirección IP se haya excluido explícitamente.

Tiempos de alquiler

El tiempo de alquiler por omisión es 24 horas. Tenga en cuenta que el tiempo de alquiler de DHCP puede afectar al funcionamiento y al rendimiento de la red:

- Los tiempos de alquiler cortos aumentan la cantidad de tráfico en la red debido a las peticiones de renovación de alquiler de DHCP. Por ejemplo, si establece un tiempo de alquiler de 5 minutos, cada cliente envía una petición de renovación cada 2,5 minutos.
- Los tiempos de alquiler demasiado largos pueden limitar la capacidad de reutilización de direcciones IP. Los tiempos de alquiler muy largos también retardan los cambios de configuración que se producen cuando un cliente se reinicia o renueva un alquiler.

El tiempo de alquiler que elija depende en gran medida de sus necesidades, para lo que debe considerar:

- El número de sistemas principales que debe dar soporte en comparación con el número de direcciones disponibles. Si tiene más sistemas principales que direcciones, puede que desee elegir un tiempo de alquiler corto de una o dos horas. Esto le ayudará a asegurar que las direcciones no utilizadas se devuelvan a la agrupación lo antes posible.
- El tiempo disponible para efectuar cambios en la red. Los sistemas principales reciben cambios en la información de configuración cuando se reinician o cuando renuevan su alquiler. Asegúrese de permitir una ventana adecuada y con suficiente tiempo para que se lleven a cabo estos cambios. Por ejemplo, si normalmente realiza cambios de noche, puede asignar un tiempo de alquiler de 12 horas.
- El número de servidores DHCP que están disponibles. Si sólo tiene unos cuantos servidores DHCP para una red grande, puede que desee elegir un tiempo de alquiler más largo para minimizar el impacto del tiempo que los servidores no están disponibles.

Para redes complejas que deben soportar una combinación de requisitos de alquiler de sistemas principales, puede definir clases de DHCP.

Conceptos y terminología

Para describir la función de servidor DHCP se utilizan los conceptos siguientes:

Ámbito El término ámbito, cuando se describe la Configuración del servidor DHCP, se utilizará para identificar a qué pertenece un valor de parámetro determinado. La Figura 38 en la página 501 ilustra los ámbitos siguientes:

- Opción global 1
- Opción global 3
- Clase global ClaseA

  La ClaseA ha redefinido la opción 1, pero heredará el valor de la opción 3 del ámbito global.
- Cliente global ClienteA

  El ClienteA ha redefinido la opción 3, pero heredará el valor de la opción 1 del ámbito global.

- subred SubA
  - Redefine la Opción 1.
  - Hereda el valor de Opción 3 del ámbito global.
  - Define la ClaseB dentro del ámbito de SubA.

    Redefine el valor de la opción 1, pero heredará el valor de la opción 3 de SubA (que también se hereda del ámbito global).
  - Define ClienteB dentro del ámbito de SubA.

    ClienteB ha redefinido la opción 3, pero heredará el valor de la opción 1 de SubA.
- opción de proveedorA

  Las opciones de proveedor son una excepción. Las opciones de proveedor son independientes y no se heredan fuera del ámbito de opción de proveedor.

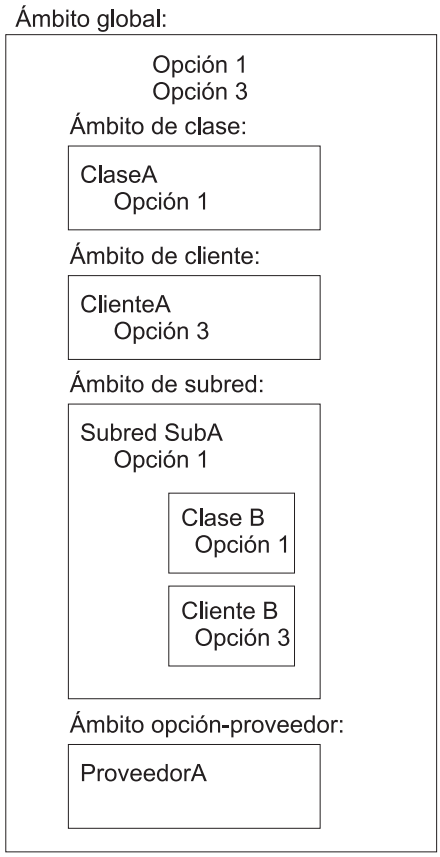


Figura 38. Conceptos de ámbito

Subred Una subred define los parámetros para una agrupación de direcciones administrada por un servidor DHCP. Una agrupación de direcciones es un rango de direcciones IP que se pueden alquilar a los clientes. Los parámetros que se pueden especificar incluyen el tiempo de alquiler y otras opciones para los clientes que utilizan la agrupación de direcciones. El tiempo de alquiler y las otras opciones se pueden heredar del ámbito global.

Grupos de subredes

Un grupo de subredes es un modo de identificar varias subredes que se van a agrupar en la misma interfaz. A todas las subredes de un grupo determinado se les proporciona el mismo nombre de grupo de subred y una prioridad exclusiva. La prioridad se utiliza para determinar el orden con el que se proporcionan las direcciones de acuerdo con la política de direcciones asociada al grupo. Una subred puede pertenecer a una de dos políticas de direcciones:

- Inorder (Por orden)

  Es la política por omisión. La política "inorder" administra las direcciones empezando por la subred con la prioridad más baja y finalizando por la subred con la prioridad más alta.

- Balance (Equilibrada)

  La política "balance" administra las direcciones del grupo de subredes definidas siguiendo un orden rotatorio. La primera dirección se administra de la subred con la prioridad más baja. La segunda dirección se administra de la subred con la siguiente prioridad más baja y así sucesivamente. Cuando se ha administrado la subred con la prioridad más alta, la política vuelve a la subred con la prioridad más baja hasta que se agotan todas las subredes del grupo.

Clases Una clase define los parámetros para un grupo definido de clientes, administrados por el servidor DHCP. Las clases se pueden definir bajo el ámbito global o de subred. Cuando se define una clase dentro de un ámbito de subred, el servidor DHCP sólo sirve a los clientes de la clase que están en la subred especificada y que solicitan la clase. Solamente las clases que están definidas dentro del ámbito de subred pueden especificar un rango de direcciones. El rango puede ser un subconjunto del rango de subred o puede ser igual que el rango de subred. Si un cliente solicita una dirección IP de una clase que ha agotado su rango, se le ofrece una dirección IP del rango de subred, si está disponible. Se ofrecen al cliente las opciones asociadas con la clase agotada.

Clientes Un cliente se puede utilizar para:

- Definir una dirección IP estática y opciones de DHCP para una estación final específica
- Excluir del servicio una estación final específica
- Excluir una dirección IP de un rango de direcciones IP disponibles

Cada cliente tiene un tipo de hardware especificado, id de cliente y dirección IP. Los tipos de hardware se definen en la RFC 1340 y se muestran a continuación. Para todos los tipos de hardware aparte de 0, el ID de cliente es la dirección de hardware de la estación final (o dirección MAC). Para el tipo de hardware de 0, el ID de cliente es una serie de caracteres. Por lo general, sería un nombre de dominio.

Cuando define un cliente, se le solicitará una dirección IP, *any* (cualquiera) o *none* (ninguna). Si define una dirección IP, esta dirección IP se reserva para el cliente. Si elige *any* (cualquiera), se proporcionará al cliente cualquier dirección IP disponible dentro de dicha subred. Si tiene varios registros de subredes definidos dentro de la misma subred, cada uno de los cuales con un rango exclusivo, un cliente configurado con *any* (cualquiera) obtendrá la primera dirección disponible de la subred,

no necesariamente del rango del registro de subred específico en el que está definido el cliente. Si elige *none* (ninguna), dicha estación final no recibirá ninguna dirección IP. Para hacer que una dirección IP no se administre, debe definir un registro de cliente con un tipo de hardware e ID de cliente de 0.

Los tipos de hardware que se definen en la RFC1340 y que pertenecen al IBM 2210 son:

```
Tipo de hardware                          Valor
-------------                             -----
Reservado                                 0
Ethernet                                  1
Redes IEEE 802 (incluyendo Red en Anillo) 6
```

Para obtener la lista completa, consulte la RFC 1340.

Servidor DHCP y parámetros de alquiler

Los siguientes parámetros de servidor DHCP se pueden definir en el nivel global:

- bootstrapserver (servidor de rutina de carga)
- canonical (canónico)
- lease expire interval (intervalo de caducidad de alquiler)
- lease time default (valor por omisión de tiempo de alquiler)
- ping time (tiempo de sondeo)
- support unlisted clients (soportar clientes no listados)
- bootp support (soporte de bootp)
- used ip address expire interval (intervalo de caducidad de dirección ip)

Consulte “Set” en la página 551 para obtener una descripción de estos parámetros.

Opciones de DHCP

DHCP le permite especificar opciones para proporcionar información de configuración adicional para un cliente. Las opciones se definen en la RFC 2132 y en otras RFC.

Formatos de opción

Todas las opciones salvo los datos de configuración deben tener uno de los formatos siguientes:

Formato	Definición
Dirección IP	Una única dirección IP en notación decimal con puntos.
Direcciones IP	Una o más direcciones IP en notación decimal con puntos, separadas por blancos.
Par de direcciones IP	Dos direcciones IP en notación decimal con puntos, separadas por blancos.

Pares de direcciones IP	Uno o más pares de direcciones IP, cada par separado del otro por un blanco.
Booleano	0 ó 1 (Verdadero o Falso).
Byte	Un número decimal entre -128 y 127 (incluidos).
Byte sin signo	Un número decimal entre 0 y 255 (incluidos). No puede especificar un valor negativo para un byte sin signo.
Lista de bytes sin signo	Uno o más números decimales entre 0 y 255 (incluidos) separados por blancos. No puede especificar un número negativo para un byte sin signo.
Corto	Un número decimal entre -32768 y 32767 (incluidos).
Corto sin signo	Un número decimal entre 0 y 65535 (incluidos). No puede especificar un número negativo para un número corto sin signo.
Lista de cortos sin signo	Uno o más números decimales entre 0 y 65535 (incluidos) separados por blancos. No puede especificar un número negativo para un número corto sin signo.
Largo	Un número decimal entre -2147483648 y 2147483647 (incluidos).
Largo sin signo	Un número decimal entre 0 y 4294967295 (incluidos). No puede especificar un número negativo para un número largo sin signo.
Serie	Una serie de caracteres.
N/D	Indica que no hace falta ninguna especificación porque el cliente genera esta información.

Cada opción de DHCP se identifica mediante un código numérico.

Las opciones con arquitectura de 0 a 127 y la opción 255 se reservan para definiciones mediante RFC. El servidor DHCP, el cliente DHCP o el servidor y el cliente utilizan opciones de este conjunto. El administrador puede modificar algunas opciones con arquitectura. Otras opciones son para el uso exclusivo por parte del cliente y el servidor.

Nota: Los valores hexadecimales no se permiten para las opciones con arquitectura con formatos conocidos.

Las opciones que el administrador no puede o no debe configurar en el servidor DHCP son las siguientes:

52 Sobrecarga de opción

53 Tipo de mensaje de DHCP

54 Identificador de servidor

55 Lista de petición de parámetros

56 Mensaje

57 Tamaño máximo de mensaje de DHCP

60 Identificador de clase

Las opciones de la 128 a la 254 representan opciones definidas por el usuario que los administradores pueden definir para pasar información al cliente DHCP para implantar parámetros de configuración específicos del emplazamiento.

Adicionalmente, IBM proporciona un conjunto de opciones específicas de IBM, como por ejemplo la opción 192: TXT RR

El formato de una opción definida por el usuario es:

Sintaxis:

opción *código valor*

donde,

código Cualquier código de opción de 1 a 254, excepto los códigos que ya están definidos en una RFC.

valor Debe ser siempre una serie. En el servidor, puede ser una serie ASCII o una serie hexadecimal. Sin embargo, en el cliente siempre aparece como una serie hexadecimal tal como se pasa al programa de proceso.

El servidor pasa el valor especificado al cliente. Sin embargo, debe crearse un programa o un archivo de mandatos para procesar el valor.

Opciones base proporcionadas al cliente

Las siguientes opciones base se proporcionan al cliente. Consulte “Formatos de opción” en la página 503 para obtener una descripción del formato de configuración.

1 **Máscara de subred** Esta opción sólo se especifica en el servidor DHCP. La máscara de subred del cliente, especificada en notación decimal con puntos de 32 bits. Aunque no es necesaria, en la mayoría de configuraciones el servidor DHCP debe enviar la opción 1, máscara de subred, a los clientes DHCP. La operación del cliente puede no ser previsible si el cliente no recibe ninguna máscara de subred desde el servidor DHCP y utiliza una máscara de subred que no es apropiada para la subred. Si no se especifica, el cliente utiliza las máscaras de subred por omisión:

- Red de Clase A 255.0.0.0
- Red de Clase B 255.255.0.0
- Red de Clase C 255.255.255.0

Formato de la opción: Direcciones IP

2 **Desplazamiento de tiempo** Esta opción sólo se especifica en el servidor DHCP. El desplazamiento (en segundos) de la subred del cliente respecto a la Hora universal coordinada (CUT). El desplazamiento es un entero son signo de 32 bits.

Formato de la opción: Largo

3 **Direccionador** Esta opción sólo se especifica en el servidor DHCP. Se trata de las direcciones IP (en orden de preferencia) de los direccionadores en la subred del cliente.

Formato de la opción: Direcciones IP

4 **Servidor de tiempo** Esta opción sólo se especifica en el servidor DHCP. Se trata de las direcciones IP (en orden de preferencia) de los servidores de tiempo disponibles para el cliente.

Formato de la opción: Direcciones IP

5 **Servidor de nombres** Esta opción sólo se especifica en el servidor DHCP. Se trata de las direcciones IP (en orden de preferencia) de los servidores de nombres IEN 116 disponibles para el cliente.

Nota: No es la opción Servidor de nombres de dominio. Utilice la Opción 6 para especificar un Servidor de nombres de dominio.

Formato de la opción: Direcciones IP

6 **Servidor de nombres de dominio** Esta opción sólo se especifica en el servidor DHCP. Se trata de las direcciones IP (en orden de preferencia) de los servidores del Sistema de nombres de dominio disponibles para el cliente.

Formato de la opción: Direcciones IP o direcciones de interfaz IP sin número (por ejemplo, 0.0.0.2)

Nota: Si se habilita la dirección dinámica en la configuración IP para una interfaz PPP, es posible que pueda recuperar una dirección DNS Primaria y Secundaria utilizando IPCP desde un Suministrador de servicio de Internet (ISP). Para pasar estas direcciones DNS a los clientes DHCP, deberá configurar la opción 6 con una dirección de interfaz IP no numerada (por ejemplo 0.0.0.n) que corresponda a la interfaz de Dirección dinámica. El servidor DHCP la convertirá en el valor recuperado del ISP cuando el cliente envíe una petición. Si se habilita Simple-Internet-Access en la configuración IP, se configurará automáticamente la opción 6 con con la interfaz IP no numerada. A cualquier cliente que solicite la información de configuración a este Servidor antes de la activación de la interfaz PPP, se le ofrecerá un tiempo de alquiler reducido (3 minutos) a fin de dejar tiempo para que se completen la conexión PPP e IPCP. Cuando se conozcan las direcciones DNS, se ofrecerán los tiempos de alquiler configurados.

7 **Servidor de registro cronológico** Esta opción sólo se especifica en el servidor DHCP. Se trata de las direcciones IP (en orden de preferencia) de los servidores de anotaciones MIT-LCS UDP disponibles para el cliente.

Formato de la opción: Direcciones IP

8 **Servidor cookie** Esta opción sólo se especifica en el servidor DHCP. Se trata de las direcciones IP (en orden de preferencia) de servidores de cookies o de "quote-of-the-day" (cita-del-día) disponibles para el cliente.

Formato de la opción: Direcciones IP

9 **Servidor LPR** Esta opción se puede especificar en el cliente DHCP y en el servidor DHCP. Sin embargo, si sólo se especifica en el cliente DHCP, la configuración estará incompleta. Se trata de las direcciones IP (en orden de preferencia) de los servidores de impresora de líneas disponibles para el cliente. La opción 9 elimina la necesidad de que los clientes especifiquen la variable de entorno LPR_SERVER.

Formato de la opción: Direcciones IP

10 **Servidor Impress** Esta opción sólo se especifica en el servidor DHCP. Se trata de las direcciones IP (en orden de preferencia) de los servidores Imagen Impress disponibles para el cliente.

Formato de la opción: Direcciones IP

11 **Servidor de ubicación de recurso** Esta opción sólo se especifica en el servidor DHCP. Se trata de las direcciones IP (en orden de preferencia) de los servidores de ubicación de recurso (RLP) disponibles para el cliente. Los servidores RLP permiten que los clientes localicen los recursos que proporcionan un servicio específico, como por ejemplo un servidor de nombres de dominio.

Formato de la opción: Direcciones IP

12 **Nombre de sistema principal** Esta opción se puede especificar en el cliente DHCP y en el servidor DHCP. Si el cliente DHCP no proporciona ningún nombre de sistema principal, el servidor DHCP ignora la opción 12. Se trata del nombre de sistema principal del cliente (que puede que incluya el nombre de dominio local). La longitud mínima para la opción de nombre de sistema principal es 1 octeto y el máximo es 32 caracteres. Consulte la RFC 1035 para conocer las limitaciones del juego de caracteres.

Formato de la opción: Serie

13 **Tamaño de archivo de arranque** Esta opción sólo se especifica en el servidor DHCP. Se trata de la longitud (en bloques de 512 octetos) del archivo de configuración de arranque por omisión para el cliente.

Formato de la opción: Corto sin signo

14 **Archivo de vuelco merit** Esta opción sólo se especifica en el servidor DHCP. Se trata del nombre de vía de acceso del archivo de vuelco merit en el que se almacena la imagen de la memoria del cliente si el cliente tiene una anomalía. La vía de acceso tiene formato de serie de caracteres formada por los caracteres del juego de caracteres ASCII de Terminal virtual de red (NVT). La longitud mínima es 1 octeto.

Formato de la opción: Serie

15 **Nombre de dominio** Esta opción se especifica en el cliente DHCP y en el servidor DHCP. Si no se especifica ningún valor en el servidor DHCP para la opción 15, es necesario que el cliente proporcione un valor para la opción 12, nombre de sistema principal, y la opción 15, nombre de dominio. Esta sentencia puede aparecer dentro del ámbito global o con un ámbito de Subred, Clase o Cliente.

Formato de la opción: Serie

16 **Servidor de intercambio** Esta opción sólo se especifica en el servidor DHCP. Se trata de la dirección IP del servidor de intercambio del cliente.

Formato de la opción: Dirección IP

17 **Vía de acceso raíz** Esta opción sólo se especifica en el servidor DHCP. Se trata de la vía de acceso que contiene el disco raíz del cliente. La vía de acceso tiene formato de serie de caracteres formada por los caracteres del juego de caracteres ASCII de NVT. La longitud mínima es 1 octeto.

Formato de la opción: Serie

18 **Vía de acceso de extensión** Esta opción sólo se especifica en el servidor DHCP. La opción de vía de acceso de extensión especifica una serie que se puede utilizar para identificar a un archivo que se puede recuperar utilizando el Trivial File Transfer Protocol (TFTP). La longitud mínima es 1 octeto.

Formato de la opción: Serie

Opciones de parámetros de capa de IP por sistema principal

19 **Reenvío de IP** Esta opción sólo se especifica en el servidor DHCP. Este parámetro permite habilitar (1) o inhabilitar (0) el reenvío por parte del cliente de sus paquetes de capa de IP.

Formato de la opción: Booleano

20 **Direccionamiento de origen no local** Esta opción sólo se especifica en el servidor DHCP. Este parámetro permite habilitar (1) o inhabilitar (0) el reenvío por parte del cliente de sus datagramas de capa de IP con rutas de origen no local.

Formato de la opción: Booleano

21 **Filtro de política** Esta opción sólo se especifica en el servidor DHCP. Se trata del par de red IP-máscara de red que se utiliza para filtrar los datagramas con rutas de origen no local. El cliente descarta cualquier datagrama cuya dirección de salto siguiente no coincida con ninguno de los pares de filtro. La longitud mínima para la opción de filtro de política es 8 octetos.

Formato de la opción: Pares de direcciones IP

22 **Tamaño máximo de reensamblaje de datagrama** Esta opción sólo se especifica en el servidor DHCP. Se trata del datagrama de tamaño máximo que el cliente reensamblará. El valor mínimo es 576.

Formato de la opción: Corto sin signo

23 **Tiempo de vida por omisión** Esta opción sólo se especifica en el servidor DHCP. Tiempo de vida (TTL) por omisión que el cliente utiliza en datagramas de salida. El TTL es un octeto con un valor entre 1 y 255.

Formato de la opción: Byte sin signo

24 **Tiempo de espera excedido de período de MTU de vía de acceso** Esta opción sólo se especifica en el servidor DHCP. Se trata del tiempo de espera excedido en segundos que se utiliza para calcular la edad de

los valores de Unidad máxima de transmisión (MTU) de vía de acceso descubiertos por el mecanismo que se describe en la RFC 1191.

Formato de opción: Largo sin signo

25 **Tabla de tamaños de MTU de vía de acceso** Esta opción sólo se especifica en el servidor DHCP. Se trata de la tabla de tamaños de MTU a solicitar en la determinación de MTU de vía de acceso tal como se define en la RFC 1191. El valor mínimo de MTU es 68. La longitud mínima para la opción de tabla de tamaños de MTU de vía de acceso es de 2 octetos. La longitud debe ser un múltiplo de 2.

Formato de la opción: Corto sin signo

Opciones de parámetros de capa de IP por interfaz

26 **MTU de interfaz** Esta opción sólo se especifica en el servidor DHCP. Se trata de la Unidad máxima de transmisión (MTU) a solicitar en esta interfaz. El valor mínimo de MTU es 68.

Formato de la opción: Corto sin signo

27 **Todas las subredes son locales** Esta opción sólo se especifica en el servidor DHCP. El cliente supone (1) o no supone (0) que todas las subredes utilizan la misma Unidad máxima de transmisión (MTU). Un valor de 0 indica que el cliente supone que algunas subredes tienen valores de MTU menores.

Formato de la opción: Booleano

28 **Dirección de mensaje de difusión general** Esta opción sólo se especifica en el servidor DHCP. Se trata de la dirección de mensaje de difusión general que se utiliza en la subred del cliente.

Formato de la opción: Dirección IP

29 **Realizar determinación de máscara** Esta opción sólo se especifica en el servidor DHCP. El cliente realiza (1) o no realiza (0) la determinación de máscara de subred utilizando el Protocolo de mensajes de control de Internet (ICMP).

Formato de la opción: Booleano

30 **Suministrador de máscara** Esta opción sólo se especifica en el servidor DHCP. El cliente responde (1) o no responde (0) a las peticiones de máscara de subred utilizando el Protocolo de mensajes de control de Internet (ICMP).

Formato de la opción: Booleano

31 **Realizar determinación de direccionador** Esta opción sólo se especifica en el servidor DHCP. El cliente solicita (1) o no solicita (0) direccionadores utilizando la determinación de direccionador tal como se define en la RFC 1256.

Formato de la opción: Booleano

32 **Dirección de solicitud de direccionador** Esta opción sólo se especifica en el servidor DHCP. Se trata de la dirección a la cual el cliente transmite peticiones de solicitud de direccionador.

Formato de la opción: Dirección IP

33 **Ruta estática** Esta opción sólo se especifica en el servidor DHCP. Se trata de las rutas estáticas (pares de dirección-direccionador de designación por orden de preferencia) que el cliente instala en su antememoria de direccionamiento. La primera dirección es la dirección de destino y la segunda dirección es el direccionador para el destino. No especifique 0.0.0.0 como destino de ruta por omisión.

Formato de la opción: Pares de direcciones IP

Opciones de parámetros de capa de enlace por interfaz

34 **Encapsulación de cola** Esta opción sólo se especifica en el servidor DHCP. El cliente negocia (1) o no negocia (0) la utilización de colas cuando se utiliza el Protocolo de conversión de direcciones (ARP). Para obtener más información consulte la RFC 893.

Formato de la opción: Booleano

35 **Tiempo de espera de antememoria de ARP** Esta opción sólo se especifica en el servidor DHCP. Tiempo de espera en segundos para las entradas de antememoria del ARP (Address Resolution Protocol).

Formato de opción: Largo sin signo

36 **Encapsulación de Ethernet** Esta opción sólo se especifica en el servidor DHCP. Para una interfaz Ethernet, el cliente utiliza la encapsulación Ethernet IEEE 802.3 (1) que se describe en la RFC 1042 o la encapsulación Ethernet V2 (0) que se describe en la RFC 894.

Formato de la opción: Booleano

Opciones de parámetros de TCP

37 **TTL por omisión de TCP** Esta opción sólo se especifica en el servidor DHCP. Se trata del tiempo de vida (TTL) por omisión que el cliente utiliza para enviar segmentos TCP.

Formato de la opción: Byte sin signo

38 **Intervalo de hacer perdurar de TCP** Esta opción sólo se especifica en el servidor DHCP. Se trata del intervalo en segundos que el cliente espera antes de enviar un mensaje de hacer perdurar en una conexión TCP. Un valor de 0 indica que el cliente no envía mensajes de hacer perdurar a menos que lo solicite la aplicación.

Formato de opción: Largo sin signo

39 **Basura de hacer perdurar de TCP** Esta opción sólo se especifica en el servidor DHCP. El cliente envía (1) o no envía (0) mensajes de hacer perdurar de TCP que contienen un octeto de basura para compatibilidad con implantaciones anteriores.

Formato de la opción: Booleano

Opciones de parámetros de aplicación y servicio

40 **Dominio de servicio de información de red** Esta opción sólo se especifica en el servidor DHCP. Se trata del dominio de Servicio de información de red (NIS) del cliente. El dominio tiene formato de serie de caracteres formada por los caracteres del juego de caracteres ASCII de NVT. La longitud mínima es 1 octeto.

Formato de la opción: Serie

41 **Dominio de servicio de información de red** Esta opción sólo se especifica en el servidor DHCP. Se trata de las direcciones IP (en orden de preferencia) de los servidores de Servicio de información de red (NIS) disponibles para el cliente.

Formato de la opción: Direcciones IP

42 **Servidores de Network Time Protocol** Esta opción sólo se especifica en el servidor DHCP. Se trata de las direcciones IP (en orden de preferencia) de los servidores de Network Time Protocol (NTP) disponibles para el cliente.

Formato de la opción: Direcciones IP

43 **Información específica del proveedor** La opción 43 sólo se especifica en el servidor DHCP, que devuelve esta opción a un cliente que envía la opción 60, Identificador de clase. Esta opción de información la utilizan los clientes y servidores para intercambiar información específica del proveedor, que se especifica en la definición de opción de proveedor. Las consideraciones a tener en cuenta para la utilización de la Opción 43 para encapsular información de proveedor son las siguientes:

- Para permitir interoperabilidad entre clientes y servidores de distintos proveedores, cada proveedor debe documentar con claridad el contenido de su opción 43 utilizando el formato estándar de la RFC 2132.
- Cada proveedor debe especificar las opciones concretas que se puedan encapsular dentro de la opción 43 de modo que los servidores DHCP de otro proveedor puedan implantarlas fácilmente. Por ejemplo, el proveedor debe:
  - Representar dichas opciones en tipos de datos ya definidos para opciones de DHCP o en otros tipos datos bien definidos.
  - Elegir opciones que se puedan codificar fácilmente en archivos de configuración para intercambiarlas con otros servidores suministrados por otros proveedores.
  - Ser fácilmente soportable por todos los servidores.

Los servidores que no pueden interpretar la información específica de un proveedor enviada por un cliente deben ignorarla. Los clientes que no reciben la información específica de un proveedor que desean deben intentar funcionar sin ella. Consulte las RFC 2131 y RFC 2132 para obtener información adicional sobre esta opción.

Nota: Debido a estas consideraciones, IBM utiliza en su lugar las opciones 192 y 200 para opciones específicas de IBM.

Formato de la opción: Serie

44 **NetBIOS sobre Servidor de nombres TCP/IP** Esta opción sólo se especifica en el servidor DHCP. Se trata de las direcciones IP (en orden de preferencia) de los servidores de nombres de NetBIOS (NBNS) disponibles para el cliente.

Formato de la opción: Direcciones IP

45 **NetBIOS sobre Servidor de distribución de datagramas TCP/IP** Esta opción sólo se especifica en el servidor DHCP. Se trata de las direcciones IP (en orden de preferencia) de los servidores de nombres de Distribución de datagramas de NetBIOS (NBDD) disponibles para el cliente.

Formato de la opción: Direcciones IP

46 **NetBIOS sobre Tipo de nodo TCP/IP** Esta opción sólo se especifica en el servidor DHCP. Se trata del tipo de nodo utilizado para clientes configurables de NetBIOS sobre TCP/IP tal como se describe en las RFC 1001 y RFC 1002. Los valores para especificar los tipos de cliente incluyen:

- nodo B 0x1
- nodo P 0x2
- nodo M 0x4
- nodo H 0x8

Formato de la opción: Byte sin signo

47 **NetBIOS sobre Ámbito TCP/IP** Esta opción sólo se especifica en el servidor DHCP. Se trata del parámetro NetBIOS sobre ámbito TCP/IP para el cliente, tal como se especifica en los RFC 1001/1002. La longitud mínima es 1 octeto.

Formato de la opción: Byte sin signo

48 **Servidor de fonts del Sistema X Window** Esta opción sólo se especifica en el servidor DHCP. Se trata de las direcciones IP (en orden de preferencia) de los servidores de fonts del Sistema X Window disponibles para el cliente.

Formato de la opción: Direcciones IP

49 **Gestor de pantallas del Sistema X Window** Esta opción sólo se especifica en el servidor DHCP. De trata de las direcciones IP (en orden de preferencia) de los sistemas que ejecutan el Gestor de pantallas del Sistema X Window disponibles para el cliente.

Formato de la opción: Direcciones IP

Opciones de ampliaciones de DHCP

50 **Dirección IP solicitada** Esta opción sólo se especifica en el cliente DHCP. El servidor DHCP puede rechazar una petición de cliente DHCP para una dirección IP específica. Permite que el cliente solicite (DHCPDISCOVER) una dirección IP particular.

Formato de opción: N/D

51 **Tiempo de alquiler de dirección IP** Esta opción se puede especificar tanto en el cliente DHCP como en el servidor DHCP. El cliente DHCP puede utilizar la opción 51 para alterar temporalmente el valor defaultLeaseInterval ofrecido por el servidor DHCP. Permite que el cliente solicite (DHCPDISCOVER o DHCPREQUEST) un tiempo de alquiler para una dirección IP. En una respuesta (DHCPOFFER), un servidor DHCP utiliza la opción para ofrecer un tiempo de alquiler. Esta opción se puede especificar dentro del ámbito global, de subred, de

clase o de cliente. Utilice X'ffffffff' para indicar un alquiler infinito (permanente).

Formato de opción: Largo sin signo

58 **Valor de tiempo de renovación (T1)** Esta opción sólo se especifica en el servidor DHCP. Se trata del intervalo en segundos entre la hora en que el servidor asigna una dirección y la hora en que el cliente pasa al estado de renovación.

Formato de opción: Largo sin signo

59 **Valor de tiempo de reenlace (T2)** Esta opción sólo se especifica en el servidor DHCP. Intervalo en segundos entre la hora en que el servidor asigna una dirección y la hora en la que los clientes pasan a estado de reenlace.

Formato de opción: Largo sin signo

60 **Identificador-clase** Esta opción sólo se especifica en el cliente DHCP. Esta información la genera el cliente y no es necesario especificarla. Se trata del tipo y configuración del cliente, proporcionados por el cliente al servidor. Por ejemplo, el identificador puede codificar la configuración de hardware específica del proveedor del cliente. La información es una serie de *n* octetos, interpretados por los servidores. Por ejemplo: hex: X'01' X'02' X'03'. Los servidores que no están equipados para interpretar la información específica de la clase enviada por un cliente deben ignorarla. La longitud mínima es 1 octeto.

Formato de opción: N/D

61 **Identificador de cliente** Esta opción se puede especificar tanto en el cliente DHCP como en el servidor DHCP. El cliente DHCP puede utilizar la opción 61 para especificar el identificador de cliente exclusivo. El servidor DHCP puede utilizar la opción 61 para indexar la base de datos de enlaces de direcciones. Este valor se espera que sea exclusivo para todos los clientes de un dominio administrativo.

Formato de la opción: Serie

62 **Nombre de dominio NetWare/IP** Esta opción sólo se especifica en el servidor DHCP. Se trata del nombre de dominio Netware/IP. La longitud mínima es 1 octeto y la longitud máxima es 255.

Formato de la opción: Serie

63 **NetWare/IP** Esta opción sólo se especifica en el servidor DHCP. Se trata del código de opción de propósito general que se utiliza para comunicar toda la información relacionada con NetWare/IP salvo el nombre de dominio NetWare/IP. Se comunicarán varias subopciones de NetWare/IP utilizando el código de opción. La longitud mínima es 1 y la longitud máxima es 255.

Formato de la opción: Serie

64 **Nombre de dominio NIS** Esta opción sólo se especifica en el servidor DHCP. Se trata del nombre de dominio de cliente de Servicio de información de red (NIS)+ V3. El dominio tiene formato de serie de caracteres formada por los caracteres del juego de caracteres ASCII de NVT. Su longitud mínima es 1.

Formato de la opción: Serie

65 **Servidores NIS** Esta opción sólo se especifica en el servidor DHCP. Se trata de las direcciones IP (en orden de preferencia) de los servidores de Servicio de información de red (NIS)+ V3 disponibles para el cliente.

Formato de la opción: Direcciones IP

66 **Nombre de servidor** Esta opción sólo se especifica en el servidor DHCP. Se trata del nombre de servidor de Trivial File Transfer Protocol (TFTP) que se utiliza cuando se ha usado el campo “sname” de la cabecera DHCP para opciones de DHCP.

Formato de la opción: Serie

67 **Nombre de archivo de arranque** Esta opción sólo se especifica en el servidor DHCP. Se trata del nombre del archivo de arranque cuando se ha utilizado el campo "file" en la cabecera DHCP para las opciones de DHCP. La longitud mínima es 1.

Nota: Utilice esta opción para pasar un nombre de archivo de arranque a un cliente DHCP. El nombre de archivo de arranque debe incluir el nombre de vía de acceso completamente calificado y debe tener menos de 128 caracteres de longitud. Por ejemplo: opción 67 c:\vía\nombre_archivo_arranque. Este archivo contiene información que se puede interpretar del mismo modo que el campo de ampliación de proveedor de 64 octetos dentro de la respuesta de BOOTP, con la excepción de que la longitud de archivo está limitada a 128 caracteres por la cabecera BootP.

Formato de la opción: Serie

68 **Dirección inicial** Esta opción sólo se especifica en el servidor DHCP. Se trata de las direcciones IP (en orden de preferencia) de los agentes iniciales de IP móviles disponibles para el cliente. La opción permite a un sistema principal móvil obtener una Dirección inicial móvil y determinar la máscara de subred para la red inicial. La longitud normal es de cuatro octetos, incluyendo la dirección inicial de un solo agente inicial, pero la longitud puede ser cero. Una longitud de cero indica que no hay disponible ningún agente inicial.

Formato de la opción: Direcciones IP

69 **Servidores SMTP** Esta opción sólo se especifica en el servidor DHCP. Se trata de las direcciones IP (en orden de preferencia) de los servidores de Simple Mail Transfer Protocol (SMTP) disponibles para el cliente.

Formato de la opción: Direcciones IP

70 **Servidor POP3** Esta opción sólo se especifica en el servidor DHCP. Se trata de las direcciones IP (en orden de preferencia) de los servidores de Post Office Protocol (POP) para el cliente.

Formato de la opción: Direcciones IP

71 **Servidor NNTP** Esta opción sólo se especifica en el servidor DHCP. Se trata de las direcciones IP (en orden de preferencia) de los servidores de Network News Transfer Protocol (NNTP) disponibles para el cliente.

Formato de la opción: Direcciones IP

72 **Servidor WWW** Esta opción sólo se especifica en el servidor DHCP. Se trata de las direcciones IP (en orden de preferencia) de los servidores de la World Wide Web (WWW) disponibles para el cliente.

Formato de la opción: Direcciones IP

73 **Servidor Finger** Esta opción sólo se especifica en el servidor DHCP. Direcciones IP (en orden de preferencia) de los servidores Finger disponibles para el cliente.

Formato de la opción: Direcciones IP

74 **Servidor IRC** Esta opción sólo se especifica en el servidor DHCP. Direcciones IP (en orden de preferencia) de los servidores de Internet Relay Chat (IRC) disponibles para el cliente.

Formato de la opción: Direcciones IP

75 **Servidor StreetTalk** Esta opción sólo se especifica en el servidor DHCP. Direcciones IP (en orden de preferencia) de los servidores StreetTalk disponibles para el cliente.

Formato de la opción: Direcciones IP

76 **Servidor STDA** Esta opción sólo se especifica en el servidor DHCP. Direcciones IP (en orden de preferencia) de los servidores de StreetTalk Directory Assistance (STDA) disponibles para el cliente.

Formato de la opción: Direcciones IP

77 **Clase de usuario** Esta opción sólo se especifica en el cliente DHCP. Los clientes DHCP utilizan la opción 77 para indicar a los servidores DHCP a qué clase de sistema principal pertenece. La clase de usuario debe entrarse manualmente en el archivo \DHCPCD.CFG como el valor para la opción 77 a fin de recibir los parámetros definidos para la clase en un servidor DHCP. El archivo DHCPCD.CFG está situado en el directorio ONDEMAND\SERVER\ETC.

Formato de la opción: Serie

78 **Agente de directorio** Esta opción sólo se especifica en el servidor DHCP. El Dynamic Host Configuration Protocol proporciona una estructura para pasar información de configuración a los sistemas principales de una red TCP/IP. Las entidades que utilizan el Service Location Protocol deben averiguar la dirección de Agentes de directorio para poder gestionar mensajes. En otros casos puede que deban averiguar el ámbito y autorización de nombre correctos que deben utilizarse junto con los atributos de servicio y los URL que se intercambian utilizando el Service Location Protocol. Un agente de directorio tiene un ámbito particular y puede tener información sobre los esquemas definidos por una autorización de nombre particular.

Formato de la opción: Dirección IP

79 **Ámbito de servicio** Esta opción sólo se especifica en el servidor DHCP. Esta extensión indica el ámbito que debe utilizar un agente de servicio, cuando responde a los mensajes de Petición de servicio tal como se especifica en el Service Location Protocol.

Formato de la opción: Serie

80 **Autorización de nombre** Esta opción sólo se especifica en el servidor DHCP. Esta ampliación indica una autorización de nombre, que especifica la sintaxis para los esquemas que pueden utilizarse en los URL que utilizan las entidades con el Service Location Protocol.

Formato de la opción: Serie

Opciones específicas de IBM

IBM proporciona un conjunto de opciones específicas de IBM definiendo opciones dentro del rango definido por el usuario (128-254). Estas opciones se utilizan en lugar de definir una opción de proveedor (opción 43) para IBM. Se recomienda no volver a definir estas opciones.

192 **TXT RR** Si esta opción se especifica en el servidor DHCP, el usuario cliente DHCP debe completar los campos de información de administrador del sistema. Nota: Esta opción sólo está soportada en TCP/IP Versión 4.1 para clientes OS/2. Esta opción proporciona un máximo de cuatro etiquetas de texto o campos de entrada necesarios para que los especifique el administrador del sistema, como por ejemplo el nombre de un usuario, el número de teléfono del usuario u otros campos que el Programa de configuración de Cliente DDNS solicita al usuario. Estos campos permiten que el administrador del sistema identifique la persona real que ha configurado el nombre de sistema principal u otros datos. El Programa de configuración DDNS no visualiza estos campos a menos que el administrador del sistema los especifique. Esta información se almacena en un registro de texto en el DNS. Los pares de etiquetas de campo y datos deben caber dentro de un único registro de recurso TXT. El espacio disponible se divide equitativamente entre los pares. El valor también se actualiza en el archivo DDNSCLI.CFG del cliente de Dirección dinámica.

Formato de la opción: Serie

Opciones del proveedor

El protocolo DHCP proporciona un medio para suministrar información específica del proveedor a un cliente DHCP utilizando las opciones de arquitectura de RFC 43 y 60.

60 La **Opción 60** se configura en un cliente DHCP y se envía al servidor DHCP para identificar al cliente como perteneciente a un proveedor específico.

43 La **Opción 43** se configura en el servidor DHCP para definir la información específica del proveedor que debe devolverse al cliente en respuesta a la petición de la opción 60 del cliente. Para el servidor DHCP de Código común, la opción 43 se configura utilizando el mandato add vendor-option. Una opción de proveedor sólo está definida dentro del ámbito global. La opción de proveedor consiste en el nombre del proveedor y los datos de la opción. Los datos de la opción tienen dos formatos:

Datos hexadecimales

Se utiliza con el nombre de proveedor cuando se emite el mandato add vendor-option. Los datos hexadecimales deben entrarse como una serie hexadecimal con blancos entre los bytes: “01 AA 55”

Opciones

Se puede añadir cualquier opción de DHCP a un ámbito de opción de proveedor utilizando el mandato add option.

Nota: Los datos hexadecimales y opciones se excluyen mutuamente en una definición de proveedor. Puede definir uno o el otro, pero no ambos.

Configuración de IP para DHCP

Para que el servidor DHCP asigne satisfactoriamente direcciones IP e información de configuración para los clientes de una subred añadida, puede que se tenga que configurar IP de forma apropiada. Esto es necesario cuando el servidor DHCP está conectado directamente a una subred para la que está configurado para dar soporte.

Si se utiliza un agente de retransmisión BOOTP para reenviar mensajes de petición de DHCP a este servidor DHCP, puede que no exista ninguna configuración de IP necesaria para dar soporte a una red que no está directamente conectada al servidor.

Adición de una dirección IP

Una dirección IP que esté dentro de la subred configurada DHCP deberá añadirse a la interfaz de conexión.

Ejemplo:

- DHCP ha añadido una subred del modo siguiente:

```
DHCP Server config>list subnet all
subnet      subnet          subnet          starting        ending
name        address         mask            IP Addr         IP Addr
-------------------------------------------------------------------------
net-one     192.168.8.0     255.255.255.0   192.168.8.2     192.168.8.50
```

- IP requerirá lo siguiente:

```
IP config>add address
Which net is this address for [0]? 0
New address []? 192.168.8.1
Address mask [255.255.255.0]?

IP config>list add
IP addresses for each interface:
intf     0   192.168.8.1      255.255.255.0    Local wire broadcast, fill 1
intf     1                                     IP disabled on this interface
intf     2   0.0.0.2          255.255.255.255  Local wire broadcast, fill 1
intf     3                                     IP disabled on this interface
```

Utilización de Simple-Internet-Access de IP

Si está habilitado Simple-Internet-Access en IP y no se ha configurado previamente DHCP, se generará automáticamente la configuración siguiente en el servidor DHCP. Simple-Internet-Access también configurará automáticamente la característica NAT y otros filtros y controles de acceso de IP. Si DHCP ya está configurado, no se realizarán cambios/adiciones en la configuración de DHCP. Consulte to Utilización de Simple Internet Access en el capítulo “Utilización de IP” de la publicación *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener mas información conocer las limitaciones.

- IP se ha configurado del modo siguiente:

```
IP config>enable simple-internet-access
Interface to Service Provider [0]? 3
SIMPLE-INTERNET-ACCESS enabled on interface 3

IP config>add address
Which net is this address for [0]? 0
New address []? 192.168.8.1
Address mask [255.255.255.0]?

IP config>list add
IP addresses for each interface:
intf     0   192.168.8.1      255.255.255.0    Local wire broadcast, fill 1
intf     1                                     IP disabled on this interface
intf     2                                     IP disabled on this interface
intf     3   0.0.0.3          255.255.255.255  Local wire broadcast, fill 1
                                               SIMPLE-INTERNET-ACCESS Enabled
```

- Se generará la siguiente configuración para el servidor DHCP:

```
DHCP Server config> list global
.
.
DHCP Server enabled: Yes
.
.
DHCP Server config>list subnet all
subnet      subnet           subnet           starting         ending
name        address          mask             IP Addr          IP Addr
-------------------------------------------------------------------------
simple-net  192.168.8.0      255.255.255.0    192.168.8.2      192.168.8.50

DHCP Server config>list option subnet
Enter the subnet name []? simple-net
 option  option
 code    data
-----------------------------------------------------------------
 1       255.255.255.0
 3       192.168.8.1
 6       0.0.0.3
```

Configuración del servidor DHCP de ejemplo

Archivo de texto ASCII

Esta sección proporciona una configuración de servidor DHCP típica en un formato de texto ASCII. Este ejemplo es estrictamente ilustrativo, para mostrar una configuración en un formato que pueda serle familiar. El IBM 2210 no soporta configuraciones ASCII.

Puede utilizar los números que van dentro de un recuadro (**1**) para relacionar las funciones que se describen en este ejemplo ASCII con la configuración de `talk 6` equivalente que se muestra en “Configuración de OPCON (Talk 6)” en la página 520.

```
1  Configuración de parámetros del Servidor

leaseTimeDefault          120                  # 120 minutes
leaseExpireInterval       20 seconds
supportBOOTP              yes
supportUnlistedClients  yes


2  Opciones globales. Se pasan a cada cliente a menos que se alteren
temporalmente en un ámbito inferior.

option 15       "raleigh.ibm.com"         # domain name
option 6         9.67.1.5                         # dns server

                 class manager
{
  option 48   6.5.4.3
  option 9    9.37.35.146
  option 210  "manager_authority"   # site specific option given to all managers
}

3  Opciones de proveedor


vendor  XI-clients hex"01 02 03"

vendor XA-clients
{
   option 23 100   # IP TTL
}

4  Subred típica

subnet  9.2.23.0  255.255.255.0        9.2.23.120-9.2.23.126
{
        option 28       9.2.23.127         # broadcast address
        option 9   5.6.7.8
        option 51  200

5  gestor de clase definido en el ámbito de subred. La opción 9
de aquí prevalecerá sobre
la opción 9 especificada en el gestor de clase global.
                 class manager

        {
                option 9   9.2.23.98
        }
```

```
6 Los programadores tienen su propio rango de subred

        class developers  9.2.23.125-9.2.23.126
        {
                option 51       -1              # infinite lease.
                option 9        9.37.35.1       # printer used by the developers
        }
}

7 Ejemplo de un cliente que aceptará cualquier dirección pero que tendrá
su propio conjunto de opciones.

client 6        0x10005aa4b9ab  ANY
{
        option 51 999
        option 1 255.255.255.0
}

8 Excluir una dirección del servicio.

client 0       0               9.2.23.121
```

Configuración de OPCON (Talk 6)

A continuación se proporciona un ejemplo de la misma configuración utilizando talk 6.

```
1 Configuración de parámetros del Servidor

Config>f dhcp-server
DHCP server user configuration
DHCP Server config> enable dhcp
DHCP Server config>

DHCP Server config> set lease-time-default hours 2
DHCP Server config>set lease-expire-interval seconds 20
DHCP Server config>set support-bootp yes
DHCP Server config>set support-unlisted-clients global yes
```

```
DHCP Server config>li glob
DHCP server Global Parameters
=============================

DHCP server enabled: Yes

Balance:  No subnet groups defined

Inorder:  No subnet groups defined

Canonical: No

Lease Expire Interval:  20 second(s)
Lease Time Default:     2 hour(s)


Support BOOTP Clients: Yes
Bootstrap Server: Not configured

Support Unlisted Clients: Yes

Ping Time:  1 second(s)
Used IP Address Expire Interval:  15 minute(s)
```

2 Opciones globales. Se pasan a cada cliente a menos que se alteren temporalmente en un ámbito inferior.

```
DHCP Server config>add option global 15 raleigh.ibm.com
DHCP Server config>add option global 6 9.67.1.5

DHCP Server config>li option global
 option  option
 code    data
------------------------------------------------------------------
15      raleigh.ibm.com
6       9.67.1.5

DHCP Server config>add class global
Enter the class name []? manager
Class record with name manager has been added

DHCP Server config>add option class-global
Enter the class name []? manager
Enter the option code [1]? 48
Enter the option data []? 6.5.4.3

DHCP Server config>add option class-global 9 9.37.35.146
DHCP Server config>add option class-global manager 210 manager_authority

DHCP Server config>li class global manager
 class
 name
------------------------------------------------------------------
 manager

 Number of Options: 3
 option  option
 code    data
 ------------------------------------------------------------------
 48       6.5.4.3
 9        9.37.35.146
 210     manager_authority
```

3 Opciones de proveedor

```
DHCP Server config>add vendor-option XI-client
Enter the vendor hex data []? 01 02 03
Vendor-option record with name XI-client has been added

DHCP Server config> add vendor-option XA-client
Enter the vendor hex data []?
Vendor-option record with name XA-client has been added
DHCP Server config> add option vendor-option XA-client 23 100

DHCP Server config>li vendor-option all
vendor      hex
name        data
-----------------------------------------------------------------
XI-client   01 02 03
XA-client
DHCP Server config>li vendor-option det XA-client
vendor      hex
name        data
-----------------------------------------------------------------
XA-client

  Number of Options: 1
 option  option
 code    data
 ----------------------------------------------------------------
 23      100
```

4 Subred típica

```
DHCP Server config>add subnet
Enter the subnet name []? sub1
Enter the IP subnet []? 9.2.23.0
Enter the IP subnet mask [255.255.255.0]?
Enter start of IP address range [9.2.23.1]? 9.2.23.120
Enter end of IP address range [9.2.23.150]? 9.2.23.126
Enter the subnet group name []?
Subnet record with name sub1 has been added
DHCP Server config>
DHCP Server config> add option subnet
Enter the subnet name []? sub1
Enter the option code []? 28
Enter the option data []? 9.2.23.127
DHCP Server config> add option subnet 9 5.6.7.8
DHCP Server config>add option subnet sub1 51 200

DHCP Server config>add class subnet
Enter the subnet name []? sub1
Enter the class name []? manager
Enter start of IP address range []?
Class record with name manager has been added

DHCP Server config>add option class-subnet sub1 manager
Enter the option code [1]? 9
Enter the option data []? 9.2.23.98
```

6 Los programadores tienen su propio rango de subred

```
DHCP Server config>add class subnet
Enter the subnet name []? sub1
Enter the class name []? developers
Enter start of IP address range []? 9.2.23.125
Enter end of IP address range []? 9.2.23.126
Class record with name developers has been added

DHCP Server config>add option class-subnet sub1 developers 51 -1
DHCP Server config>add option class-subnet sub1 developers 9 9.37.35.1
```

```
DHCP Server config>li subnet detailed sub1
subnet      subnet           subnet           starting         ending
name        address          mask             IP Addr          IP Addr
-------------------------------------------------------------------------
sub1        9.2.23.0         255.255.255.0    9.2.23.120       9.2.23.126


 Number of Classes: 2
 class
 name
 ----------------------------------------------------------------
 manager

  Number of Options: 1
 option  option
 code    data
  ----------------------------------------------------------------
  9       9.2.23.98
 developers
  starting IP address: 9.2.23.125
  ending   IP address: 9.2.23.126

 Number of Options: 2
 option  option
 code    data
  ----------------------------------------------------------------
  51      -1
  9       9.37.35.1

 Number of Options: 3
 option  option
 code    data
 ----------------------------------------------------------------
 28      9.2.23.127
 9       5.6.7.8
 51      200
```

7 Ejemplo de un cliente que aceptará cualquier dirección pero que tendrá su propio conjunto de opciones.

```
DHCP Server config>add client global
Enter the client name []? any-addr
Enter the client's hardware type (0 - 21) [1]? 6
Enter the client ID (MAC address or string) []? 10005aa4b9ab
Enter the client's IP address (IP address, any, none) []? any

DHCP Server config>add option client-global any-addr 51 999
DHCP Server config>add option client-global any-addr 1 255.255.255.0
```

8 Excluir una dirección del servicio.

```
Enter the client name []? excl-addr
Enter the client's hardware type (0 - 21) [1]? 0
Enter the client ID (MAC address or string) []? 0
Enter the client's IP address (IP address, any, none) []? 9.2.23.121

 DHCP Server config>li cli all
client      client  client                        attached    IP
name        type    identifier                    to subnet   address
-------------------------------------------------------------------------------
any-addr    6       10005aa4b9ab                  Any
excl-addr   0       0                                         9.2.23.121


DHCP Server config>li client global any-addr
client      client  client                        IP
name        type    identifier                    address
-----------------------------------------------------------------------
any-addr    6       10005aa4b9ab                  Any

 Number of Options: 2
 option  option
 code    data
 ---------------------------------------------------------------
 51      999
 1       255.255.255.0
```

Configuración y supervisión del servidor de DHCP

Este capítulo describe cómo utilizar los mandatos de operación y configuración de servidor DHCP e incluye las secciones siguientes:

Acceso al entorno de configuración del Servidor DHCP

Utilice el procedimiento siguiente para acceder al proceso de *configuración* del servidor DHCP.

1. En el indicador de mandatos OPCON, entre **talk 6**. Por ejemplo:

```
* talk 6
Config>
```

   Después de entrar el mandato **talk 6**, el indicador de mandatos Config (`Config>`) se visualiza en el terminal. Si el indicador de mandatos no aparece cuando inicia la configuración, pulse **Retorno** de nuevo.

2. En el indicador de mandatos Config, entre el mandato **feature dhcp-server** para llegar al indicador de mandatos `DHCP Server config>`.

Mandatos de configuración del Servidor DHCP

Tabla 61. Resumen de los mandatos de configuración del Servidor DHCP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxx.
Add	Añade una clase, cliente, subred u opción-proveedor.
Change	Cambia la definición de una clase, cliente, subred u opción-proveedor.
Default	Devuelve determinadas variables globales a sus valores por omisión.
Delete	Suprime una clase, subred u opción-proveedor.
Disable	Inhabilita el Servidor DHCP globalmente.
Enable	Habilita el Servidor DHCP globalmente.
List	Lista las definiciones de clase, cliente, global, subred u opción-proveedor.
Set	Establece definiciones para parámetros u opciones globales dentro de un ámbito especificado.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxi.

Add

Utilice el mandato **add** para añadir una clase, subred u opción-proveedor.

Sintaxis:

add **d**

class

client

option

subnet

vendor-option

class *ámbito [nombre_subred] nombre_clase [inicio_rango] [final_rango]*

Define una clase.

ámbito Especifica el ámbito al cual se añade la clase.

Valores válidos: global o subred

Valor por omisión: Ninguno

nombre_subred

Sólo es válido si el **ámbito** es *subred*. Indica el nombre de la subred a la que se añade la clase.

Valores válidos: Cualquier nombre de subred existente

Valor por omisión: Ninguno

nombre-clase

Indica el nombre de la clase.

Valores válidos: Una serie ASCII con un máximo de 40 caracteres de longiud

Valor por omisión: Ninguno

inicio-rango

Sólo es válido si el **ámbito** es *subred*. Especifica la dirección IP inicial para la agrupación de direcciones a la cual se asignarán clientes.

Valores válidos: Cualquier dirección IP válida dentro del rango de la subred a la cual se añade la clase.

Valor por omisión: La primera dirección IP del rango de subred que pertenece a la subred especificada.

final-rango

Sólo es válido si el **ámbito** es *subred*. Especifica la dirección IP final de la agrupación de direcciones a la cual se asignarán clientes.

Valores válidos: Cualquier dirección IP válida dentro del rango de la subred a la cual se añade la clase. Este valor debe ser mayor que el valor especificado para **inicio-rango**.

Valor por omisión: La dirección IP inicial más 5 del rango de subred que pertenece a la subred especificada. Si la dirección IP resultante no está dentro del rango de subred, el valor por omisión es la dirección IP final del rango de subred.

Ejemplo:

```
DHCP Server config> add class global
Enter class name? ClassA

DHCP Server config> add class subnet
Enter the subnet name[]? subA
Enter class name[]? ClaA
Enter start of IP address range[10.1.1.1]?
Enter end of IP address range[10.1.1.6]?
```

client *ámbito [nombre_subred] nombre_cliente tipo-id valor-id dirección*

Define un cliente

ámbito Especifica el ámbito al cual se añade el cliente.

Valores válidos: global o subred

Valor por omisión: Ninguno

nombre-subred

Sólo es válido si el **ámbito** es *subred*. Especifica el nombre de la subred a la cual se añade el cliente.

Valores válidos: Cualquier nombre de subred existente

Valor por omisión: Ninguno

nombre-cliente

Indica el nombre del cliente.

Valores válidos: Cualquier serie ASCII de 10 caracteres

Valor por omisión: Ninguno

tipo-id Indica el tipo de hardware del cliente. Los tipos de hardware definidos en la RFC 1340 que son aplicables al IBM 2210 se indican a continuación como valores válidos.

Valores válidos:

0 No especificado. Indica un nombre simbólico para el cliente.

1 Ethernet

6 Redes IEEE 802 (incluyedo Red en Anillo 802.5)

Valor por omisión: 1

valor-id Especifica el identificador del cliente. Si el **tipo-id** es *0*, el **valor-id** es una serie de 64 caracteres. De lo contrario, el **valor-id** es una dirección de MAC.

Nota: Un **tipo-id** de *0* y un **valor-id** de *0* indican que el servidor no debe distribuir la dirección IP especificada.

Valores válidos: 0 o cualquier dirección de MAC válida (12 dígitos hexadecimales)

Valor por omisión: Ninguno

dirección Especifica la dirección IP que debe proporcionarse al cliente o una serie de caracteres que indica que el cliente no recibirá servicio o que puede proporcionarse al cliente cualquier dirección de la agrupación de direcciones IP.

Valores válidos:

Cualquier dirección IP válida En formato decimal con puntos. Si el cliente está definido dentro de un ámbito de subred, la dirección IP debe estar dentro del rango de subred.

none Indica que el cliente correspondiente no recibirá servicio

any Indica que se puede proporcionar al cliente cualquier dirección IP de la agrupación de la subred.

Valor por omisión: Ninguno

Nota: Un **tipo-id** de *0* y un **valor-id** de *0* indican que el servidor no debe distribuir la dirección IP especificada.

Ejemplo:

```
DHCP Server config> add client global
     Enter the client name []? ClientA
     Enter the client's hardware type (0 - 21) [1]? 0
     Enter the client ID (MAC address or string) []? ClientA
     Enter the client's IP address (IP address, any, none) []? 9.1.1.1
     Client record with name ClientA has been added

DHCP Server config> add client subnet
     Enter the subnet name []? subA
     Enter the client name []? CliA
     Enter the client's hardware type (0 - 21) [1]? 1
     Enter the client ID (MAC address or string) []? 400000000010
     Enter the client's IP address (IP address, any, none) []? 10.1.1.10
     Client record with name CliA has been added
```

option *ámbito [nombre-subred] [nombre-clase] [nombre-cliente] [nombre-proveedor] código datos*

Define una opción. Las opciones pueden existir globalmente o dentro de una subred, clase, cliente o ámbito de opción-proveedor.

ámbito Especifica el ámbito al cual se añade la opción.

Valores válidos:

- clase-global
- clase-subred
- cliente-global
- cliente-subred
- global
- subred
- opción-proveedor

Valor por omisión: Ninguno

nombre-subred

Sólo es válido si el **ámbito** es *subred, clase-subred* o *cliente-subred*. Especifica el nombre de la subred a la cual se añade el cliente.

Valores válidos: Cualquier nombre de subred existente

Valor por omisión: Ninguno

nombre-clase
Sólo es válido si el **ámbito** es *clase-global* o *clase-subred*. Indica el nombre de la clase a la cual se añade la opción.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

nombre-cliente
Sólo es válido si el **ámbito** es *cliente-global* o *cliente-subred*. Indica el nombre del cliente al cual se añade la opción.

Valores válidos: Cualquier nombre de cliente existente

Valor por omisión: Ninguno

nombre-proveedor
Sólo es válido si el **ámbito** es *opción-proveedor*. Indica el nombre del proveedor al cual se añade la opción.

Valores válidos: Cualquier nombre de proveedor existente

Valor por omisión: Ninguno

código Especifica el código de la opción. Las opciones de DHCP se definen en la RFC 2132. Consulte “Opciones de DHCP” en la página 503 para obtener una descripción de las opciones y sus formatos.

Valores válidos: 1 - 255

Valor por omisión: 1

datos Especifica los datos de la opción. Los datos de la opción se pueden definir de tres maneras.

- Series ASCII para formatos específicos definidos en la RFC 2132.
- Conversión hexadecimal en el tiempo de inicialización. Los datos deben entrarse como *hex: 01 aa 04*.
- Serie de caracteres. Los datos deben entrarse como *abcdef*.

Ejemplo:

```
DHCP Server config> add option global
     Enter the option code [1]? 3
     Enter the option data []? 9.167.100.1
```

Ejemplo:

```
DHCP Server config> add option subnet
     Enter the subnet name []? subA
     Enter the option code [1]? 3
     Enter the option data []? 9.167.100.1
```

Ejemplo:

```
DHCP Server config> add option class-global
     Enter the class name []? ClassA
     Enter the option code [1]? 3
     Enter the option data []? 9.167.100.1
```

Ejemplo:

```
DHCP Server config> add option client
     Enter the client name []? ClientA
     Enter the option code [1]? 3
     Enter the option data []? 9.167.100.1
```

Ejemplo:

```
DHCP Server config> add option class-subnet
     Enter the subnet name []? subA
     Enter the class name []? ClaA
     Enter the option code [1]? 3
     Enter the option data []? 9.167.100.1
```

Ejemplo:

```
DHCP Server config> add option client-subnet
     Enter the subnet name []? subA
     Enter the client name []? CliA
     Enter the option code [1]? 3
     Enter the option data []? 9.167.100.1
```

Ejemplo:

```
DHCP Server config> add option vendor-option
     Enter the vendor name []? 200
     Enter the option code [1]? 85
     Enter the option data []? hex:01 AA 04
```

Ejemplo:

```
DHCP Server config> add option vendor-option
     Enter the vendor name []? 200
     Enter the option code [1]? 86
     Enter the option data []? 9.67.85.4
```

subnet *nombre_subred dirección-subred máscara-subred inicio-rango final-rango [nombre_grupo_subred] [prioridad_grupo_subred] [lista-política]*
Define una subred.

nombre-subred

Indica el nombre de la subred.

Valores válidos: Cualquier serie ASCII de 10 caracteres

Valor por omisión: Ninguno

dirección-subred

Especifica la dirección de la subred. La dirección se especifica en formato decimal con puntos.

Valores válidos: Cualquier dirección de la subred de IP válida

Valor por omisión: Ninguno

máscara-subred

Especifica la máscara de dirección de la subred. La dirección de subred debe estar dentro de la máscara de subred y no puede contener un número más alto de bits que la máscara.

Valores válidos: Cualquier máscara de IP válida en formato decimal con puntos

Valor por omisión: Se calcula basándose en la dirección de subred

inicio-rango

Especifica la dirección IP inicial de la agrupación de direcciones IP que este servidor administrará para esta subred. Si *inicio-rango* no se especifica, el servidor administrará todas las direcciones de la subred.

Valores válidos: Cualquier dirección de sistema principal IP válida dentro de la subred especificada en formato decimal con puntos

Valor por omisión: La primera dirección IP de la subred

final-rango

Especifica la dirección IP final de la agrupación de direcciones IP que este servidor administrará para esta subred.

Valores válidos: Cualquier dirección de sistema principal IP válida dentro de la subred especificada en formato decimal con puntos

Valor por omisión: inicio-rango más 50. Si la dirección IP resultante no está dentro de la subred, el valor por omisión es la última dirección IP de la subred.

nombre-grupo-subredes

Especifica el nombre de grupo de subred al cual pertenece esta subred.

Valores válidos: Cualquier serie ASCII con un máximo de 64 caracteres de longitud

Valor por omisión: Ninguno

prioridad-grupo-subredes

Especifica la prioridad de esta subred dentro del grupo de subredes. Esta prioridad se utiliza para determinar el orden con el que se asignan las direcciones dentro de un grupo de la subred específico.

Valores válidos: 1 - 65535

Valor por omisión: 1

lista-política

Identifica a qué lista de direcciones de política, Balance (Equilibrada) o Inorder (Por orden), se añadirá el grupo de la subred. Si el grupo de la subred ya existe en una lista y se especifica la otra, el grupo de subred se trasladará a la lista nueva.

Valores válidos: Inorder (Por orden) o Balance (Equilibrada)

Valor por omisión: Si es una subred nueva, el valor por omisión es Inorder (Por orden). De lo contrario, es la lista de política actual a la que pertenece el grupo de la subred.

Ejemplo:

```
DHCP Server config> add subnet
     Enter the subnet name []? subA
 Enter the IP subnet []? 10.1.1.0
 Enter the IP subnet mask [255.255.255.0]?
 Enter start of IP address range [10.1.1.1]?
 Enter end of IP address range [10.1.1.31]?
Enter the subnet group name []? group1
 Enter the subnet group priority (1 - 65535) [1]?
 Enter the access policy list (Inorder or Balance) [Inorder]?
 Subnet record with name sub1 has been added
 Subnet group group1 is being added to the Inorder List
```

vendor-option *nombre_proveedor [valor_hex]*

Añade una opción-proveedor. Existen dos formas de proporcionar datos de opción-proveedor:

- Entrar datos hexadecimales cuando se soliciten
- Añadir opciones específicas al proveedor utilizando el mandato **add option vendor**. Vea la página 530 para obtener información sobre la opción.

nombre_proveedor

Especifica el nombre del proveedor.

Valores válidos: Una serie ASCII con un máximo de 40 caracteres de longitud

Valor por omisión: Ninguno

valor-hex Especifica la serie ASCII hexadecimal que representa el valor hexadecimal de la parte de datos de la opción.

Valores válidos: Cualquier serie hexadecimal válida con el formato siguiente: *01 aa 04*

Valor por omisión: Ninguno

Ejemplo:

```
DHCP Server config> add vendor-option
     Enter the vendor name []? XA-client
     Enter the vendor hex data [] 01 aa 04?
     Vendor-option record with name XA-client has been added
```

Change

Utilice el mandato **change** para modificar la configuración de una clase, cliente, subred u opción-proveedor.

Sintaxis:

change class

client

subnet

vendor-option

class *ámbito [nombre_subred] nombre_clase nuevo_nombre_clase [nuevo_inicio_rango] [nuevo_final_rango]*
Modifica una clase.

ámbito Especifica el ámbito de la clase que se modifica.

Valores válidos: global o subred

Valor por omisión: Ninguno

nombre-subred
Sólo es válido si el **ámbito** es *subred*. Indica el nombre de la subred a la que pertenece la clase.

Valores válidos: Cualquier nombre de subred existente.

Valor por omisión: Ninguno

nombre-clase
Indica el nombre de la clase.

Valores válidos: Nombre de una clase existente

Valor por omisión: Ninguno

nuevo-nombre-clase
Indica el nuevo nombre de la clase.

Valores válidos: Una serie ASCII con un máximo de 40 caracteres de longiud

Valor por omisión: Nombre de clase existente

nuevo-inicio-rango
Sólo es válido si el **ámbito** es *subred*. Especifica la nueva dirección IP inicial para la agrupación de direcciones IP a la que se asignarán clientes.

Valores válidos: Cualquier dirección IP dentro del rango de subred

Valor por omisión: Inicio-rango existente

nuevo-final-rango
Especifica la nueva dirección IP final para la agrupación de direcciones IP a la que se asignarán clientes.

Valores válidos: Cualquier dirección IP válida dentro del rango de subred, mayor que **nuevo-final-rango**

Valor por omisión: Final-rango existente

Ejemplo:

```
DHCP Server config> change class global
     Enter the class name []? ClassA
     Enter the new class name [ClassA]?
```

Ejemplo:

```
DHCP Server config> change class subnet
     Enter the subnet name []? subA
     Enter the class name []? ClaA
     Enter the new class name [ClaA]?
     Enter start of IP address range [10.1.1.1]?
     Enter end of IP address range [10.1.1.6]?
```

client *ámbito [nombre_subred] nombre_cliente nuevo-nombre_cliente nuevo-tipo-id nuevo-valor-id nueva-dirección*
Modifica un cliente

ámbito Especifica el ámbito del cliente que se modifica.

Valores válidos: global o subred

Valor por omisión: Ninguno

nombre-subred
Sólo es válido si el **ámbito** es *subred*. Indica el nombre de la subred a la que pertenece el cliente.

Valores válidos: Cualquier nombre de subred existente

Valor por omisión: Ninguno

nombre-cliente
Indica el nombre del cliente.

Valores válidos: Un nombre de cliente existente

Valor por omisión: Ninguno

nuevo-nombre-cliente
Indica el nuevo nombre del cliente.

Valores válidos: Una serie ASCII con un máximo de 10 caracteres de longitud

Valor por omisión: Nombre de cliente existente

nuevo-tipo-id
Indica el nuevo tipo de hardware del cliente.

Valores válidos: 0 - 21. Vea la página 529.

Valor por omisión: Tipo de hardware existente del cliente

nuevo-valor-id
Especifica el nuevo identificador de cliente.

Valores válidos: 0 o cualquier dirección de MAC válida (12 dígitos hexadecimales)

Valor por omisión: Tipo-id de cliente existente

Nota: Un **tipo-id** de *0* y un **valor-id** de *0* indican que el servidor no debe distribuir la dirección IP especificada.

nueva-dirección

Especifica la nueva dirección IP que debe proporcionarse al cliente o una serie de caracteres que indica que el cliente no recibirá servicio o que se puede proporcionar al cliente cualquier dirección de la agrupación de direcciones IP.

Valores válidos:

Cualquier dirección IP válida

ninguna Indica que el cliente correspondiente no recibirá servicio

cualquiera Indica que se puede proporcionar al cliente cualquier dirección IP de la agrupación de la subred.

Valor por omisión: Ninguno

Nota: Un **tipo-id** de *0* y un **valor-id** de *0* indican que el servidor no debe distribuir la dirección IP especificada.

Ejemplo:

```
DHCP Server config> change client global
     Enter the client name []? ClientA
     Enter the new client name [ClientA]?
     Enter the new client hardware type (0 - 21) [0]?
     Enter the new client ID  [ClientA]?
     Enter the client's new IP address (IP address, any, none) [9.1.1.1]?
     Client ClientA has been changed
```

Ejemplo:

```
DHCP Server config> change client subnet
     Enter the subnet name []? subA
     Enter the client name []? CliA
Enter the new client name [ClientA]?
     Enter the new client hardware type (0 - 21) [1]?
     Enter the new client ID  [400000000010]?
     Enter the client's new IP address (IP address, any, none) [10.1.1.10]?
     Client CliA has been changed
```

subnet *nombre_subred nuevo_nombre_subred nueva_dirección_subred nueva_máscara_subred nuevo-inicio_rango nuevo-final_rango*

Modifica una subred.

nombre_subred

Indica el nombre de la subred específica que debe modificarse.

Valores válidos: Un nombre de subred existente

Valor por omisión: Ninguno

nuevo_nombre_subred

Indica el nuevo nombre de la subred especificada.

Valores válidos: Cualquier serie ASCII de 10 caracteres

Valor por omisión: Nombre de subred original

nueva_dirección_subred

Especifica la nueva dirección de la subred. La dirección se especifica en notación decimal con puntos.

Valores válidos: Cualquier dirección de la subred de IP válida

Valor por omisión: Dirección de subred existente

nueva_máscara_subred
Especifica la nueva máscara de dirección de subred. La dirección de subred debe estar dentro de la máscara de subred y no puede contener un número más alto de bits que la máscara.

Valores válidos: Cualquier máscara de IP válida

Valor por omisión: Máscara de subred existente

nuevo-inicio-rango
Especifica la nueva dirección IP inicial de la agrupación de direcciones IP que este servidor administrará para esta subred. Si *inicio-rango* no se especifica, el servidor administrará todas las direcciones de la subred.

Valores válidos: Cualquier dirección IP válida dentro del rango de la subred

Valor por omisión: Dirección inicial de la agrupación existente

nuevo-final-rango
Especifica la nueva dirección IP final de la agrupación de direcciones IP que este servidor administrará para esta subred.

Valores válidos: Cualquier dirección IP válida dentro del rango de la subred y mayor que la dirección final de la agrupación

Valor por omisión: Dirección final de la agrupación existente

Ejemplo:

```
DHCP Server config> change subnet
     Enter the subnet name []? subA
     Enter the new subnet name [subA]?
     Enter the new IP subnet[10.1.1.0]?
     Enter the new IP subnet mask[255.255.0.0]?
     Enter new start of IP address range [10.1.1.1]?
     Enter new end of IP address range [10.1.1.31]?
     Enter the new subnet group name [group11]?
     Enter the new subnet group priority [1]?
     Enter the new access policy list (Inorder or Balance) [Inorder]?
```

vendor-option *nombre_proveedor nuevo_nombre_proveedor [nuevo_valor_hex]*
Modifica una opción-proveedor.

nombre_proveedor
Especifica el nuevo nombre de la opción de proveedor.

Valores válidos: Un nombre de proveedor existente

Valor por omisión: Ninguno

nuevo_nombre_proveedor
Especifica el nuevo nombre de la opción de proveedor.

Valores válidos: Una serie ASCII con un máximo de 40 caracteres de longiud

Valor por omisión: Nombre de opción de proveedor existente

nuevo_valor_hex
Especifica la nueva serie ASCII hexadecimal que representa el valor hexadecimal de la parte de datos de la opción. No se puede añadir ningún valor hexadecimal si se han añadido opciones específicas a esta opción de proveedor.

Valores válidos: Cualquier serie hexadecimal válida

Valor por omisión: Serie hexadecimal existente

Ejemplo:

```
DHCP Server config> change vendor-option
     Enter the vendor name []? XA-clients
     Enter the new vendor name [XA-clients]?
     Enter the new vendor data [01 aa 04]?
```

Delete

Utilice el mandato **delete** para suprimir una clase, cliente, opción, subred, grupo-subredes u opción-proveedor.

Sintaxis:

de**lete**	class
	client
	option
	subnet
	subnet-group
	vendor-option

class *ámbito [nombre_subred] nombre_clase*
Suprime una clase y todas las opciones definidas bajo su ámbito.

ámbito Especifica el ámbito del cual se suprime la clase.

Valores válidos: global o subred

Valor por omisión: Ninguno

nombre-subred
Sólo es válido si el **ámbito** es *subred*. Especifica el nombre de la subred de la que se suprime la clase.

Valores válidos: Cualquier nombre de subred existente

Valor por omisión: Ninguno

nombre-clase
Indica el nombre de la clase que debe suprimirse.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

Ejemplo:

```
DHCP Server config> delete class global
     Enter the class name []? ClassA
```

Ejemplo:

```
DHCP Server config> delete class subnet
     Enter the subnet name []? subA
     Enter the class name []? ClaA
```

client *ámbito [nombre_subred] nombre_cliente*

Suprime un cliente y todas las opciones definidas bajo su ámbito.

ámbito Especifica el ámbito del cual se suprime el cliente.

Valores válidos: global o subred

Valor por omisión: Ninguno

nombre_subred

Sólo es válido si el **ámbito** es *subred*. Especifica el nombre de la subred de la que se suprime el cliente.

Valores válidos: Un nombre de subred existente

Valor por omisión: Ninguno

nombre_cliente

Indica el nombre del cliente que debe suprimirse.

Valores válidos: Un nombre de cliente existente

Valor por omisión: Ninguno

Ejemplo:

```
DHCP Server config> delete client global
     Enter the client name []? ClientA
```

Ejemplo:

```
DHCP Server config> delete client subnet
     Enter the subnet name []? subA
     Enter the client name []? CliA
```

option *ámbito [nombre_subred] [nombre_clase] [nombre_cliente] [nombre_proveedor] código*

Suprime una opción del ámbito especificado.

ámbito Especifica el ámbito del cual se suprime la opción.

Valores válidos:

- clase-global
- clase-subred
- cliente-global
- cliente-subred
- global
- subred
- opción-proveedor

Valor por omisión: Ninguno

nombre-subred
Sólo es válido si el **ámbito** es *subred, clase-subred* o *cliente-subred*. Especifica el nombre de la subred de la cual se suprime el cliente.

Valores válidos: Cualquier nombre de subred existente

Valor por omisión: Ninguno

nombre-clase
Sólo es válido si el **ámbito** es *clase-global* o *clase-subred*. Indica el nombre de la clase de la cual se suprime la opción.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

nombre-cliente
Sólo es válido si el **ámbito** es *cliente-global* o *cliente-subred*. Indica el nombre del cliente del cual se suprime la opción.

Valores válidos: Cualquier nombre de cliente existente

Valor por omisión: Ninguno

nombre-proveedor
Sólo es válido si el **ámbito** es *opción-proveedor*. Indica el nombre del proveedor del cual se suprime la opción.

Valores válidos: Cualquier nombre de proveedor existente

Valor por omisión: Ninguno

código Especifica el código de la opción. Las opciones de DHCP se definen en la RFC 2132. Consulte “Opciones de DHCP” en la página 503 para obtener una descripción de las opciones y sus formatos.

Valores válidos: 1 - 255

Valor por omisión: 1

Ejemplo:

```
DHCP Server config> delete option global
     Enter the option code [1]? 3
```

Ejemplo:

```
DHCP Server config> delete option subnet
     Enter the subnet name []? subA
     Enter the option code [1]? 3
```

Ejemplo:

```
DHCP Server config> delete option class-global
     Enter the class name []? ClassA
     Enter the option code [1]? 3
```

Ejemplo:

```
DHCP Server config> delete option client
     Enter the client name []? ClientA
     Enter the option code [1]? 3
```

Ejemplo:

```
DHCP Server config> delete option class-subnet
     Enter the subnet name []? subA
     Enter the class name []? ClaA
     Enter the option code [1]? 3
```

Ejemplo:

```
DHCP Server config> delete option client-subnet
     Enter the subnet name []? subA
     Enter the client name []? CliA
     Enter the option code [1]? 3
```

Ejemplo:

```
DHCP Server config> delete option vendor-option
          Enter the vendor name []? XI-clients
     Enter the option code [1]? 85
```

Ejemplo:

```
DHCP Server config> delete option vendor-option
     Enter the vendor name []? 200
     Enter the option code [1]? 86
```

subnet *nombre_subred*

Suprime una subred y todas las clases, clientes y opciones que están definidas dentro de su ámbito.

nombre_subred

Especifica el nombre de la subred que se suprime.

Valores válidos: Cualquier nombre de subred existente

Valor por omisión: Ninguno

Ejemplo:

```
DHCP Server config> delete subnet
     Enter the subnet name []? subA
     You are about to delete a subnet subA
     and all the associated class, client, and option records associated with it
     Are you sure you want to continue? [No]:
```

subnet-group *nombre_grupo_subred*

Suprime todas las subredes asociadas con un grupo de subredes particular y todas las clases, clientes y opciones definidas en los ámbitos de las subredes.

nombre_grupo_subred

Especifica el nombre que identifica el grupo de subredes.

Valores válidos: Un nombre de grupo de subredes existente

Valor por omisión: Ninguno

Ejemplo:

```
DHCP Server config> delete subnet-group
     Enter the subnet group name []? group2
     You are about to delete a all subnets in group group2
     and all the associated class, client, and option records associated with them
     Are you sure you want to continue? [No]:
```

vendor-option *nombre_proveedor*

Suprime una opción-proveedor y las opciones definidas dentro de su ámbito.

nombre_proveedor

Especifica el nombre del proveedor.

Valores válidos: Una serie ASCII con un máximo de 40 caracteres de longiud

Valor por omisión: Ninguno

Ejemplo:

```
DHCP Server config> delete vendor-option
     Enter the vendor name []? XA-clients
```

Disable

Utilice el mandato **disable** para inhabilitar el servidor DHCP globalmente.

Sintaxis:

disable dhcp-server

Ejemplo:

```
DHCP Server config> disable dhcp-server
```

Enable

Utilice el mandato **enable** para habilitar el servidor DHCP globalmente.

Sintaxis:

enable dhcp-server

Ejemplo:

```
DHCP Server config> enable dhcp-server
```

List

Utilice el mandato **list** para listar información de configuración sobre clase, cliente, parámetros globales, subredes u opciones-proveedor y cualquier opción asociada.

Sintaxis:

list	class
	client
	global
	option
	subnet
	vendor-option
class	all
	global *nombre-clase*
	subnet *nombre-clase*

Lista un resumen de todas las clases configuradas o los detalles de una clase específica.

nombre-clase

Indica el nombre de la clase que debe visualizarse.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

Ejemplo:

```
DHCP Server config> list class all

     class              attached
     name               to subnet
     ------------------------------------------------------------
     ClassA
     ClaA               subA
```

Ejemplo:

```
DHCP Server config> list class global
     Enter the class name []? ClassA

class
     name
     ------------------------------------------------------------
     ClassA
     Bootstrap Server:   100.100.100.100
     Canonical: Yes
    Support Unlisted Clients: Yes
     Number of Options: 1
          option    option
          code      data
     ------------------------------------------------------------
     1         255.255.0.0
```

Ejemplo:

```
DHCP Server config> list class subnet
     Enter the subnet name []? subA
     Enter the class name []? ClaA

class
     name
     ------------------------------------------------------------
     ClaA
     starting IP address: 10.1.1.3
     ending IP address: 10.1.1.5
     Bootstrap Server:   100.100.100.100
     Canonical: Yes
     Support Unlisted Clients: DHCP

     Number of Options: 1
          option    option
          code      data
     ------------------------------------------------------------
     6      9.67.100.1
```

client all

global *nombre-cliente*

subnet *nombre-cliente*

Lista un resumen de todos los clientes configurados o los detalles de un cliente específico.

nombre-cliente

Indica el nombre del cliente que debe visualizarse.

Valores válidos: Un nombre de cliente existente

Valor por omisión: Ninguno

Ejemplo:

```
DHCP Server config> list client all
     client   client   client         attached    IP
     name     type     identifier     to subnet   address
     ------------------------------------------------------------------------------
     ClientA   0       ClientA                    9.1.1.1

     CliA      1       400000000010    subA       10.1.1.10
```

Ejemplo:

```
DHCP Server config> list client global
     Enter the client name []? ClientA
```

Ejemplo:

```
DHCP Server config> list client subnet
     Enter the subnet name []? subA
     Enter the client name []? CliA

     client     client     client            IP
     name       type       identifier        address
     ------------------------------------------------------------------
     CliA       1          400000000010      10.1.1.10
     Bootstrap Server: 200.200.200.200
     Canonical: Yes

     Number of Options: 1
          option    option
          code      data
     ------------------------------------------------------------
     6      9.67.100.1
```

global

Lista parámetros globales.

Ejemplo:

```
DHCP Server config> list global

    DHCP server Global Parameters
    =============================
    DHCP server enabled: Yes

    Balance: group2

    Inorder: group1

    Canonical: No

    Lease Expire Interval: 1 minute(s)
    Lease Time Default: 1 day(s)

    Support BOOTP Clients: No
    Bootstrap Server: Not configured

    Support Unlisted Clients: Yes
    Ping Time: 1 second(s)
    Used IP Address Expire Interval: 15 minute(s)
```

option *ámbito [nombre-subred] [nombre-clase] [nombre-cliente] [nombre-proveedor] código*

ámbito Especifica el ámbito en el cual se lista la opción.

Valores válidos:

- clase-global
- clase-subred
- cliente-global
- cliente-subred
- global
- subred
- opción-proveedor

Valor por omisión: Ninguno

nombre-subred
Sólo es válido si el **ámbito** es *subred*, *clase-subred* o *cliente-subred*. Especifica el nombre de la subred a la cual pertenece la opción que se lista.

Valores válidos: Cualquier nombre de subred existente

Valor por omisión: Ninguno

nombre-clase
Sólo es válido si el **ámbito** es *clase-global* o *clase-subred*. Indica el nombre de la clase a la cual pertenece la opción que se lista.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

nombre-cliente
Sólo es válido si el **ámbito** es *cliente-global* o *cliente-subred*. Indica el nombre del cliente al cual pertenece la opción que se lista.

Valores válidos: Cualquier nombre de cliente existente

Valor por omisión: Ninguno

nombre-proveedor
Sólo es válido si el **ámbito** es *opción-proveedor*. Indica el nombre del proveedor al cual pertenece la opción que se lista.

Valores válidos: Cualquier nombre de proveedor existente

Valor por omisión: Ninguno

código Especifica el código de la opción. Las opciones de DHCP se definen en la RFC 2132. Consulte “Opciones de DHCP” en la página 503 para obtener una descripción de las opciones y sus formatos.

Valores válidos: 1 - 255

Valor por omisión: 1

Ejemplo:

```
DHCP Server config> list option global

          option    option
          code      data
     ------------------------------------------------------------
     3        9.67.100.1
```

Ejemplo:

```
DHCP Server config> list option class-global
     Enter the class name []? ClassA
          option    option
          code      data
     ------------------------------------------------------------
     3        9.67.100.1
```

Ejemplo:

```
DHCP Server config> list option class-subnet
     Enter the subnet name []? subA
     Enter the class name []? claA

          option    option
          code      data
     ------------------------------------------------------------
     3        9.67.100.1
```

Ejemplo:

```
DHCP Server config> list option client-global
     Enter the client name []? ClientA
          option    option
          code      data
     ------------------------------------------------------------
     3        9.67.100.1
```

Ejemplo:

```
DHCP Server config> list option client-subnet
     Enter the subnet name []? subA
     Enter the client name []? cliA

          option    option
          code      data
     ------------------------------------------------------------
     3        9.67.100.1
```

Ejemplo:

```
DHCP Server config> list option subnet
     Enter the subnet name []? subA


          option    option
          code      data
     ----------------------------------------------------------------
     6      9.67.100.1
Ejemplo:

DHCP Server config> list option vendor-option
          Enter the vendor name []? XI-clients


          option    option
          code      data
     ----------------------------------------------------------------
     85        hex:01 aa 04
          86        9.67.85.4
```

subnet all

detailed *nombre-subred*

Lista un resumen de todas las subredes configuradas o los detalles de una subred específica.

nombre-subred

Indica el nombre de la subred que debe visualizarse.

Valores válidos: Un nombre de subred existente

Valor por omisión: Ninguno

Ejemplo:

```
DHCP Server config> list subnet all

     name      address    mask          IP Addr       IP Addr
     ------------------------------------------------------------------------
     subA      10.1.1.0   255.255.0.0   10.1.1.1      10.1.1.31
     subB    11.1.1.0   255.255.0.0   11.1.1.1   11.1.1.31
```

Ejemplo:

```
DHCP Server config> list subnet detailed
     Enter the subnet name []? subA

     subnet    subnet     subnet        starting      ending
     name      address    mask          IP Addr       IP Addr
     ------------------------------------------------------------------------
     subA      10.1.1.0   255.255.0.0   10.1.1.1      10.1.1.31
     Subnet Group: group1/1

     Number of Classes: 1
class
     name
    ----------------------------------------------------------------
     ClaA
     starting IP address: 10.1.1.1
     ending   IP address: 10.1.1.6
     Bootstrap Server:   100.100.100.100
     Canonical: Yes
     Support Unlisted Clients: DHCP

     Number of Options: 1
          option    option
          code      data
     ----------------------------------------------------------------
     6      9.67.100.1

     Number of Clients: 1
     client     client     client            IP
     name       type       identifier        address
     ------------------------------------------------------------------------
     CliA       1          400000000010      10.1.1.10
     Bootstrap Server: 200.200.200.200
     Canonical: Yes

     Number of Options: 1
          option    option
          code      data
     ----------------------------------------------------------------
     6      9.67.100.1

     Number of Options: 1
          option    option
          code      data
     ----------------------------------------------------------------
     1      255.255.255.0
```

vendor-option all

detailed *nombre-proveedor*

Lista un resumen de todos los proveedores configurados o los detalles de una opción-proveedor específica.

nombre-proveedor

Indica el nombre de la opción-proveedor que debe visualizarse.

Valores válidos: Un nombre-proveedor existente

Valor por omisión: Ninguno

Ejemplo:

```
DHCP Server config> list vendor-option all

          vendor          hex
          name            data
          ----------------------------------------------------------------
          XA-clients      01 AA 04
          XI-clients

DHCP Server config> list vendor-option detailed
          Enter the vendor name []? XI-clients
          vendor          hex
          name            data
          ----------------------------------------------------------------
          XI-clients

          Number of Options: 2
          option    option
          code      data
          ----------------------------------------------------------------
          85        hex:01 AA 04
          86        9.67.85.4
```

Set

Utilice el mandato **set** para especificar valores para parámetros globales y para añadir grupos de subredes a las listas de Balance (Equilibrada) e Inorder (Por orden).

Sintaxis:

set	balance
	bootstrapserver
	canonical
	inorder
	lease-expire-interval
	lease-time-default
	ping-time
	support-bootp
	support-unlisted-clients
	used-ip-address-expire-interval

balance *nombre_grupo_subred*

Añade o mueve un grupo de subredes a la lista de Balance (Equilibrada). Las direcciones se asignarán de un modo rotatorio entre todas las subredes asociadas con el grupo o grupos definidos dentro de un grupo de subredes, de acuerdo con su prioridad.

nombre_grupo_subred
Especifica el nombre del grupo de subredes al cual pertenece esta subred.

Valores válidos: Un nombre de grupo de subredes existente

Valor por omisión: Ninguno

Ejemplo:

```
DHCP Server config> set balance
Enter the subnet group name []? group1
```

bootstrapserver *ámbito [nombre-subred] [nombre-clase] [nombre-cliente] dirección*
Especifica si el servidor DHCP especifica un servidor de rutina de carga para los clientes. Si desea que el servidor DHCP especifiqe un servidor de rutina de carga, debe definir la dirección IP del servidor. Este parámetro puede especificarse dentro del ámbito global, subred, clase o cliente.

ámbito Especifica el ámbito del parámetro "bootstrapserver" (rutina de carga).

Valores válidos:

- clase-global
- clase-subred
- cliente-global
- cliente-subred
- global
- subred

Valor por omisión: Ninguno

nombre-subred
Sólo es válido si el ámbito es *subred*, *clase-subred* o *cliente-subred*. Indica el nombre de la subred para la cual se especifica el servidor de rutina de carga.

Valores válidos: Un nombre de subred existente

Valor por omisión: Ninguno

nombre-clase
Válido si el ámbito es *clase-global* o *clase-subred*. Indica el nombre de la clase para la cual se especifica el servidor de rutina de carga.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

nombre-cliente
Válido si el ámbito es *cliente-global* o *cliente-subred*. Indica el nombre del cliente para el cual se especifica el servidor de rutina de carga.

Valores válidos: Un nombre de cliente existente

Valor por omisión: Ninguno

Dirección IP del servidor

Especifica la dirección IP del servidor de rutina de carga.

Valores válidos: Cualquier dirección IP en formato decimal con punto

Valor por omisión: Ninguno

Ejemplo:

```
DHCP Server config> set bootstrap-server class-global
     Enter the class name []? ClassA
Enter the IP address of the server []? 100.100.100.100
```

Ejemplo:

```
DHCP Server config> set bootstrap-server class-subnet
     Enter the subnet name []? subA
     Enter the class name []? ClassA
Enter the IP address of the server []? 100.100.100.100
```

Ejemplo:

```
DHCP Server config> set bootstrap-server client-global
     Enter the client name []? ClientA
Enter the IP address of the server []? 100.100.100.100
```

Ejemplo:

```
DHCP Server config> set bootstrap-server client-subnet
     Enter the subnet name []? subA
     Enter the client name []? ClientA
Enter the IP address of the server []? 100.100.100.100
```

Ejemplo:

```
DHCP Server config> set bootstrap-server global
Enter the IP address of the server []? 100.100.100.100
```

Ejemplo:

```
DHCP Server config> set bootstrap-server subnet
     Enter the subnet name []? subA
Enter the IP address of the server []? 100.100.100.100
```

canonical *ámbito [nombre-subred] [nombre-clase] [nombre-cliente] valor*

Especifica si el servidor DHCP transformará direcciones de MAC a formato canónico.

Las direcciones de MAC para clientes de Ethernet/802.3 se almacenan en formato canónico (el byte empieza con el bit menos significativo). Las direcciones de MAC para clientes de Red en Anillo se almacenan en formato no canónico (el byte empieza con el bit más significativo). Este parámetro debe utilizarse cuando el servidor DHCP está en un tipo de medio (Red en Anillo o Ethernet/802.3), el cliente está en el otro tipo de medio y existe un puente de conversión entre los dos. Cuando este parámetro se establece en *sí*, el servidor DHCP hace que la dirección de MAC del cliente pase de canónica a no canónica o de no canónica a canónica. Puesto que el servidor DHCP no sabe qué formato tiene la dirección de MAC originalmente, establezca este parámetro en *sí* simplemente cambiará la dirección. "Canonical" se puede establecer en el ámbito global, subred, clase o cliente.

ámbito Especifica el ámbito del parámetro "bootstrapserver" (rutina de carga).

Valores válidos:

- clase-global
- clase-subred
- cliente-global
- cliente-subred
- global
- subred

Valor por omisión: Ninguno

nombre-subred
Sólo es válido si el ámbito es *subred*, *clase-subred* o *cliente-subred*. Indica el nombre de la subred para la cual se especifica "canonical".

Valores válidos: Un nombre de subred existente

Valor por omisión: Ninguno

nombre-clase
Válido si el ámbito es *clase-global* o *clase-subred*. Indica el nombre de la clase para la cual se especifica "canonical".

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

nombre-cliente
Válido si el ámbito es *cliente-global* o *cliente-subred*. Indica el nombre del cliente para el cual se especifica "canonical".

Valores válidos: Un nombre de cliente existente

Valor por omisión: Ninguno

valor Especifica si las direcciones de MAC deben transformarse a formato canónico

Valores válidos: sí, no

Valor por omisión: no, si el **ámbito** es *global*. De lo contrario, el valor por omisión lo determina la jerarquía del ámbito. Consulte “Conceptos y terminología” en la página 500 para obtener una explicación del ámbito.

Ejemplo:

```
DHCP Server config> set canonical class-global
     Enter the class name []? ClassA
Would you like MAC addresses to be transformed to canonical format? [No] yes
```

Ejemplo:

```
DHCP Server config> set canonical class-subnet
     Enter the subnet name []? subA
     Enter the class name []? ClassA
Would you like MAC addresses to be transformed to canonical format? [No] yes
```

Ejemplo:

```
DHCP Server config> set canonical client-global
     Enter the client name []? ClientA
Would you like MAC addresses to be transformed to canonical format? [No] yes
```

Ejemplo:

```
DHCP Server config> set canonical client-subnet
     Enter the subnet name []? subA
     Enter the client name []? ClientA
Would you like MAC addresses to be transformed to canonical format? [No] yes
```

Ejemplo:

```
DHCP Server config> set canonical global
Would you like MAC addresses to be transformed to canonical format? [No] yes
```

Ejemplo:

```
DHCP Server config> set canonical subnet
     Enter the subnet name []? subA
Would you like MAC addresses to be transformed to canonical format? [No] yes
```

inorder *lista-etiquetas*

Añade o mueve un grupo de subredes a la lista de Inorder (Por orden). Las direcciones se asignarán de subredes de un grupo de subredes según el orden de prioridad asignado a dicha subred.

nombre_grupo_subred

Especifica el grupo de subredes al cual pertenece esta subred.

Valores válidos: Un nombre de grupo de subredes existente

Valor por omisión: Ninguno

Ejemplo:

```
DHCP Server config> set inorder
Enter the subnet group name []? g2
```

lease-expire-interval *tiempo duración*

Especifica el intervalo durante el cual se examina la condición de alquiler de todas las direcciones de la agrupación de direcciones para determinar qué alquileres han caducado. El intervalo de caducidad de alquiler sólo se puede establecer en el nivel global.

tiempo Especifica la unidad de medida del tiempo.

Valores válidos: segundos, minutos, horas

Valor por omisión: Ninguno

duración Especifica cuánto tiempo durará el intervalo.

Valores válidos: 15 segundos - 12 horas

Valor por omisión:

- 15 (si la unidad de tiempo es segundos)
- 1 (si la unidad de tiempo es minutos)
- 1 (si la unidad de tiempo es horas)

Ejemplo:

```
DHCP Server config> set lease-expire-interval seconds
How long is the interval in seconds (max:59) [15]? 59
```

Ejemplo:

```
DHCP Server config> set lease-expire-interval minutes
How long is the interval in minutes (max:59) [1]? 45
```

Ejemplo:

```
DHCP Server config> set lease-expire-interval hours
How long is the interval in hours (max:12) [1]? 2
```

lease-time-default *tiempo duración*

Especifica la duración del alquiler por omisión para los alquileres emitidos por el Servidor DHCP. Un intervalo infinito significa que los alquileres no caducan nunca. El valor por omisión de tiempo de alquiler sólo se puede establecer en el nivel global.

tiempo Especifica la unidad de medida del tiempo.

Valores válidos: minutos, horas, días, semanas, meses, años, infinito

Valor por omisión: Ninguno

duración Especifica cuánto tiempo durará el intervalo.

Valores válidos: 3 minutos - infinito

Valor por omisión:

- 3 (si la unidad de tiempo es minutos)
- 1 (si la unidad de tiempo es horas)
- 1 (si la unidad de tiempo es días)
- 1 (si la unidad de tiempo es meses)
- 1 (si la unidad de tiempo es años)

Ejemplo:

```
DHCP Server config> set lease-time-default minutes
How long is the interval in minutes (max:59) [3]? 2
```

Ejemplo:

```
DHCP Server config> set lease-time-default hours
     How long is the interval in hours (max:23) [1]? 12
```

Ejemplo:

```
DHCP Server config> set lease-time-default days
How long is the interval in days (max:6) [1]? 2
```

Ejemplo:

```
DHCP Server config> set lease-time-default weeks
How long is the interval in weeks (max:3) [1]? 1
```

Ejemplo:

```
DHCP Server config> set lease-time-default months
How long is the interval in months (max:11) [1]? 3
```

Ejemplo:

```
DHCP Server config> set lease-time-default years
How long is the interval in years (max:10) [1]? 3
```

Ejemplo:

```
DHCP Server config> set lease-time-default infinity
```

ping-time *tiempo duración*

Antes de asignar una dirección IP, el servidor DHCP realiza pruebas para asegurarse de que la dirección IP no esté en uso. Este valor especifica el tiempo esperará el servidor DHCP una respuesta de sondeo antes de marcar una dirección como disponible. Un valor de 0 inhabilita los sondeos, con lo cual el servidor DHCP no prueba una dirección antes de asignarla.

tiempo Especifica la unidad de medida del tiempo.

Valores válidos: segundos

Valor por omisión: Ninguno

duración Especifica cuánto tiempo durará el intervalo.

Valores válidos: 0 - 5 segundos

Valor por omisión: 1

Ejemplo:

```
DHCP Server config> set ping-time seconds
   How long is the interval in seconds (max:5) [1]? 3
```

support-bootp *valor*

Especifica si el servidor responderá a las peticiones realizadas desde los clientes BOOTP. Si el servidor DHCP se había configurado previamente para dar soporte a clientes BOOTP y se ha reconfigurado para no dar soporte a clientes BOOTP, el enlace de dirección para los clientes BOOTP que se había establecido antes de la reconfiguración

se mantendrá hasta que el cliente BOOTP envíe otra petición (cuando se reinicie). Cuando esto suceda, el servidor no responderá y el enlace se eliminará. Este parámetro sólo se puede establecer en el nivel global.

Valores válidos: sí o no

Valor por omisión: no

Ejemplo:

```
DHCP Server config> set support-bootp
     Would you like the server to support BOOTP clients? [No] yes
```

support-unlisted-clients *ámbito [nombre-subred] [nombre-clase] valor*

Especifica si el servidor responderá a las peticiones de los clientes DHCP cuyos ID de cliente no se listen específicamente en esta configuración. Este parámetro tiene varios valores posibles:

ámbito Especifica el ámbito del parámetro **support-unlisted-clients**.

Valores válidos:

- clase-global
- clase-subred
- global
- subred

Valor por omisión: Ninguno

nombre-subred

Válido si el ámbito es *subred*, *clase-subred* o *cliente-subred*. Indica el nombre de la subred par la cual se especifica este parámetro.

Valores válidos: Un nombre de subred existente

Valor por omisión: Ninguno

nombre-clase

Válido si el ámbito es *clase-global* o *clase-subred*. Indica el nombre de la clase para la cual se especifica este parámetro.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

valor

sí El servidor DHCP debe responder a cualquier cliente sin importar el tipo ni si está configurado.

no El servidor DHCP sólo responderá a las peticiones de clientes DHCP que estén configurados.

bootp El servidor DHCP soportará los clientes BOOTP no listados, pero no los clientes DHCP no listados

dhcp El servidor DHCP responderá a los clientes DHCP no listados, pero no a los clientes BOOTP no listados.

Valores válidos: sí, no, bootp, dhcp

Valor por omisión: sí, si el **ámbito** es *global*. De lo contrario, el valor por omisión lo determina la jerarquía del ámbito. Consulte “Conceptos y terminología” en la página 500 para obtener una explicación del ámbito.

Ejemplo:

```
DHCP Server config> set support-unlisted-clients class-global yes
     Enter the class name []? ClassA
```

Ejemplo:

```
DHCP Server config> set support-unlisted-clients class-subnet no
     Enter the subnet name []? subA
     Enter the class name []? ClassA
```

Ejemplo:

```
DHCP Server config> set support-unlisted-clients global bootp
```

Ejemplo:

```
DHCP Server config> set support-unlisted-clients subnet dhcp
     Enter the subnet name []? subA
```

used-ip-address-expire-interval *tiempo duración*

Especifica el intervalo durante el cual el servidor retendrá una dirección IP en uso antes de hacer que la dirección esté disponible para ser asignada. Antes de asignar una dirección IP, el servidor sondea la dirección para asegurarse de que no se esté utilizando en la red. A continuación, el servidor marca la dirección que está en uso como reservada. Este parámetro especifica el tiempo que una dirección en uso se mantiene como reservada antes de hacer que la dirección quede disponible para ser asignada. Este parámetro sólo se puede establecer en el nivel global.

tiempo Especifica la unidad de medida del tiempo.

Valores válidos: segundos, minutos, horas, días, semanas, meses, años, infinito

Valor por omisión: Ninguno

duración Especifica cuánto tiempo durará el intervalo.

Valores válidos: 30 segundos - infinito

Valor por omisión:

- 30 (si la unidad de tiempo es segundos)
- 15 (si la unidad de tiempo es minutos)
- 1 (si la unidad de tiempo es horas)
- 1 (si la unidad de tiempo es días)
- 1 (si la unidad de tiempo es meses)
- 1 (si la unidad de tiempo es años)

Ejemplo:

```
DHCP Server config> set used-ip-address-expire-interval seconds
How long is the interval in seconds (max:59) [30]? 2
```

Ejemplo:

```
DHCP Server config> set used-ip-address-expire-interval minutes
How long is the interval in minutes (max:59) [15]? 2
```

Ejemplo:

```
DHCP Server config> set used-ip-address-expire-interval hours
How long is the interval in hours (max:23) [1]? 5
```

Ejemplo:

```
DHCP Server config> set used-ip-address-expire-interval days
How long is the interval in days (max:6) [1]? 2
```

Ejemplo:

```
DHCP Server config> set used-ip-address-expire-interval weeks
How long is the interval in weeks (max:3) [1]? 1
```

Ejemplo:

```
DHCP Server config> set used-ip-address-expire-interval months
How long is the interval in months (max:11) [1]? 3
```

Ejemplo:

```
DHCP Server config> set used-ip-address-expire-interval years
How long is the interval in years (max:10) [1]? 3
```

Ejemplo:

```
DHCP Server config> set used-ip-address-expire-interval infinity
```

Acceso al entorno de supervisión del Servidor DHCP

Utilice el procedimiento siguiente para acceder al proceso de *supervisión* del servidor DHCP.

1. En el indicador de mandatos OPCON, entre **talk 5**. Por ejemplo:

   ```
   * talk 5
   Config>
   ```

   Después de entrar el mandato **talk 5**, el indicador de mandatos CONFIG (+) se visualiza en el terminal. Si el indicador de mandatos no aparece cuando inicia la configuración, pulse **Retorno** de nuevo.

2. En el indicador de mandatos +, entre el mandato **feature dhcp-server** para llegar al indicador de mandatos `DHCP Server>`.

Mandatos de supervisión del Servidor DHCP

Tabla 62. Resumen de mandatos de supervisión del Servidor DHCP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Disable	Inhabilita dinámicamente el servidor DHCP.
Enable	Habilita dinámicamente el servidor DHCP.
List	Visualiza parámetros para clases, clientes, globales, subredes y opciones-proveedor.
Reset	Restablece dinámicamente la configuración del Servidor DHCP.
Request	
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxi.

Disable

Utilice el mandato **disable** para inhabilitar dinámicamente el servidor DHCP.

Sintaxis:

disa**ble** dhcp

Enable

Utilice el mandato **enable** para habilitar dinámicamente el servidor DHCP.

Sintaxis:

en**able** dhcp

List

Utilice el mandato **list** para listar información de configuración sobre clase, cliente, parámetros globales, subredes u opción-proveedor y cualquier opción asociada. Consulte “List” en la página 544 para obtener ejemplos del mandato **list**.

Sintaxis:

list class
client
global
option
subnet
vendor-option

Reset

Utilice el mandato **reset** para restablecer dinámicamente la configuración del Servidor DHCP.

Sintaxis:

reset dhcp

Ejemplo:

```
DHCP Server> reset dhcp
You are about to reset the DHCP Server.
Are you sure you want to continue? [No]: y
DHCP Server has been reset
DHCP Server>
```

Request

Utilice el mandato **request** para visualizar información administrativa.

Sintaxis:

request clientid

delete

ipquery

poolquery

stats

status

clientid *id_cliente*

Visualiza información para un cliente.

id_cliente

Indica el identificador del cliente.

Valores válidos: Un id de cliente existente

Valor por omisión: Ninguno

Ejemplo:

```
DHCP Server> request clientid
     Enter the client name []? 0020351FB371

     Client id:              1-0x0020351FB371
     Status: BOUND
     Address last assigned: 192.9.200.10
     Most recent lease time: 16:41:25 December 3, 1998
     Proxy flag: FALSE
     Hostname:               Win-XY-1
     Domain name:            city.net
```

delete *dirección*

Suprime un alquiler para una dirección IP de un cliente específico.

dirección Indica la dirección IP del cliente que debe suprimirse.

Valores válidos: Cualquier dirección IP válida de un cliente existente

Valor por omisión: Ninguno

Ejemplo:

```
DHCP Server> request delete
Enter the client's IP address []? 194.3.200.10
```

ipquery *dirección*

Visualiza información para una dirección IP.

Ejemplo:

```
DHCP Server>req ipquery 192.168.8.3
IP address:       192.168.8.3
Status:           RECLAIMED
    Lease time:            86400 seconds
Start time:       Not Leased
Last time leased: 04:16:33  March 9, 1999
DHCP Server>
```

poolquery *dirección*

Visualiza información para una agrupación de direcciones IP.

dirección Indica una dirección IP de la agrupación que debe visualizarse.

Valores válidos: Cualquier dirección IP válida de la agrupación a visualizar

Valor por omisión: Ninguno

Ejemplo:

```
DHCP Server> request poolquery

Enter the client's IP address []? 194.3.200.10
     IP address:            194.3.200.10
     Status:                LEASED
     Lease time:            86400 seconds
     Start time:            16:41:25 December 3, 1998
     Last time leased:      16:41:25 December 3, 1998
     Client id:             1-0x0020351FB371
     Hostname:              Win-XY-1
     Domain name:           city.net
     IP address:            194.3.200.11
     Status:                STOCKED
     IP address:            194.3.200.12
     Status:                STOCKED
```

stats Visualiza información de estadísticas sobre la agrupación de direcciones administradas por el servidor. Las estadísticas incluyen: determinación de paquetes procesados, determinación de paquetes sin respuesta, ofertas efectuadas, alquileres otorgados, acuses de recido negativos (NAK), informes procesados, incluyendo informes más acuses de recibo (ACK), renovaciones, liberaciones, clientes BOOTP procesados, proxyARec actualizado intentado, paquetes no soportados. Sintaxis: request stats

Ejemplo:

```
DHCP Server> request stats
       Number of DISCOVER requests received:      8
       Number of OFFER responses sent:            4
       Number of ACK responses sent:              3
       Number of NACK responses sent:             0
       Number of RELEASE requests received:       0
       Number of DECLINE packets received:        0
       Number of INFORM requests received:        0
       Number of BOOTP requests received:         0
       Number of requests received via proxy:     0
       Number of UNSUPPORTED requests received:   0
       Total number of request/responses:        15
       Number of lease expirations:               0
```

status Visualiza información sobre las agrupaciones de direcciones.

Ejemplo:

```
DHCP Server> request status

     IP address:            194.3.200.10
     Status:                LEASED
     Lease time:            86400 seconds
     Start time:            16:41:25 December 3, 1998
     Last time leased:      16:41:25 December 3, 1998
     Client id:             1-0x0020351FB371
     Hostname:              Win-XY-1
     Domain name:           city.net

     IP address:            194.3.200.11
     Status:                STOCKED

     IP address:            194.3.200.12
     Status:                STOCKED

     IP address:            194.3.200.10
     Status:                STOCKED
```

Soporte de reconfiguración dinámica de DHCP

Esta sección describe la reconfiguración dinámica (DR) en lo que afecta a los mandatos de Talk 6 y Talk 5.

Delete interface de CONFIG (Talk 6)

El DHCP (Dynamic Host Configuration Protocol) no soporta el mandato de CONFIG (Talk 6) **delete interface**.

Activate interface de GWCON (Talk 5)

El mandato de GWCON (Talk 5) **activate interface** no es aplicable para DHCP (Dynamic Host Configuration Protocol). La configuración de DHCP no se basa en interfaces específicas.

Reset interface de GWCON (Talk 5)

El mandato de GWCON (Talk 5) **reset interface** no es aplicable para DHCP (Dynamic Host Configuration Protocol). La configuración de DHCP no se basa en interfaces específicas.

Mandatos reset de componente GWCON (Talk 5)

El DHCP (Dynamic Host Configuration Protocol) soporta los mandatos de GWCON (Talk 5) **reset** siguientes específicos de DHCP (Dynamic Host Configuration Protocol):

Mandato GWCON, feature DHCP, reset DHCP

Descripción: Restablecer el Servidor DHCP e inicializar con la configuración cambiada.

Efecto en la red: Si la configuración cambiada soporta los mismos clientes, se les ofrecerá a éstos un alquiler nuevo en el momento de la renovación. Si la configuración cambiada no soporta los mismos clientes, su alquiler caducará.

Limitaciones:

- En direccionadores sin tarjeta de disco fijo o de almacenamiento Flash, después de un restablecimiento, los clientes DHCP continuarán operando con sus alquileres pero el Servidor DHCP ya no les conocerá.
- En direccionadores sin tarjeta de disco fijo o de almacenamiento Flash, las direcciones IP alquiladas anteriormente por el Servidor DHCP se marcarán “USED” en el mandato “GWCON, feature DHCP, request status” cuando se intente alquilar dicha dirección otra vez.

La tabla siguiente resume los cambios de configuración de DHCP (Dynamic Host Configuration Protocol) que se activan cuando se invoca el mandato **GWCON, feature DHCP, reset dhcp**:

Mandatos cuyos cambios activa el mandato GWCON, feature DHCP, reset dhcp
CONFIG, feature DHCP, add class
CONFIG, feature DHCP, add client
CONFIG, feature DHCP, add option
CONFIG, feature DHCP, add subnet
CONFIG, feature DHCP, add vendor-option
CONFIG, feature DHCP, change class
CONFIG, feature DHCP, change client
CONFIG, feature DHCP, change subnet
CONFIG, feature DHCP, change vendor-option
CONFIG, feature DHCP, delete class
CONFIG, feature DHCP, delete client
CONFIG, feature DHCP, delete option
CONFIG, feature DHCP, delete subnet
CONFIG, feature DHCP, delete subnet-group
CONFIG, feature DHCP, delete vendor-option
CONFIG, feature DHCP, disable dhcp-server
CONFIG, feature DHCP, enable dhcp-server
CONFIG, feature DHCP, set balance
CONFIG, feature DHCP, set bootstrapserver
CONFIG, feature DHCP, set canonical
CONFIG, feature DHCP, set inorder
CONFIG, feature DHCP, set lease-expire-interval
CONFIG, feature DHCP, set lease-time-default
CONFIG, feature DHCP, set ping-time
CONFIG, feature DHCP, set support-bootp
CONFIG, feature DHCP, set support-unlisted-clients
CONFIG, feature DHCP, set used-ip-address-expire-interval

Mandatos de cambio temporal de GWCON (Talk 5)

El DHCP (Dynamic Host Configuration Protocol) soporta los mandatos de GWCON siguientes que cambian temporalmente el estado operativo del dispositivo. Estos cambios se pierden siempre que se vuelve a cargar o se reinicia el dispositivo o se ejecuta cualquier mandato reconfigurable dinámicamente.

Mandatos
GWCON, feature DHCP, disable dhcp
GWCON, feature DHCP, enable dhcp

Mandatos no reconfigurables dinámicamente

Todos los parámetros de configuración de DHCP (Dynamic Host Configuration Protocol) pueden cambiarse dinámicamente.

Configuración y supervisión de VCRM

El Gestor de recursos de circuito virtual (VCRM) es una característica que soporta el Resource ReSerVation Protocol (RSVP), que se describe en “Utilización de RSVP” y “Configuración y supervisión de RSVP” en la publicación *Consulta de configuración y supervisión de protocolos Volumen 1*. Basándose en la petición de reserva del RSVP, el VCRM crea la conexión para el flujo de datos a través de la interfaz física. Para ello, el VCRM primero debe determinar si existe suficiente ancho de banda para acomodar la reserva.

Nota: Si utiliza interfaces de WAN como por ejemplo Frame Relay o X.25, debe establecer la velocidad de línea de modo que el VCRM sepa qué ancho de banda está disponible. El procedimiento para establecer la velocidad de línea se describe en los capítulos de configuración y supervisión de la interfaz Frame Relay y X.25 de la publicación *Guía del usuario de software*.

Si la interfaz es ATM SVC, el VCRM correlaciona peticiones de QoS de RSVP con peticiones de configuración de SVC. La petición de reserva del RSVP se cumple si la configuración del SVC es satisfactoria. El VCRM se asegura de que exista el espacio de almacenamiento intermedio adecuado para los paquetes de QoS y de que estos paquetes se envíen a través del SVC correcto para su transmisión.

Si la interfaz no es ATM, como por ejemplo enlace PPP, LAN o WAN, el VCRM utiliza puesta en cola de software de los paquetes de QoS y de mayor eficacia para dar prioridad a los paquetes en el enlace de salida.

Este capítulo incluye las secciones siguientes:

- “Acceso al entorno de configuración de VCRM”
- “Acceso al entorno de supervisión de VCRM”
- “Mandatos de supervisión de VCRM” en la página 570

Acceso al entorno de configuración de VCRM

Para acceder al entorno de configuración de VCRM, entre el mandato siguiente en el indicador de mandatos `Config>`:

```
Config> feature vcrm
VC & Resource Management config console
  --Currently no configurable objects.
Config>
```

La finalidad del mensaje visualizado es indicar que el VCRM no se puede configurar por separado. La habilitación del RSVP habilita el VCRM, que obtiene sus parámetros de la configuración del RSVP.

Acceso al entorno de supervisión de VCRM

Para acceder al entorno de supervisión de VCRM, entre

```
* t 5
```

A continuación, entre el mandato siguiente en el indicador de mandatos **+**:

```
+ feature VCRM
VCRM console
VCRM Console>
```

Aparece el indicador de mandatos `VCRM Console>`.

Mandatos de supervisión de VCRM

Esta sección describe los mandatos de supervisión de VCRM. Entre estos mandatos en el indicador de mandatos `VCRM Console>`.

Tabla 63. Mandatos de supervisión de VCRM

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxx.
Clear	Restablece las estadísticas de cola.
Queue	Muestra estadísticas de puesta en cola de software no ATM.
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 restablecer las estadísticas de cola de software.

Sintaxis:

c**lear**

Consulte el mandato **queue** para obtener un ejemplo del mandato **clear**.

Queue

Utilice el mandato **queue** para mostrar la puesta en cola de software de los flujos de tráfico que no son ATM.

Sintaxis:

q**ueue**

La lista siguiente define los términos utilizados en la visualización de las colas de software no ATM:

Quota (Cuota)
Cantidad de ancho de banda reservado. Originalmente, mayor eficacia (B.E.) tiene todas las cuotas. Cuando se realiza una reserva, el ancho de banda (b/w) reservado cambia de la cuota B.E. a la cota QoS.

Max-q (Cola máx.)
Longitud máxima de cola, indicada en los paquetes.

Curr-q (Cola actual)
Longitud de cola actual, indicada en los paquetes.

In quota (Dentro de cuota)
Paquetes o kilobytes enviados dentro del ancho de banda asignado.

Outside quota (Fuera de cuota)
Paquetes o kilobytes enviados fuera del ancho de banda asignado, cuando había disponible ancho de banda desocupado.

Packets/bytes dropped (Paquetes/bytes excluidos)
Paquetes o bytes excluidos por la puesta en cola de software.

DLC packets/bytes dropped (Paquetes/bytes excluidos por DLC)
Paquetes o bytes excluidos por el DLC después de que los paquetes hayan pasado por la cola de software.

Ejemplo:

```
*t 5

+feature vcrm
VCRM console
VCRM Console>?
CLEAR
QUEUE
EXIT
VCRM Console>queue
Flow-control Queues at sys-clock 346781 Second:
---------
Intf    B.E. Quota:       10000 Kbps            QoS Quota:        0     Kbps
0/Eth   B.E. Max-q        0                     QoS Max-q         0
        B.E. curr-q       0                     QoS curr-q        0
        B.E. pkts/Kbytes sent:                  QoS pkts/Kbytes sent:
        in quota:        54169/   3926          in quota:            0/      0
        outside quota:       0/      0          outside quota:       0/      0
        B.E. pkts/bytes dropped: 0/0            QoS pkts/bytes dropped:  0/0
        DLC pkts/bytes dropped:  B.E.: 0/0      QoS: 0/0
Intf    B.E. Quota:       2048  Kbps            QoS Quota:        0     Kbps
2/PPP   B.E. Max-q        0                     QoS Max-q         0
        B.E. curr-q       0                     QoS curr-q        0
        B.E. pkts/Kbytes sent:                  QoS pkts/Kbytes sent:
        in quota:           62/      6          in quota:            0/      0
        outside quota:       0/      0          outside quota:       0/      0
        B.E. pkts/bytes dropped: 0/0            QoS pkts/bytes dropped:  0/0
        DLC pkts/bytes dropped:  B.E.: 0/0      QoS: 0/0
Intf    B.E. Quota:       2032  Kbps            QoS Quota:        16    Kbps
3/FR    B.E. Max-q        1                     QoS Max-q         1
        B.E. curr-q       0                     QoS curr-q        0
        B.E. pkts/Kbytes sent:                  QoS pkts/Kbytes sent:
        in quota:        53160/   4920          in quota:       346596/  31886
        outside quota:       0/      0          outside quota:       0/      0
        B.E. pkts/bytes dropped: 0/0            QoS pkts/bytes dropped:  0/0
        DLC pkts/bytes dropped:  B.E.: 0/0      QoS: 0/0
Intf    B.E. Quota:       2048  Kbps            QoS Quota:        0     Kbps
4/PPP   B.E. Max-q        1                     QoS Max-q         1
        B.E. curr-q       0                     QoS curr-q        0
        B.E. pkts/Kbytes sent:                  QoS pkts/Kbytes sent:
        in quota:           66/      6          in quota:          109/     1
        outside quota:       0/      0          outside quota:       0/
        B.E. pkts/bytes dropped: 0/0            QoS pkts/bytes dropped:  0/0
        DLC pkts/bytes dropped:  B.E.: 0/0      QoS: 0/0

Max total queue length=1;  current total length=0
VCRM Console>clear
Flow-control Queues cleared at sys-clock 346786 Second:
-------
VCRM Console>
```

Apéndice A. Atributos de AAA remota

Esta sección identifica los Atributos de AAA remota utilizados por los servidores Radius, TACACS y TACACS+.

Radius

ID de proveedor IBM: 211

Atributos de Autorización

Borrador estándar

TUNNEL_TYPE	64
TUNNEL_MEDIUM_TYPE	65
TUNNEL_CLIEN_TYPE	66
TUNNEL_SERVER_EP	67
TUNNEL_CONN_ID	68
TUNNEL_PASSWORD	69

valores

TUNNEL_TYPE		entero
1	PPTP	
2	L2F	
3	L2TP	
TUNNEL_MEDIUM_TYPE		entero
1	IP	
TUNNEL_SERVER_EP		serie
	dirección ip	

Específicos del proveedor de IBM

NAS_TUNNEL_PASSWORD	101
INBYTES_AH	110
INBYTES_ESP	111
OUTBYTES_AH	112
OUTBYTES_ESP	113
INPKTS_BAD	114
OUTPKTS_BAD	115
INPKTS_BAD_AH	116
INPKTS_BAD_ESP	117
OUTPKTS_BAD_AH	118
OUTPKTS_BAD_ESP	119
INPKTS_AH	120
AH INPKTS_ESP	121
OUTPKTS_AH	122
AH OUTPKTS_ESP	123
INPKTS_BAD_AH_RPLY	124
INPKTS_BAD_ESP_RPLY	125
INBYTES_WRAP	128
OUTBYTES_WRAP	129
INB_AH_WRAP	130
INB_ESP_WRAP	131
OUB_AH_WRAP	132

OUB_ESP_WRAP	133
POLICY_NAME	135
P1_ID	136
TRANSFORMS	137
REFR_CNT	138
COMPR	139
ESP_ALGO	140
AH_ALGO	141
ESPAUTH_ALGO	142
P1_NAME	143
VC-ACTIVE	177
VC-IDLETIME	179
VC-SUSPENDTIME	180
CALLBACK_FLAGS	210
ENCRYPTION	211
HOSTNAME	213
DIALOUT	214
SUBNETMASK	215
PRIVILEGE	216

Palabras clave

Se utilizan palabras clave para servidores Radius que permiten la entrada de campos específicos del proveedor `<palabra-clave>=<valor>`.

KWD_VC_ACTIVE	VCN
KWD_VC_IDLETIME	VCI
KWD_VC_SUSPENDTIME	VCS
KWD_CALLBACK_FLAGS	CBF
KWD_ENCRYPTION	ENC
KWD_HOSTNAME	HSN
KWD_DIALOUT	DOF
KWD_SUBNETMASK	SNM
KWD_PRIVILEGE	PRV

Valores

CALLBACK_FLAGS

REQ	devolución de llamada necesaria
ROAM	devolución de llamada itinerante

DIALOUT

TRUE	habilitar dialout para este usuario
FALSE	inhabilitar dialout para este usuario
ONLY	premitir sólo dialout para este usuario (no dial in)

PRIVILEGE:

ADMIN
OPER
MONITOR

Ejemplo de archivo de configuración de RADIUS

A continuación se proporciona un ejemplo de archivo de configuración de RADIUS:

```
VENDOR IBM 211
ATTRIBUTE    User-Name               1    serie
ATTRIBUTE    User-Password           2    serie
ATTRIBUTE    CHAP-Password           3    serie
ATTRIBUTE    NAS-IP-Address          4    ipaddr
ATTRIBUTE    NAS-Port                5    entero
ATTRIBUTE    Service-Type            6    entero
ATTRIBUTE    Framed-Protocol         7    entero
ATTRIBUTE    Framed-IP-Address       8    ipaddr
ATTRIBUTE    Framed-IP-Netmask       9    ipaddr
ATTRIBUTE    Framed-Routing          10   entero
ATTRIBUTE    Filter-Id               11   serie
ATTRIBUTE    Framed-MTU              12   entero
ATTRIBUTE    Framed-Compression      13   entero
ATTRIBUTE    Login-IP-Host           14   ipaddr
ATTRIBUTE    Login-Service           15   entero
ATTRIBUTE    Login-TCP-Port          16   núm. entero
ATTRIBUTE    Old-Password            17   serie
ATTRIBUTE    Reply-Message           18   serie
ATTRIBUTE    Callback-Number         19   serie
ATTRIBUTE    Callback-Id             20   núm. serie
ATTRIBUTE    Unassigned              21   serie
ATTRIBUTE    Framed-Route            22   serie
ATTRIBUTE    Framed-IPX-Network      23   entero
ATTRIBUTE    State                   24   serie
ATTRIBUTE    Class                   25   serie
ATTRIBUTE    Vendor-Specific         26   serie
ATTRIBUTE    Session-Timeout         27   entero
ATTRIBUTE    Idle-Timeout            28   entero
ATTRIBUTE    Termination-Action      29   entero
ATTRIBUTE    Called-Station-Id       30   serie
ATTRIBUTE    Calling-Station-Id      31   serie
ATTRIBUTE    NAS-Identifier          32   serie
ATTRIBUTE    Proxy-State             33   serie
ATTRIBUTE    Login-LAT-Service       34   serie
ATTRIBUTE    Login-LAT-Node          35   serie
ATTRIBUTE    Login-LAT-Group         36   serie
ATTRIBUTE    Framed-Appletalk-Link   37   entero
ATTRIBUTE    Framed-Appletalk-Net    38   entero
ATTRIBUTE    Framed-Appletalk-Zone   39   serie
ATTRIBUTE    Acct-Status-Type        40   entero
ATTRIBUTE    Acct-Delay-Time         41   entero
ATTRIBUTE    Acct-Input-Octets       42   entero
ATTRIBUTE    Acct-Output-Octets      43   entero
ATTRIBUTE    Acct-Session-Id         44   serie
ATTRIBUTE    Acct-Authentic          45   entero
ATTRIBUTE    Acct-Session-Time       46   entero
ATTRIBUTE    Acct-Input-Packets      47   entero
ATTRIBUTE    Acct-Output-Packets     48   entero
ATTRIBUTE    Acct-Terminate-Cause    49   entero
ATTRIBUTE    Acct-Multi-Session-Id   50   serie
ATTRIBUTE    Acct-Link-Count         51   entero
ATTRIBUTE    CHAP-Challenge          60   serie
ATTRIBUTE    NAS-Port-Type           61   entero
ATTRIBUTE    Port-Limit              62   entero
ATTRIBUTE    Login-LAT-Port          63   serie
```

```
---------- START IBM ----------
ATTRIBUTE   Tunnel-Type          64    entero
ATTRIBUTE   Tunnel-Medium        65    entero
ATTRIBUTE   Tunnel-Client-EP     66    serie
ATTRIBUTE   Tunnel-Server-EP     67    serie
ATTRIBUTE   Tunnel-Conn-ID       68    serie
ATTRIBUTE   Tunnel-Password      69    serie
ATTRIBUTE   Tunnel-NAS-Password  101   serie
ATTRIBUTE   VC-ACTIVE            177   entero
ATTRIBUTE   VC-IDLETIME          179   entero
ATTRIBUTE   VC-SUSPENDTIME       180   entero
ATTRIBUTE   IBM-Callback-Flags   210   serie
ATTRIBUTE   IBM-Encryption       211   serie
ATTRIBUTE   IBM-DialOut          214   serie
ATTRIBUTE   IBM-Hostname         213   serie
ATTRIBUTE   IBM-Subnetmask       215   serie
ATTRIBUTE   IBM-Privilege        216   serie
ATTRIBUTE   IBM-ipsec-inb-ah     110   entero
ATTRIBUTE   IBM-ipsec-inb-esp    111   entero
ATTRIBUTE   IBM-ipsec-ob-ah      112   entero
ATTRIBUTE   IBM-ipsec-ob-esp     113   entero
ATTRIBUTE   IBM-ipsec-ip-bad     114   entero
ATTRIBUTE   IBM-ipsec-op-bad     115   entero
ATTRIBUTE   IBM-ipsec-ip-bad-ah  116   entero
ATTRIBUTE   IBM-ipsec-ip-bad-esp 117   entero
ATTRIBUTE   IBM-ipsec-op-bad-ah  118   entero
ATTRIBUTE   IBM-ipsec-op-bad-esp 119   entero
ATTRIBUTE   IBM-ipsec-ip-ah      120   entero
ATTRIBUTE   IBM-ipsec-ip-esp     121   entero
ATTRIBUTE   IBM-ipsec-op-ah      122   entero
ATTRIBUTE   IBM-ipsec-op-esp     123   entero
ATTRIBUTE   IBM-ipsec-ip-bad-ah-r  124 entero
ATTRIBUTE   IBM-ipsec-ip-bad-esp-r 125 entero
ATTRIBUTE   IBM-ipsec-inb-wrap   128   entero
ATTRIBUTE   IBM-ipsec-ob-wrap    129   entero
ATTRIBUTE   IBM-ipsec-ib-ah-wrap 130   entero
ATTRIBUTE   IBM-ipsec-ib-esp-wrap 131  entero
ATTRIBUTE   IBM-ipsec-ob-ah-wrap 132   entero
ATTRIBUTE   IBM-ipsec-ob-esp-wrap 133  entero
ATTRIBUTE   IBM-ipsec-policy-name 135  serie
ATTRIBUTE   IBM-ipsec-p1-id      136   serie
ATTRIBUTE   IBM-ipsec-p1-name    143   serie
ATTRIBUTE   IBM-ipsec-esp-algo   140   serie
ATTRIBUTE   IBM-ipsec-ah-algo    141   serie
ATTRIBUTE   IBM-ipsec-esp-algo   142   serie

VALUE   Tunnel-Type          L2TP          3
VALUE   Tunnel-Type          L2F           2
VALUE   Tunnel-Type          PPTP          1
VALUE   Tunnel-Medium        IP            1
VALUE   VC-ACTIVE            YES           1
VALUE   VC-ACTIVE            NO            0
VALUE   IBM-Callback-Flags   Required      REQ
VALUE   IBM-Callback-Flags   Roaming       OAM
VALUE   IBM-Dialout          Enable        TRUE
VALUE   IBM-Dialout          Disable       FALSE
VALUE   IBM-Dialout          ONLY          ONLY
VALUE   IBM-Privilege        Administrator ADMIN
VALUE   IBM-Privilege        Operator      OPER
VALUE   IBM-Privilege        Monitor       MONITOR
```

TACACS+

Autentificación

Autorización

PPP service=ppp protocol=ip
LOGIN service=shell cmd=null pri_lvl*0

Atributos estándar de TACACS+

service	
protocol	
cmd	
addr	
timeout	
priv_lvl	0 (privilegio supervisor), 1 (privilegio operador), 15 (privilegio administrador)
callback-dialstring	

Atributos específicos de IBM

encryption_key	16 caracteres hexadecimales
dial_out	TRUE FALSE ONLY

Contabilidad

task_id
start_time
stop_time
elasped_time
timezone
event
reason
bytes
bytes_in
bytes_out
paks
paks_in
paks_out
status
err_msg

Apéndice B. Lista de Abreviaturas

AARP	AppleTalk Address Resolution Protocol
ABR	Direccionador de marco de área
ack	Acuse de recibo
AIX	Advanced Interactive Executive
AMA	Direccionamiento del MAC arbitrario
AMP	Supervisor presente activo
ANSI	American National Standards Institute
AP2	AppleTalk Phase 2
APPN	Advanced Peer-to-Peer Networking
ARE	Explorador de todas las rutas
ARI	Interfaz ATM real
ARI/FCI	Indicador de dirección reconocida/indicador de trama copiada
ARP	Address Resolution Protocol
AS	Sistema autónomo
ASBR	Direccionador de límite de sistema autónomo
ASCII	American National Standard Code for Information Interchange
ASN.1	Notación de sintaxis de abstracción 1
ASRT	Direccionamiento transparente de origen adaptable
ASYNC	Asíncrono
ATCP	AppleTalk Control Protocol
ATP	AppleTalk Transaction Protocol
AUI	Interfaz de unidad de conexión
AVI	Interfaz ATM virtual
ayt	¿Hay alguien ahí?
BAN	Boundary Access Node
BBCM	Bridging Broadcast Manager
BECN	Notificación de congestión explícita hacia atrás
BGP	Border Gateway Protocol
BNC	Bayonet Niell-Concelman
BNCP	Bridging Network Control Protocol
BOOTP	Protocolo BOOT
BPDU	Unidad de datos de protocolo de puente
bps	Bits por segundo
BR	Función de puente/direccionamiento

BRS Reserva de ancho de banda

BSD Distribución de software de Berkeley

BTP Agente de relay de BOOTP

BTU Unidad básica de transmisión

CAM Memoria dirigible a través del contenido

CCITT Comisión Consultiva de la Telefonía y Telegrafía Internacionales

CD Detección de colisión

CGWCON Consola de pasarela

CIDR Direccionamiento entre dominios sin clase

CIP Classical IP

CIR Velocidad de información comprometida

CLNP Connectionless-Mode Network Protocol

CPU Unidad central de proceso

CRC Comprobación de redundancia cíclica

CRS Servidor de informes de configuración

CTS Preparado para transmitir

CUD Datos de usuario de llamada

DAF Filtrado 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 de anotación cronológica de sucesos

ESI Identificador de sistema final

EST Horario Estándar del Este de los EE.UU

Eth Ethernet

fa-ga Dirección funcional-dirección de grupo

FCS Secuencia de comprobación de trama

FECN Notificación de congestión explícita hacia adelante

FIFO Primero en entrar, primero en salir

FLT Biblioteca de filtros

FR Frame Relay

FRL Frame Relay

FTP File Transfer Protocol

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 Servicios de sistema principal de TCP/IP

HTF Formato de tabla de sistema principal

IBD Dispositivo de arranque integrado

ICMP Internet Control Message Protocol

ICP Internet Control Protocol

ID Identificación

IDP Parte de dominio inicial

IDP Internet Datagram Protocol

IEEE Institute of Electrical and Electronics Engineers

Ifc# Número de interfaz

IGP Interior Gateway Protocol

InARP Inverse Address Resolution Protocol

IP Internet Protocol

IPCP IP Control Protocol

IPPN IP Protocol Network

IPX Internetwork Packet Exchange

IPXCP IPX Control Protocol

RDSI Red digital de servicios integrados

ISO Organización Internacional para la Normalización

Kbps Kilobits por segundo

LAC Concentrador del acceso a la red L2TP

LAN Red de área local

LAPB Protocolo de acceso a enlace equilibrado

LAT Transporte de área local

LCP Link Control Protocol

LED Diodo emisor de luz

LF Trama mayor; salto de línea

LIS Subred IP lógica

LLC Control de enlace lógico

LLC2 Control de enlace lógico 2

LMI Interfaz de gestión local

LNS Servidor de red L2TP

LRM Mecanismo de información de LAN

LS Estado de los enlaces

LSA Notificación del estado de los enlaces

LSB Bit menos significativo

LSI Interfaz de métodos abreviados de LAN

LSreq Petición del estado de los enlaces

LSrxl Lista de retransmisiones del estado de los enlaces

LU Unidad lógica

MAC Control del acceso al medio

Mb Megabit

MB Megabyte

Mbps Megabits por segundo

MBps Megabytes por segundo

MC Multidifusión

MCF Filtrado del MAC

MIB Base de la información de gestión

MIB II Base de la información de gestión II

MILNET Red militar

MOS Micro Operating System

MOSDBG Micro Operating System Debugging Tool

MOSPF Open Shortest Path First con extensiones de multidifusión

MSB Bit más significativo

MSDU Unidad de datos de servicio MAC

MRU Unidad máxima de recepción

MTU Unidad máxima de transmisión

nak Sin acuse de recibo

NBMA Acceso múltiple sin difusión

NBP Name Binding Protocol

NBR Direccionador contiguo

NCP Network Control Protocol

NCP Network Core Protocol

NetBIOS Network Basic Input/Output System

NHRP Next Hop Resolution Protocol

NIST National Institute of Standards and Technology

NPDU Unidad de datos de protocolo de red

NRZ Sin vuelta a cero

NRZI Sin vuelta a cero invertido

NSAP Punto de acceso a servicios de red

NSF National Science Foundation

NSFNET National Science Foundation NETwork

NVCNFG Configuración permanente

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 Supervisor de errores de anillo

REV Recepción

RFC Request for Comments

RI Indicador de llamada; información de direccionamiento

RIF Campo de información de direccionamiento

RII Indicador de información de direccionamiento

RIP Routing Information Protocol

RISC Sistema de juego reducido de instrucciones

RNR Recepción no preparada

ROM Memoria de sólo lectura

ROpcon Consola del operador remota

RPS Servidor de parámetros de anillo

RTMP Routing Table Maintenance Protocol

RTP RouTing update Protocol

RTS Petición de emisión

Rtype Tipo de ruta

rxmits Retransmisiones

rxmt Retransmisión

SAF Filtrado de direcciones de origen

SAP Punto de acceso a servicios

SAP Service Advertising Protocol

SCR Velocidad sostenida de célula

SCSP Server Cache Synchronization Protocol

sdel Delimitador de inicio

SDLC Relay de SDLC, control síncrono de enlace de datos

seqno Número de secuencia

SGID Identificación de grupo de servidores

SGMP Simple Gateway Monitoring Protocol

SL Línea serie

SMP Supervisor presente en espera

SMTP Simple Mail Transfer Protocol

SNA Systems Network Architecture

SNAP Subnetwork Access Protocol

SNMP Simple Network Management Protocol

SNPA Punto de conexión de subred

SPF Ruta intraárea OSPF

SPE1 Tipo 1 de ruta externa OSPF

SPE2 Tipo 2 de ruta externa OSPF

SPIA Tipo de ruta interárea OSPF

SPID Identificación de perfil de servicio

SPX Sequenced Packet Exchange

SQE Error en calidad de señal

SRAM Memoria de acceso aleatorio estática

SRB Puente de direccionamiento de origen

SRF Trama específicamente direccionada

SRLY Relay de SDLC

SRT Direccionamiento transparente de origen

SR-TB Puente de direccionamiento transparente de origen

STA Estático

STB Puente de árbol de expansión

STE Explorador de árbol de expansión

STP Par trenzado y apantallado; protocolo de árbol de expansión

SVC Circuito virtual conmutado

TB Puente transparente

TCN Notificación de cambio de topología

TCP Transmission Control Protocol

TCP/IP Transmission Control Protocol/Internet Protocol

TEI Identificador de punto de terminal

TFTP Trivial File Transfer Protocol

TKR Red en Anillo

TMO Tiempo de espera excedido

TOS Tipo de servicio

TSF Tramas de expansión transparentes

TTL Período de duración

TTY Teletipo

TX Transmisión

UA Acuse de recibo sin número

UDP User Datagram Protocol

UI Información sin número

UTP Par trenzado y no apantallado

VCC Conexión de canal virtual

VINES VIrtual NEtworking System

VIR Velocidad de información variable

VL Enlace virtual

VNI Virtual Network Interface

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

Este glosario incluye términos y definiciones de la documentación siguiente:

- El *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 del American National Standards Institute (ANSI). Los ejemplares pueden adquirirse en el American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Las definiciones se identifican mediante el símbolo (A) que aparece después de la definición.
- La *Norma ANSI/EIA 440-A de la Fiber Optic Terminology*. Los ejemplares pueden adquirirse en la Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006. Las definiciones se identifican mediante el símbolo (E) que aparece después de la definición.
- El *Information Technology Vocabulary* desarrollado por la Subcomisión 1, Comisión Técnica Mixta 1, de la Organización Internacional para la Normalización y la Comisión Electrotécnica Internacional (JTC1/SC1 de la ISO/IEC). Las definiciones de las secciones publicadas de este vocabulario se identifican mediante el símbolo (I) que aparece después de la definición; las definiciones de los borradores de normas internacionales, borradores de comisiones y documentos de trabajo que está desarrollando la JTC1/SC1 de la ISO/IEC se identifican mediante el símbolo (T) que aparece después de la definición, símbolo que indica que las Corporaciones Nacionales de la SC1 participantes todavía no han llegado a un acuerdo definitivo.
- El *IBM Dictionary of Computing*, New York: McGraw-Hill, 1994.
- Internet Request for Comments: 1208, *Glossary of Networking Terms*
- Internet Request for Comments: 1392, *Internet Users' Glossary*
- El *Object-Oriented Interface Design: IBM Common User Access Guidelines*, Carmel, Indiana: Que, 1992.

En este glosario, se utilizan las siguientes referencias cruzadas:

Compárese con: Se refiere a un término que tiene un significado opuesto o esencialmente distinto.

Sinónimo de: Indica que el término tiene el mismo significado que un término preferente, el cual está definido en el lugar que le corresponde dentro del glosario.

Sinónimo con: Es una referencia hacia atrás de un término definido a los otros términos que tienen el mismo significado.

Véase: Remite al lector a términos de diversas palabras que tienen la misma palabra al principio.

Véase también: Remite al lector a términos que tienen un significado relacionado, pero no sinónimo.

A

AAL-5. Capa de adaptación de ATM 5, una de las diversas AAL estándares. AAL-5 se ha diseñado para las comunicaciones de datos y la utilizan la Emulación de LAN y el IP clásico.

AAL. Capa de adaptación de ATM, que es la que adapta los datos de usuario a/de la red ATM añadiendo/eliminando cabeceras y segmentando/volviendo a ensamblar los datos en/a partir de células.

acceso de memoria directo (DMA). Recurso del sistema que permite que un dispositivo del bus Micro Channel obtenga acceso directo a la memoria del sistema o a la memoria del bus sin la intervención del procesador del sistema.

acceso múltiple con detección de portadora y detección de colisión (CSMA/CD). Protocolo que necesita detección de portadora y en el que una estación de datos transmisora que detecta otra señal mientras transmite detiene la emisión, envía una señal de atasco y luego espera durante un período variable antes de volver a intentar la acción. (T) (A)

ACCESS. En el protocolo Simple Network Management Protocol (SNMP), cláusula de un módulo de la Base de la información de gestión (MIB) que define el nivel mínimo de soporte que proporciona un nodo gestionado para un objeto.

activo. (1) Operativo. (2) Perteneciente a un nodo o dispositivo que está conectado o está disponible para la conexión con otro nodo o dispositivo.

actualización de base de datos de topología (TDU). Mensaje sobre un nodo o enlace nuevo o modificado que se difunde entre los nodos de red APPN para mantener la base de datos de topología de red, que está reproducida en su totalidad en cada nodo de red. Una TDU contiene información para identificar lo siguiente:

- El nodo emisor.
- Las características de nodo y enlace de diversos recursos de la red.
- El número de secuencia de la actualización más reciente para cada uno de los recursos descritos.

acuse de recibo. (1) Transmisión, por parte de un receptor, de caracteres de acuse de recibo como respuesta afirmativa a un remitente. (T) (2) Indicación de que se ha recibido un elemento enviado.

Address Resolution Protocol (ARP). (1) En el conjunto de protocolos de Internet, protocolo que correlaciona dinámicamente una dirección IP con una dirección utilizada por una red de área metropolitana o local de soporte, como, por ejemplo, Ethernet o Red en Anillo. (2) Véase también *Reverse Address Resolution Protocol (RARP)*.

Advanced Peer-to-Peer Networking (APPN). Extensión de SNA que ofrece (a) un control superior de las redes distribuidas que evita las dependencias jerárquicas críticas y, por lo tanto, aisla los efectos de puntos anómalos individuales; (b) intercambio dinámico de información de topología de red para facilitar la conexión, reconfiguración y selección de rutas adaptables; (c) definición dinámica de recursos de red; y (d) automatización en el registro de recursos y la búsqueda en directorios. APPN hace extensiva la orientación de igual de la LU 6.2 para los servicios de usuario final al control de redes y da soporte a diversos tipos de LU, incluidas la LU 2, la LU 3 y la LU 6.2.

agencia operativa privada reconocida (RPOA). Cualquier individuo, empresa o corporación (que no sea un departamento o servicio del gobierno) que realiza operaciones en un servicio de telecomunicaciones y está sujeta a las obligaciones definidas en el Convenio de la unión de telecomunicaciones internacionales y en la legislación; por ejemplo, una empresa de telecomunicación.

agente. Sistema que asume un papel de agente.

alerta. Mensaje enviado a un punto focal de servicios de gestión de una red para identificar un problema o un problema inminente.

American National Standards Institute (ANSI). Organización compuesta por productores, clientes y grupos con intereses generales que establece los procedimientos mediante los cuales organizaciones acreditadas crean y mantienen normas voluntarias de la industria en los Estados Unidos. (A)

analógico. (1) Perteneciente a datos compuestos por cantidades físicas continuamente variables. (A) (2) Compárese con *digital*.

ancho de banda. El ancho de banda de un enlace óptico designa la capacidad de contener información del enlace y está relacionado con la máxima velocidad en bits a la que puede dar soporte un enlace de fibra.

anillo. Véase *red de tipo anillo*.

anomalía en la autentificación. En el protocolo Simple Network Management Protocol (SNMP), detección (de condición de excepción) que una entidad de autentificación puede haber generado cuando un cliente peticionario no es miembro de la comunidad de SNMP.

antememoria. (1) Almacenamiento intermedio de fines especiales más pequeño y rápido que el almacenamiento principal; se utiliza para que contenga una copia de instrucciones y datos obtenidos del almacenamiento principal y que probablemente necesitará a continuación el procesador. (T) (2) Almacenamiento intermedio que contiene instrucciones y datos a los que se accede frecuentemente; se utiliza para reducir el tiempo del acceso. (3) Parte opcional de la base de datos de directorios existente en los nodos de red donde puede almacenarse información de directorios de uso frecuente para acelerar las búsquedas en directorios. (4) Colocar, ocultar o almacenar en antememoria.

aparato de datos preparado (DSR). Sinónimo de *DCE preparado*.

AppleTalk. Protocolo de red desarrollado por Apple Computer, Inc. Este protocolo se utiliza para la interconexión de dispositivos de red, que pueden ser una mezcla de productos Apple y productos que no son Apple.

AppleTalk Address Resolution Protocol (AARP). En redes AppleTalk, protocolo que (a) convierte las direcciones de nodo AppleTalk en direcciones de hardware y (b) soluciona las discrepancias de direccionamiento en las redes que dan soporte a más de un conjunto de protocolos.

AppleTalk Transaction Protocol (ATP). En redes AppleTalk, protocolo que proporciona funciones de petición y respuesta de cliente/servidor a los sistemas principales que acceden al protocolo Zone Information Protocol (ZIP) para la información de zonas.

árbol de expansión. En contextos de LAN, método mediante el cual los puentes desarrollan automáticamente una tabla de direccionamiento y actualizan esta tabla en respuesta a un cambio de la topología para asegurarse de la existencia de una sola ruta entre dos LAN cualesquiera en la red con puentes. Este método evita bucles de paquetes, donde un paquete vuelve en una ruta de circuito al direccionador emisor.

archivo de configuración. Archivo que especifica las características de un dispositivo del sistema o una red.

área. En los protocolos de direccionamiento de Internet y DECnet, subconjunto de una red o pasarela que se ha agrupado por definición del administrador de red. Cada área es independiente; la información sobre la topología de un área permanece oculta respecto a las otras áreas.

arquitectura de red. Estructura lógica y principios operativos de una red de sistema. (T)

Nota: Los principios operativos de una red incluyen los principios de los servicios, funciones y protocolos.

arquitectura interconexión de sistemas abiertos (OSI). Arquitectura de red que se ajusta al conjunto particular de normas ISO relacionado con interconexión de sistemas abiertos. (T)

arreglo temporal del programa (PTF). Solución o ajuste temporal de un problema diagnosticado por IBM en un release actual no modificado del programa.

asequibilidad. Capacidad de un nodo o recurso para comunicarse con otro nodo o recurso.

asíncrono (ASYNC). Perteneciente a dos o más procesos que no dependen de la aparición de sucesos específicos, como, por ejemplo, señales comunes de temporización. (T)

ATM. Asynchronous Transfer Mode, tecnología de red de gran velocidad orientada a las conexiones que se basa en la conmutación de células.

ATMARP. ARP en Classical IP.

B

base de datos de configuración (CDB). Base de datos que almacena los parámetros de configuración de uno o diversos dispositivos. Se prepara y actualiza utilizando el Programa de configuración.

base de la información de gestión (MIB). (1) Conjunto de objetos a los que se puede acceder por medio de un protocolo de gestión de red. (2) Definición de información de gestión que especifica la información disponible de un sistema principal o una pasarela y las operaciones permitidas. (3) En OSI, depósito conceptual de información de gestión dentro de un sistema abierto.

baudio. En la transmisión asíncrona, unidad de velocidad de modulación correspondiente al intervalo de una unidad por segundo; es decir, si la duración del intervalo de la unidad es de 20 milisegundos, la velocidad de modulación es de 50 baudios. (A)

bit D. Bit de confirmación de entrega. En comunicaciones X.25, bit de un paquete de datos o paquete de petición de llamada que se establece en 1 si el destinatario necesita acuse de recibo (confirmación de entrega) de extremo a extremo.

Border Gateway Protocol (BGP). Protocolo de direccionamiento de Internet Protocol (IP) utilizado entre dominios y sistemas autónomos.

bucle de direccionamiento. Situación que ocurre cuando los direccionadores hacen circular información entre ellos hasta que se produce la convergencia o hasta que se consideran inasequibles las redes implicadas.

C

cabecera. (1) Información de control definida por el sistema que precede a los datos de usuario. (2) Parte de un mensaje que contiene información de control para el mismo, como, por ejemplo, uno o más campos de destino, el nombre de la estación de origen, el número de secuencia de entrada, una serie de caracteres que indica el tipo de mensaje y el nivel de prioridad del mensaje.

cabecera de transmisión (TH). Información de control, seguida opcionalmente de una unidad básica de información (BIU) o de un segmento de BIU, que crea y utiliza el control de la vía de acceso para direccionar unidades de mensajes y controlar su flujo dentro de la red. Véase también *unidad de información de vía de acceso*.

canal. (1) Vía de acceso por la que pueden enviarse señales, como, por ejemplo, canal de datos, canal de salida. (A) (2) Unidad funcional, controlada por el procesador, que maneja la transferencia de datos entre el almacenamiento del procesador y el equipo de periféricos local.

canal de entrada/salida. En un sistema de proceso de datos, unidad funcional que maneja la transferencia de datos entre el equipo interno y el equipo de periféricos. (I) (A)

canal lógico. En el funcionamiento en modalidad de paquete, canal de emisión y canal de recepción que se utilizan conjuntamente para enviar y recibir datos sobre un enlace de datos al mismo tiempo. Pueden establecerse varios canales lógicos en el mismo enlace de datos si se interpone la transmisión de paquetes.

capa. (1) En una arquitectura de red, grupo de servicios que está completo desde un punto de vista conceptual, que es uno de los grupos de un conjunto de grupos ordenados jerárquicamente y que se extiende por todos los sistemas que se ajustan a la arquitectura de red. (T) (2) En el modelo de referencia interconexión de sistemas abiertos, uno de los siete grupos de servicios, funciones y protocolos ordenados jerárquicamente y completos conceptualmente que se extienden por todos los sistemas abiertos. (T) (3) En SNA, agrupación de funciones relacionadas que están separadas lógicamente de las funciones de otros grupos. La implementación de las funciones de una

capa puede cambiar sin que ello afecte a las funciones de otras capas.

capa de control de enlace de datos (DLC). En SNA, capa que está compuesta por las estaciones de enlace que planifican la transferencia de datos sobre un enlace entre dos nodos y realizan un control de errores para el enlace. Ejemplos de control de enlace de datos son: el SDLC para la conexión de enlaces serie por bit y el control de enlace de datos para el canal de System/370.

Nota: Normalmente, la capa de DLC es independiente del mecanismo de transporte físico y asegura la integridad de los datos que alcanzan las capas superiores.

capa de enlace de datos. En el modelo de referencia de OSI (interconexión de sistemas abiertos), capa que proporciona servicios para la transferencia de datos entre las entidades de la capa de red sobre un enlace de comunicaciones. La capa de enlace de datos detecta los errores que puedan producirse en la capa física y posiblemente los corrige. (T)

capa de red. En la arquitectura interconexión de sistemas abiertos (OSI), capa que es responsable del direccionamiento, de la conmutación y del acceso a la capa de enlace a lo largo del entorno de OSI.

capa de transporte. En el modelo de referencia interconexión de sistemas abiertos, capa que proporciona un servicio fiable de transferencia de datos de extremo a extremo. Puede haber sistemas abiertos del tipo Relay en la vía de acceso. (T) Véase también *modelo de referencia interconexión de sistemas abiertos*.

capa física. En el modelo de referencia interconexión de sistemas abiertos, capa que proporciona los medios mecánicos, eléctricos, funcionales y de procedimiento para establecer, mantener y liberar conexiones físicas sobre el medio de transmisión. (T)

carácter comodín. Sinónimo de *carácter de coincidencia con el patrón*.

carácter de coincidencia con el patrón. Carácter especial, como, por ejemplo, un asterisco (*) o un signo de interrogación (?), que puede utilizarse para representar uno o más caracteres. Cualquier carácter o conjunto de caracteres puede sustituir a un carácter de coincidencia con el patrón. Sinónimo con *carácter global* y *carácter comodín*.

CCITT. Comisión consultiva de la telefonía y telegrafía Internacionales. Era una organización de la Unión de Telecomunicaciones Internacionales (ITU). El 1 de marzo de 1993 se reorganizó la ITU y las responsabilidades de la normalización recayeron en una organización subordinada que se denomina Sector de normalización de telecomunicaciones de la unión de telecomunicaciones (ITU-TS). La “CCITT” sigue funcionando para las recomendaciones que se aprobaron antes de la reorganización.

central privada (PBX). Central telefónica privada para la transmisión de llamadas desde y hacia la red telefónica pública.

centro de información de la red (NIC). En comunicaciones de Internet, grupos locales, regionales y nacionales de todo el mundo que proporcionan ayuda, documentación, formación y otros servicios a los usuarios.

circuito de datos. (1) Par de canales de transmisión y recepción asociados que proporcionan un medio de comunicación de datos de dos direcciones. (I) (2) En SNA, sinónimo de *conexión de enlace*. (3) Véase también *circuito físico* y *circuito virtual*.

Notas:

1. Entre los intercambios de conmutaciones de datos, el circuito de datos puede incluir un equipo de terminación de circuito de datos (DCE) de acuerdo con el tipo de interfaz que se utilice en el intercambio de conmutaciones de datos.
2. Entre una estación de datos y un intercambio de conmmutaciones de datos o concentrador de datos, el circuito de datos incluye el equipo de terminación de circuito de datos en el extremo de la estación de datos y puede incluir un equipo similar a un DCE en el intercambio de conmutaciones de datos o en la ubicación del concentrador de datos.

circuito físico. Circuito establecido sin multiplexación. Véase también *circuito de datos*. Compárese con *circuito virtual*.

circuito huérfano. Circuito no configurado cuya disponibilidad se aprende dinámicamente.

circuito virtual. (1) En la conmutación de paquetes, recursos proporcionados por una red que ofrecen el aspecto de una conexión real ante el usuario. (T) Véase también *circuito de datos*. Compárese con *circuito físico*. (2) Conexión lógica establecida entre dos DTE.

circuito virtual conmutado (SVC). Circuito X.25 que se establece dinámicamente cuando es necesario. El equivalente, en X.25, de una línea conmutada. Compárese con *circuito virtual permanente (PVC)*.

circuito virtual permanente (PVC). En comunicaciones de X.25 y Frame-Relay, circuito virtual que tiene un canal lógico asignado permanentemente al mismo en cada equipo terminal de datos (DTE). No son necesarios protocolos de establecimiento de llamada. Compárese con *circuito virtual conmutado (SVC)*.

clase de productividad. En la conmutación de paquetes, velocidad a la que circulan los paquetes de un equipo terminal de datos (DTE) por la red de conmutación de paquetes.

clase de servicio (COS). Conjunto de características (como, por ejemplo, seguridad de ruta, prioridad de transmisión y ancho de banda) utilizadas para crear una ruta entre los asociados a una sesión. La clase de servicio deriva de un nombre de modalidad especificado por el iniciador de una sesión.

cliente. (1) Unidad funcional que recibe servicios compartidos de un servidor. (T) (2) Usuario.

cliente de emulación de LAN (LEC). Componente de la emulación de LAN que representa a los usuarios de la LAN emulada.

cliente/servidor. En comunicaciones, modelo de interacción en el proceso de datos distribuidos en el que un programa de un sitio envía una petición a un programa de otro sitio y espera una respuesta. El programa peticionario se denomina cliente; el programa que responde se denomina servidor.

codificar. Convertir datos mediante el uso de un código de manera que sea posible la reconversión al formato original. (T)

colisión. Condición no deseada que deriva de la existencia de transmisiones simultáneas en un canal. (T)

compresión. (1) Proceso consistente en eliminar claros, campos vacíos, redundancias y datos innecesarios para disminuir la longitud de los registros o los bloques. (2) Cualquier codificación destinada a reducir el número de bits utilizados para representar un mensaje o un registro determinado.

comunidad. En el protocolo Simple Network Management Protocol (SNMP), relación administrativa entre las entidades.

Concentrador del acceso a L2TP (LAC). Dispositivo conectado a una o más líneas RDSI o de red telefónica de servicios públicos (PSTN) con posibilidades de manejar el funcionamiento de PPP y el del protocolo L2TP. El LAC implementa el medio sobre el que funciona L2TP. L2TP pasa el tráfico a uno o más Servidores de red L2TP (LNS). L2TP puede proporcionar la función de túnel para cualquier protocolo que conlleve la red PPP.

concentrador (inteligente). Concentrador de cableado, como, por ejemplo, el IBM 8260, que proporciona funciones de puente y direccionamiento a las LAN con diferentes cables y protocolos.

conectado mediante enlace. (1) Perteneciente a dispositivos que están conectados a una unidad de control por medio de un enlace de datos. (2) Compárese con *conectado mediante canal*. (3) Sinónimo con *remoto*.

conexión. En la comunicación de datos, asociación establecida entre unidades funcionales para comunicar información. (I) (A)

conexión de enlace. (1) Equipo físico que proporciona comunicación en dos direcciones entre una estación de enlace y otra u otras estaciones de enlace; por ejemplo, un equipo de terminación de circuito de datos (DCE) y una línea de telecomunicaciones. (2) En SNA, sinonimia con *circuito de datos*.

conexión Rapid Transport Protocol (RTP). En el direccionamiento de alto rendimiento (HPR), conexión establecida entre los puntos finales de la ruta para transportar tráfico de sesión.

conexión virtual. En Frame Relay, vía de acceso de vuelta de una conexión potencial.

configuración. (1) Manera en que están organizados e interconectados el hardware y el software de un sistema de proceso de información. (T) (2) Dispositivos y programas que componen un sistema, un subsistema o una red.

configuración del sistema. Proceso que especifica los dispositivos y programas que componen un sistema de proceso de datos determinado.

congestión. Véase *congestión de la red*.

congestión de la red. Condición no deseada de carga excesiva causada por la presencia de más tráfico del que puede manejar una red.

conmutación de la línea. Sinónimo de *conmutación del circuito*.

conmutación del circuito. (1) Proceso que, a petición, conecta dos o más equipos terminales de datos (DTE) y permite el uso exclusivo de un circuito de datos entre ellos hasta que se libera la conexión. (I) (A) (2) Sinónimo con *conmutación de la línea*.

conmutación del enlace de datos (DLSw). Método para transportar protocolos de red que utilizan el tipo 2 de control de enlace lógico (LLC) de IEEE 802.2. SNA y NetBIOS son ejemplos de protocolos que utilizan el tipo 2 de LLC. Véase también *encapsulación* y *simulación*.

conmutación de paquetes. (1) Proceso consistente en direccionar y transferir datos por medio de paquetes dirigidos de manera que un canal esté ocupado durante la transmisión de un paquete solamente. Cuando se completa la transmisión, el canal queda disponible para la transferencia de otros paquetes. (I) (2) Sinónimo

con *funcionamiento en modalidad de paquete*. Véase también *conmutación del circuito*.

contigua activa de donde proceden los datos (NAUN). En la Red en Anillo de IBM, estación que envía datos directamente a una estación determinada del anillo.

control de enlace de datos de alto nivel (HDLC). En la comunicación de datos, utilización de una serie de bits especificada para controlar enlaces de datos de acuerdo con las normas internacionales respecto al HDLC: la estructura de trama de ISO 3309 y los elementos de procedimientos de ISO 4335.

control de enlace de datos (DLC). Conjunto de normas utilizado por los nodos de un enlace de datos (como, por ejemplo, un enlace de SDLC o una Red en Anillo) para efectuar un intercambio de información ordenado.

control de enlace lógico (LLC). Subcapa de LAN de control de enlace de datos (DLC) que proporciona dos tipos de operaciones de DLC para el intercambio ordenado de información. El primer tipo es el servicio sin conexiones, que permite enviar y recibir información sin establecer un enlace. La subcapa de LLC no efectúa recuperación de errores ni control del flujo para el servicio sin conexiones. El segundo tipo es el servicio orientado a las conexiones, que requiere el establecimiento de un enlace antes del intercambio de información. El servicio orientado a las conexiones proporciona transferencia de información en secuencia, control del flujo y recuperación de errores.

control del acceso al medio (MAC). En las LAN, subcapa de la capa de control de enlace de datos que da soporte a funciones dependientes del medio y utiliza los servicios de la capa física para proporcionar servicios a la subcapa de control de enlace lógico (LLC). La subcapa del MAC incluye el método para determinar cuándo un dispositivo tiene acceso al medio de transmisión.

control de la vía de acceso (PC). Función que direcciona unidades de mensajes entre las unidades de red accesibles de la red y proporciona las vías de acceso entre éstas. Convierte las unidades básicas de información (BIU) del control de transmisión (posiblemente segmentándolas) en unidades de información de vía de acceso (PIU) e intercambia unidades básicas de transmisión que contienen una o más PIU con el control de enlace de datos. El control de la vía de acceso difiere según el tipo de nodo: algunos nodos (los nodos APPN, por ejemplo) utilizan identificadores de sesión generados localmente para el direccionamiento y otros (los nodos de subárea) utilizan direcciones de red para el direccionamiento.

control del flujo. (1) En SNA, proceso consistente en gestionar la velocidad a la que pasa el tráfico de datos entre los componentes de la red. La finalidad del control del flujo es optimizar la velocidad del flujo de unidades de mensajes con la congestión mínima de la red; es decir, ni desbordar los almacenamientos intermedios del receptor o de nodos de direccionamiento intermedio ni dejar al receptor esperando más unidades de mensajes. (2) Véase también *ritmo*.

Control síncrono de enlace de datos (SDLC). (1) Disciplina que se ajusta a los subconjuntos de los Advanced Data Communication Control Procedures (ADCCP) del American National Standards Institute (ANSI) y del High-level Data Link Control (HDLC) de la organización internacional para la normalización, y está destinada a la gestión de la transferencia síncrona de información serie por bit de código transparente sobre una conexión de enlace. Los intercambios de transmisiones pueden ser dúplex o semi-dúplex sobre enlaces conmutados o no conmutados. La configuración de la conexión de enlace puede ser de punto a punto, de multipunto o de bucle. (I) (2) Compárese con *comunicación síncrona en binario (BSC)*.

correlación. Proceso consistente en convertir datos que el emisor transmite con un formato determinado en el formato de datos que puede aceptar el receptor.

corriente de datos general (GDS). Corriente de datos utilizada para las conversaciones en sesiones de LU 6.2.

coste de la vía de acceso. En los protocolos de direccionamiento de estado de los enlaces, suma de los costes de enlace a lo largo de la vía de acceso entre dos nodos o redes.

cronometraje. (1) En la comunicación síncrona en binario, utilización de pulsaciones de reloj para controlar la sincronización de los datos y caracteres de control. (2) Método para controlar el número de bits de datos enviados en una línea de telecomunicaciones en un momento determinado.

cuenta de saltos. (1) Métrica o medida de distancia entre dos puntos. (2) En comunicaciones de Internet, número de direccionadores por los que pasa un datagrama cuando se dirige a su destino. (3) En SNA, medida consistente en el número de enlaces por los que se debe pasar en la vía de acceso a un destino.

D

daemon. Programa que se ejecuta desatendido para realizar un servicio estándar. Algunos daemon se desencadenan de manera automática para realizar su tarea; otros realizan las operaciones periódicamente.

datagrama. (1) En la conmutación de paquetes,

paquete individual e independiente de otros paquetes que contiene información suficiente para el direccionamiento desde el equipo terminal de datos (DTE) de origen al DTE de destino sin apoyarse en intercambios anteriores entre los DTE y la red. (I) (2) En TCP/IP, unidad básica de información que pasa a través del entorno de Internet. Un datagrama contiene direcciones de origen y de destino junto con los datos. Un datagrama de Internet Protocol (IP) está compuesto por una cabecera de IP seguida de los datos de capa de transporte. (3) Véase también *paquete* y *segmento*.

datagrama de IP. En el conjunto de protocolos de Internet, unidad básica de información transmitida a través de una internet. Contiene direcciones de origen y de destino, datos de usuario e información de control, como, por ejemplo, la longitud del datagrama, la suma de comprobación de cabecera y distintivos que indican si el datagrama puede fragmentarse o si se ha fragmentado.

Datagram Delivery Protocol (DDP). En redes AppleTalk, protocolo que proporciona conectividad de red por medio de un servicio de entrega de socket a socket sin conexiones de la capa de internet.

DCE preparado. En la norma EIA 232, señal que indica al equipo terminal de datos (DTE) que el equipo de terminación de circuito de datos (DCE) local está conectado al canal de comunicaciones y se encuentra preparado para enviar datos. Sinónimo con *aparato de datos preparado (DSR)*.

DECnet. Arquitectura de red que define el funcionamiento de una familia de módulos de software, bases de datos y componentes de hardware que se utilizan normalmente con el fin de conectar entre sí sistemas Digital Equipment Corporation para el compartimiento de recursos, cálculo distribuido o configuración de sistemas remotos. Las implementaciones de la red DECnet siguen el modelo Digital Network Architecture (DNA).

detección de colisión. En el acceso múltiple con detección de portadora y detección de colisión (CSMA/CD), señal que indica que dos o más estaciones están transmitiendo simultáneamente.

detección (de condición de excepción). En Simple Network Management Protocol (SNMP), mensaje enviado por un nodo gestionado (la función de agente) a una estación de gestión para informarle de una condición de excepción.

detección de portadora. En una red de área local, actividad continua de una estación de datos para detectar si otra estación está transmitiendo. (T)

detector de portadora. Sinónimo de *detector de señal de línea recibida (RLSD)*.

detector de portadora de datos (DCD). Sinónimo de *detector de señal de línea recibida (RLSD)*.

detector de señal de línea recibida (RLSD). En la norma EIA 232, señal que indica al equipo terminal de datos (DTE) que está recibiendo una señal del equipo de terminación de circuito de datos (DCE) remoto. Sinónimo con *detector de portadora* y *detector de portadora de datos (DCD)*.

determinación de problemas. Proceso consistente en determinar el origen de un problema; por ejemplo, un componente de un programa, una anomalía en una máquina, recursos de telecomunicaciones, programas o equipos instalados por el contratista o por el usuario, una anomalía del entorno, como, por ejemplo, pérdida de alimentación, o un error del usuario.

difusión. (1) Transmisión de los mismos datos a todos los destinos. (T) (2) Transmisión simultánea de datos a más de un destino. (3) Compárese con *multidifusión*.

digital. (1) Perteneciente a datos compuestos por dígitos. (T) (2) Perteneciente a datos con formato de dígitos. (A) (3) Compárese con *analógico*.

Digital Network Architecture (DNA). Modelo para todas las implementaciones de hardware y software DECnet.

dirección. En la comunicación de datos, código exclusivo asignado a cada dispositivo, estación de trabajo o usuario conectado a una red.

dirección administrada localmente. En una red de área local, dirección de adaptador que el usuario puede asignar para alterar temporalmente la dirección administrada universalmente. Compárese con *dirección administrada universalmente*.

dirección administrada universalmente. En una red de área local, dirección codificada de forma permanente en un adaptador en el momento de la fabricación. Todas las direcciones administradas universalmente son exclusivas. Compárese con *dirección administrada localmente*.

direccionador. (1) Sistema que determina la vía de acceso del flujo de tráfico de red. La selección de vía de acceso se realiza entre diversas vías de acceso sobre la base de la información obtenida a partir de protocolos específicos, algoritmos que intentan identificar la vía de acceso mejor o la más corta, y otros criterios, como, por ejemplo, direcciones de destino específicas de los protocolos o la métrica. (2) Dispositivo de conexión que conecta dos segmentos de LAN, los cuales utilizan arquitecturas similares o diferentes, en la capa de red del modelo de referencia. (3) En terminología de OSI, función que determina una vía de

acceso mediante la cual puede accederse a una entidad. (4) En TCP/IP, sinonimia con *pasarela*. (5) Compárese con *puente*.

direccionador contiguo. Direccionador de una subred común designado por un administrador de red para recibir información de direccionamiento.

direccionador de frontera. En comunicaciones de Internet, direccionador que está posicionado al borde de un sistema autónomo y se comunica con un direccionador que está posicionado al borde de un sistema autónomo diferente.

direccionador de germinación. En redes AppleTalk, direccionador que mantiene datos de configuración (números de red de rango y listas de zonas, por ejemplo) para la red. Cada red debe tener, como mínimo, un direccionador de germinación. El direccionador de germinación debe configurarse inicialmente por medio de la herramienta configuradora. Compárese con *direccionador sin germinación*.

direccionador de IP. Dispositivo de una internet IP que tiene la responsabilidad de tomar decisiones acerca de las vías de acceso por las que fluirá tráfico de red. Los protocolos de direccionamiento se utilizan para obtener información sobre la red y para determinar la mejor ruta por la que debe reenviarse el datagrama hacia el destino final. Los datagramas se direccionan sobre la base de direcciones de destino IP.

direccionador designado. Direccionador que informa a los nodos finales de la existencia y la identidad de los otros direccionadores. La selección del direccionador designado se basa en el direccionador con la prioridad superior. Cuando diversos direccionadores comparten la prioridad superior, se selecciona el direccionador con la dirección de estación superior.

direccionador sin germinación. En redes AppleTalk, direccionador que obtiene información del rango de números de red y de la lista de zonas de un direccionador de germinación conectado a la misma red.

direccionador troncal. (1) Direccionador utilizado para transmitir datos entre áreas. (2) Direccionador de una serie que se utiliza para interconectar redes de manera que formen una internet mayor.

direccionamiento. En la comunicación de datos, manera que tiene una estación de seleccionar la estación a la que va a enviar datos.

direccionamiento. (1) Asignación de la vía de acceso mediante la cual un mensaje va a alcanzar su destino. (2) En SNA, reenvío de una unidad de mensaje por una vía de acceso determinada a través de una red tal como lo determinan los parámetros contenidos en la unidad de mensaje, como, por ejemplo, la dirección de red de destino de una cabecera de transmisión.

direccionamiento de alto rendimiento (HPR). Adición para la arquitectura Advanced Peer-to-Peer Networking (APPN) que mejora el rendimiento y la fiabilidad del direccionamiento de datos, especialmente en la utilización de enlaces de gran velocidad.

direccionamiento del MAC arbitrario (AMA). En la arquitectura DECnet, esquema de direccionamiento utilizado por DECnet Phase IV-Prime que da soporte a direcciones administradas universalmente y direcciones administradas localmente.

direccionamiento de origen. En las LAN, método mediante el cual la estación emisora determina la ruta que la trama seguirá e incluye la información de direccionamiento en la trama. A continuación, los puentes leen la información de direccionamiento para determinar si deben reenviar la trama.

direccionamiento de sesiones intermedias (ISR). Tipo de función de direccionamiento de un nodo de red APPN que proporciona información de indisponibilidad y control del flujo de nivel de sesión para todas las sesiones que pasan por el nodo pero cuyos puntos finales están en otra parte.

direccionamiento dinámico. Direccionar utilizando rutas aprendidas en lugar de las rutas configuradas estáticamente durante la inicialización.

direccionamiento intraárea. En comunicaciones de Internet, direccionamiento de datos dentro de un área.

dirección canónica. En las LAN, formato de IEEE 802.1 de la transmisión de direcciones del control del acceso al medio (MAC) para adaptadores de Red en Anillo y Ethernet. En el formato canónico, el bit menos significativo (situado más a la derecha) de cada byte de dirección se transmite en primer lugar. Compárese con *dirección no canónica*.

dirección de difusión. En comunicaciones, dirección de estación (ocho números 1) reservada como dirección común a todas las estaciones de un enlace. Sinónimo con *dirección de todas las estaciones*.

dirección de red. Según ISO 7498-3, nombre que no es ambiguo en el entorno de OSI y que identifica a un conjunto de puntos de acceso a servicios de red.

dirección de subred. En comunicaciones de Internet, extensión del esquema básico de direccionamiento de IP donde una parte de la dirección de sistema principal se interpreta como dirección de red local.

dirección de todas las estaciones. En comunicaciones, sinónimo de *dirección de difusión*.

dirección de usuario de red (NUA). En comunicaciones de X.25, dirección X.121 que contiene hasta 15 dígitos en código binario.

dirección Internet. Véase *dirección IP*.

dirección IP. Dirección de 32 bits definida por Internet Protocol, norma 5, Request for Comments (RFC) 791. Normalmente, se representa mediante formato decimal con puntos.

dirección no canónica. En las LAN, formato de la transmisión de direcciones del control del acceso al medio (MAC) para adaptadores de Red en Anillo. En el formato no canónico, el bit más significativo (situado más a la izquierda) de cada byte de dirección se transmite en primer lugar. Compárese con *dirección canónica*.

directorio. Tabla de identificadores y referencias para los elementos de datos correspondientes. (I) (A)

dispositivo. Aparato mecánico, eléctrico o electrónico con un fin específico.

dominio. (1) Parte de una red de sistema en la que los recursos de proceso de datos están bajo un control común. (T) (2) En interconexión de sistemas abiertos (OSI), parte de un sistema distribuido o conjunto de objetos gestionados a los que se aplica una política común. (3) Véase *Dominio administrativo* y *nombre de dominio*.

Dominio administrativo. Conjunto de sistemas principales y direccionadores, y las redes de interconexión, que gestiona una sola autoridad administrativa.

dominio de direccionamiento. En comunicaciones de Internet, grupo de sistemas intermedios que utilizan un protocolo de direccionamiento para que la representación de la red en un conjunto sea la misma en cada sistema intermedio. Los dominios de direccionamiento se conectan entre sí mediante enlaces exteriores.

E

eco. En la comunicación de datos, señal de un canal de comunicaciones reflejada. Por ejemplo, en un terminal de comunicaciones, cada señal se visualiza dos veces, una cuando entra en el terminal local y otra cuando vuelve sobre el enlace de comunicaciones. Esto permite comprobar la exactitud de las señales.

EIA 232. En la comunicación de datos, especificación de la Electronic Industries Association (EIA) que define la interfaz entre el equipo terminal de datos (DTE) y el equipo de terminación de circuito de datos (DCE), que utiliza el intercambio de datos binarios serie.

Electronic Industries Association (EIA). Organización de fabricantes del campo de la electrónica que anticipa el crecimiento tecnológico de la industria, representa los puntos de vista de sus miembros y desarrolla normas para la industria.

Emulación de LAN (LE). Norma del ATM Forum que da soporte a aplicaciones de legado de LAN sobre redes ATM.

encapsulación. (1) En comunicaciones, técnica utilizada por protocolos de capa mediante la cual una capa añade a la unidad de datos de protocolo (PDU) información de control de la capa a la que da soporte. A este respecto, la capa encapsula los datos de la capa soportada. En el conjunto de protocolos de Internet, por ejemplo, un paquete contendrá información de control de la capa física, a continuación información de control de la capa de red y a continuación los datos de protocolo de la aplicación. (2) Véase también *conmutación del enlace de datos*.

enlace. Combinación de la conexión de enlace (el medio de transmisión) y dos estaciones de enlace, una a cada extremo de la conexión de enlace. Una conexión de enlace puede estar compartida entre diversos enlaces en una configuración de multipunto o Red en Anillo.

enlace lógico. Par de estaciones de enlace, una en cada uno de dos nodos adyacentes, y su conexión de enlace subyacente que proporcionan una sola conexión de capa de enlace entre los dos nodos. Pueden distinguirse diversos enlaces lógicos mientras comparten el uso del mismo medio físico de conexión de dos nodos. Ejemplos son los enlaces lógicos de 802.2 utilizados en recursos de red de área local (LAN) y los enlaces lógicos de LAP E del mismo enlace físico punto a punto entre dos nodos. El término enlace lógico también incluye los diversos canales lógicos de X.25 que comparten el uso del enlace de acceso de un DTE con una red X.25.

enlace virtual. En Open Shortest Path First (OSPF), interfaz punto a punto que conecta direccionadores de frontera separados por un área de tránsito no troncal. Puesto que los direccionadores de área forman parte del troncal OSPF, el enlace virtual conecta el troncal. Los enlaces virtuales aseguran que el troncal OSPF no se vuelva discontinuo.

equipo de terminación de circuito de datos (DCE). En una estación de datos, equipo que proporciona la conversión de señal y la codificación entre el equipo terminal de datos (DTE) y la línea. (I)

Notas:

1. El DCE puede ser un equipo independiente o parte integral del DTE o del equipo intermedio.
2. Un DCE puede realizar otras funciones que normalmente se llevan a cabo al final de red de la línea.

equipo terminal de datos (DTE). Parte de una estación de datos que funciona como origen y/o destino de datos. (I) (A)

esfera de control (SOC). Conjunto de dominios de punto de control servidos por un solo punto focal de servicios de gestión.

estación. Punto de entrada o salida de un sistema que utiliza recursos de telecomunicaciones; por ejemplo, uno o más sistemas, terminales, dispositivos y programas asociados de una ubicación determinada que pueden enviar o recibir datos sobre una línea de telecomunicaciones.

estación de enlace. (1) Componentes de hardware y software de un nodo que representan una conexión con un nodo adyacente sobre un enlace específico. Por ejemplo, si el nodo A es el extremo primario de una línea multipunto que se conecta con tres nodos adyacentes, el nodo A tendrá tres estaciones de enlace que representarán las conexiones con los nodos adyacentes. (2) Véase también *estación de enlace adyacente (ALS)*.

estación de gestión. En comunicaciones de Internet, sistema responsable de la gestión de toda una red o de parte de la misma. La estación de gestión se comunica con agentes de gestión de red que residen en el nodo gestionado por medio de un protocolo de gestión de red, como, por ejemplo, Simple Network Management Protocol (SNMP).

estación de gestión de red. En el protocolo Simple Network Management Protocol (SNMP), estación que ejecuta programas de aplicación de gestión que supervisan y controlan elementos de red.

estado de los enlaces. En los protocolos de direccionamiento, información anunciada sobre las interfaces utilizables y los direccionadores contiguos a un direccionador o una red asequibles. La base de datos topológica del protocolo se forma a partir de los anuncios reunidos sobre el estado de los enlaces.

estructura de la información de gestión (SMI). (1) En el protocolo Simple Network Management Protocol (SNMP), normas utilizadas para definir los objetos a los que puede accederse por medio de un protocolo de gestión de red. (2) En OSI, conjunto de normas relativas a la información de gestión. El conjunto incluye el *Management Information Model* y las *Guidelines for the Definition of Managed Objects.*

Ethernet. Red de área local de banda base de 10 Mbps que permite que diversas estaciones accedan al medio de transmisión a voluntad sin coordinación previa, evita la contención utilizando la detección y deferencia de portadora y resuelve la contención utilizando la detección de colisión y la retransmisión retardada. Ethernet utiliza el acceso múltiple con detección de portadora y detección de colisión (CSMA/CD).

excepción. Condición anormal, como, por ejemplo, un error de E/S encontrado durante el proceso de un conjunto de datos o archivo.

extensión de ruta (REX). En SNA, componentes de red de control de la vía de acceso, incluido un enlace periférico, que componen la parte de una vía de acceso que está entre un nodo de subárea y una unidad de red dirigible (NAU) de un nodo periférico adyacente. Véase también *ruta explícita (ER)*, *vía de acceso* y *ruta virtual (VR)*.

Exterior Gateway Protocol (EGP). En el conjunto de protocolos de Internet, protocolo utilizado entre dominios y sistemas autónomos que permite anunciar e intercambiar información sobre la asequibilidad de la red. Las direcciones de red IP de un sistema autónomo se anuncian en otro sistema autónomo por medio de direccionadores que participan de EGP. Un ejemplo de EGP es Border Gateway Protocol (BGP). Compárese con Interior Gateway Protocol (IGP).

F

fax. Copia impresa que se recibe de una máquina de facsímil. Sinónimo con ***telecopia.***

File Transfer Protocol (FTP). En el conjunto de protocolos de Internet, protocolo de capa de aplicación que utiliza servicios de TCP y Telnet para transferir archivos de datos generales entre máquinas o sistemas principales.

formato decimal con puntos. Representación sintáctica de un entero de 32 bits que consta de cuatro números de 8 bits escritos en base 10 con puntos que los separan. Se utiliza para representar direcciones IP.

fragmentación. (1) Proceso consistente en dividir un datagrama en partes más pequeñas, o fragmentos, para que se ajuste a las posibilidades del medio físico por el que se va a transmitir. (2) Véase también *segmentación*.

fragmento. Véase *fragmentación*.

Frame Relay. (1) Norma de interfaz que describe el límite entre el equipo de un usuario y una red de paquetes rápidos. En los sistemas Frame-Relay, se eliminan las tramas defectuosas; la recuperación se

produce de extremo a extremo en lugar de efectuarse salto a salto. (2) Técnica derivada de la norma de canal D de red digital de servicios integrados (RDSI). Supone que las conexiones son fiables y prescinde de la actividad general de control y detección de errores en la red.

funcionamiento en modalidad de paquete. Sinónimo de *conmutación de paquetes*.

función de puente. En las LAN, el reenvío de una trama de un segmento de LAN a otro. El destino está especificado mediante la dirección de subcapa del control del acceso al medio (MAC) codificada en el campo de dirección de destino de la cabecera de la trama.

función de puente de ruta de origen. En las LAN, método de función de puente que utiliza el campo de información de direccionamiento de la cabecera del control del acceso al medio (MAC) de IEEE 802.5 de una trama para determinar los anillos o segmentos de Red en Anillo que debe recorrer la trama. El nodo de origen inserta el campo de información de direccionamiento en la cabecera del MAC. La información del campo de información de direccionamiento deriva de los paquetes exploradores generados por el sistema principal de origen.

función de puente local. Función de un programa de puente que permite que un solo puente conecte diversos segmentos de LAN sin la utilización de un enlace de telecomunicaciones. Compárese con *función de puente remota*.

función de puente remota. Función de un puente que permite que dos puentes conecten diversas LAN utilizando un enlace de telecomunicaciones. Compárese con *función de puente local*.

función de puente transparente. En las LAN, método para relacionar redes de área local individuales entre sí en el nivel del control del acceso al medio (MAC). Un puente transparente almacena las tablas que contienen direcciones del MAC para que las tramas que ve el puente puedan reenviarse a otra LAN si las tablas lo indican así.

función de túnel. Trata a una red de transporte como si fuera una sola LAN o un solo enlace de comunicaciones. Véase también *encapsulación*.

G

gestión de red. Proceso consistente en planificar, organizar y controlar un proceso de datos o sistema de información orientado a las comunicaciones.

gestor de red. Programa o grupo de programas que se utiliza para supervisar y gestionar una red así como para diagnosticar los problemas de la misma.

grupo de transmisión (TG). (1) Conexión entre nodos adyacentes que se identifica mediante un número de grupo de transmisión. (2) En una red de subárea, enlace o grupo de enlaces entre nodos adyacentes. Cuando un grupo de transmisión está compuesto por un grupo de enlaces, los enlaces se ven como un solo enlace lógico y el grupo de transmisión se denomina *grupo de transmisión multienlace (MLTG)*. Un *grupo de transmisión multienlace de mezcla de medios (MMMLTG)* contiene enlaces de diferentes tipos de medios (por ejemplo, Red en Anillo, SDLC conmutado, SDLC no conmutado y enlaces Frame-Relay). (3) En una red APPN, enlace entre nodos adyacentes. (4) Véase también *grupos de transmisión paralelo*.

grupos de transmisión paralelo. Diversos grupos de transmisión entre nodos adyacentes, teniendo cada grupo un número de grupo de transmisión distinto.

H

Hello. Protocolo utilizado por un grupo de direccionadores que cooperan y se apoyan entre sí para poder descubrir rutas de retardo mínimo.

heurístico. Perteneciente a métodos exploratorios para la resolución de problemas en los que se descubren soluciones mediante una evaluación del progreso realizada respecto al resultado final.

histéresis. Cantidad que indica cuánto debe cambiar la temperatura una vez pasado el umbral del establecimiento de alerta y antes de que se elimine la condición de alerta.

horizonte dividido. Técnica destinada a minimizar el tiempo para conseguir la convergencia en la red. Un direccionador registra la interfaz sobre la que ha recibido una ruta en particular y no propaga su información sobre la ruta otra vez sobre la misma interfaz.

I

identificación de intercambio (XID). Tipo específico de unidad básica de enlace que se utiliza para la comunicación de características de nodo y enlace entre nodos adyacentes. Los XID se intercambian entre estaciones de enlace antes de la activación del enlace

y durante la misma para establecer y negociar las características de enlace y nodo, y después de la activación del enlace para comunicar los cambios de estas características.

identificador de conexión de enlace de datos (DLCI). Identificador numérico de un subpuerto Frame-Relay o segmento de PVC en una red Frame-Relay. Cada subpuerto de un puerto Frame-Relay individual tiene un DLCI exclusivo. La tabla siguiente, extraída de la norma T1.618 del American National Standards Institute (ANSI) y la norma Q.922 de la Comisión Consultiva de la telefonía y telegrafía internacionales (ITU-T/CCITT), indica las funciones asociadas con determinados valores de DLCI:

Valores de DLCI	Función
0	Señalización de canal de entrada
1–15	Se reserva
16–991	Se asigna utilizando procedimientos de conexión de Frame-Relay
992–1007	Gestión de capa 2 de servicio portador de Frame-Relay
1008–1022	Se reserva
1023	Gestión de capa de canal de entrada

identificador de puente. Campo de 8 bytes que se utiliza en un protocolo de árbol de expansión y está compuesto por la dirección MAC del puerto con el identificador de puerto más bajo y un valor definido por el usuario.

identificador de red. (1) En TCP/IP, parte de la dirección IP que define a una red. La longitud del identificador de red depende del tipo de la clase de red (A, B o C). (2) Nombre de 1 a 8 bytes seleccionado por el cliente o nombre de 8 bytes registrado por IBM que identifica de forma exclusiva una subred específica.

inhabilitado. (1) Perteneciente a un estado de una unidad de proceso que evita la aparición de determinados tipos de interrupciones. (2) Perteneciente al estado en el cual una unidad de control de transmisión o unidad de respuestas audibles no puede aceptar llamadas de entrada de una línea.

inhabilitar. Convertir en no funcional.

Integrated Digital Network Exchange (IDNX). Procesador que integra aplicaciones a base de voz, datos e imágenes. También gestiona los recursos de transmisión y se conecta a multiplexores y sistemas de soporte de gestión de redes. Permite la integración de equipos de diferentes proveedores.

intercambio de conmutaciones de datos (DSE). Equipo instalado en una ubicación individual para proporcionar funciones de conmutación, como, por ejemplo, conmutación del circuito, conmutación de mensajes y conmutación de paquetes. (I)

interconexión de sistemas abiertos (OSI). (1) Interconexión de sistemas abiertos que sigue las normas de la organización internacional para la normalización (ISO) para el intercambio de información. (T) (A) (2) Utilización de procedimientos normalizados para permitir la interconexión de sistemas de proceso de datos.

Nota: La arquitectura OSI establece una infraestructura para coordinar el desarrollo de normas actuales y futuras de cara a la interconexión de sistemas. Las funciones de red se dividen en siete capas. Cada capa representa un grupo de funciones relacionadas de proceso de datos y comunicación que pueden llevarse a cabo de una manera estándar para dar soporte a diferentes aplicaciones.

interfaz. (1) Límite compartido entre dos unidades funcionales en cuya definición entran características funcionales, características de señalización u otras características según lo que corresponda. El concepto incluye la especificación de la conexión de dos dispositivos que tienen funciones diferentes. (T) (2) Hardware y/o software para el enlace de sistemas, programas o dispositivos.

interfaz de gestión local (LMI). Véase *protocolo de interfaz de gestión local (LMI)*.

interfaz de unidad de conexión (AUI). En una red de área local, interfaz entre la unidad de conexión al medio y el equipo terminal de datos de una estación de datos. (I) (A)

Interior Gateway Protocol (IGP). En el conjunto de protocolos de Internet, protocolo utilizado para propagar información sobre la asequibilidad y direccionamiento de la red dentro de un sistema autónomo. Ejemplos de IGP son Routing Information Protocol (RIP) y Open Shortest Path First (OSPF).

Internet. Red internet administrada por la Internet Architecture Board (IAB) y compuesta por grandes redes troncales nacionales así como por muchas redes regionales y de campus en todo el mundo. Internet utiliza el conjunto de protocolos de Internet.

internet. Conjunto de redes interconectadas por una serie de direccionadores que les permiten funcionar como una sola red grande. Véase también *Internet*.

Internet Architecture Board (IAB). Corporación técnica que supervisa el desarrollo del conjunto de protocolos de Internet conocidos como TCP/IP.

Internet Control Message Protocol (ICMP). Protocolo utilizado para manejar mensajes de control y

errores en la capa de Internet Protocol (IP). Los informes sobre problemas y destinos incorrectos de datagramas se devuelven al origen del datagrama. ICMP forma parte de Internet Protocol.

Internet Control Protocol (ICP). Protocolo de VIrtual NEtworking System (VINES) que proporciona notificaciones de excepciones, notificaciones sobre métrica y el soporte del programa PING. Véase también *RouTing update Protocol (RTP)*.

Internet Engineering Task Force (IETF). Grupo de operaciones de la Internet Architecture Board (IAB) que es responsable de la resolución de las necesidades técnicas de la Internet a corto plazo.

Internet Protocol (IP). Protocolo sin conexiones que direcciona datos a través de una red o redes interconectadas. IP actúa como intermediario entre las capas de protocolos superiores y la red física. No obstante, este protocolo no proporciona recuperación de errores ni control del flujo ni garantiza la fiabilidad de la red física.

Internetwork Packet Exchange (IPX). (1) Protocolo de red utilizado para conectar servidores Novell, o cualquier estación de trabajo o direccionador que implemente IPX, con otras estaciones de trabajo. Aunque es similar a Internet Protocol (IP), IPX utiliza unos formatos de paquete y una terminología diferentes. (2) Véase también *Xerox Network Systems (XNS)*.

interoperatividad. Posibilidad de comunicarse, ejecutar programas o transferir datos entre diversas unidades funcionales de tal forma que el usuario necesite tener poco conocimiento, o ninguno, de las características exclusivas de estas unidades. (T)

interposición. (1) Alternancia de dos o más operaciones o funciones mediante el uso solapado de un recurso de sistema. (2) En transmisión de datos, alternancia de paquetes de una corriente de datos con paquetes a otra.

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 a un usuario gestionar y supervisar recursos de LAN desde una estación de trabajo central.

LE. Emulación de LAN. Norma del ATM Forum que da soporte a aplicaciones de legado de LAN sobre redes ATM.

LEC. Cliente de emulación de LAN. Componente de la emulación de LAN que representa a los usuarios de la LAN emulada.

LECS. Servidor de configuración de emulación de LAN. Componente de LAN Emulation Service que centraliza y difunde datos de configuración.

LES. Servidor de emulación de LAN. Componente de LAN Emulation Service que resuelve destinos de LAN en direcciones ATM.

local. (1) Perteneciente a un dispositivo al que se accede directamente sin utilizar una línea de telecomunicaciones. (2) Compárese con *remoto*. (3) Sinónimo de *conectado mediante canal*.

M

mandato ping. Mandato que envía un paquete de petición con eco de Internet Control Message Protocol (ICMP) a una pasarela, direccionador o sistema principal esperando recibir una respuesta.

máscara. (1) Patrón de caracteres utilizado para controlar la retención o eliminación de partes de otro patrón de caracteres. (I) (A) (2) Utilizar un patrón de caracteres para controlar la retención o eliminación de partes de otro patrón de caracteres. (I) (A)

máscara de dirección. Respecto a las subredes de internet, máscara de 32 bits utilizada para identificar los bits de dirección de subred de la parte del sistema principal de una dirección IP. Sinónimo con *máscara de subred* y *máscara de subred (grupo de nodos)*.

máscara de subred. Sinónimo de *máscara de dirección*.

máscara de subred (grupo de nodos). Sinónimo de *máscara de dirección*.

memoria de almacenamiento dinámico. Cantidad de RAM utilizada para asignar estructuras de datos dinámicamente.

memoria de sólo lectura (ROM). Memoria en la que el usuario no puede modificar los datos almacenados salvo en condiciones especiales.

memoria instantánea. Dispositivo de almacenamiento de datos que puede programarse y borrarse y que no necesita alimentación continua. La ventaja principal de la memoria instantánea sobre otros dispositivos de almacenamiento de datos que pueden programarse y borrarse es que puede volver a programarse sin quitarla de la placa de circuitos.

mensaje hello. (1) Mensaje enviado periódicamente para establecer y probar la asequibilidad entre direccionadores o entre direccionadores y sistemas principales. (2) En el conjunto de protocolos de Internet, mensaje definido por el protocolo Hello como Interior Gateway Protocol (IGP).

métrica. En comunicaciones de Internet, valor asociado con una ruta que se utiliza para establecer diferencias entre los múltiples puntos de entrada o salida respecto al mismo sistema autónomo. Se prefiere la ruta con la métrica inferior.

MIB. (1) Módulo de la MIB. (2) Base de la información de gestión.

MIB estándar. En el protocolo Simple Network Management Protocol (SNMP), módulo de la MIB que se ubica bajo la rama de gestión de la estructura de la información de gestión (SMI) y que se considera una norma en Internet Engineering Task Force (IETF).

MILNET. Red militar que formaba parte de ARPANET en un principio. Quedó separada de ARPANET en 1984. MILNET proporciona un servicio de red fiable para las instalaciones militares.

modelo de referencia interconexión de sistemas abiertos (OSI). Modelo que describe los principios generales de interconexión de sistemas abiertos así como la finalidad y la ordenación jerárquica de sus siete capas. (T)

módem (modulador/demodulador). (1) Unidad funcional que modula y demodula señales. Una de las funciones de un módem es permitir que los datos digitales se transmitan sobre recursos de transmisión analógicos. (T) (A) (2) Dispositivo que convierte los datos digitales de un sistema en una señal analógica que pueda transmitirse en una línea de telecomunicaciones, y convierte la señal analógica recibida en datos para el sistema.

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 (diferencia). Número, como por ejemplo un entero positivo, de una relación que divide la diferencia entre dos números relacionados sin dejar un resto; por ejemplo, 9 y 4 tienen un módulo de 5 (9 - 4 = 5; 4 - 9 = -5; y 5 divide tanto 5 como -5 sin dejar un resto).

N

Name Binding Protocol (NBP). En redes AppleTalk, protocolo que proporciona la función de conversión de nombre a partir del nombre (serie de caracteres) de una entidad (recurso) AppleTalk en una dirección IP AppleTalk (número de 16 bits) en la capa de transporte.

NetBIOS. Network Basic Input/Output System. Interfaz estándar para redes, IBM personal computers (PC) y PC compatibles, que se utiliza en las LAN para proporcionar funciones de mensajes, de servidor de impresión y de servidor de archivos. Los programas de aplicación que utilizan NetBIOS no necesitan manejar los detalles de protocolos de control de enlace de datos (DLC) de la LAN.

nivel de enlace. (1) Parte de la recomendación X.25 que define el protocolo de enlace utilizado para entrar datos en la red y sacarlos de la misma a través del enlace dúplex que conecta la máquina del abonado con el nodo de red. LAP y LAPB son los protocolos de acceso de enlace recomendados por la CCITT. (2) Véase *nivel de enlace de datos*.

nivel de enlace de datos. (1) En la estructura jerárquica de una estación de datos, nivel conceptual de control o lógica de proceso entre la lógica de alto nivel y el enlace de datos que mantiene el control del enlace de datos. El nivel de enlace de datos realiza funciones tales como la inserción de bits de transmisión y supresión de bits de recepción; interpretación de campos de dirección y control; generación, transmisión e interpretación de mandatos y respuestas; y cálculo e interpretación de secuencias de comprobación de trama. Véase también *nivel de paquete* y *nivel físico*. (2) En comunicaciones de X.25, sinónimo de *nivel de trama*.

nivel de trama. Sinónimo con *nivel de enlace de datos*. Véase *nivel de enlace*.

nodo. (1) En una red, punto donde una o más unidades funcionales conectan canales o circuitos de datos. (I) (2) Cualquier dispositivo conectado a una red que transmite y recibe datos.

nodo Advanced Peer-to-Peer Networking (APPN). Nodo de red APPN o nodo final APPN.

nodo de destino. Nodo al que se envían datos o una petición.

nodo de esfera de control (SOC). Nodo que está incluido directamente en la esfera de control de un punto focal. Un nodo de SOC ha intercambiado elementos de habilitación de los servicios de gestión con su punto focal. Un nodo final APPN puede ser un nodo de SOC si da soporte a la función de intercambio de elementos de habilitación de los servicios de gestión.

nodo de red Advanced Peer-to-Peer Networking (APPN). Nodo que ofrece un amplio rango de servicios de usuario final y que puede proporcionar lo siguiente:

- servicios de directorios distribuidos, incluido el registro de los recursos del dominio con un servidor de directorios central
- Intercambios de bases de datos de topología con otros nodos de red APPN, lo que permite que los nodos de red de la red seleccionen las rutas óptimas para sesiones de LU-LU basándose en las clases de servicio solicitadas
- Servicios de sesiones para los nodos finales clientes y las LU locales
- Servicios de direccionamiento intermedio de una red APPN

nodo de red APPN. Véase *nodo de red Advanced Peer-to-Peer Networking (APPN)*.

nodo de red de entrada baja (LEN). Nodo que proporciona un rango de servicios de usuario final, se conecta directamente con otros nodos utilizando protocolos de igual a igual y hace derivar servicios de red de un nodo de red APPN adyacente implícitamente, es decir, sin el uso directo de sesiones de CP-CP.

nodo de red (NN). Véase *nodo de red Advanced Peer-to-Peer Networking (APPN)*.

nodo final Advanced Peer-to-Peer Networking (APPN). Nodo que proporciona un amplio rango de servicios de usuario final y da soporte a las sesiones entre su punto de control (CP) local y el CP de un nodo de red adyacente. Utiliza estas sesiones con el fin de registrar dinámicamente sus recursos con el CP adyacente (su servidor de nodos de red) para enviar y recibir peticiones de búsqueda en directorios y obtener servicios de gestión. Un nodo final APPN también puede conectarse a una red de subárea como nodo periférico o a otros nodos finales.

nodo final de red de entrada baja (LEN). Nodo LEN que recibe servicios de red de un nodo de red APPN adyacente.

nodo final (EN). (1) Véase *nodo final Advanced Peer-to-Peer Networking (APPN)* y *nodo final de red de entrada baja (LEN)*. (2) En comunicaciones, nodo que se conecta frecuentemente a un solo enlace de datos y no puede realizar funciones de direccionamiento intermedio.

nodo intermedio. Nodo que está al final de más de una rama. (T)

nodos adyacentes. Dos nodos conectados conjuntamente por una vía de acceso, como mínimo, que no conecta ningún otro nodo. (T)

nombre de comunidad. En el protocolo Simple Network Management Protocol (SNMP), serie de octetos que identifica a una comunidad.

nombre de dominio. En el conjunto de protocolos de Internet, nombre de un sistema principal. Un nombre de dominio está compuesto por una secuencia de subnombres separados por un carácter delimitador. Por ejemplo, si el nombre de dominio calificado al completo (FQDN) de un sistema principal es `ralvm7.vnet.ibm.com`, cada uno de los siguientes es un nombre de dominio:

- `ralvm7.vnet.ibm.com`
- `vnet.ibm.com`
- `ibm.com`

notación de sintaxis de abstracción 1 (ASN.1). Método de Interconexión de Sistemas Abiertos (OSI) para la sintaxis de abstracción que se especifica en las normas siguientes:

- ITU-T recomendación X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T recomendación X.680 (1994) | ISO/IEC 8824-1: 1994

Véase también *normas básicas de codificación (BER)*.

número de puerto. En comunicaciones de Internet, identificación de una entidad de aplicación para el servicio de transporte.

número de secuencia. En comunicaciones, número asignado a una trama o paquete en particular para controlar el flujo de la transmisión y la recepción de datos.

número de sistema autónomo. En TCP/IP, número asignado a un sistema autónomo por la misma autorización central que también asigna direcciones IP. El número de sistema autónomo hace posible que los algoritmos de direccionamiento automatizado distingan los sistemas autónomos.

O

objeto de la MIB. Sinónimo de *variable de la MIB*.

Open Shortest Path First (OSPF). En el conjunto de protocolos de Internet, función que proporciona transferencia de información intradominio. Como alternativa al protocolo Routing Information Protocol (RIP), OSPF permite el direccionamiento de menor coste y lo maneja en grandes redes regionales o corporativas.

organización internacional para la normalización (ISO). Organización de corporaciones nacionales de normas de varios países establecida para promocionar el desarrollo de normas con el fin de facilitar el intercambio internacional de artículos y servicios además de desarrollar la cooperación en la actividad intelectual, científica, tecnológica y económica.

origen. Unidad lógica (LU) externa o programa de aplicación de donde parten un mensaje u otros datos. Véase también *destino*.

P

paquete. En la comunicación de datos, secuencia de dígitos binarios, con inclusión de señales de control y datos, que se transmite y se conmuta como un todo compuesto. Los datos, las señales de control y, posiblemente, la información de control de errores se ordenan siguiendo un formato específico. (I)

paquete de datos. En comunicaciones de X.25, paquete utilizado para la transmisión de datos de usuario dentro de un circuito virtual en la interfaz DTE/DCE.

paquete de petición de llamada. (1) Paquete de supervisión de llamada que un equipo terminal de datos (DTE) transmite con el fin de solicitar que se establezca una conexión para una llamada en la red. (2) En comunicaciones de X.25, paquete de supervisión de llamada transmitido por un DTE para solicitar el establecimiento de una llamada en la red.

paquete de petición de restablecimiento. En comunicaciones X.25, paquete transmitido por el equipo terminal de datos (DTE) al equipo de terminación de circuito de datos (DCE) para solicitar que se restablezca una llamada virtual o un circuito virtual permanente. En el paquete también puede especificarse la razón de la petición.

paquete de recepción no preparada (RNR). Véase *paquete de RNR*.

paquete de RNR. Paquete utilizado por un equipo terminal de datos (DTE) o por un equipo de terminación de circuito de datos (DCE) con el fin de indicar una incapacidad temporal para aceptar paquetes adicionales de petición de llamada virtual o circuito virtual permanente.

paquete explorador. En las LAN, paquete que está generado por el sistema principal de origen y que atraviesa toda la parte de direccionamiento de origen de una LAN con el fin de recoger información sobre las posibles vías de acceso que se encuentran disponibles para el sistema principal.

parámetro de configuración. Variable de una definición de configuración cuyos valores pueden caracterizar la relación de un producto con otros productos de la misma red o pueden definir características del producto en sí.

par de valores de atributo (AVP). Método uniforme de codificación de tipos y cuerpos de mensajes. Este método maximiza la extensibilidad mientras permite la interoperatividad de L2TP.

pasarela. (1) Unidad funcional que interconecta dos redes de sistema con arquitecturas de red diferentes. Una pasarela conecta redes o sistemas de arquitecturas diferentes. Un puente interconecta redes o sistemas con la misma arquitectura o con arquitecturas similares. (T) (2) En la Red en Anillo de IBM, dispositivo y software asociado que conectan una red de área local a otra red de área local o sistema principal que utiliza protocolos de enlace lógico diferentes. (3) En TCP/IP, sinónimo de *direccionador*.

pasarela exterior. En comunicaciones de Internet, pasarela de un sistema autónomo que comunica con otro sistema autónomo. Compárese con *pasarela interior*.

pasarela interior. En comunicaciones de Internet, pasarela que sólo comunica con su propio sistema autónomo. Compárese con *pasarela exterior*.

período de duración (TTL). Técnica utilizada por los protocolos de entrega de mayor eficacia para impedir que los paquetes se repitan en bucle de manera interminable. El paquete se elimina si el contador de TTL alcanza el valor de 0.

peticionario de LU dependientes (DLUR). Nodo final APPN o nodo de red APPN que posee LU dependientes pero solicita que un servidor de LU dependientes proporcione los servicios del SSCP para estas LU dependientes.

Point-to-Point Protocol (PPP). Protocolo que proporciona un método para encapsular y transmitir paquetes sobre enlaces serie punto a punto.

portadora. Tren de pulsaciones u ondas eléctricas o electromagnéticas que puede variar según una señal

con información a transmitir sobre un sistema de comunicaciones. (T)

procesador de componente frontal. Procesador, como, por ejemplo, el IBM 3745 ó el 3174, que releva a un sistema principal de las tareas de control de comunicaciones.

proceso a tiempo real. Manipulación de los datos que un proceso necesita o genera mientras el proceso está en funcionamiento. Normalmente, los resultados se utilizan para influir en el proceso y quizá en procesos relacionados, mientras se está desarrollando.

proporción de pérdida de un paquete. Probabilidad que tiene un paquete de no alcanzar su destino o de no alcanzarlo dentro del período especificado.

protocolo. (1) Conjunto de normas semánticas y sintácticas que determinan el comportamiento de las unidades funcionales a la hora de conseguir la comunicación. (I) (2) En la arquitectura interconexión de sistemas abiertos, conjunto de normas semánticas y sintácticas que determinan el comportamiento de las entidades de la misma capa a la hora de desempeñar funciones de comunicación. (T) (3) En SNA, significados y normas de puesta en secuencia de las peticiones y respuestas que se utilizan para gestionar la red, transferir datos y sincronizar los estados de los componentes de la red. Sinónimo con *disciplina de control de línea* y *disciplina de línea*. Véase *protocolo delimitador* y *protocolo de enlace*.

protocolo de acceso de enlace equilibrado (LAPB). Protocolo utilizado para acceder a una red X.25 en el nivel de enlace. LAPB es un protocolo simétrico, asíncrono y dúplex que se utiliza en la comunicación punto a punto.

protocolo de control de enlace lógico (LLC). En una red de área local, protocolo que dirige el intercambio de tramas de transmisión entre estaciones de datos independientemente de cómo está compartido el medio de transmisión. (T) El protocolo de LLC se desarrolló en la comisión de IEEE 802 y es común a todas las normas de LAN.

protocolo de control del acceso al medio (MAC). En una red de área local, protocolo que dirige el acceso al medio de transmisión, teniendo en cuenta los aspectos topológicos de la red, con el fin de permitir el intercambio de datos entre estaciones de datos. (T)

protocolo de direccionamiento. Técnica utilizada por un direccionador para encontrar otros direccionadores y mantener información actualizada sobre la mejor manera de acceder a las redes asequibles.

protocolo de interfaz de gestión local (LMI). En un NCP, conjunto de procedimientos y mensajes de gestión de red Frame-Relay utilizados por nodos Frame-Relay adyacentes para intercambiar información de estado de línea sobre el DLCI X'00'. Un NCP da soporte tanto a la versión del protocolo de LMI del American National Standards Institute (ANSI) como a la de la Comisión Consultiva de la Telefonía y Telegrafía Internacionales (ITU-T/CCITT). Estas normas se refieren al protocolo de LMI como *pruebas de verificación de integridad de enlace (LIVT)*.

prueba de bucle de retorno. Prueba donde las señales de un comprobador se repiten en bucle en un módem u otro elemento de red hacia el comprobador para tomar medidas que determinen o verifiquen la calidad de la vía de acceso de comunicaciones.

puente. Unidad funcional que interconecta diversas LAN (local o remotamente) que utilizan el mismo protocolo de control de enlace lógico pero que pueden utilizar diferentes protocolos de control del acceso al medio. Un puente reenvía una trama a otro puente basándose en la dirección del control del acceso al medio (MAC).

puente de ruta. Función de un programa de puente de IBM que permite a dos sistemas de puente utilizar un enlace de telecomunicaciones para conectar dos LAN. Cada sistema de puente se conecta directamente a una de las LAN y el enlace de telecomunicaciones conecta los dos sistemas de puente.

puente raíz. Puente que es la raíz de un árbol de expansión formado entre otros puentes activos de la red de funciones de puente. El puente raíz origina y transmite unidades de datos de protocolo de puente (BPDU) a otros puentes activos para mantener la topología de árbol de expansión. Es el puente con la prioridad superior de la red.

puentes paralelo. Par de puentes conectados al mismo segmento de LAN que crean vías de acceso redundantes para el segmento.

puerto. (1) Punto de acceso para la entrada o salida de datos. (2) Conector de un dispositivo al que se conectan cables para otros dispositivos, como, por ejemplo, estaciones de pantalla o impresoras. (3) Representación de una conexión física con el hardware de enlace. A veces, un puerto viene referido como adaptador; no obstante, en un adaptador puede haber más de un puerto. Un solo proceso de DLC puede controlar uno o más puertos. (4) En el conjunto de protocolos de Internet, número de 16 bits utilizado para la comunicación entre TCP o el protocolo User Datagram Protocol (UDP) y una aplicación o protocolo de nivel superior. Algunos protocolos, como, por ejemplo, File Transfer Protocol (FTP) y Simple Mail Transfer Protocol (SMTP), utilizan el mismo número de puerto conocido en todas las implementaciones de TCP/IP. (5) Abstracción utilizada por protocolos de transporte para establecer diferencias entre los diversos

destinos en una máquina de sistema principal. (6) Sinónimo con *socket*.

puerto de destino. Adaptador asíncrono de 8 puertos que sirve de punto de conexión con un servicio serie.

punto de acceso a servicios de destino (DSAP). En SNA y TCP/IP, dirección lógica que permite que un sistema direccione datos desde un dispositivo remoto al soporte de comunicaciones correspondiente. Compárese con *punto de acceso a servicios de origen (SSAP)*.

punto de acceso a servicios de origen (SSAP). En SNA y TCP/IP, dirección lógica que permite que un sistema envíe datos a un dispositivo remoto desde el soporte de comunicaciones correspondiente. Compárese con *punto de acceso a servicios de destino (DSAP)*.

punto de acceso a servicios (SAP). (1) En la arquitectura interconexión de sistemas abiertos (OSI), punto en el que una entidad de una capa proporciona los servicios de esta capa a una entidad de la capa superior más próxima. (T) (2) Punto lógico que queda disponible mediante un adaptador y donde puede recibirse y transmitirse información. Muchos enlaces pueden terminar en un solo punto de acceso a servicios.

punto de control (CP). (1) Componente de un nodo APPN o LEN que gestiona los recursos de dicho nodo. En un nodo APPN, el CP puede dedicarse a establecer sesiones de CP-CP con otros nodos APPN. En un nodo de red APPN, el CP también proporciona servicios a nodos finales adyacentes de la red APPN. (2) Componente de un nodo que gestiona los recursos de dicho nodo y, opcionalmente, proporciona servicios a otros nodos de la red. Pueden citarse como ejemplos el punto de control de servicios del sistema (SSCP) de un nodo de subárea de tipo 5, el punto de control de nodo de red (NNCP) de un nodo de red APPN y el punto de control de nodo final (ENCP) de un nodo final APPN o LEN. Un SSCP y un NNCP pueden proporcionar servicios a otros nodos.

punto de control de servicios del sistema (SSCP). Componente de una red de subárea destinado a gestionar la configuración, coordinar las peticiones del operador de red y las de determinación de problemas y proporcionar servicios de directorios además de otros servicios de sesiones para los usuarios de la red. Diversos SSCP, cooperando como iguales entre sí, pueden dividir la red en dominios de control y tener, cada uno de los SSCP, una relación de control jerárquica con las unidades físicas y las unidades lógicas de su propio dominio.

punto de entrada (EP). En SNA, nodo de tipo 2.0, tipo 2.1, tipo 4 ó tipo 5 que proporciona soporte de gestión de redes distribuidas. Envía datos de gestión de redes sobre sí mismo y los recursos que controla a un punto focal para el proceso centralizado, y recibe y ejecuta los mandatos iniciados por el punto focal para gestionar y controlar sus recursos.

R

rastreo. (1) Registro de la ejecución de un programa de sistema. Muestra las secuencias en que se han ejecutado las instrucciones. (A) (2) Para los enlaces de datos, registro de las tramas y bytes transmitidos o recibidos.

recepción no preparada (RNR). En comunicaciones, mandato o respuesta de enlace de datos que indica una condición temporal de incapacidad para aceptar tramas de entrada.

reconfiguración dinámica (DR). Proceso consistente en cambiar la configuración de una red (las PU y LU periféricas) sin regenerar las tablas de configuración al completo ni desactivar el nodo principal afectado.

red. (1) Configuración de software y dispositivos de proceso de datos conectados para el intercambio de información. (2) Grupo de nodos y los enlaces que los interconectan.

red Advanced Peer-to-Peer Networking (APPN). Conjunto de nodos de red interconectados y sus nodos finales clientes.

red APPN. Véase *red Advanced Peer-to-Peer Networking (APPN)*.

red de área amplia (WAN). (1) Red que proporciona servicios de comunicación a un área geográfica mayor que la servida por una red de área local o una red de área metropolitana, y que puede utilizar o proporcionar recursos públicos de comunicación. (T) (2) Red de comunicación de datos diseñada para servir a un área de cientos o miles de kilómetros; por ejemplo, las redes públicas y privadas de conmutación de paquetes y las redes telefónicas nacionales. (3) Compárese con *red de área local (LAN)* y *red de área metropolitana (MAN)*.

red de área local (LAN). (1) Red de sistema ubicada en el lugar de un usuario dentro de un área geográfica limitada. La comunicación dentro de una red de área local no está sujeta a reglamentos externos; no obstante, la comunicación más allá del límite de una LAN puede estar sujeta a alguna forma de reglamento. (T) (2) Red en la que un conjunto de dispositivos están conectados entre sí para la comunicación y que puede conectarse a una red mayor. (3) Véase también *Ethernet* y *Red en Anillo*. (4) Compárese con *red de área metropolitana (MAN)* y *red de área amplia (WAN)*.

red de área metropolitana (MAN). Red formada por la interconexión de dos o más redes que puede fun-

cionar a una velocidad mayor que éstas, puede atravesar límites administrativos y puede utilizar diversos métodos de acceso. (T) Compárese con *red de área local (LAN)* y *red de área amplia (WAN)*.

red de clase A. En comunicaciones de Internet, red en la que el bit situado más a la izquierda (más significativo) de la dirección IP está establecido en 0 y el identificador de sistema principal ocupa los tres octetos situados más a la derecha.

red de clase B. En comunicaciones de Internet, red en la que los dos bits situados más a la izquierda (más significativo y próximo al más significativo) de la dirección IP están establecidos en 1 y 0, respectivamente, y el identificador de sistema principal ocupa los dos octetos situados más a la derecha.

red de entrada baja (LEN). Posibilidad de los nodos de conectarse directamente entre sí utilizando protocolos básicos de igual a igual para dar soporte a sesiones múltiples y en paralelo entre unidades lógicas.

red de tipo anillo. (1) Red en la que cada nodo tiene exactamente dos ramas conectadas y en la que hay exactamente dos vías de acceso entre dos nodos cualesquiera. (T) (2) Configuración de red en la que los dispositivos están conectados mediante enlaces de transmisión unidireccional para formar una vía de acceso cerrada.

red digital de servicios integrados (RDSI). Red digital de telecomunicaciones de extremo a extremo que da soporte a diversos servicios, los cuales incluyen voz y datos pero no se limitan a ello.

Nota: Las RDSI se utilizan en arquitecturas de red públicas y privadas.

Red en Anillo. (1) Según la norma IEEE 802.5, tecnología de red que controla el acceso al medio pasando una señal (paquete o trama especial) entre las estaciones conectadas al medio. (2) IEEE 802.5 con una topología de anillo que pasa señales de una estación de anillo de conexión (nodo) a otra. (3) Véase también *red de área local (LAN)*.

red según Red en Anillo. (1) Red de tipo anillo que permite la transmisión de datos unidireccional entre estaciones de datos, mediante un procedimiento consistente en pasar señales, de tal manera que los datos transmitidos vuelven a la estación transmisora. (T) (2) Red que utiliza una topología de anillo, según la cual pasan señales en un circuito de nodo a nodo. Un nodo que está preparado para emitir puede capturar la señal e insertar datos para la transmisión.

red troncal. Red central a la que se conectan redes más pequeñas, casi siempre de menor velocidad. Normalmente, la red troncal tiene una capacidad muy superior a las redes a las que ayuda a interconectarse o es una red de área amplia (WAN), como, por ejemplo, una red pública de datagramas de paquetes conmutados.

reensamblaje. En comunicaciones, proceso consistente en volver a juntar paquetes segmentados después de haberlos recibido.

Registro sin vuelta a cero y con cambios en los unos (NRZ-1). Método de registro donde los unos están representados mediante un cambio en la condición de magnetización y los ceros están representados mediante la ausencia de cambio. Sólo se registran explícitamente las señales de los unos. (Denominado anteriormente registro ***sin vuelta a cero invertido***, NRZI.)

Remote Execution Protocol (REXEC). Protocolo que permite la ejecución de un mandato o programa en cualquier sistema principal de la red. El sistema principal local recibe los resultados de la ejecución del mandato.

remoto. (1) Perteneciente a un sistema, programa o dispositivo al que se accede mediante una línea de telecomunicaciones. (2) Sinónimo de *conectado mediante enlace*. (3) Compárese con *local*.

Request for Comments (RFC). En comunicaciones de Internet, serie de documentos que describe una parte del conjunto de protocolos de Internet y experimentos relacionados. Todas las normas de Internet están documentadas como RFC.

resolución de direcciones. (1) Método para correlacionar direcciones de capa de red con direcciones específicas de los medios. (2) Véase también *Address Resolution Protocol (ARP)* y *AppleTalk Address Resolution Protocol (AARP)*.

resolución de nombres. En comunicaciones de Internet, proceso consistente en correlacionar un nombre de máquina con la dirección Internet Protocol (IP) correspondiente. Véase también *Sistema de nombres de dominio (DNS)*.

respuesta a excepción (ER). En SNA, protocolo solicitado en el campo de formato de respuesta solicitado de la cabecera de una petición que indica al receptor que devuelva una respuesta sólo si la petición no es aceptable tal como se recibe o si no puede procesarse; es decir, puede devolverse una respuesta negativa, pero no una respuesta positiva. Compárese con *respuesta definida* y *sin respuesta*.

restablecimiento. En un circuito virtual, reinicialización del control del flujo de datos. En el restablecimiento, se eliminan todos los datos en tránsito.

ritmo. (1) Técnica mediante la cual un componente de recepción controla la velocidad de transmisión de un componente de emisión para evitar un desbordamiento o una congestión. (2) Véase también *control del flujo*, *ritmo de recepción*, *ritmo de emisión*, *ritmo de nivel de sesión* y *ritmo de ruta virtual (VR)*.

rlogin (inicio de sesión remoto). Servicio ofrecido por los sistemas de Berkeley basados en UNIX que permite que los usuarios autorizados de una máquina se conecten con otros sistemas UNIX en una internet e interactúen como si sus terminales estuvieran conectados directamente. El software rlogin pasa información sobre el entorno del usuario (por ejemplo, el tipo de terminal) a la máquina remota.

Routing Information Protocol (RIP). En el conjunto de protocolos de Internet, protocolo de pasarela interior utilizado para intercambiar información de direccionamiento intradominio y para determinar las rutas óptimas entre los sistemas principales de internet. RIP determina las rutas óptimas sobre la base de la métrica de ruta y no sobre la base de la velocidad de transmisión de un enlace.

Routing Table Maintenance Protocol (RTMP). En redes AppleTalk, protocolo que proporciona generación y mantenimiento de información de direccionamiento en la capa de transporte por medio de la tabla de direccionamiento AppleTalk. La tabla de direccionamiento AppleTalk dirige la transmisión de paquetes por la internet de socket de origen a socket de destino.

RouTing update Protocol (RTP). Protocolo de VIrtual NEtworking System (VINES) que mantiene la base de datos de direccionamiento y permite el intercambio de información de direccionamiento entre nodos VINES. Véase también *Internet Control Protocol (ICP)*.

rsh. Variante del mandato rlogin que invoca un interpretador de mandatos en una máquina remota UNIX y pasa los argumentos de línea de mandatos al interpretador de mandatos saltándose completamente el paso de inicio de sesión.

ruta. (1) Secuencia ordenada de nodos y grupos de transmisión (TG) que representan una vía de acceso de un nodo de origen a un nodo de destino por la que pasa el tráfico intercambiado entre éstos. (2) Vía de acceso que el tráfico de red utiliza para ir del origen al destino.

ruta estática. Ruta entre sistemas principales y/o redes que se entra manualmente en una tabla de direccionamiento.

ruta explícita (ER). En SNA, serie de uno o más grupos de transmisión que conectan dos nodos de subárea. Una ruta explícita se identifica mediante una dirección de subárea de origen, una dirección de subárea de destino, un número de ruta explícita y un número de ruta explícita inversa. Compárese con *ruta virtual (VR)*.

ruta virtual (VR). (1) En SNA, (a) conexión lógica entre dos nodos de subárea que se realiza físicamente como una ruta explícita en particular o (b) conexión lógica contenida en su totalidad dentro de un nodo de subárea para las sesiones intranodo. Una ruta virtual entre nodos de subárea distintos impone una prioridad de transmisión sobre la ruta explícita subyacente, proporciona control del flujo mediante el ritmo de ruta virtual y proporciona la integridad de los datos mediante la numeración en secuencia de las unidades de información de vía de acceso (PIU). (2) Compárese con *ruta explícita (ER)*. Véase también *vía de acceso* y *extensión de ruta (REX)*.

rutina de carga. (1) Secuencia de instrucciones cuya ejecución hace que se carguen y se ejecuten unas instrucciones adicionales hasta que se haya almacenado todo el programa de sistema. (T) (2) Técnica o dispositivo diseñado para que entre en un estado determinado por medio de su propia acción, por ejemplo, una rutina de máquina cuyas primeras instrucciones sean suficientes para que el resto de la misma entre en el sistema desde un dispositivo de entrada. (A)

S

salto. (1) En APPN, parte de una ruta que no tiene nodos intermedios. Está compuesto por un solo grupo de transmisión que conecta nodos adyacentes. (2) Para la capa de direccionamiento, distancia lógica entre dos nodos en una red.

SAP. Véase punto de acceso a servicios.

segmentación. En OSI, función realizada por una capa para correlacionar una unidad de datos de protocolo (PDU) de la capa a la que da soporte con diversas PDU.

segmento. (1) Sección de cable entre componentes o dispositivos. Un segmento puede estar compuesto por un solo cable provisional, diversos cables provisionales conectados o una combinación de cables provisionales y de construcción conectados. (2) En comunicaciones de Internet, unidad de transferencia entre funciones de TCP en diferentes máquinas. Cada segmento contiene campos de control y de datos; la posición de corriente de bytes actual y los bytes de datos reales se identifican conjuntamente con una suma de comprobación para validar los datos recibidos.

segmento de anillo. Parte de un anillo que puede aislarse (desenchufando conectores) del resto del anillo. Véase *segmento de LAN*.

segmento de LAN. (1) Cualquier parte de una LAN (por ejemplo, un bus o un anillo) que puede funcionar independientemente pero está conectada a otras partes de la red por medio de puentes. (2) Red de tipo bus o anillo sin puentes.

señal. (1) En una red de área local, símbolo de autorización pasado sucesivamente de una estación de datos a otra para indicar la estación que tiene temporalmente el control del medio de transmisión. Cada estación de datos tiene una oportunidad de obtener y utilizar la señal para controlar el medio. Una señal es un mensaje o patrón de bits determinado que significa el permiso para transmitir. (T) (2) En las LAN, secuencia de bits pasada de un dispositivo a otro por el medio de transmisión. Cuando la señal tiene datos añadidos, se convierte en una trama.

Serial Line Internet Protocol (SLIP). Protocolo utilizado sobre una conexión punto a punto entre dos sistemas principales de IP de una línea serie, como, por ejemplo, un cable serie o una conexión RS232 con un módem, de una línea telefónica.

Service Advertising Protocol (SAP). En Internetwork Packet Exchange (IPX), protocolo que proporciona lo siguiente:

- Un mecanismo que permite que los servidores IPX de una internet anuncien sus servicios por el nombre y el tipo. Los servidores que utilizan este protocolo tienen registrados su nombre, tipo de servicios y dirección en todos los servidores de archivos que ejecutan NetWare.
- Un mecanismo que permite que una estación de trabajo difunda una consulta para descubrir las identidades de todos los servidores de todos los tipos, todos los servidores de un tipo específico o el servidor más cercano de un tipo específico.
- Un mecanismo que permite que una estación de trabajo consulte cualquier servidor de archivos que ejecute NetWare para descubrir nombre y dirección de todos los servidores de un tipo específico.

servicio de directorios (DS). Elemento de servicio de aplicaciones que convierte los nombres simbólicos utilizados por procesos de aplicaciones en direcciones de red completas utilizadas en un entorno de OSI. (T)

servicios de directorios (DS). Componente del punto de control de un nodo APPN que mantiene la información sobre la ubicación de los recursos de red.

servicios de gestión de punto de control (CPMS). Componente de un punto de control que consta de conjuntos de funciones de servicios de gestión y proporciona recursos de ayuda para realizar la gestión de problemas, gestión del rendimiento y de la contabilidad, gestión de los cambios y gestión de la configuración. Las posibilidades proporcionadas por los CPMS incluyen el envío de peticiones a los servicios de gestión de unidad física (PUMS) para probar recursos del sistema, la reunión de información estadística (por ejemplo, datos de errores y del rendimiento) de los PUMS sobre los recursos del sistema y el análisis y presentación de los resultados de las pruebas y la información estadística reunida sobre los recursos del sistema. Las responsabilidades del análisis y de la presentación para la determinación de problemas y la supervisión del rendimiento pueden distribuirse entre los diversos CPMS.

servicios de gestión de SNA (SNA/MS). Servicios proporcionados como ayuda para la gestión de las redes SNA.

servidor. Unidad funcional que proporciona servicios compartidos a estaciones de trabajo sobre una red; por ejemplo, un servidor de archivos, un servidor de impresión, un servidor de correo. (T)

servidor de acceso a red (NAS). Dispositivo que proporciona a los usuarios acceso a red temporal a petición. Este acceso es punto a punto por medio de líneas PSTN o RDSI.

servidor de configuración de emulación de LAN (LECS). Componente de LAN Emulation Service que centraliza y difunde datos de configuración.

servidor de emulación de LAN (LES). Componente de LAN Emulation Service que resuelve destinos de LAN en direcciones ATM.

servidor de informes de configuración (CRS). En el programa Bridge para la Red en Anillo de IBM, servidor que acepta mandatos del LAN Network Manager (LNM) para obtener información de estaciones, establecer parámetros de estación y eliminar estaciones de su anillo. Este servidor también recoge y reenvía informes de configuración generados por estaciones de su anillo. Los informes de configuración incluyen los nuevos informes del supervisor activo y los informes de estación contigua activa de donde proceden los datos (NAUN).

servidor de nombres. En el conjunto de protocolos de Internet, sinónimo de *servidor de nombres de dominio*.

servidor de nombres de dominio. En el conjunto de protocolos de Internet, programa servidor que suministra la conversión de nombres en direcciones correlacionando nombres de dominio con direcciones IP. Sinónimo con *servidor de nombres*.

servidor de puentes de LAN (LBS). En el programa Bridge para la Red en Anillo de IBM, servidor que mantiene información estadística acerca de las tramas reenviadas entres dos o más anillos (mediante un puente).

El LBS envía estas estadísticas a los gestores de LAN correspondientes mediante el mecanismo de información de LAN (LRM).

servidor de red L2TP (LNS). Un LNS funciona en cualquier plataforma capacitada que pueda ser una estación final de PPP. El LNS maneja la parte del servidor del protocolo L2TP. Puesto que L2TP sólo se apoya en el único medio por el que llegan los túneles de L2TP, el LNS sólo tiene una interfaz LAN o WAN, aunque puede terminar las llamadas que lleguen de cualquier interfaz del rango completo de interfaces PPP soportadas por un LAC. Entre éstas se incluyen la RDSI asíncrona, RDSI síncrona, V.120 y otros tipos de conexiones.

sesión. (1) En la arquitectura de red, con el fin de la comunicación de datos entre unidades funcionales, todas las actividades que tienen lugar durante el establecimiento, mantenimiento y liberación de la conexión. (T) (2) Conexión lógica entre dos unidades de red accesibles (NAU) que puede activarse, adaptarse, para proporcionar varios protocolos y desactivarse de la manera solicitada. Cada sesión está identificada de manera exclusiva en la cabecera de transmisión (TH) que acompaña a cualquier transmisión intercambiada durante la sesión. (3) En L2TP, L2TP crea una sesión cuando se intenta una conexión PPP de extremo a extremo entre un usuario de marcación y los LNS; sin tener en cuenta si el usuario inicia la sesión o si el LNS inicia una llamada hacia fuera. Los datagramas para la sesión se envían por el túnel entre el LAC y el LNS. Los LNS y LAC mantienen la información de estado para cada usuario conectado a un LAC.

Simple Network Management Protocol (SNMP). En el conjunto de protocolos de Internet, protocolo de gestión de red que se utiliza para supervisar direccionadores y redes conectadas. SNMP es un protocolo de capa de aplicación. La información sobre los dispositivos gestionados está definida y almacenada en la base de la información de gestión (MIB) de la aplicación.

simulación. Para los enlaces de datos, técnica mediante la cual un protocolo iniciado en una estación final se reconoce con acuse de recibo y se procesa en un nodo intermedio en nombre del destino final. En la conmutación del enlace de datos del IBM 6611, por ejemplo, las tramas de SNA se encapsulan en paquetes de TCP/IP para el transporte a través de una red de área amplia diferente de SNA, se desempaquetan en otro IBM 6611 y pasan al destino final. Una ventaja de la simulación es que se evitan tiempos de espera excedidos de sesión de final a final.

síncrono. (1) Perteneciente a dos o más procesos que dependen de la aparición de sucesos específicos, como, por ejemplo, señales comunes de temporización. (T) (2) Que se produce con una relación temporal regular o previsible.

sintaxis de abstracción. Especificación de datos que incluye todas las distinciones necesarias en las transmisiones de datos, pero que omite (excluye) otros detalles, como, por ejemplo, los que dependen de las arquitecturas específicas de los sistemas. Véase también *notación de sintaxis de abstracción 1 (ASN.1)* y *normas básicas de codificación (BER)*.

sistema. En el proceso de datos, conjunto de personas, máquinas y métodos organizados para llevar a cabo un conjunto de funciones específicas. (I) (A)

sistema autónomo. En TCP/IP, grupo de redes y direccionadores bajo una sola autorización administrativa. Estas redes y estos direccionadores cooperan estrechamente para propagar la información de asequibilidad (y direccionamiento) de la red entre ellos utilizando un protocolo de pasarela interior de su elección.

sistema de juego reducido de instrucciones (RISC). Sistema que utiliza un juego pequeño y simplificado de instrucciones de uso frecuente para la ejecución rápida.

sistema de nombres de dominio (DNS). En el conjunto de protocolos de Internet, sistema de bases de datos distribuidas utilizado para correlacionar nombres de dominio con direcciones IP.

sistema principal. En el conjunto de protocolos de Internet, sistema final. El sistema final puede ser cualquier estación de trabajo; no es necesario que sea un sistema principal.

socket. (1) Punto final para la comunicación entre procesos o programas de aplicación. (2) Abstracción proporcionada por la Distribución de software de Berkeley de la Universidad de California (software que suele recibir el nombre de UNIX de Berkeley o UNIX de BSD) que funciona como punto final para la comunicación entre procesos o aplicaciones.

sonda de paquetes Internet (PING). (1) En comunicaciones de Internet, programa utilizado en redes TCP/IP para probar la capacidad de alcanzar destinos enviando a los mismos una petición con eco de Internet Control Message Protocol (ICMP) y esperando una respuesta. (2) En comunicaciones, prueba de asequibilidad.

sondeo. (1) En una conexión multipunto o conexión punto a punto, proceso consistente en invitar a las estaciones de datos a transmitir, una por una. (I) (2) Interrogar a dispositivos con el fin de evitar contenciones, determinar el estado operativo o determinar la disposición para enviar o recibir datos. (A)

soporte de diversos dominios (MDS). Técnica para transportar datos de servicios de gestión entre conjuntos de funciones de servicios de gestión sobre sesiones de LU-LU y CP-CP. Véase también *unidad de mensaje de soporte de diversos dominios (MDS-MU).*

StreetTalk. En VIrtual NEtworking System (VINES), sistema exclusivo de denominación y direccionamiento de red amplia que permite que los usuarios ubiquen cualquier recurso de la red y accedan al mismo sin conocer la topología de la red. Véase también *Internet Control Protocol (ICP)* y *RouTing update Protocol (RTP)*.

subárea. Parte de la red SNA compuesta por un nodo de subárea, nodos periféricos conectados y recursos asociados. En un nodo de subárea, todas las unidades de red accesibles (NAU), enlaces y estaciones de enlace adyacentes (de nodos de subárea o nodos periféricos conectados) que son dirigibles dentro de la subárea comparten una dirección de subárea común y tienen direcciones de elementos distintas.

subcapa del control del acceso al medio (MAC). En una red de área local, parte de la capa de enlace de datos que aplica un método de acceso al medio. La subcapa del MAC da soporte a funciones dependientes de la topología y utiliza los servicios de la capa física para proporcionar servicios a la subcapa de control de enlace lógico. (T)

Subnetwork Access Protocol (SNAP). En las LAN, protocolo encargado de establecer diferencias entre protocolos de 5 bytes que identifica la familia de protocolos estándares distintos de IEEE a la que pertenece un paquete. El valor de SNAP se utiliza para diferenciar los protocolos que utilizan `$AA` como valor de punto de acceso a servicios (SAP).

subred. (1) En TCP/IP, parte de una red que se identifica mediante una parte de la dirección IP. (2) Sinónimo de *subred (grupo de nodos)*.

subred (grupo de nodos). (1) Cualquier grupo de nodos que tienen un conjunto de características comunes, como, por ejemplo, el mismo identificador de red. (2) Sinónimo con *subred*.

subsistema. Sistema secundario o subordinado que a menudo puede funcionar de manera independiente o asíncrona respecto a un sistema de control. (T)

suma de comprobación. (1) Suma de un grupo de datos que se asocia con el grupo y se utiliza con fines de comprobación. (T) (2) En la detección de errores, función de todos los bits de un bloque. Si las sumas grabadas y las calculadas no coinciden, se indica que hay un error. (3) En un disquete, datos grabados en un sector con fines de detección de errores; una suma de comprobación calculada que no coincide con la suma de comprobación de los datos grabados en el sector indica que hay un sector anómalo. Los datos son numéricos u otras series de caracteres consideradas numéricas con el fin de calcular la suma de comprobación.

supervisor. (1) Dispositivo que observa y registra actividades seleccionadas en un sistema de proceso de datos para el análisis. Sus usos posibles son para indicar cualquier desviación significativa de la norma o para determinar los niveles de utilización de unidades funcionales en particular. (T) (2) Software o hardware que observa, supervisa, controla o verifica operaciones de un sistema. (A) (3) Función necesaria para iniciar la transmisión de una señal del anillo y para proporcionar recuperación de errores de software en el caso de que se pierdan señales, tramas en circulación u otras dificultades. La posibilidad está presente en todas las estaciones de anillo.

supervisor activo. En una Red en Anillo, función realizada en cualquier momento por una estación de anillo que inicia la transmisión de señales y proporciona recursos de recuperación de errores de señales. Cualquier adaptador activo del anillo tiene la posibilidad de proporcionar la función de supervisor activo si falla el supervisor activo actual.

SYNTAX. En el protocolo Simple Network Management Protocol (SNMP), cláusula del módulo de la MIB que define la estructura de datos abstracta correspondiente a un objeto gestionado.

Systems Network Architecture (SNA). Descripción de la estructura lógica, formatos, protocolos y secuencias operativas para la transmisión de unidades de información a través de las redes y para el control de la configuración y del funcionamiento de las mismas. La estructura de capas de SNA permite que los orígenes y destinos finales de la información, es decir, los usuarios, sean independientes de los servicios y recursos de red SNA específicos utilizados para el intercambio de información y que no se vean afectados por dichos servicios y recursos.

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 la que la capa 4 era TCP y la capa 3 era IP.

Telnet. En el conjunto de protocolos de Internet, protocolo que proporciona un servicio de conexión de terminales remotos. Permite que los usuarios de un sistema principal se conecten con un sistema principal remoto e interactúen como usuarios de terminal conectado directamente de este sistema principal.

terminal de datos preparado (DTR). Señal para el módem que se utiliza con el protocolo EIA 232.

tiempo de espera excedido. (1) Suceso que se produce al final de un período predeterminado de tiempo que ha empezado al aparecer otro suceso especificado. (I) (2) Intervalo de tiempo asignado para que tengan lugar determinadas operaciones; por ejemplo, la respuesta a un sondeo o direccionamiento antes de que se interrumpa el funcionamiento del sistema y deba reiniciarse.

topología. En comunicaciones, ordenación física o lógica de los nodos de una red, especialmente las relaciones de un nodo con otro nodo y los enlaces entre los mismos.

trama. (1) En la arquitectura interconexión de sistemas abiertos, estructura de datos perteneciente a un área particular de información y compuesta por ranuras que pueden aceptar los valores de atributos específicos y de las que pueden deducirse inferencias mediante conexiones apropiadas de procedimiento. (T) (2) Unidad de transmisión en algunas redes de área local, incluida la Red en Anillo de IBM. Incluye delimitadores, caracteres de control, información y caracteres de comprobación. (3) En SDLC, vehículo para cada mandato, cada respuesta y toda información transmitida con procedimientos de SDLC.

trama de información (I). Trama de formato I que se utiliza para la transferencia de información numerada.

trama exploradora. Véase *paquete explorador*.

trama I. Trama de información.

transceptor (transmisor-receptor). En las LAN, dispositivo físico que conecta una interfaz de sistema principal a una red de área local, como, por ejemplo, Ethernet. Los transceptores de Ethernet contienen elementos electrónicos que aplican señales al cable y que detectan colisiones.

Transmission Control Protocol/Internet Protocol (TCP/IP). Conjunto de protocolos de comunicaciones que dan soporte a funciones de conectividad de igual a igual para redes de área local y amplia.

Transmission Control Protocol (TCP). Protocolo de comunicaciones utilizado en Internet y en cualquier red que siga las normas del Departamento de Defensa de los EE.UU. para el protocolo interredes. TCP proporciona un protocolo fiable de sistema principal a sistema principal entre sistemas principales en redes de comunicaciones de paquetes conmutados y en los sistemas interconectados de dichas redes. Utiliza Internet Protocol (IP) como protocolo subyacente.

transporte de vector de gestión de red (NMVT). Unidad de petición/respuesta (RU) de servicios de gestión que fluye sobre una sesión activa entre servicios de gestión de unidad física y servicios de gestión de punto de control (sesión de SSCP-PU).

troncal. (1) En una configuración de anillo de diversos puentes de una red de área local, enlace de gran velocidad al que se conectan los anillos por medio de puentes o direccionadores. Un troncal puede configurarse como bus o como anillo. (2) En una red de área amplia, enlace de gran velocidad al que se conectan nodos o intercambios de conmutaciones de datos (DSE).

túnel. Un túnel está definido mediante un par LNS-LAC. El túnel lleva datagramas de PPP entre el LAC y el LNS. Un solo túnel puede multiplexar muchas sesiones. Una conexión de control que funciona sobre el mismo túnel controla el establecimiento, liberación y mantenimiento de todas las sesiones y del túnel en sí.

U

umbral. (1) En programas de puente de IBM, valor establecido para el número máximo de tramas que no se reenvían a través de un puente debido a errores, antes de que se cuente una aparición de “umbral excedido” y se indique en los programas de gestión de red. (2) Valor inicial a partir del cual un contador disminuye hasta 0 o valor hasta el que aumenta o disminuye un contador a partir de un valor inicial.

unidad básica de transmisión (BTU). En SNA, unidad de datos e información de control que pasa entre los componentes del control de la vía de acceso.

Una BTU puede constar de una o más unidades de información de vía de acceso (PIU).

unidad de datos de protocolo de control de enlace lógico (LLC). Unidad de información intercambiada entre estaciones de enlace de diferentes nodos. La unidad de datos de protocolo de LLC contiene un punto de acceso a servicios de destino (DSAP), un punto de acceso a servicios de origen (SSAP), un campo de control y datos de usuario.

unidad de datos de protocolo (PDU). Unidad de datos especificada en un protocolo de una capa determinada y compuesta por información de control de protocolo de esta capa además de, posiblemente, datos de usuario de esta capa. (T)

unidad de información de vía de acceso (PIU). Unidad de mensaje compuesta por una sola cabecera de transmisión (TH) o por una TH seguida de una unidad básica de información (BIU) o un segmento de BIU.

unidad de mensaje de soporte de diversos dominios (MDS-MU). Unidad de mensaje utilizada en el soporte de diversos dominios que contiene datos de servicios de gestión y fluye entre conjuntos de funciones de servicios de gestión sobre las sesiones de LU-LU y CP-CP. Esta unidad de mensaje, así como los datos reales de servicios de gestión que contiene, tiene el formato de corriente de datos general (GDS). Véase también *unidad de servicios de gestión de punto de control (CP-MSU)*, *unidad de servicios de gestión (MSU)* y *transporte de vector de gestión de red (NMVT)*.

unidad de red accesible (NAU). Unidad lógica (LU), unidad física (PU), punto de control (CP) o punto de control de servicios del sistema (SSCP). Es el origen o el destino de la información transmitida por la red de control de la vía de acceso. Sinónimo con *unidad de red direccionable*.

unidad de red direccionable (NAU). Sinónimo de *unidad de red accesible*.

unidad de servicio de canal (CSU). Unidad que proporciona la interfaz a una red digital. La CSU proporciona funciones de acondicionamiento (o igualación) de línea, que mantienen la uniformidad del rendimiento de la señal a lo largo del ancho de banda de canal; remodelación de señal, que constituye la corriente de pulsaciones binarias; y prueba de bucle de retorno, que incluye la transmisión de señales de prueba entre la CSU y la unidad de canal de oficina de la portadora de red. Véase también *unidad de servicio de datos (DSU)*.

unidad de servicio de datos (DSU). Dispositivo que proporciona una interfaz de servicio de datos digital al equipo terminal de datos de manera directa. La DSU proporciona igualación de bucle y posibilidades de pruebas locales y remotas, así como una interfaz EIA/CCITT estándar.

unidad de servicios de gestión de punto de control (CP-MSU). Unidad de mensaje que contiene datos de servicios de gestión y fluye entre los conjuntos de funciones de servicios de gestión. Esta unidad de mensaje tiene el formato de corriente de datos general (GDS). Véase también *unidad de servicios de gestión (MSU)* y *transporte de vector de gestión de red (NMVT)*.

unidad EIA. Unidad de medida que ha establecido la Electronic Industries Association y es igual a 44,45 milímetros (1,75 pulgadas).

unidad física (PU). (1) Componente que gestiona y supervisa los recursos (como, por ejemplo, enlaces conectados y estaciones de enlace adyacentes) asociados con un nodo tal como lo solicita un SSCP mediante una sesión de SSCP-PU. Un SSCP activa una sesión con la unidad física con el fin de gestionar indirectamente, a través de la PU, recursos del nodo, como, por ejemplo, enlaces conectados. Este término sólo se aplica a los nodos de tipo 2.0, tipo 4 y tipo 5. (2) Véase también *PU periférica* y *PU de subárea*.

unidad lógica (LU). Tipo de unidad de red accesible que permite que los usuarios obtengan acceso a recursos de red y se comuniquen entre sí.

unidad máxima de transmisión (MTU). En las LAN, la mayor unidad de datos posible que puede enviarse por un medio físico determinado en una sola trama. Por ejemplo, la MTU para Ethernet tiene 1500 bytes.

unión de telecomunicaciones internacionales (ITU). Agencia de telecomunicaciones especializada de las Naciones Unidas que se ha establecido con el fin de proporcionar procedimientos y prácticas para la normalización de las comunicaciones, lo cual incluye asignación de frecuencia y regulaciones de la radio universales.

User Datagram Protocol (UDP). En el conjunto de protocolos de Internet, protocolo que proporciona un servicio no fiable de datagramas sin conexiones. Permite que un programa de aplicación de una máquina o proceso envíe un datagrama a un programa de aplicación de otra máquina o proceso. UDP utiliza Internet Protocol (IP) para entregar datagramas.

V.25. En la comunicación de datos, especificación de la CCITT que define el equipo de respuesta automática y el equipo de llamada automática paralelo de la red telefónica general conmutada, incluidos los procedimientos de inhabilitación de dispositivos controlados con eco para las llamadas establecidas de manera manual y automática.

V.34. Recomendación del ITU-T para la comunicación por módem sobre canales estándares de transmisión de voz de 33,6 Kbps (y más lentos) disponibles comercialmente.

V.36. En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito de datos (DCE) con las velocidades de 48, 56, 64 ó 72 kilobits por segundo.

V.35. En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito de datos (DCE) con varias velocidades de datos.

V.24. En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito de datos (DCE).

V

valor por omisión. Perteneciente a un atributo, condición, valor u opción que se supone cuando no se especifica nada de forma explícita. (I)

variable de corriente de datos general (GDS). Tipo de subestructura de RU que va precedida de un identificador y un campo de longitud e incluye datos de aplicación, datos de control de usuario o datos de control definidos según SNA.

variable de la MIB. En el protocolo Simple Network Management Protocol (SNMP), instancia específica de datos definida en un módulo de la MIB. Sinónimo con *objeto de la MIB*.

vector de control de selección de ruta (RSCV). Vector de control que describe una ruta de una red APPN. El RSCV consta de una secuencia ordenada de vectores de control que identifican los TG y nodos que componen la vía de acceso de un nodo de origen a un nodo de destino.

velocidad de información comprometida. Cantidad máxima de datos en bits que la red acepta entregar.

velocidad de transferencia de datos. Promedio de los bits, caracteres o bloques por unidad de tiempo que pasan entre los miembros del equipo correspondiente en un sistema de transmisión de datos. (I)

Notas:

1. La velocidad se expresa en bits, caracteres o bloques por segundo, minuto u hora.
2. Debe indicarse el equipo correspondiente; por ejemplo, módems, equipo intermedio u origen y destino.

versión. Programa bajo licencia independiente que a menudo tiene un nuevo código o una nueva función significativos.

vertimiento múltiple. (1) Transmisión de los mismos datos a un grupo seleccionado de destinos. (T) (2) Forma especial de difusión en que se entregan copias de un paquete a un subconjunto de todos los destinos posibles solamente.

vía de acceso. (1) En una red, cualquier ruta entre dos nodos cualesquiera. Una vía de acceso puede incluir más de una rama. (T) (2) Serie de componentes de red de transporte (control de la vía de acceso y control de enlace de datos) por los que pasa la información intercambiada entre dos unidades de red accesibles. Véase también *ruta explícita (ER)*, *extensión de ruta* y *ruta virtual (VR)*.

VINES. VIrtual NEtworking System.

VIrtual NEtworking System (VINES). Sistema operativo de red y software de red de Banyan Systems, Inc. En una red VINES, la función de enlace virtual permite que todos los dispositivos y servicios aparenten estar conectados directamente entre sí cuando en realidad pueden encontrarse a miles de kilómetros de distancia. Véase también *StreetTalk*.

vista de la MIB. En el protocolo Simple Network Management Protocol (SNMP), conjunto de objetos gestionados, conocidos por el agente, que es visible en una comunidad en particular.

vuelco. (1) Datos que se han volcado. (T) (2) Copiar el contenido de la totalidad o de parte del almacenamiento virtual con el fin de reunir información de errores.

W

X.25. (1) recomendación de la comisión consultiva de la telefonía y telegrafía internacionales (CCITT) relativa a la interfaz entre un equipo terminal de datos y las redes de datos de paquetes conmutados. (2) Véase también *conmutación de paquetes*.

X

X.21. recomendación de la comisión consultiva de la telefonía y telegrafía internacionales (CCITT) relativa a una interfaz de fines generales entre un equipo terminal de datos y un equipo de terminación de circuito de datos para las operaciones síncronas en una red pública de datos.

Xerox Network Systems (XNS). Conjunto de protocolos de internet desarrollados por Xerox Corporation. Aunque es similar a los protocolos TCP/IP, XNS utiliza unos formatos de paquete y una terminología diferentes. Véase también *Internetwork Packet Exchange (IPX)*.

Z

zona. En redes AppleTalk, subconjunto de nodos dentro de una internet.

Zone Information Protocol (ZIP). En redes AppleTalk, protocolo que proporciona un servicio de gestión de zonas manteniendo una correlación de los nombres de zonas y los números de red de la internet en la capa de sesión.

Índice

CH

D

E

F

G

I

L

M

N

P

Q

R

S

T

U

V

W

Hoja de Comentarios

Nways Multiprotocol Routing Services
Utilización y configuración de las características Versión 3.4

Número de Publicación SC10-3429-01

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
SC10-3429-01

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

SC10-3429-01

Corte o Doble
Por la Línea

SC10-3429-01