Access Integration Services

Utilización y configuración de las funciones Versión 3.4

SC10-3437-01

Access Integration Services

Utilización y configuración de las funciones Versión 3.4

SC10-3437-01

Nota

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

Segunda edición (octubre de 1999)

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

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

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

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

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

http://www.networking.ibm.com

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

Contenido

Figuras

Tablas

Avisos

Es posible que en otros países IBM no ofrezca los productos, los servicios o las características que se describen en este documento. Consulte con el representante local de IBM para obtener información acerca de los productos y servicios que actualmente están disponibles en su localidad. Cualquier referencia a un producto, programa o servicio de IBM no implica que únicamente pueda utilizarse dicho producto, programa o servicio IBM. En su lugar puede utilizarse cualquier otro producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente pendientes de aprobación que cubran los temas descritos en este documento. La entrega de este documento no otorga ninguna licencia sobre estas patentes. Puede enviar por escrito sus consultas sobre licencias a la siguiente dirección:

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

Para realizar consultas sobre licencias relativas a los caracteres de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM de su país o bien envíe su consulta por escrito a:

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

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

Marcas registradas

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

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

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

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

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

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

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

Prefacio

Este manual contiene la información que necesitará para utilizar la interfaz de usuario del direccionador con el fin de configurar las funciones instaladas en el IBM 2212 y poder trabajar con ellas. Es posible que un determinado IBM 2212 no dé soporte a todas las funciones que se describen en este manual. Se informa de que una función es específica de un dispositivo determinado mediante:

- Un aviso en el capítulo o apartado adecuado
- Una sección en el prefacio, donde se listan todas las funciones y los dispositivos que les dan soporte.

Este manual trata del IBM 2212 y se hace referencia a él como “direccionador” o “dispositivo”. Los ejemplos del manual representan la configuración de un IBM 2212, pero la salida real que vea puede ser distinta. Los ejemplos son orientativos de lo que verá durante la configuración del dispositivo.

A quién está dirigido este manual

Este manual está dirigido a las personas que instalan y gestionan redes de ordenadores. Aunque puede ser de gran ayuda tener experiencia en el hardware y el software de alguna red de ordenadores, para utilizar el software de los protocolos no es necesario tener conocimientos de programación.

Obtener información adicional

Pueden realizarse cambios en la documentación después de que se impriman los manuales. Si se dispone de información adicional o hay que realizar cambios después de que se impriman los manuales, encontrará los cambios en un archivo del CD-ROM denominado README. Podrá visualizar el archivo con un editor de texto de código ASCII.

Acerca del software

IBM Access Integration Services es el software que da soporte al IBM 2212 (número de programa bajo licencia 5639-F73). Este software tiene los componentes siguientes:

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

  El código base viene instalado de fábrica en el 2212.
- El programa de configuración programa de configuración para IBM Access Integration Services (denominado en este manual: *programa de configuración*)

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

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

También puede obtener el programa de configuración para IBM Access Integration Services a partir de la página de presentación del soporte técnico de redes de IBM. Consulte el manual *Guía del usuario del programa de configuración para Nways Multiprotocol y Access Services,*, GC10-3430 (GC30-3830), para obtener la dirección del servidor y los directorios.

Convenios utilizados en este manual

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

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

   ```
   reload
   ```

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

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

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

   Elija una de las palabras clave como valor del parámetro.

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

   ```
   time host ...
   ```

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

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

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

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

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

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

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

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

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

Nombre de archivo: nombarchivo.ext

Visión general de la biblioteca

Actualizaciones y correcciones de la información: Para mantenerse informado de los cambios técnicos, aclaraciones y arreglos implementados después de la impresión de los manuales, consulte las páginas de presentación del IBM 2212 en:

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

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

Planificación

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

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

Instalación

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

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

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

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

Diagnóstico y mantenimiento

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

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

Operaciones y gestión de red

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

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

En este manual se explica cómo:

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

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

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

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

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

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

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

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

Configuración

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

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

Seguridad

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

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

Información comercial

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

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

Resumen de los cambios correspondientes a la biblioteca software IBM 2212

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

- Mejoras en Frame Relay:
  - Soporte del nuevo manejador de tramas (FH)
  - Aceleración PU para manejar ráfagas de tráfico para soportar controladores 3745
  - Nuevo tipo de interfaz (subinterfaz Frame Relay) para permitir interfaces virtuales en la misma interfaz física

- Soporte de IP no numerado

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

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

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

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

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

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

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

Aclaraciones y correcciones

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

Cómo obtener ayuda

En los indicadores de mandatos, puede obtener ayuda en forma de listado de los mandatos disponibles 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 2212 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 la reserva de ancho de banda y de colas de prioridad

En este capítulo se describen las funciones del sistema de reserva de ancho de banda y de las colas de prioridad disponibles actualmente para las interfaces Frame Relay y PPP. Consta de los apartados siguientes:

Sistema de reserva de ancho de banda

El sistema de reserva de ancho de banda (BRS, Bandwidth Reservation System) le permite decidir qué paquetes descartar cuando la demanda (tráfico) en una conexión de red es mayor que la oferta (rendimiento). Cuando la utilización del ancho de banda alcanza el 100%, BRS determina qué tráfico debe descartarse, dependiendo de la configuración.

La reserva de ancho de banda "reserva" ancho de banda de transmisión para determinadas clases de tráfico. Cada clase tiene asignado un porcentaje mínimo del ancho de banda de la conexión. Consulte la Figura 1 en la página 2 y la Figura 2 en la página 2.

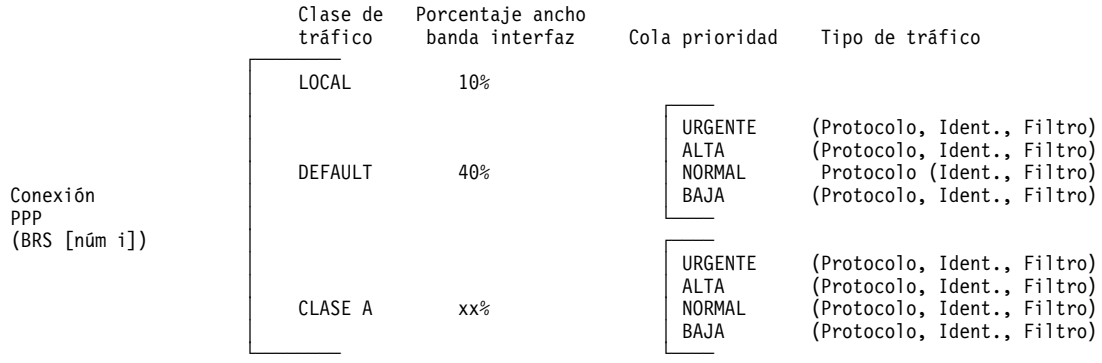
Para las interfaces PPP, se definen clases de tráfico (clases-t) y a cada una se le asigna un porcentaje del ancho de banda de la interfaz PPP. Existen al menos dos clases de tráfico:

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

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

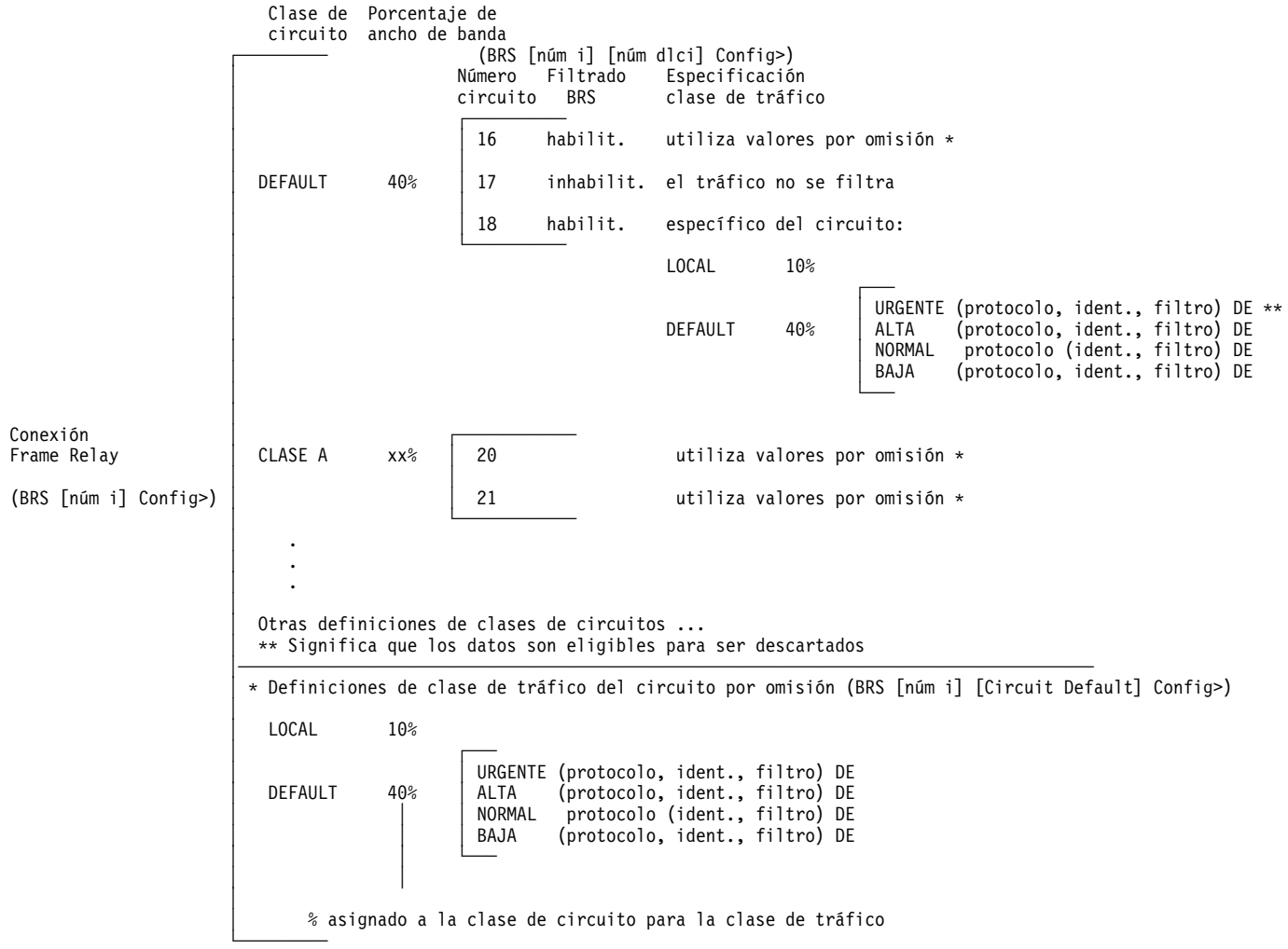
Para las interfaces Frame Relay, se definen clases de circuito (clases-c) y a cada una se le asigna un porcentaje del ancho de banda de la interfaz Frame Relay. Existe al menos una clase de circuito: la clase de circuito DEFAULT, a la que inicialmente se asignan todos los circuitos. Se pueden crear clases de circuito adicionales y asignar circuitos a estas clases-c. Para cada circuito Frame Relay se pueden definir clases de tráfico (clases-t) y a cada clase de tráfico se le asigna un porcentaje del ancho de banda del circuito Frame Relay. Los circuitos Frame Relay dan soporte a las clases de tráfico de manera análoga a las interfaces PPP. En la Figura 2 en la página 2 se puede ver la relación entre las clases de circuito y las clases de tráfico Frame Relay.

Utilización de BRS y colas de prioridad



Nota: Inicialmente, a todos los protocolos se les asigna la cola de prioridad NORMAL de la clase de tráfico DEFAULT. Se puede asignar un protocolo, un filtro o un identificador a cualquier cola de una clase de tráfico.

Figura 1. Relación entre la clase de tráfico y la cola de prioridad de la clase de tráfico para una interfaz PPP en BRS



Nota: Inicialmente, a todos los protocolos se les asigna la cola de prioridad NORMAL de la clase de tráfico DEFAULT. Se puede asignar un protocolo, un filtro o un identificador a cualquier cola de una clase de tráfico.

Figura 2. Relación entre la clase de circuito y la clase de tráfico para una interfaz Frame Relay en BRS

Los porcentajes que se reservan son una mínima *parte* del ancho de banda para la conexión de red. Si una red está funcionando al máximo de su capacidad, los men-

sajes de cada clase sólo podrán transmitirse mientras utilicen el ancho de banda asignado a la clase. En este caso, las transmisiones adicionales se retendrán hasta que se hayan satisfecho otras transmisiones que ocupan ancho de banda. En el caso de que exista una ruta de tráfico poco cargada, una corriente de paquetes podrá utilizar un ancho de banda mayor que el mínimo asignado, llegando al 100% en caso de que no haya más tráfico.

En realidad, la reserva de ancho de banda es un sistema de *salvaguardia*. En general, un dispositivo no debe intentar utilizar más del 100% de la velocidad de la línea. Si lo hace, posiblemente es que se necesita una línea más rápida. Sin embargo, la naturaleza “fluctuante” del tráfico, puede hacer que la velocidad de transmisión supere el 100% durante un corto intervalo de tiempo. En estos casos, se habilita la reserva de ancho de banda y se garantiza la entrega del tráfico de mayor prioridad (es decir, no se descarta).

La reserva de ancho de banda funciona 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 sobre Frame Relay

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

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

Cuando BRS recibe un paquete de Frame Relay, se utilizan las clases-c y las clases-t configuradas para determinar cuándo se transmitirá el mismo. BRS pone el paquete en cola de acuerdo a estos 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 éstas se clasifican según un algoritmo justo ponderado de puesta en cola. En una clase-c, los circuitos que tienen paquetes que transmitir se envían utilizando un algoritmo rotativo. Las clases-t de cada clase-c también se clasifican según un algoritmo justo ponderado de puesta en cola. A su vez, los paquetes de la clase-t se ponen en cola según su prioridad (urgente, alta, normal o baja).

Un paquete se saca de la cola y se transmite cuando cumple todas estas condiciones:

1. Es el próximo paquete de la siguiente clase-c
2. Es el próximo paquete del siguiente circuito de la clase-c
3. Es uno de los paquetes de la siguiente clase-t de esta clase-c
4. Es el próximo paquete del siguiente grupo de prioridad de esta clase-t

Si se habilita la interfaz y uno o más circuitos de BRS, y no se configuran clases-c ni clases-t, todos los circuitos se asignarán a una clase-c llamada *default (por*

omisión). Con esta configuración, sólo existirá la clase-c por omisión en la cola de clases-c, y cada uno de los circuitos de la clase-c con paquetes que transmitir se manejará según una estrategia rotativa. Si quiere que BRS haga esto, deje todos los circuitos en la clase-c por omisión y no cree ninguna clase de circuito.

Los circuitos huérfanos (no asignados a ninguna clase) y los circuitos para los que no se ha habilitado explícitamente el sistema BRS, utilizarán por omisión este entorno de puesta en cola de BRS en cualquier situación. BRS los asigna a la clase-c por omisión.

Para configurar BRS, debe seguir la secuencia siguiente:

1. Habilite BRS para la interfaz
2. Habilite BRS para los circuitos y añada las clases-c.
3. Asigne los circuitos a las clases-c.
4. Si lo desea, defina clases-t para cada clase-c.

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

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

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

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

Soporte de colas

Con la reserva de ancho de banda sobre Frame Relay, cada circuito puede poner en cola tramas cuando está congestionado. Esto es válido incluso para interfaces y circuitos para los que no está habilitada la reserva de ancho de banda.

Elegibilidad para ser descartado

La red Frame Relay puede descartar los datos transmitidos que sobrepasen la CIR de un PVC. El direccionador puede poner en 1 el bit DE para indicar que parte del tráfico se debe considerar elegible para ser descartado. En caso necesario, la red Frame Relay descartará las tramas marcadas como elegibles para ser descartadas, lo que permitirá que las tramas que no están marcadas como elegibles para ser descartadas sean transmitidas por la red. Al asignar un protocolo, filtro o identificador a una clase de tráfico, se puede especificar si el tráfico del protocolo, del filtro o del identificador será elegible para ser descartado. En el apartado “Assign” en la página 33 hallará más información sobre cómo configurar el tráfico para que sea elegible para ser descartado. El tráfico de voz (identificado por el protocolo VOFR) debe configurarse como **no** elegible para ser descartado.

Definiciones de circuito por omisión para manejar clases de tráfico

Se pueden definir muchos circuitos para una interfaz Frame Relay. En lugar de tener que configurar totalmente las definiciones de las clases de tráfico de cada circuito, BRS le permite definir un conjunto de clases de tráfico y de asignaciones de protocolos, filtros e identificadores por omisión, llamado definiciones de circuito por omisión, que puede utilizar cualquier circuito de la interfaz. Al habilitar inicialmente BRS para un circuito, éste se inicializa utilizando las definiciones de circuito por omisión. Si un circuito no puede utilizar las definiciones de circuito por omisión para manejar clases de tráfico, se pueden crear definiciones específicas de circuito mediante los mandatos **add-class**, **change-class**, **assign**, **deassign**, **tag** y **untag**.

Si un circuito utiliza definiciones específicas de circuito y a usted le interesa que utilice las definiciones de circuito por omisión, puede utilizar el mandato **use-circuit-defaults** en el indicador BRS del circuito.

Las definiciones de circuito por omisión para manejar clases de tráfico se definen ejecutando el mandato **set-circuit-defaults** en el indicador de la interfaz Frame Relay de BRS. Este mandato le sitúa en un indicador de valores por omisión de circuitos BRS, en el que puede añadir, cambiar y suprimir clases de tráfico, asignar y desasignar protocolos, filtros e identificadores, y crear identificadores de BRS. Si se cambian las definiciones de circuito por omisión para las clases de tráfico, el manejo de las clases de tráfico se actualizará dinámicamente para todos los circuitos que utilicen las definiciones de circuito por omisión.

Configuración de BRS para voz sobre Frame Relay

Las tramas de voz pueden transmitirse por circuitos dedicados. En este caso, habilite BRS para la interfaz y los circuitos, y acepte los valores por omisión de los circuitos asociados con voz. Es posible que quiera crear varias clases-c y asignar los circuitos dedicados a voz a una clase-c asociada con un porcentaje alto de ancho de banda y asignar los circuitos asociados con datos a una clase de circuito asociada con un porcentaje menor de ancho de banda.

Si tanto el tráfico de voz como el resto de tráfico se transmiten por los mismos circuitos, habilite BRS para la interfaz y los circuitos. Si quiere que se atienda a todos los circuitos de forma rotativa, sin favorecer a ningún circuito en particular, puede decidir no crear más clases-c que la clase-c por omisión ya existente. A continuación, se recomienda que para cada circuito por el que se transmita voz y datos, cree una clase-t con el mandato **create-super-class** y que asigne el tráfico VOFR a esta clase. Cree también tantas clases-t adicionales como necesite y asigne otros tipos de tráfico a estas clases-t. Esta configuración ayudará a garantizar que el tráfico de voz tenga prioridad sobre el resto de tráfico y que se pueden intercalar tramas de voz sin segmentar entre segmentos de datos fragmentados, si se habilita la fragmentación. Se recomienda que habilite la fragmentación para la interfaz Frame Relay, si quiere enviar voz y datos por la misma interfaz. La fragmentación conlleva que las tramas sean más pequeñas y, de esta forma, que el retardo entre tramas de voz consecutivas también sea menor.

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

Colas de prioridad

La reserva de ancho de banda asigna porcentajes del ancho de banda de conexión total para las *clases* de tráfico o *clases-t* especificadas, definidas por el usuario. Exceptuando la clase-t creada con el mandato **create-super-class**, que tiene prioridad sobre las otras clases-t, las clases-t de BRS están asociadas con un porcentaje del ancho de banda. Los datos de protocolos y de filtros pueden asignarse a clases-t y a colas de prioridad concretas de una clase-t. Al utilizar colas de prioridad, puede asignarse un protocolo o un filtro a una cola determinada de una clase de tráfico con valores: una clase-t de BRS es un grupo de paquetes identificados por el mismo nombre; por ejemplo, una clase llamada “ipx” designa a todos los paquetes IPX.

Al utilizar colas de prioridad, se puede asignar a cada clase-t de ancho de banda los niveles de prioridad siguientes:

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

para las clases de tráfico (o clases-t) especificadas, definidas por el usuario.

Además, para cada nivel de prioridad de cada clase-t de ancho de banda, se puede definir el número de paquetes que están esperando en la cola. El mandato **queue-length** de BRS establece el número máximo de almacenamientos intermedios de salida que pueden ponerse en cada cola de prioridad de BRS, y el número máximo de almacenamientos intermedios de salida que pueden ponerse en cada cola de prioridad de BRS cuando escasean los almacenamientos intermedios de entrada del direccionador. Se puede configurar la longitud de las colas de prioridad tanto para PPP como para Frame Relay.

Atención: Si define una longitud de cola demasiado grande, es posible que el rendimiento del direccionador se degrade mucho.

Para BRS, se pueden establecer las longitudes de las colas de prioridad para conexiones WAN PPP y Frame Relay. En el apartado “Queue-length” en la página 47 hallará una descripción del mandato **queue-length**.

Los valores de prioridad de una clase-t de ancho de banda no afectarán a las otras clases de ancho de banda. Ninguna clase de ancho de banda tiene prioridad sobre las otras.

Colas de prioridad sin reserva de ancho de banda

Si las colas de prioridad se configuran sin reserva de ancho de banda, el tráfico que tenga mayor prioridad se entregará primero. En caso de que exista gran cantidad de tráfico con prioridad alta, el tráfico que tenga niveles de prioridad bajos puede quedar totalmente bloqueado. Sin embargo, combinando las colas de prioridades con la reserva de ancho de banda, la transmisión de paquetes puede asignarse a todos los tipos de tráfico.

Configuración de las clases de tráfico

Se pueden crear clases de tráfico mediante el mandato **add-class** y, a continuación, asignar tipos de tráfico a las clases utilizando el mandato **assign**. El tráfico se asigna a una clase de tráfico basándose en su *tipo de protocolo* o en un filtro que a su vez identifica un tipo concreto de *tráfico de protocolo* (por ejemplo, paquetes IP de SNMP).

Los tipos de protocolos soportado son:

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

Filtros BRS

Si se utiliza la reserva de ancho de banda, se puede tratar el tráfico de un protocolo concreto de forma distinta al de otro tráfico que utilice el mismo tipo de protocolo. Por ejemplo, se puede asignar el tráfico IP de SNMP a una clase de tráfico y prioridad distintas que las del resto de tráfico IP. En este ejemplo, SNMP es un filtro BRS, ya que *filtra* (o sea, identifica de modo exclusivo) el tráfico de un protocolo concreto. El tráfico de los protocolos IP, ASRT (puentes) y APPN-HPR puede filtrarse mediante la reserva de ancho de banda. Los filtros soportados son los 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 de red
- HPR alto
- HPR medio
- HPR bajo
- XTP
- Números de puerto o sockets TCP/UDP
- Byte TOS
- bit de prioridad

BRS y filtros

En los apartados siguientes se describe cómo utilizar BRS con distintos tipos de filtros.

Filtros de direcciones MAC e identificadores

La reserva de ancho de banda y los filtros MAC (MCF) manejan conjuntamente los filtros de direcciones MAC utilizando *identificadores*. Por ejemplo, un usuario con reserva de ancho de banda puede categorizar el tráfico que se transmite por un puente asignándole un identificador.

El proceso de identificación consiste en crear un elemento de filtro en la consola de configuración de filtros MAC y asignarle un número de identificador. Este número de identificador se utiliza para configurar una clase de tráfico para todos los paquetes asociados con este identificador. El valor de un identificador debe estar comprendido entre 1 y 64. Consulte el “Utilización de filtros MAC” en la página 57 para obtener información adicional sobre los filtros MAC.

Nota: Los identificadores ***solamente*** pueden aplicarse a los paquetes que se transmiten por puentes. En una conexión PPP o Frame Relay, se pueden asignar como filtros de reserva de ancho de banda hasta cinco filtros MAC con identificador, llamados TAG1 a TAG5. En primer lugar se busca TAG1, después TAG2, y así sucesivamente hasta llegar a TAG5. El identificador de un filtro MAC consta de varias direcciones MAC definidas en MCF.

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

Los identificadores también pueden hacer referencia a “grupos,” como en el ejemplo del Túnel IP. Los extremos de un Túnel IP pueden pertenecer a un número indeterminado de grupos. Los paquetes se asignan a un grupo determinado mediante la función de identificación de filtros de direcciones MAC. Para obtener información adicional sobre los filtros MAC, consulte el “Utilización de filtros MAC” en la página 57 y el “Configuración y supervisión de filtros MAC” en la página 61.

Para aplicar la reserva de ancho de banda y las colas de prioridad a los paquetes con identificador:

1. Utilice los mandatos de configuración de filtros MAC del indicador `filter config>` para configurar los identificadores de paquetes que se transmiten por el puente. Consulte el “Utilización de filtros MAC” en la página 57 para obtener más información.
2. Utilice el mandato **tag** de la reserva de ancho de banda para referirse a un identificador de reserva de ancho de banda.
3. Con el mandato **assign** de la reserva de ancho de banda, asigne el identificador de BRS a una clase-t. El mandato **assign** también le solicitará que especifique una prioridad de cola para esta clase-t de BRS.

Filtros de número de puerto TCP/UDP

Se pueden asignar paquetes TCP/IP de un rango de puertos TCP o UDP a una clase-t y prioridad de BRS basándose en el número de puerto UDP o TCP de los paquetes y, opcionalmente, del socket. Se pueden especificar hasta 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 (combinación de número de puerto y dirección IP). Después se puede asignar este filtro a una clase de tráfico y prioridad de BRS dentro de la clase.

Si se habilitan los filtros de puertos UDP/TCP, BRS examinará cada paquete TCP o UDP y comprobará si el número de puerto destino u origen coincide con uno de los números de puerto a filtrar. Además, si se define una dirección IP como parte del filtro UDP/TCP de BRS, y la dirección IP destino u origen coincide con la dirección definida para el filtro, BRS asigna el paquete a la clase de tráfico y prioridad de este filtro de número de puerto.

Por ejemplo, se puede configurar un filtro de número de puerto UDP para los números de puerto UDP que van del 25 al 29, y asignar el filtro a la clase de tráfico 'A' con prioridad 'normal'. BRS pone en cola los paquetes UDP cuyo número de puerto origen o destino va del 25 al 29 en la cola de prioridad normal para la clase de tráfico 'A'.

También se puede configurar un filtro de número de puerto TCP para el número de puerto TCP 50 y dirección IP 5.5.5.25, y asignar el filtro a la clase de tráfico 'B' con prioridad 'urgente'. BRS pone en cola los paquetes TCP cuyo número de puerto origen o destino es 50 y cuya dirección IP origen o destino es 5.5.5.25, en la cola de prioridad urgente para la clase de tráfico 'B'.

Filtros de bits TOS de IPv4

Se pueden crear filtros que distingan entre distintos tipos de tráfico IP según el valor de los bits del Tipo de servicio (TOS). Dichos filtros TOS pueden utilizarse para asignar el tráfico IPv4 que tenga determinados valores para los bits TOS a clases y prioridades diferentes de las del tráfico IP. Cada filtro permite el tráfico IPv4 cuyo valor del byte TOS coincide con la definición de un filtro TOS configurado para que se asigne a una clase de tráfico y prioridad exclusivas. Configurar un filtro TOS consiste en especificar un valor de máscara que sirve para definir qué bits del byte TOS deben compararse, así como especificar los valores superior e inferior de los bits que forman parte de la máscara. El mecanismo de filtrado se basa únicamente en los valores del TOS de IPv4; por lo tanto, no se basa en la identificación del tipo de protocolo IPv4 ni en la información del número de puerto, como hacen la mayoría de filtros IP.

Este filtro puede ampliarse más que el filtrado de prioridad de IPv4 de BRS, que sólo tienen en cuenta los 3 bits más significativos del byte TOS. El soporte de filtros de bits TOS de BRS, combinado con el soporte de control de acceso de IP, permite filtrar el tráfico que se envía por un túnel seguro, que esté fragmentado o que no pueda identificarse mediante el soporte de filtros de número de puerto UDP o TCP de BRS. Además, el soporte de control de acceso de IP permite establecer los bits TOS en valores definidos por el usuario, en lugar de tener que utilizar los valores de los bits de prioridad para APPN y DLSw, que no pueden modificarse, asociados con los filtros de bits de prioridad de IPv4 de BRS. Por lo tanto, se reco-

mienda que utilice el soporte de control de acceso de IP y de filtros de bits TOS, en lugar del método de filtrado de bits de prioridad de IPv4 de BRS.

Como se indica en el apartado “Orden de prioridad de filtros” en la página 12, la comprobación de las coincidencias con los filtros TOS se realiza antes que la de los filtros de bits de prioridad de IPv4 y que la de otros filtros específicos de IP. La comprobación de las coincidencias con los filtros TOS1 a TOS5 se hace secuencialmente, empezando por el filtro TOS1. Pueden definirse hasta 5 filtros TOS.

Importante: Tenga presente que un paquete con un determinado valor del TOS, se manejará según sea la primera definición de los filtros TOS con que coincida el valor. Los filtros deben configurarse cuidadosamente para que un determinado byte TOS se filtre por el filtro adecuado y no, accidentalmente, por un filtro que tenga un número inferior. En el apartado “Utilización de IP”, de la publicación *Utilización y configuración de las funciones*, hallará más información.

Proceso de bits de prioridad de IP versión 4 para tráfico SNA en túneles seguros IP y fragmentos secundarios

Normalmente, BRS distingue entre el tráfico TCP de IP y el tráfico UDP de IP según sus números de puerto. Sin embargo, BRS no puede identificar los puertos después de que el tráfico se haya encapsulado dos veces, como es el caso del tráfico IP transmitido a través de un túnel seguro o en un fragmento UDP o TCP secundario. Se ha añadido a BRS el proceso de bits de prioridad de IP versión 4, para permitir el filtrado de los paquetes transmitidos a través de un túnel seguro IP o en paquetes de fragmentos secundarios de TCP y UDP.

Nota: Se recomienda que utilice el método de filtrado de bits TOS de IPv4 de BRS en lugar del proceso de bits de prioridad de IPv4. Para obtener más detalles, consulte el apartado “Filtros de bits TOS de IPv4” en la página 9.

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

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

Si se habilitan los filtros de prioridad de IPv4 para BRS y los bits de prioridad de un paquete IP coinciden con uno de los valores utilizados por el tráfico APPN/HPR, el paquete se pondrá en la cola de prioridad de la clase-t de BRS a la que esté asignada la correspondiente prioridad de transmisión de HPR. Por ejemplo, si un paquete IP tiene un valor de prioridad de `'110'b` y el filtro HPR de red de BRS está asignado a una clase-t A con un nivel de prioridad normal, el paquete se pondrá en la cola de prioridad normal de la clase-t A. Si no se ha configurado ningún filtro de prioridad de la transmisión de HPR de BRS, el paquete se pondrá en la cola de prioridad de la clase-t a la que esté asignado el filtro APPN-HPR.

Las tres clases de tráfico siguientes se correlacionan con el valor de prioridad de IPv4 '011'b:

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

Al correlacionar distintos tipos de tráfico con un solo valor, BRS no puede distinguirlos cuando se habilita el método de filtrado basado en los bits de prioridad de IPv4. Por lo tanto, cuando BRS se encuentra un paquete IP con un valor de prioridad de '011'b, evalúa los filtros BRS en el orden siguiente para determinar si el filtro está habilitado o no. Si encuentra un filtro BRS configurado, el paquete se pone en la cola de prioridad de clase-t a la que está asignado el filtro BRS:

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

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

Si un cliente envía tráfico TN3270 al 2212 a través de una red de área amplia en la que está habilitado BRS, éste no podrá asignar prioridades al tráfico del cliente, a menos que el cliente defina los bits de prioridad como '011'b.

El manejo de bits de prioridad de IPv4 debe configurarse en varios sitios:

1. En BRS se configura si BRS debe filtrar o no basándose en los bits de prioridad de IPv4. Este tipo de filtros sólo se aplicarán a los paquetes transmitidos por túneles seguros IP y a los paquetes que estén en fragmentos secundarios de TCP y UDP.
2. Al configurar DLSw, HPR sobre IP y TN3270, se especifica si el 2212 debe o no debe establecer los bits de prioridad de IPv4 para los paquetes que cree para cada uno de estos tipos de protocolo.

Para utilizar el método de filtrado de bits de prioridad de IPv4 siga estos tres pasos:

1. Active los filtros de prioridad de IPv4 en BRS.
2. Configure las clases-t de BRS y asigne protocolos y filtros para tantas categorías de tráfico SNA como quiera, para el tráfico SNA que no se transmita a través de un túnel seguro IP o que no esté fragmentado.
3. Habilite los valores de los bits de prioridad de IPv4 al configurar los protocolos DLSw, HPR sobre IP y TN3270.
4. Configure IPSec para crear un túnel seguro por el que se transmitirá el tráfico DLSw, HPR sobre IP e TN3270.

Filtros SNA y APPN para tráfico que se transmite por un puente

El filtro SNA/APPN-ISR le permite asignar a una clase de tráfico de BRS el tráfico SNA y APPN-ISR transmitido por un puente. El tráfico SNA y APPN-ISR se identifica como los paquetes transmitidos por un puente cuyo SAP origen o destino es 0x04, 0x08 ó 0x0C y cuyo campo de control LLC (802.2) 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 a una clase-t de BRS el tráfico HPR transmitido por un puente. El tráfico HPR se identifica como los paquetes transmitidos por un puente cuyo SAP origen o destino es `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 de red, HPR alto, HPR medio y HPR bajo permiten que el tráfico HPR transmitido por un puente vuelva a filtrarse dependiendo de la prioridad de transmisión de HPR. Por ejemplo, si quiere asignar el tráfico HPR con prioridad de transmisión de red a una determinada clase-t y prioridad, y el resto de tráfico HPR transmitido por un puente a una clase-t y prioridad diferentes, asigne el filtro HPR de red a la clase-t y prioridad adecuadas y utilice el filtro APPN-HPR para asignar el resto de tráfico HPR a una clase-t o prioridad distintas.

El tráfico APPN-HPR que se va a direccionar a través de IP se filtra utilizando el número de puerto UDP asignado para las prioridades de red, alta, media y baja de la transmisión de HPR. Para los intercambios XID se utiliza un número de puerto UDP adicional. Todos los números de puerto UDP utilizados para dar soporte a APPN-HPR sobre IP son configurables.

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

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

Para los filtros SNA/APPN-ISR y APPN-HPR, si quiere que la comprobación se realice con otros SAP distintos de los anteriores, cree un filtro de ventana desplazada utilizando filtros MAC e identificando el filtro. A continuación, asigne el filtro MAC con identificador a una clase-t de BRS.

Orden de prioridad de filtros

Es posible que al comparar un paquete, éste coincida con más de un tipo de filtro BRS. Por ejemplo, un paquete IP transmitido por un puente y un túnel que contiene datos SNA puede coincidir con el filtro de túnel IP y con el filtro SNA/APPN-ISR. El orden de evaluación de los filtros para determinar si un paquete coincide o no con un tipo de filtro BRS es el siguiente:

1. Filtros TOS (IP)
2. Manejo de prioridad de IPv4
3. Comparación del identificador de un filtro MAC para paquetes transmitidos por puentes (IP/ASRT)

4. NetBIOS para paquetes transmitidos por puentes (IP/ASRT)
5. SNA/APPN-ISR para paquetes transmitidos por puentes (IP/ASRT)
6. HPR de red (IP/ASRT/APPN-HPR)
7. HPR alto (IP/ASRT/APPN-HPR)
8. HPR medio (IP/ASRT/APPN-HPR)
9. HPR bajo (IP/ASRT/APPN-HPR)
10. APPN-HPR (IP/ASRT)
11. Filtros de números 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 relacionados con el filtro aparecen entre paréntesis.

Configuraciones de ejemplo

Utilización de las definiciones de circuito por omisión para manejar clases de tráfico de circuitos Frame Relay

Notas:

1 Configura la función BRS.
2 Habilita la función BRS para la interfaz 1.
3 Habilita la función BRS para los circuitos 16, 17, 18. Estos circuitos utilizan las definiciones de circuito por omisión para manejar clases de tráfico.
4 Accede al menú set-circuit-defaults para definir las definiciones de circuito por omisión para manejar clases de tráfico.
5 Añade clases de tráfico y asigna protocolos y filtros a dichas clases de tráfico.
6 Lista y muestra las definiciones de BRS para el circuito 16. Puesto que el circuito 16 utiliza las definiciones de circuito por omisión, se mostrarán las clases de tráfico y las asignaciones de protocolos y filtros definidas por las definiciones de circuito por omisión.
7 Cambia el circuito 17 para que pase de utilizar las definiciones de circuito por omisión a utilizar definiciones de circuito propias para manejar clases de tráfico, creando una clase exclusiva, CIRC171. A esta clase se le pueden asignar protocolos, filtros o identificadores.
8 Cambia las definiciones de circuito por omisión de forma que las clases de tráfico DEF1 y DEF2 reserven cada una el 10% del ancho de banda y, a continuación, se muestra que los cambios se han aplicado al circuito 16, pero no al circuito 17, puesto que éste utiliza ahora definiciones de circuito propias.
9 Altera el circuito 17 para que utilice las definiciones de circuito por omisión para manejar clases de tráfico en lugar de las definiciones de circuito propias.

```
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 la reserva de ancho de banda

En este capítulo se describen los mandatos de configuración y de funcionamiento del sistema de reserva de ancho de banda (BRS).

Este capítulo consta de los apartados siguientes:

Visión general de la configuración de la reserva de ancho de banda

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

1. En el indicador `OPCON (*)`, escriba **talk 6**.
2. En el indicador `Config>`, escriba **feature brs**.
3. En el indicador `BRS Config>`, escriba **interface** #. La interfaz deber ser punto a punto o Frame Relay. BRS no puede configurarse en subinterfaces Frame Relay. Para obtener más información, consulte el apartado "Utilización de interfaces Frame Relay" en la publicación *Access Integration Services Guía del usuario de software*.
4. En el indicador `BRS [i 0] Config>`, escriba **enable**.

   Este es el nivel de indicador de interfaz y en esta instancia el número de interfaz es cero. Para cada interfaz que vaya a configurar, tendrá que repetir los pasos 3 y 4.

   Si está configurando el BRS para una interfaz Frame Relay, continúe en el paso 4a:

   Si está configurando BRS para otra interfaz, vaya directamente al paso 5.

   a. En el indicador `BRS [i 0] Config>`, escriba **circuit** #, donde # es el número del circuito que quiere configurar.

   b. En el indicador `BRS [i 0] [dlci 16] Config>`, escriba **enable**. Este es el nivel de indicador de circuito y en esta instancia el número de circuito (DLCI) es 16.

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

   d. Repita los pasos 4a a 4c para cada circuito para el que quiera definir clases-t de BRS.
5. Reinicie el direccionador.
6. Repita los pasos 1 a 3 para configurar la reserva de ancho de banda para la interfaz concreta que acaba de habilitar.

7. Si está configurando BRS para una interfaz PPP, configure las clases de tráfico y asígneles protocolos, filtros e identificadores en el indicador `BRS[i 0]Config>` mediante los mandatos que se listan en la Tabla 3 en la página 29. Si está configurando BRS para una interfaz FR (Frame Relay), continúe con los pasos 8 a 10.
8. Si está configurando BRS para una interfaz FR, puede configurar clases de circuitos y asignarles circuitos mediante los mandatos que se listan en la Tabla 2 en la página 28
9. Si quiere utilizar las definiciones de circuito por omisión, entonces escriba el mandato **set-circuit-defaults** en el indicador `BRS[i 0]Config>`. Esto le lleva al indicador `BRS[i 0][circuit defaults]` en el que podrá utilizar los mandatos adecuados de la Tabla 3 en la página 29 para configurar las clases de tráfico y asignarles protocolos, filtros e identificadores. Una vez haya terminado de definir las definiciones de circuito por omisión para manejar clases de tráfico, escriba "exit" para volver al indicador `BRS[i 0] Config>`.
10. Si tiene circuitos FR que no pueden utilizar las definiciones de circuito por omisión para manejar clases de tráfico, escriba **circuit** *circuito-permanente-virtual número_circuito*. Esto le llevará al indicador de circuito, donde podrá utilizar los mandatos que se listan en la Tabla 3 en la página 29 para crear definiciones de circuito propias para manejar clases de tráfico.

Nota: No es necesario que reinicie el direccionador para que los cambios realizados en la configuración de las clases-t y de las clases-c entren en vigor.

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

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

El mandato **interface #** le permite seleccionar la interfaz concreta que se quiere configurar para la reserva de ancho de banda. Antes de configurar las clases de BRS, deberá utilizar el mandato **enable** para habilitar BRS para la interfaz. En el paso 4 en la página 25, el indicador muestra que el número de interfaces seleccionadas es cero.

El mandato **circuit #** le permite seleccionar el circuito de la interfaz FR para el que se quiere configurar las clases de tráfico de BRS. Antes de configurar las clases-t de BRS para el circuito, debe utilizar el mandato **enable** para habilitar BRS para el circuito. En el paso 4b en la página 25, el indicador muestra que se ha seleccionado el circuito 16 de la interfaz 0.

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

Para volver al indicador `Config>` sólo tiene que entrar el mandato **exit** en cada uno de los niveles de indicador de BRS, hasta llegar al indicador `Config>`.

Mandatos de configuración de la reserva de ancho de banda

En este apartado se describen los mandatos de configuración de la reserva de ancho de banda. Los mandatos que pueden utilizarse varían dependiendo del indicador de configuración de BRS que se muestre (`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 los mandatos de configuración de la reserva de ancho de banda (disponibles desde el indicador 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 xxxii.
Activate-IP-precedence-filtering	Activa el filtrado de prioridad de IPv4 de BRS para paquetes APPN y SNA que se envían por túneles IP seguros o que están en fragmentos TCP o UDP secundarios. También debe configurar el valor de los bits de prioridad de IPv4 al configurar DLSw, HPR sobre IP o TN3270.
Deactivate-IP-precedence-filtering	Desactiva el proceso de filtrado de prioridad de IPv4.
Enable-hpr-over-ip-port-numbers	Habilita los filtros BRS para el tráfico APPN-HPR sobre IP y permite la configuración de los números de puerto UDP utilizados para identificar los paquetes HPR sobre IP. **Nota:** Si APPN está incluido en la imagen de carga, no se da soporte a este mandato puesto que BRS averigua de APPN si se ha configurado HPR sobre IP y, si es así, BRS averigua de APPN los números de puerto UDP que utilizarán los paquetes HPR sobre IP.
Disable-hpr-over-ip-port-numbers	Inhabilita los filtros BRS para el tráfico APPN-HPR sobre IP. **Nota:** Si APPN está incluido en la imagen de carga, no se dará soporte a este mandato puesto que BRS averigua de APPN si se ha configurado o no HRP sobre IP.

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

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

Tabla 2 (Página 1 de 2). Mandatos de configuración de interfaz de BRS disponibles desde el indicador BRS [núm i] 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 xxxii.
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 determinado a la clase-c de ancho de banda especificada.
Change-circuit-class	Cambia el ancho de banda configurado para una clase-c de ancho de banda.
Circuit	Accede al indicador de nivel de circuito de BRS (`BRS [i x][dlci y] Config>`) desde el que se pueden utilizar los mandatos que se listan en la Tabla 3 en la página 29 para configurar la reserva de ancho de banda para el circuito Frame Relay.
Clear-block	Borra de la SRAM los datos de configuración asociados con la interfaz actual. Se borran los datos de configuración de la clase de circuito y las definiciones de circuito por omisión para manejar 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 para la interfaz.
Enable	Habilita la reserva de ancho de banda para la interfaz.

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

Mandato	Función
List	Visualiza las clases-c y las definiciones de circuito asignadas, almacenadas en la SRAM.
Queue-length	Establece el número máximo y mínimo de paquetes que puede haber en una cola de prioridad.
Set-circuit-defaults	Accede al indicador de mandatos `BRS [i x] [circuit defaults] Config>` lo que le permitirá utilizar los mandatos de la Tabla 3 en la página 29 para crear las definiciones de circuito por omisión para manejar clases de tráfico.
Show	Visualiza las clases-c definidas y los circuitos asignados actualmente, almacenados en SRAM.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxiii.

En la tabla siguiente se listan los mandatos de circuito de BRS disponibles desde los indicadores `BRS [i x] Config>` para interfaces PPP, `BRS [i x] dlci [y] Config>` para circuitos Frame Relay y `BRS [i x] [circuit defaults] Config>`.

Tabla 3 (Página 1 de 2). Mandatos para manejar 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 xxxii.
Add-class	Asigna un determinado ancho de banda a una clase de tráfico definida por el usuario.
Create-super-class	Define la clase-t llamada *super-class*.
Assign	Asigna un protocolo o filtro a una clase de tráfico ya configurada.
Change-class	Cambia el ancho de banda configurado para una clase-t de ancho de banda.
Clear-block	Borra de la memoria SRAM los datos de configuración de la clase de tráfico y de la asignación de protocolos, filtros e identificadores, para la interfaz PPP o el circuito Frame Relay. **Nota:** Este mandato no puede utilizarse desde el indicador `BRS [i x] [circuit defaults] Config>`.
Deassign	Restaura la clase-t y prioridad por omisión a la cola del paquete o filtro especificados.
Default-class	Establece la clase-t y prioridad por omisión a los valores deseados y asigna todos los protocolos que no están asignados a la nueva clase-t por omisión.
Del-class	Suprime una clase-t de ancho de banda ya configurada.
Disable	Inhabilita la reserva de ancho de banda para la interfaz PPP o el circuito Frame Relay. **Nota:** BRS no puede habilitarse ni inhabilitarse desde el indicador `BRS [i x] [circuit defaults] Config>`.

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

Mandato	Función
Enable	Habilita la reserva de ancho de banda para la interfaz PPP o el circuito Frame Relay. **Nota:** BRS no puede habilitarse ni inhabilitarse desde el indicador `BRS [i x] [circuit defaults] Config>`.
List	Lista las clases-t y las asignaciones de protocolos, filtros e identificadores configuradas, almacenadas en la memoria SRAM.
Queue-length	Establece el número máximo y mínimo de paquetes que puede haber en una cola de prioridad. **Nota:** Este mandato no puede utilizarse desde el indicador `BRS [i x] [circuit defaults] Config>`.
Show	Visualiza las clases-t y las asignaciones de protocolos, filtros e identificadores definidas actualmente, almacenadas en la memoria SRAM. **Nota:** Este mandato no puede utilizarse desde el indicador `BRS [i x] [circuit defaults] Config>`.
Tag	Asigna un nombre de identificador de BRS (TAG1 a TAG5) a un filtro MAC al que se ha asignado un identificador durante la configuración de la función de filtrado MAC.
Untag	Elimina la relación entre un nombre de identificador de BRS (TAG1 a TAG5) y un filtro MAC al que se ha asignado un identificador durante la configuración de la función de filtrado MAC.
Use-circuit-defaults	Permite que el usuario suprima las definiciones de circuito propias y utilice las definiciones de circuito por omisión para manejar clases de tráfico. Este mandato es válido en el indicador `BRS [i x] dlci [y] Config>`, sólo para Frame Relay. **Nota:** Para que los valores por omisión sean operativos, deberá reiniciar el direccionador.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiii.

Utilice los mandatos adecuados para configurar la reserva de ancho de banda para Frame Relay y el protocolo Punto a punto (PPP). Para Frame Relay, se debe configurar el circuito y la interfaz de red. Para PPP, sólo se debe configurar la interfaz de red.

Notas:

1. Si se ejecutan los mandatos **clear-block**, **disable**, **enable**, **list** o **show** desde el menú de interfaz de BRS, la información de reserva de ancho de banda configurada para la interfaz seleccionada se modificará o se listará. Si los mandatos se ejecutan desde el menú de circuito de BRS, sólo se modificará o se listará 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 presentes los puntos siguientes:
   - Antes de utilizar otro mandato de configuración, debe utilizar el mandato **interface** para seleccionar una interfaz. (Obligado por la configuración de BRS).

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

3. No es necesario que reinicie el direccionador para que los cambios realizados en la configuración de las clases-t y de las clases-c entren en vigor.

Activate-IP-precedence-filtering

Utilice el mandato **activate-ip-precedence-filtering** para activar el filtrado de prioridad de IPv4 de BRS para paquetes APPN y SNA que se envían por un túnel IP seguro o que están en fragmentos TCP o UDP secundarios. También debe configurar el valor de los bits de prioridad de IPv4 al configurar DLSw, HPR sobre IP o TN3270. Para obtener más información, consulte el apartado “Proceso de bits de prioridad de IP versión 4 para tráfico SNA en túneles seguros IP y fragmentos secundarios” en la página 10.

Sintaxis:

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

Add-circuit-class

Nota: Sólo se utiliza en la configuración de Frame Relay.

Utilice el mandato **add-circuit-class** en el nivel de interfaz para asignar un determinado ancho de banda que utilizará un grupo de circuitos asignados 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 un determinado ancho de banda a una clase-t de ancho de banda definida por el usuario.

Nota: Si el mandato se ejecuta para un circuito Frame Relay que está utilizando actualmente definiciones de circuito por omisión para manejar clases de tráfico, se le preguntará si quiere alterar temporalmente las definiciones de circuito por omisión. Si la respuesta es afirmativa, el circuito se cambiará para que utilice las definiciones de circuito propias para manejar clases de tráfico, y se aceptará el mandato. Si la respuesta es “No”, el mandato se cancelará anormalmente y el circuito seguirá utilizando las definiciones de circuito por omisión. Si quiere 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 a 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 clase1 a 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 clase1
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 clase1 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, paquetes de protocolos o filtros a una clase-t determinada, y asignarle prioridad. Los cuatro tipos de prioridad son:

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

Nota: El protocolo Voz sobre Frame Relay (VOFR) se utiliza para enviar paquetes de voz a través de una interfaz Frame Relay. Si un circuito transportará únicamente paquetes de voz, asigne una sola clase-t al circuito y especifique que el protocolo es VOFR. Sólo se permite una clase-t porque así no tendrá prioridad sobre otras. Si hubiera más de una clase-t, las que no transportaran voz podrían hacerse con el control del ancho de banda e interferir en la transmisión del tráfico de voz. Para garantizar que el tráfico de voz se transmita inmediatamente, debe asignarse el tipo de prioridad *Urgente* al tráfico VOFR y únicamente a este tráfico.

Debe configurarse la función de Fragmentación en Frame Relay, descrita en el mandato **enable fragmentation**, en el capítulo “Configuración y supervisión de interfaces Frame Relay”, de la publicación *Access Integration Services Guía del usuario de software*, en caso de que el tráfico que se vaya a transportar por el circuito sea tanto de datos como de voz. Esto es necesario para evitar que grandes paquetes de datos utilicen todo el ancho de banda, impidiendo que los paquetes de voz se envíen lo suficientemente deprisa.

Sintaxis:

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

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

Nota: Si el mandato se ejecuta para un circuito Frame Relay que está utilizando actualmente definiciones de circuito por omisión para manejar clases de tráfico, se le preguntará si quiere alterar temporalmente las definiciones de circuito por omisión. Si la respuesta es afirmativa, el circuito se cambiará para que utilice las definiciones de circuito propias para manejar clases de tráfico, y se aceptará el mandato. Si la respuesta es “No”, el mandato se cancelará anormalmente y el circuito seguirá utilizando las definiciones de circuito por omisión. Si quiere 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 TOS a la clase clase1; clase1 se ha añadido previamente a la configuración con 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]? clase1  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 clase1 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 clase1 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                 clase1               NORMAL             NO
   with TOS range x1 - x3
    and TOS mask xFF

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

1 Para utilizar el filtro TOS debe entrar tres parámetros: TOS mask, TOS range-low y TOS range-high. Consulte el mandato “Add” en el capítulo “Configuración y supervisión IP”, de la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 1*, para obtener una descripción de estos parámetros.

Assign-circuit

Nota: Sólo se utiliza en la configuración de 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 el DLCI para asignar un PVC a una clase de circuito y el nombre del circuito para asignar un SVC a una clase de circuito.

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

Sintaxis:

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

Change-circuit-class

Nota: Sólo se utiliza en la configuración de Frame Relay.

Utilice el mandato **change-circuit-class** en el nivel de interfaz para cambiar el porcentaje de ancho de banda que utilizará 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 el ancho de banda configurado para una clase-t de ancho de banda.

Nota: Si el mandato se ejecuta para un circuito Frame Relay que está utilizando actualmente definiciones de circuito por omisión para manejar clases de tráfico, se le preguntará si quiere alterar temporalmente las definiciones de circuito por omisión. Si la respuesta es afirmativa, el circuito se cambiará para que utilice las definiciones de circuito propias para manejar clases de tráfico, y se aceptará el mandato. Si la respuesta es “No”, el mandato se cancelará anormalmente y el circuito seguirá utilizando las definiciones de circuito por omisión. Si quiere 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: Sólo se utiliza en la configuración de Frame Relay.

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

Sintaxis:

c**ircuit**

Antes de utilizar los mandatos **add-class**, **assign**, **default-class**, **del-class**, **deassign** o **change-class**, deberá habilitar BRS para el circuito y reiniciar o volver a cargar el direccionador.

Ejemplo de PVC:

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

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

Ejemplo de 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 ejecutar el mandato **enable** para el circuito Frame Relay y de volver a cargar o reiniciar el direccionador, los mandatos siguientes estarán disponibles 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 memoria SRAM los datos de la configuración actual de la reserva de ancho de banda.

Sintaxis:

c**lear-block**

- Si escribe el mandato en el indicador de interfaz para PPP, se borrarán todos los datos de configuración de BRS para la interfaz.
- Si escribe el mandato en el indicador de interfaz para Frame Relay, BRS ya no estará habilitado para la interfaz ni para los circuitos de la interfaz y, además, se borrarán todos los datos de configuración de las clases de circuito y las definiciones de circuito por omisión para manejar clases de tráfico. Sin embargo, no se borrarán los datos de configuración de las clases de tráfico de cada circuito individual y estarán disponibles si se vuelve a habilitar BRS para la interfaz.
- Para borrar los datos de configuración de las clases de tráfico de un circuito, primero deberá entrar el mandato **circuit** desde el indicador de nivel de interfaz y, a continuación, el mandato **clear-block** desde el indicador de nivel de circuito. Después de borrar los datos de configuración de las clases de tráfico para todos los circuitos, escriba el mandato **clear-block** desde el indicador de nivel de interfaz para borrar los datos de configuración de las clases de circuito. Los cambios no entrarán en vigor hasta que se reinicie o se vuelva a cargar el direccionador.

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-class* para la interfaz PPP o el circuito Frame Relay. Sólo se puede configurar una clase super-class para cada interfaz PPP o circuito Frame Relay. No se asocia ningún porcentaje de ancho de banda a la clase super-class. Los datos de un protocolo o filtro asignados a una clase super-class se transmitirán antes que los datos de un protocolo o filtro asignados a otras clases-t de la interfaz PPP o el circuito Frame Relay. Para el protocolo Voz sobre Frame Relay (VOFR), se debe

configurar una clase super-class para un circuito que transporte tanto paquetes de voz como de datos. En este entorno, si se configura la clase super-class para que transporte voz, es más probable que los paquetes de voz tengan mayor prioridad.

Sintaxis:

cr**eate-super-class**

Deactivate-IP-precedence-filtering

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

Sintaxis:

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

Deassign

Utilice el mandato **deassign** para restaurar la clase-t y prioridad por omisión de la cola del paquete de un protocolo o filtro especificados.

Nota: Si el mandato se ejecuta para un circuito Frame Relay que está utilizando actualmente definiciones de circuito por omisión para manejar clases de tráfico, se le preguntará si quiere alterar temporalmente las definiciones de circuito por omisión. Si la respuesta es afirmativa, el circuito se cambiará para que utilice las definiciones de circuito propias para manejar clases de tráfico, y se aceptará el mandato. Si la respuesta es “No”, el mandato se cancelará anormalmente y el circuito seguirá utilizando las definiciones de circuito por omisión. Si quiere 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: Sólo se utiliza en la configuración de Frame Relay.

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

Sintaxis:

deassign-c #

Default-circuit-class

Nota: Sólo se utiliza en la configuración de 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 del ancho de banda asignado a esta clase de circuitos, incluidos 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: Sólo se utiliza en la configuración de 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 la prioridad por omisión en el valor que se quiera. Si no se había asignado ningún valor anteriormente, se utilizarán los valores por omisión del sistema. En caso contrario, se utilizará el último valor previamente asignado.

Nota: Si el mandato se ejecuta para un circuito Frame Relay que está utilizando actualmente definiciones de circuito por omisión para manejar clases de tráfico, se le preguntará si quiere alterar temporalmente las definiciones de circuito por omisión. Si la respuesta es afirmativa, el circuito se cambiará para que utilice las definiciones de circuito propias para manejar clases de tráfico, y se aceptará el mandato. Si la respuesta es “No”, el mandato se cancelará anormalmente y el circuito seguirá utilizando las definiciones de circuito por omisión. Si quiere 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 de la interfaz o circuito especificados una clase-t de ancho de banda previamente configurada.

Nota: Si el mandato se ejecuta para un circuito Frame Relay que está utilizando actualmente definiciones de circuito por omisión para manejar clases de tráfico, se le preguntará si quiere alterar temporalmente las definiciones de circuito por omisión. Si la respuesta es afirmativa, el circuito se cambiará para que utilice las definiciones de circuito propias para manejar clases de tráfico, y se aceptará el mandato. Si la respuesta es “No”, el mandato se cancelará anormalmente y el circuito seguirá utilizando las definiciones de circuito por omisión. Si quiere 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 para la interfaz (si se entra en el indicador de interfaz) o para el circuito (si se entra en el indicador de circuito). Los cambios no entrarán en vigor hasta que se reinicie o se vuelva a cargar el direccionador.

Para verificar que la reserva de ancho de banda está inhabilitada, escriba el mandato **list**.

Sintaxis:

disable

Disable-hpr-over-ip-port-numbers

Utilice el mandato **disable-hpr-over-ip-port-numbers** para inhabilitar los filtros BRS para el tráfico HPR sobre IP.

Sintaxis:

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

Para verificar que los filtros BRS para el tráfico HPR sobre IP están inhabilitados, escriba el mandato **list**.

Nota: Si APPN está incluido en la imagen de carga, configure en el indicador de mandatos `APPN Config>` si se utilizará o no el tráfico HPR sobre IP.

Enable

Utilice el mandato **enable** para habilitar la reserva de ancho de banda para la interfaz (si se entra en el indicador de interfaz) o para el circuito (si se entra en el indicador de circuito). Los cambios no entrarán en vigor hasta que se reinicie o se vuelva a cargar el direccionador.

Sintaxis:

enable

Notas:

1. Si se configura BRS para una interfaz PPP, ejecute el mandato **enable** desde el indicador de interfaz y, a continuación, reinicie o vuelva a cargar el direccionador antes de configurar las clases de tráfico y asignarles protocolos y filtros.
2. Si inicialmente se habilita BRS para un circuito Frame Relay, éste se inicializará con las definiciones de circuito por omisión para manejar clases de tráfico. Ejecute el mandato **enable** en el indicador de interfaz y en el indicador de circuito de todos los circuitos para los que quiera definir clases de tráfico. A continuación, reinicie o vuelva a cargar el direccionador antes de configurar las clases de circuitos de la interfaz y las clases de tráfico de 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 los filtros BRS para el tráfico APPN-HPR sobre IP y para configurar los números de puerto UDP utilizados para identificar los paquetes HPR sobre IP.

Nota: Si APPN está incluido en la imagen de carga, habilite HPR sobre IP y especifique los números de puerto UDP utilizados por el tráfico HPR sobre 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]?
```

XID exchange port number

Este parámetro especifica el número de puerto UDP que utilizará el intercambio XID. Este número de puerto debe ser el mismo que el definido en otros dispositivos de la red.

Valores válidos: de 1024 a 65535

Valor por omisión: 12000

Network priority port number

Este parámetro especifica el número de puerto UDP que utilizará el tráfico con prioridad de red. Este número de puerto debe ser el mismo que el definido en otros dispositivos de la red.

Valores válidos: de 1024 a 65535

Valor por omisión: 12001

High exchange port number
Este parámetro especifica el número de puerto UDP que utilizará el tráfico con prioridad alta. Este número de puerto debe ser el mismo que el definido en otros dispositivos de la red.

Valores válidos: de 1024 a 65535

Valor por omisión: 12002

Medium exchange port number
Este parámetro especifica el número de puerto UDP que utilizará el tráfico con prioridad media. Este número de puerto debe ser el mismo que el definido en otros dispositivos de la red.

Valores válidos: de 1024 a 65535

Valor por omisión: 12003

Low exchange port number
Este parámetro especifica el número de puerto UDP que utilizará el tráfico con prioridad baja. Este número de puerto debe ser el mismo que el definido en otros dispositivos de la red.

Valores válidos: de 1024 a 65535

Valor por omisión: 12004

Interface

Utilice el mandato **interface** para elegir la interfaz serie a la que se referirán los mandatos de configuración de la reserva de ancho de banda. *Los direccionadores que ejecutan las interfaces PPP (protocolo punto a punto) y Frame Relay dan soporte a la reserva de ancho de banda.*

Nota: Las subinterfaces Frame Relay no soportan la reserva de ancho de banda. Para obtener más información, consulte el apartado Utilización de interfaces Frame Relay en la publicación *Access Integration Services Guía del usuario de software*.

Sintaxis:

interface *número-interfaz*

Notas:

1. Si se quieren ejecutar mandatos de reserva de ancho de banda para otra interfaz, este mandato debe ejecutarse ***antes*** de utilizar ningún otro mandato de configuración de la reserva de ancho de banda. Si sale del indicador de la reserva de ancho de banda y quiere volver para hacer cambios en la reserva de ancho de banda de una interfaz previamente configurada, primero deberá volver a ejecutar este mandato.
2. Si se utiliza la función de restauración de WAN y el sistema BRS está configurado para una interfaz principal, BRS también deberá configurarse para la interfaz secundaria. Lo normal, cuando se utiliza la función de restauración de WAN, es que la interfaz secundaria adopte la identidad de la interfaz principal. Esto no es cierto para BRS; por lo tanto, BRS debe ser configurado tanto para la interfaz principal como para la secundaria.

Para habilitar la reserva de ancho de banda para una interfaz determinada, escriba en el indicador `BRS Config>` el número de la interfaz que da soporte al protocolo o función en particular. Se puede utilizar el mandato **enable** (Talk 6) de BRS, tal y como se describe en este capítulo. Para que el mandato entre en vigor, después de habilitar el número de interfaz, deberá reiniciar o volver a cargar el 2212 antes de poder hacer más cambios a la configuración de la interfaz.

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

List

Utilice el mandato **list** para visualizar las clases de anchos de banda actualmente definidas y sus porcentajes garantizados.

Los mandatos **list** y **show** son parecidos. El mandato **list** muestra las definiciones almacenadas actualmente en la memoria SRAM y el mandato **show** muestra las definiciones almacenadas actualmente en la memoria RAM.

Sintaxis:

list *número-interfaz*

Dependiendo del indicador desde el que se ejecute el mandato **list**, la salida será diferente. Puede ejecutar el mandato **list** desde los indicadores siguientes:

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

Nota: Si este mandato se ejecuta desde un indicador de circuito Frame Relay (`BRS [i x] [dlci y] Config>`), indicará si el circuito está utilizando las definiciones de circuito por omisión o las definiciones de circuito propias para manejar clases de tráfico. Si el circuito está utilizando las definiciones de circuito por omisión, se visualizarán la clase de tráfico y las asignaciones de protocolos, filtros e identificadores definidas actualmente para las definiciones de circuito por omisión. Sin embargo, para modificar las definiciones de circuito por omisión, deberá ir al indicador `BRS [i x] [circuit defaults] Config>`.

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

En el indicador de nivel de interfaz de BRS para Frame Relay, el mandato **list** muestra las clases de circuitos, sus porcentajes de ancho de banda configurados y los circuitos que tienen 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 CLASE1 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 definir el número de paquetes que pueden ponerse en cada cola de prioridad de BRS. Cada clase de BRS tiene una prioridad asignada a sus protocolos, filtros e identificadores y cada cola de prioridad puede almacenar el número de paquetes especificado en este mandato.

Sintaxis:

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

Este mandato establece el número máximo de almacenamientos intermedios que pueden ponerse en cada cola de prioridad de BRS, así como el número máximo que puede ponerse en cada cola de prioridad de BRS cuando el número de almacenamientos intermedios de entrada del direccionador es reducido.

Si ejecuta el mandato **queue-length** para una interfaz PPP los valores de longitud de cola se establecerán para todas las colas de prioridad de cada clase-t de BRS definida para la interfaz.

Si ejecuta el mandato **queue-length** para una interfaz Frame Relay (desde el indicador: `BRS [i 0] Config>`), los valores de longitud de cola por omisión se establecerán para todas las colas de prioridad de cada clase-t de BRS definida para los circuitos virtuales permanentes de la interfaz.

Si ejecuta el mandato **queue-length** para un PVC de Frame-Relay (desde un indicador parecido a este: `BRS [i 0] [dlci 16] Config>`), los valores de longitud de cola se establecerán para todas las colas de prioridad de cada clase-t de 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 ejecute este mandato, excepto que sea imprescindible. Los valores de longitud de cola por omisión son adecuados para la mayoría de usuarios. Si se establece una longitud de cola demasiado grande, es posible que el rendimiento del direccionador se degrade mucho.

Set-circuit-defaults

Utilice el mandato **set-circuit-defaults** para acceder a los mandatos que se utilizan para definir las definiciones de circuito por omisión para manejar clases de tráfico. Cualquier circuito Frame Relay de la interfaz que pueda utilizar las mismas clases de tráfico y asignaciones de protocolos, filtros e identificadores, puede utilizar dichas definiciones de circuito por omisión.

Sintaxis:

set**-circuit-defaults**

Show

Utilice el mandato **show** para visualizar las clases de ancho de banda definidas actualmente almacenadas en la memoria RAM.

Sintaxis:

sh**ow** *número-interfaz*

Dependiendo del indicador desde el que se ejecute el mandato **show**, la salida será diferente. Los indicadores desde los que se puede ejecutar el mandato **show** son los siguientes:

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

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

Protocol/Filter      Class              Priority    Discard Eligible
---------------      -----              --------    ----------------
IP                   CLASE1               NORMAL             NO
ARP                  CLASE1               NORMAL             NO
DNA                  CLASE1               NORMAL             NO
VINES                CLASE1               NORMAL             NO
IPX                  CLASE1               NORMAL             YES
OSI                  CLASE1               NORMAL             NO
VOFR                 CLASE1               NORMAL             NO
AP2                  CLASE1               NORMAL             NO
ASRT                 DEFAULT              NORMAL             NO
NETBIOS              DEFAULT              NORMAL             NO
```

En el indicador de interfaz para PPP y en el indicador de circuito para Frame Relay, se muestra información sobre la clase de tráfico. En el indicador de interfaz para Frame Relay, se muestra información sobre la clase de circuito.

Notas:

1. Si este mandato se ejecuta desde un indicador de circuito Frame Relay (`BRS [i x] [dlci y] Config>`), indicará si el circuito está utilizando las definiciones de circuito por omisión o las definiciones de circuito propias para manejar clases de tráfico. Si el circuito está utilizando las definiciones de circuito por omisión, se visualizarán las clases de tráfico y las asignaciones de protocolos, filtros e identificadores definidas actualmente para las definiciones de circuito por omisión. Sin embargo, para modificar las definiciones de circuito por omisión, deberá ir al indicador `BRS [i x] [circuit defaults] Config>`.
2. Este mandato no puede utilizarse desde el indicador `BRS [i x] [circuit defaults] Config>`.

Tag

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

Sintaxis:

t**ag** *número-ident_filtro_mac*

Utilice el mandato **list** para mostrar los identificadores de filtros MAC asignados a un nombre de identificador BRS y los nombres de identificadores BRS asignados a una clase de tráfico de ancho de banda.

Nota: Si el mandato se ejecuta para un circuito Frame Relay que está utilizando actualmente definiciones de circuito por omisión para manejar clases de tráfico, se le preguntará si quiere alterar temporalmente las definiciones de circuito por omisión. Si la respuesta es afirmativa, el circuito se cambiará para que utilice las definiciones de circuito propias para manejar clases de tráfico, y se aceptará el mandato. Si la respuesta es “No”, el mandato se cancelará anormalmente y el circuito seguirá utilizando las definiciones de circuito por omisión. Si quiere 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 el número de identificador del filtro MAC y el nombre de identificador BRS asociado. Un identificador se puede eliminar solamente si el nombre de identificador BRS asociado no está asignado a una clase de tráfico de ancho de banda.

Sintaxis:

u**ntag** *número-ident_filtro_mac*

Utilice el mandato **list** para mostrar los identificadores de filtros MAC asignados a un nombre de identificador BRS y los nombres de identificadores BRS asignados a una clase de tráfico de ancho de banda.

Nota: Si el mandato se ejecuta para un circuito Frame Relay que está utilizando actualmente definiciones de circuito por omisión para manejar clases de tráfico, se le preguntará si quiere alterar temporalmente las definiciones de circuito por omisión. Si la respuesta es afirmativa, el circuito se cambiará para que utilice las definiciones de circuito propias para manejar clases de tráfico, y se aceptará el mandato. Si la respuesta es “No”, el mandato se cancelará anormalmente y el circuito seguirá utilizando las definiciones de circuito por omisión. Si quiere 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 indicador de nivel de circuito para suprimir las definiciones de circuito propias y utilizar las definiciones de circuito por omisión para manejar clases de tráfico. Se le pedirá que confirme si quiere utilizar las definiciones de circuito por omisión.

Sintaxis:

use-circuit-defaults

Notas:

1. Este mandato se utiliza solamente en la configuración de Frame Relay
2. Para que los valores por omisión sean operativos, deberá reiniciar o volver a cargar el direccionador.

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 supervisión de la reserva de ancho de banda

Para acceder a los mandatos de supervisión de la reserva de ancho de banda y para supervisar la reserva de ancho de banda del direccionador, siga estos pasos:

1. En el indicador OPCON prompt (*), escriba **talk 5**.
2. En el indicador GWCON prompt (+), escriba **feature brs.**
3. En el indicador BRS>, escriba **interface #**, donde # es el número de interfaz que quiere supervisar. Esto le llevará al indicador de nivel de interfaz de BRS, BRS [i x]>, donde x es el número de interfaz.
4. Sólo para Frame Relay, escriba **circuit #** en el indicador de interfaz para especificar el circuito de esta interfaz que se quiere supervisar.

   Esto le llevará al indicador 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, 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 de BRS. Puede escribir este mandato utilizando el nombre (brs) o el número (1) de la función.

   El mandato **interface #** selecciona la interfaz concreta que se quiere supervisar para la reserva de ancho de banda.

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

Siempre puede volver al indicador GWCON escribiendo el mandato **exit** en el indicador BRS>.

Una vez en el indicador de supervisión de la reserva de ancho de banda (BRS>), puede entrar cualquiera de los mandatos de supervisión que se describen en la Tabla 4.

Mandatos de supervisión de la reserva de ancho de banda

En este apartado se resumen los mandatos de supervisión de la reserva de ancho de banda y, a continuación, se explican con más detalle. La 4 muestra los mandatos de supervisión de la reserva de ancho de banda. Los mandatos que pueden utilizarse varían dependiendo del indicador de supervisión de BRS (BRS>, BRS [i x]> o BRS [i x] [dlci y]>) desde el que se ejecuten.

Tabla 4. Resumen de mandatos de supervisión de la reserva de ancho de banda

Mandato	Utilizado sólo con FR	Función
? (Ayuda)		Visualiza todos los mandatos disponibles en este nivel de mandato o lista las opciones de un mandato concreto (si está disponible). Consulte el apartado “Cómo obtener ayuda” en la página xxxii
Circuit	sí	Selecciona el DLCI de un circuito virtual permanente (PVC) de Frame Relay. Para supervisar la reserva de ancho de banda del tráfico de Frame Relay, debe estar en el nivel de indicador de circuito.
Clear		Borra los contadores actuales de las clases-t y los almacena como contadores **last** de las clases-t. Los contadores se listan por clase.
Clear-circuit-class	sí	Borra los contadores actuales de las clases-c y los almacena como contadores **last** de las clases-c. Los contadores se listan por clase.
Counters		Visualiza los contadores actuales de las clases-t.
Counters-circuit-class	sí	Visualiza los contadores actuales de las clases-c.
Interface		Selecciona la interfaz a supervisar. **Nota:** Este mandato debe ejecutarse antes de utilizar cualquier mandato de supervisión de reserva de ancho de banda.
Last		Visualiza los últimos contadores que se guardaron de las clases-t.
Last-circuit-class	sí	Visualiza los últimos contadores que se guardaron de las clases-c.
Exit		Vuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiii

Circuit

Nota: Sólo se utiliza en la supervisión de Frame Relay.

Utilice el mandato **circuit** para seleccionar el DLCI de un PVC de Frame Relay que se quiere supervisar. Este mandato sólo puede ejecutarse desde el indicador de supervisión de interfaz de BRS (`BRS [núm i]>`).

Sintaxis:

ci**rcuit** *circuito-virtual-permanente-#*

de seleccionar el circuito Frame Relay, se podrán utilizar los mandatos siguientes desde el indicador de circuito:

```
CLEAR
COUNTERS
LAST
EXIT
```

Clear

Utilice el mandato **clear** para guardar los contadores actuales de las clases-t de la reserva de ancho de banda (de manera que puedan recuperarse con el mandato **last**) y borrar los valores. Los contadores se guardan por clase de tráfico de ancho de banda.

Sintaxis:

clear

Clear-Circuit-Class

Nota: Sólo se utiliza en la supervisión de Frame Relay.

Utilice el mandato **clear-circuit-class** para guardar los contadores actuales de las clases-c de la reserva de ancho de banda (de manera que puedan recuperarse con el mandato **last-circuit-class**) y borrar los valores. Los contadores se guardan por clase de circuito.

Sintaxis:

clear-c**ircuit-class**

Counters

Utilice el mandato **counters** para mostrar las estadísticas que describen el tráfico de la reserva de ancho de banda de las clases de tráfico configuradas para una interfaz PPP o un 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
CLASE_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
CLASE_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 por paquete que no han podido transmitirse porque se ha alcanzado la longitud máxima de una cola de prioridad o porque el paquete no ha podido ponerse en cola, ya que la cola de prioridad estaba en el umbral mínimo de longitud de cola y el paquete provenía de una interfaz que estaba quedándose sin almacenamientos intermedios de recepción.

Pkt Ovfl Lista el número de paquetes que no han podido transmitirse porque se ha alcanzado la longitud máxima de una cola de prioridad o porque el paquete no ha podido ponerse en cola, ya que la cola de prioridad estaba en el umbral mínimo de longitud de cola y el paquete provenía de una interfaz que estaba quedándose sin almacenamientos intermedios de recepción.

Q_len El número actual de paquetes que esperan ser transmitidos en cada cola de prioridad para cada clase de tráfico.

Counters-circuit-class

Nota: Sólo se utiliza en la supervisión de Frame Relay.

Utilice el mandato **counters-circuit-class** para mostrar las estadísticas de 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
CIRCLASE1            1             56              0
CIRCLASE2            0              0              0

TOTAL               26           3458             26
```

Interface

Utilice el mandato **interface** para seleccionar la interfaz serie a la que se referirán los mandatos de supervisión de la reserva de ancho de banda. *Los direccionadores que ejecutan las interfaces PPP (protocolo punto a punto) y Frame Relay dan soporte la reserva de ancho de banda.*

Sintaxis:

i**nterface** *número-interfaz*

Nota: Si se quieren entrar mandatos de reserva de ancho de banda para una interfaz nueva, este mandato debe ejecutarse antes de utilizar cualquier mandato de supervisión de la reserva de ancho de banda. Si sale del indicador de supervisión de la reserva de ancho de banda (BRS>) y quiere volver a supervisar la reserva de ancho de banda, primero deberá volver a entrar este mandato.

Para supervisar la reserva de ancho de banda para una interfaz en particular, escriba el número de la interfaz en el indicador de supervisión BRS>. A continuación podrá utilizar los mandatos de supervisión de reserva de ancho de banda que se describen en este capítulo.

Last

Utilice el mandato **last** para visualizar las últimas estadísticas que se guardaron de las clases-t. Las estadísticas de las clases-t se muestran en el mismo formato que las del mandato **counters**.

Sintaxis:

last

Last-circuit-class

Nota: Sólo se utiliza en la supervisión de Frame Relay.

Utilice el mandato **last-circuit-class** para visualizar las últimas estadísticas que se guardaron de las clases de circuitos. Las estadísticas de las clases-c se muestran en el mismo formato que las del mandato **counters-circuit-class**.

Sintaxis:

last-c**ircuit-class**

Reconfiguración dinámica del sistema de reserva de ancho de banda

En este apartado se describe la reconfiguración dinámica (DR) y cómo afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

El sistema de reserva de ancho de banda da soporte al mandato **delete interface** de CONFIG (Talk 6) sin restricciones.

Mandato activate interface de GWCON (Talk 5)

El sistema de reserva de ancho de banda da soporte al mandato **activate interface** de GWCON (Talk 5) sin restricciones.

El mandato **activate interface** de GWCON (Talk 5) da soporte a todos los mandatos específicos de la interfaz del sistema de reserva de ancho de banda.

Mandato reset interface de GWCON (Talk 5)

El sistema de reserva de ancho de banda da soporte al mandato **reset interface** de GWCON (Talk 5) sin restricciones.

El mandato **reset interface** de GWCON (Talk 5) da soporte a todos los mandatos específicos de la interfaz del sistema de reserva de ancho de banda.

Mandatos de cambio inmediato de CONFIG (Talk 6)

El sistema de reserva de ancho de banda da soporte a los siguientes mandatos CONFIG que permiten modificar inmediatamente el estado operativo del dispositivo. Estos cambios se guardan y se mantienen si el dispositivo se reinicia, si se vuelve a cargar 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 puede utilizarse para interfaces Frame Relay desde el indicador de nivel de circuito.
GWCON, feature brs, interface, assign **Nota:** Este mandato también puede utilizarse para interfaces Frame Relay desde el indicador de nivel de circuito.
GWCON, feature brs, interface, change-class **Nota:** Este mandato también puede utilizarse para interfaces Frame Relay desde el indicador de nivel de circuito.

GWCON, feature brs, interface, create-super-class **Nota:** Este mandato también puede utilizarse para interfaces Frame Relay desde el indicador de nivel de circuito.
GWCON, feature brs, interface, deassign **Nota:** Este mandato también puede utilizarse para interfaces Frame Relay desde el indicador de nivel de circuito.
GWCON, feature brs, interface, default-class **Nota:** Este mandato también puede utilizarse para interfaces Frame Relay desde el indicador de nivel de circuito.
GWCON, feature brs, interface, del-class **Nota:** Este mandato también puede utilizarse para interfaces Frame Relay desde el indicador de nivel de circuito.
GWCON, feature brs, interface, disable **Nota:** Este mandato también puede utilizarse para interfaces Frame Relay desde el indicador de nivel de circuito.
GWCON, feature brs, interface, enable **Nota:** Este mandato también puede utilizarse para interfaces Frame Relay desde el indicador de nivel de circuito.
GWCON, feature brs, interface, tag **Nota:** Este mandato también puede utilizarse para interfaces Frame Relay desde el indicador de nivel de circuito.
GWCON, feature brs, interface, untag **Nota:** Este mandato también puede utilizarse para interfaces Frame Relay desde el indicador de nivel de circuito.

Utilización de filtros MAC

En este capítulo se describe cómo utilizar el control de acceso al medio (MAC) para especificar filtros de paquetes que se aplicarán a los paquetes durante el proceso. Consta de los apartados siguientes:

Un filtro es un conjunto de reglas que se aplican a un paquete para determinar cómo manejarlo durante la transmisión por un puente. Los filtros MAC afectan únicamente al tráfico que se transmite por puentes.

Nota: Se permite el filtrado MAC del tráfico transmitido por túneles.

Durante el proceso de filtrado, los paquetes se procesan, se filtran o se identifican durante la transmisión por el puente. Las acciones son:

- **Procesado** – Se permite que los paquetes atraviesen el puente sin ser afectados.
- **Filtrado** – No se permite que los paquetes atraviesen el puente.
- **Identificado** – Se permite que los paquetes atraviesen el puente, pero se identifican con un número comprendido entre 1 y 64, que depende de un parámetro configurable.

Un filtro MAC consta de los objetos siguientes:

1. Elemento de filtro – regla única que se aplica al campo dirección o a una ventana arbitraria de datos de un paquete. El resultado de aplicar la regla es una condición verdadera (la comparación es satisfactoria) o falsa (no coincide).
2. Lista de filtro – que contiene una lista de uno o varios elementos de filtro.
3. Filtro – que contiene un conjunto de listas de filtro.

Filtros MAC y tráfico DLSw

Se puede filtrar el tráfico LLC entrante para la red DLSw implementando filtros MAC.

Para configurar un filtro para LLC, utilice el número de *red de puente* como número de interfaz del filtro. El número de red de puente se calcula sumando dos al número de interfaces configuradas por el direccionador. Para ver una lista de las interfaces, escriba el mandato **list devices** en el indicador `Config>`, o escriba **configuration** en el indicador +.

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

```
Ifc 0 Token Ring                    Slot: 1  Port: 1
Ifc 1 Token Ring                    Slot: 1  Port: 2
Ifc 2 Token Ring                    Slot: 2  Port: 1
Ifc 3 Token Ring                    Slot: 2  Port: 2
Ifc 4 Ethernet                      Slot: 4  Port: 1
Ifc 5 Ethernet                      Slot: 4  Port: 2
```

Cuando se configura un filtro para la red de puente, por ejemplo, el direccionador no descartará las tramas que coincidan con filtros de exclusión. Al contrario, reenviará las tramas al puente.

Parámetros de los filtros MAC

Para crear un filtro, se pueden especificar algunos o todos los parámetros siguientes:

- Dirección MAC origen o destino
- Datos que se compararán en el paquete
- Máscara que se aplicará a los campos del paquete que se van a filtrar
- Número de interfaz
- Clase Input u Output
- Clase Include, Exclude o Tag
- Valor de identificador (si se da la clase Identificar)

Parámetros de los elementos de filtro

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

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

Cada elemento de filtro especifica un tipo de dirección (SOURCE o DESTINATION) que se comparará con el tipo de dirección del paquete.

La máscara de dirección es una serie de números hexadecimales, que sirve para comparar las direcciones del paquete. La máscara se aplica a la dirección MAC (SOURCE o DESTINATION) del paquete antes de compararla con la dirección MAC especificada.

La longitud de la máscara de dirección debe ser igual a la de la dirección MAC. Se realizará una operación AND lógica entre los bytes especificados por la máscara de dirección y los bytes de la dirección MAC, antes de comparar si es igual a la dirección MAC especificada. Si no se especifica ninguna máscara, se supondrá que todos son 1.

Parámetros de las listas de filtro

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

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

A partir de uno o varios elementos de filtro se crea una lista de filtro. A cada lista de filtro se le asigna un nombre único.

Aplicar una lista de filtro a un paquete consiste en comparar cada elemento de filtro en el orden en que se añadieron a la lista. Si un elemento de filtro de la lista devuelve una condición TRUE (verdadera), la lista de filtro devolverá la acción que se le ha asignado.

Parámetros de los filtros

Los parámetros siguientes se utilizan para crear un filtro:

- Nombres de listas de filtro: *serie de caracteres ASCII 1 . . . serie de caracteres ASCII n*
- Número de interfaz: un *número de IFC*
- Sentido del puerto: INPUT u OUTPUT
- Acción por omisión: INCLUDE, EXCLUDE o TAG
- Identificador por omisión: un *valor de identificador*

Un filtro se crea asociando un grupo de nombres de listas de filtro con un número de interfaz y asignando una clase INPUT u OUTPUT. Aplicar un filtro a un paquete significa que debe aplicarse cada una de las listas de filtro asociadas a los paquetes que se reciben (INPUT) o que se envían (OUTPUT) para el número de interfaz especificada.

Si al evaluar un paquete, un filtro obtiene una condición INCLUDE, el paquete se reenvía. Si al evaluar un paquete, un filtro obtiene una condición EXCLUDE, el paquete se descartará. Si al evaluar un paquete, un filtro obtiene una condición TAG, el paquete se reenviará con un identificador.

Un parámetro adicional para cada filtro es la acción por omisión, que se ejecutará en caso de que ninguna de las comparaciones realizadas con sus listas de filtro haya sido satisfactoria. La acción por omisión es INCLUDE. Puede establecerse como INCLUDE, EXCLUDE o TAG. Si la acción por omisión es TAG, además tendrá que establecerse un valor de identificador.

Utilización de identificadores de los filtros MAC

En la lista siguiente se describen algunos usos de los identificadores de los filtros MAC:

- La reserva de ancho de banda y la función de filtrado MAC (MCF) manejan conjuntamente el filtrado de direcciones MAC utilizando identificadores. Por ejemplo, un usuario con reserva de ancho de banda puede categorizar el tráfico que pasa por un puente asignándole un identificador.
- El proceso de identificación consiste en crear un elemento de filtro en la consola de configuración de filtros MAC y asignarle un identificador. A continuación, el identificador se utiliza para configurar una clase de ancho de banda para todos los paquetes asociados con este identificador. El valor de los identificadores debe estar comprendido entre 1 y 64.
- Una vez creado un filtro con identificador en el proceso de configuración de filtros MAC, se utiliza el mandato **tag** de la reserva de ancho de banda (BRS) para asignar un nombre de identificador de BRS (TAG1, TAG2, TAG3, TAG4 o TAG5) al número de identificador del filtro MAC. A partir de ahora, el nombre de identificador de BRS se utilizará en el mandato de configuración **assign** de BRS para asignar el filtro MAC correspondiente a una clase de tráfico y prioridad de ancho de banda.
- Se pueden establecer hasta 5 direcciones MAC con identificador, con valores de 1 a 5. En primer lugar se buscará TAG1, después TAG2, y así sucesivamente hasta TAG5.

Los identificadores también pueden hacer referencia a “grupos” de un Túnel IP. Los extremos de un Túnel IP pueden pertenecer a un número indeterminado de

grupos, y recibir paquetes asignados a un grupo concreto mediante la función de identificación de filtros de direcciones MAC.

Configuración y supervisión de filtros MAC

En este capítulo se describe cómo acceder a los indicadores de configuración y supervisión de filtros MAC y cómo utilizar los mandatos disponibles. Consta de los apartados siguientes:

Acceso al indicador de configuración de filtros MAC

Utilice el mandato **feature** desde el proceso CONFIG para acceder a los mandatos de configuración de filtros MAC. El mandato **feature** le permite acceder a los mandatos de configuración de determinadas funciones externas al protocolo y a los procesos de configuración de la interfaz de red.

Para obtener una lista de las funciones disponibles en este release del software, escriba un interrogante después del mandato **feature**. Por ejemplo:

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

Para acceder al indicador de configuración de filtros MAC, entre el mandato **feature** seguido del *número de función* (3) o del *nombre corto* (MCF). Por ejemplo:

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

Una vez se accede al indicador de configuración de filtros MAC, pueden empezarse a entrar mandatos específicos de configuración. Siempre puede volver al indicador CONFIG escribiendo el mandato **exit** en el indicador de configuración de filtros MAC.

Mandatos de configuración de filtros MAC

En este apartado se resumen los mandatos de configuración de filtros MAC. Escriba los mandatos en el indicador `Filter config>`.

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

Tabla 5 (Página 1 de 2). Resumen de mandatos de configuración de filtros 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 xxxii.
Attach	Añade una lista de filtro a un filtro.
Create	Crea una lista de filtro o un filtro INPUT u OUTPUT.
Default	Establece para el filtro especificado la acción por omisión: EXCLUDE, INCLUDE o TAG.

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

Mandato	Función
Delete	Elimina toda la información asociada con una lista de filtro. También suprime un filtro creado con el mandato create.
Detach	Elimina una lista de filtro de un filtro.
Disable	Inhabilita totalmente la función de filtrado MAC o inhabilita un filtro determinado.
Enable	Habilita totalmente la función de filtrado MAC o inhabilita un filtro determinado.
List	Muestra un resumen de todas las listas de filtro y de todos los filtros configurados por el usuario. También genera una lista de las listas de filtro conectadas con este filtro y toda la información correspondiente al filtro.
Move	Vuelve a ordenar las listas de filtro conectadas con un filtro determinado.
Reinit	Reinicializa todo el sistema de filtrado MAC después de haber actualizado la configuración, sin afectar al resto del direccionador.
Set-Cache	Cambia el tamaño de la antememoria de un filtro.
Update	Añade o suprime información de una lista de filtro determinada. Le lleva al menú de submandatos apropiado.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiii.

Attach

Utilice el mandato **attach** para añadir a un filtro una lista de filtro.

Un filtro se crea asociando un grupo de listas de filtro con un número de interfaz. Una lista de filtro 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 filtro o un filtro INPUT u OUTPUT.

Sintaxis:

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

filter [input u output] *número-interfaz*

list *nombre-lista-filtros*

Crea una lista de filtro. El usuario debe dar nombre a la lista, que consiste en una serie de caracteres (nombre-lista-filtros) exclusiva de hasta 16 caracteres de longitud. Este nombre sirve para identificar la lista de filtro que se va a crear. Además, lo utilizan otros mandatos asociados con la lista de filtro.

filter [input u output] *número-interfaz*

Crea un filtro y lo pone en la red asociada con el sentido de entrada (INPUT) o salida (OUTPUT) de la interfaz indicada por el número de

interfaz. Por omisión, este filtro se crea sin listas de filtro conectadas, su acción por omisión es INCLUDE y está habilitado (ENABLED).

Default

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

Sintaxis:

def**ault** exclude *número-filtro*

include *número-filtro*

tag *número-ident número-filtro*

exclude *número-filtro*
Establece la acción por omisión del filtro (especificado por un número de filtro) como exclude.

include *número-filtro*
Establece la acción por omisión del filtro (especificado por un número de filtro) como include.

tag *número-ident número-filtro*
Establece la acción por omisión del filtro (especificado por un número de filtro) como TAG, y establece como número de identificador el valor de identificador asociado.

Delete

Utilice el mandato **delete** para eliminar toda la información asociada con una lista de filtro y para liberar la serie de caracteres asignada a la lista, de forma que pueda volver a utilizarse para nombrar una lista de filtro nueva. Si la lista de filtro está conectada a un filtro ya existente creado por el usuario, este mandato mostrará un mensaje de error en la consola y no eliminará nada. También se eliminarán todos los elementos de filtro que pertenezcan a la lista.

Además, este mandato también elimina los filtros creados con 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 filtro y libera la serie de caracteres asignada a la lista, de forma que pueda volver a utilizarse para nombrar una lista de filtro nueva. La lista de filtro debe ser una serie de caracteres entrada anteriormente en un mandato **create list**.

Si la lista de filtro está conectada a un filtro ya existente creado por el usuario, el mandato mostrará un mensaje de error en la consola y no eliminará nada. Además, cuando se ejecute el mandato, también se eliminarán todos los elementos de filtro que pertenezcan a la lista.

filter *número-filtro*
Suprime un filtro creado con el mandato **create filter**.

Detach

Utilice el mandato **detach** para suprimir el nombre de una lista de filtro (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 la función de filtrado MAC o para inhabilitar un filtro determinado.

Sintaxis:

di**sable** all

filter *número-filtro*

all Inhabilita totalmente la función de filtrado MAC. Sin embargo, si los filtros se habilitaron previamente, seguirán estando habilitados (ENABLED).

filter *número-filtro*
Inhabilita un filtro determinado. El parámetro número-filtro se corresponde con los números mostrados al ejecutar el mandato **list filters**.

Enable

Utilice el mandato **enable** para habilitar totalmente la función de filtrado MAC o para habilitar un filtro determinado.

Sintaxis:

en**able** all

filter *número-filtro*

all Habilita totalmente la función de filtrado MAC, aunque es posible que los propios filtros estén inhabilitados (DISABLED).

filter *número-filtro*
Habilita un filtro determinado. El parámetro número-filtro se corresponde con los números mostrados al ejecutar el mandato **list filters**.

List

Utilice el mandato **list** para mostrar un resumen de todos los filtros y listas de filtro configurados por el usuario. No se muestra la lista de todas las listas de filtro conectadas a un filtro. También se muestra la información siguiente:

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

Además, se muestra la información siguiente para cada filtro:

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

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

Por último, también genera una lista de las listas de filtro conectadas con este filtro y toda la información correspondiente al filtro.

Sintaxis:

l**ist** all

filter *número-filtro*

all Muestra un resumen de todas las listas de filtro y filtros configuradas.

filter *número-filtro*
Genera una lista de listas de filtro conectadas con el filtro especificado y toda la información correspondiente al filtro.

Move

Utilice el mandato **move** para volver a ordenar las listas de filtro conectadas al filtro especificado (por un parámetro número-filtro). La lista especificada por el nombre-lista-filtros1 se coloca inmediatamente delante de la lista especificada por el nombre-lista-filtros2.

Sintaxis:

m**ove** *nombre-lista-filtros1 nombre-lista-filtros2 número-filtro*

Reinit

Utilice el mandato **reinit** para reinicializar todo el sistema de filtrado MAC después de haber actualizado la configuración, sin afectar al resto del direccionador.

Sintaxis:

r**einit**

Set-Cache

Utilice el mandato **set-cache** para cambiar el tamaño por omisión de la antememoria (16) a un número comprendido entre 4 y 32768.

Sintaxis:

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

Update

Utilice el mandato **update** para añadir o eliminar información de una lista de filtro determinada. Si utiliza este mandato con el nombre-lista-filtros deseado, le llevará al indicador `Filter nombre-lista-filtros Config>` de la lista de filtro especificada. Desde este nuevo indicador se puede cambiar la información de la lista especificada.

El nuevo nivel de indicador se utiliza para añadir o eliminar elementos de filtro de listas de filtro. Es importante el orden en que se especifican los elementos de filtro de una lista de filtro dada, ya que determina el orden en que se aplicarán a un paquete.

Sintaxis:

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

Submandatos de actualización

Es este apartado se resumen los submandatos de configuración de filtros MAC. Estos submandatos se escriben en el indicador `Filter nombre-lista-filtros 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 xxxii.
Add	Añade filtros de direcciones MAC origen y destino o un filtro de ventana. Añade elementos de filtro a una lista de filtro.
Delete	Elimina elementos de filtro de una lista de filtro.
List	Muestra un resumen de todas las listas de filtro y filtros configuradas por el usuario. También genera una lista de las listas de filtro conectadas con este filtro y toda la información correspondiente al filtro.
Move	Vuelve a ordenar las listas de filtro conectadas al filtro especificado.
Set-Action	Configura un elemento de filtro para que evalúe la condición INCLUDE, EXCLUDE o TAG (con una opción número identificador).
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiii.

Utilice los submandatos siguientes para actualizar una lista de filtro.

Add

Utilice el submandato **add** para añadir elementos de filtro a una lista de filtro. Este submandato le permite añadir un número hexadecimal que se comparará con la dirección MAC origen o destino, o una secuencia de datos de ventana con una máscara que se comparará con los datos de un paquete.

Es importante el orden en que se añadan los elementos de filtro a una lista de filtro dada, ya que determina el orden en que se aplicarán a un paquete.

Cada vez que se ejecuta el submandato **add** se crea un elemento de filtro en la lista de filtro. Al primer elemento de filtro que se crea se le asigna el número de elemento de filtro 1, al siguiente, se le asigna el número 2, y así sucesivamente. Después de ejecutar satisfactoriamente un submandato **add**, el direccionador mostrará el número del elemento de filtro que se acaba de añadir.

La primera coincidencia que se produzca interrumpirá la aplicación de los elementos de filtro y la lista de filtro evaluará la condición INCLUDE, EXCLUDE o TAG, dependiendo de la acción asignada en la lista de filtro. Si ninguna de las comparaciones de los elementos de filtro de la lista de filtro produce una coincidencia, se devolverá la acción por omisión (INCLUDE, EXCLUDE o TAG) del filtro.

Sintaxis: a**dd** source *dir-MAC-hex máscara-hex*

destination *dir-MAC-hex máscara-hex*

window MAC *valor-desplaz datos-hex máscara-hex*

window INFO *valor-desplaz datos-hex máscara-hex*

source *dir-MAC-hex máscara-hex*
Añade un número hexadecimal que se comparará con la dirección MAC. El valor ***dir-MAC-hex*** debe ser un número par de dígitos hexadecimales de, como máximo, 16 dígitos de longitud y debe escribirse sin el prefijo 0x.

El parámetro máscara-hex debe ser de la misma longitud que la dirección MAC hexadecimal, y se realiza una operación AND lógica entre éste y la dirección MAC del paquete. El argumento máscara-hex por omisión es una serie de unos binarios.

El orden de bits del parámetro dir-MAC-hex puede especificarse en forma canónica o no canónica. El orden de bits canónico se especifica como un número hexadecimal (por ejemplo, 000003001234). También puede representarse como una serie de pares de dígitos hexadecimales separados por guiones (-) (por ejemplo, 00-00-03-00-12-34).

Un orden de bits no canónico se especifica como una serie de pares de dígitos hexadecimales separados por el signo de dos puntos (por ejemplo, 00:00:C9:09:66:49). Las direcciones MAC de los elementos de filtro siempre se mostrarán con guiones (-) o el signo de dos puntos (:) para distinguir las representaciones canónica y no canónica.

destination *dir-MAC-hex máscara-hex*
Actúa de la misma forma que el submandato **add source** excepto que la comparación se hace con la dirección MAC destino del paquete, en lugar de hacerse con la dirección origen.

window MAC *valor-desplaz datos-hex máscara-hex*
Añade un elemento de filtro de ventana desplazada que utiliza el desplazamiento especificado (calculado a partir del inicio de la trama) que compara los datos hexadecimales de la máscara, con los datos del paquete.

window INFO *valor-desplaz datos-hex máscara-hex*
Similar al mandato **add window mac** excepto que el desplazamiento se calcula respecto al inicio del campo información.

Delete

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

Cuando se ejecuta el submandato **delete**, se cubre cualquier hueco creado en la secuencia de números. Por ejemplo, si existen los elementos de filtro 1, 2, 3 y 4, y se elimina el elemento de filtro 3, el elemento de filtro número 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 elementos de filtro. Se mostrará la información siguiente de cada elemento de filtro de direcciones MAC:

- dirección MAC y máscara de dirección en forma canónica y no canónica.
- números de los elementos de filtro
- tipo de dirección (origen o destino)
- acción de la lista de filtro

Sintaxis:

list	canonical
	noncanonical
	mac-address canonical
	mac-address noncanonical
	window

canonical
Imprime una lista de todos los registros de los elementos de filtro de una lista de filtro, en la que aparecen los números de elemento, el tipo de dirección (SRC, DST), la dirección MAC y la máscara de dirección en forma canónica. También aparece la acción de la lista de filtro.

mac-address canonical
Imprime una lista de todos los registros de los elementos de filtro de una lista de filtro, en la que aparecen los números de elemento, el tipo de dirección (SRC, DST), la dirección MAC y la máscara de dirección en forma canónica. Además, aparece la acción de la lista de filtro.

noncanonical
Imprime una lista de todos los registros de los elementos de filtro de una lista de filtro, en la que aparecen los números de elemento, el tipo de dirección (SRC, DST), y la dirección MAC y la dirección de máscara en forma no canónica. También aparece la acción de la lista de filtro.

mac-address noncanonical
Imprime una lista de todos los registros de los elementos de filtro de una lista de filtro, en la que aparecen los números de elemento, el tipo de dirección (SRC, DST), y la dirección MAC y la dirección de máscara en forma no canónica. También aparece la acción de la lista de filtro.

window Imprime una lista de todos los registros de los elementos de filtro de la ventana desplazada de la lista de filtro, en la que aparecen los números de elemento, la base, el desplazamiento, los datos y la máscara. También aparece la acción de la lista de filtro.

Move

El submandato **move** vuelve a ordenar los elementos de filtro de la lista de filtro. El número del elemento de filtro especificado por el *nombre-elemento-filtro1* se coloca junto antes que el *nombre-elemento-filtro2* y se vuelve a numerar.

Sintaxis:

move	*nombre-elemento-filtro1 nombre-elemento-filtro2*

Set-Action

El submandato **set-action** le permite configurar un elemento de filtro para que evalúe una de las condiciones INCLUDE, EXCLUDE o TAG (con una opción número identificador). Si la comparación entre uno de los elementos de filtro de la lista de filtro y el contenido del paquete que se está considerando si filtrar o no, es satisfactoria, la lista de filtro evaluará la condición especificada. El valor por omisión es INCLUDE.

Sintaxis:

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

Acceso al indicador de supervisión de filtros MAC

Utilice el mandato **feature** desde el proceso GWCON para acceder a los mandatos de supervisión de filtros MAC. El mandato **feature** le permite acceder a los mandatos de supervisión de determinadas funciones del direccionador, externas al protocolo y a los procesos de supervisión de la interfaz de red.

Para obtener una lista de las funciones disponibles en este release del software, escriba un interrogante después del mandato **feature**. Por ejemplo:

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

Para acceder al indicador de supervisión de filtros MAC, entre el mandato **feature** seguido del número de función (3) o del nombre corto (MCF). Por ejemplo:

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

Una vez se accede al indicador de supervisión de filtros MAC, pueden empezarse a entrar mandatos específicos de supervisión. Siempre se puede volver al indicador GWCON escribiendo el mandato **exit** en el indicador de supervisión de filtros MAC.

Mandatos de supervisión de filtros MAC

En este apartado se resumen los mandatos de supervisión de filtros MAC. Entre estos mandatos en el indicador `Filter>`.

Tabla 7. Resumen de mandatos de supervisión de filtros 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 xxxii.
Clear	Borra las estadísticas de "un filtro" listadas en el mandato list filter.
Disable	Inhabilita globalmente el filtrado MAC o inhabilita "un filtro" determinado.
Enable	Habilita globalmente el filtrado MAC o habilita "un filtro" determinado.
List	Muestra un resumen de las estadísticas y valores de cada filtro que se está ejecutando actualmente en el direccionador.
Reinit	Reinicializa todo el sistema de filtrado MAC después de haber actualizado la configuración, sin afectar al 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 xxxiii.

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

Clear

Utilice el mandato **clear** para borrar las estadísticas de filtros.

Sintaxis:

c**lear** all

filter *número-filtro*

all Borra las estadísticas que se listan en el mandato **list all**.

filter *número-filtro*
Borra las estadísticas que se listan en el mandato **list filter**.

Disable

Utilice el mandato **disable** para inhabilitar globalmente el filtrado MAC. Este mandato no inhabilita individualmente todos los filtros.

El mandato también permite inhabilitar un filtro si se especifica su número de filtro. Este filtro se inhabilita sin modificar los registros de configuración. Si no se indica ningún argumento, la función de filtrado MAC se inhabilita globalmente.

Sintaxis:

d**isable** all

filter *número-filtro*

all Inhabilita globalmente el filtrado MAC. Este mandato no inhabilita individualmente todos los filtros.

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 indica ningún número de filtro, el filtrado MAC se inhabilita globalmente.

Enable

Utilice el mandato **enable** para habilitar globalmente el filtrado MAC. Este mandato no habilita individualmente todos los filtros.

El mandato también permite habilitar un filtro si se especifica su número de filtro. Este filtro se habilita sin modificar los registros de configuración. Si no se indica ningún argumento, el filtrado MAC se habilita globalmente.

Sintaxis:

enable all

filter *número-filtro*

all Habilita globalmente el filtrado MAC. Este mandato no habilita individualmente todos los filtros.

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 indica ningún número de filtro, el filtrado MAC se habilita globalmente.

List

Utilice el mandato **list** para mostrar un resumen de las estadísticas y valores de cada filtro que se está ejecutando actualmente en el direccionador. Cundo se ejecuta el mandato **list all**, se muestra la información siguiente de cada filtro:

- Acción por omisión
- Tamaño de la antememoria
- Identificador por omisión
- Estado (habilitado/inhabilitado)
- Número de paquetes filtrados como INCLUDE, EXCLUDE o TAG.

Además, si se ejecuta el mandato **list filter**, se muestra la información siguiente del filtro especificado:

- Toda la información que se muestra al ejecutar el mandato list all
- Todas las listas de filtro que se están ejecutando actualmente para este filtro:
  - Nombre de la lista
  - Acción de la lista
  - Identificador de la lista
  - Número de paquetes filtrados por cada lista de filtro.

Sintaxis:

list all

filter *número-filtro*

all Lista las estadísticas y valores de cada filtro que se está ejecutando actualmente en el direccionador.

filter *número-filtro*
Genera estadísticas y valores para cada filtro además de para todas las listas de filtro que se están ejecutando actualmente en el direccionador.

Reinit

Utilice el mandato **reinit** para reinicializar todo el sistema de filtrado MAC después de haber actualizado la configuración, sin afectar al resto del direccionador.

Sintaxis:

r**einit**

Soporte de reconfiguración dinámica de filtros MAC

En este apartado se describe la reconfiguración dinámica (DR) y cómo afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

La función de filtrado MAC da soporte al mandato **delete interface** de CONFIG (Talk 6) sin restricciones.

Mandato activate interface de GWCON (Talk 5)

El sistema de filtrado MAC da soporte al mandato **activate interface** de GWCON (Talk 5) teniendo en cuenta que:

Si se han definido filtros MAC para la interfaz recién activada, se reinicializarán todos los filtros MAC de todas las interfaces.

El mandato GWCON (Talk 5) **activate interface** da soporte a todos los mandatos específicos de las interfaces del sistema de filtrado MAC.

Mandato reset interface de GWCON (Talk 5)

El sistema de filtrado MAC da soporte al mandato **reset interface** de GWCON (Talk 5) teniendo en cuenta que:

Si se han definido filtros MAC para la interfaz recién restablecida, se reinicializarán todos los filtros MAC de todas las interfaces.

El mandato **reset interface** de GWCON (Talk 5) da soporte a todos los mandatos específicos de las interfaces del sistema de filtrado MAC.

Mandatos de restablecimiento de mandato de GWCON (Talk 5)

El sistema de filtrado MAC da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos del sistema de filtrado 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** da soporte a todos los mandatos específicos del sistema de filtrado MAC.

Mandato activate de CONFIG (Talk 6)

El sistema de filtrado MAC da soporte a los siguientes mandatos **activate** de CONFIG (Talk 6):

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** da soporte a todos los mandatos del sistema de filtrado MAC.

Utilización de la restauración de WAN

Este capítulo consta de los apartados siguientes:

Visión general de las funciones de restauración de WAN, redireccionamiento de WAN y de llamada por desbordamiento

Las funciones de restauración de WAN, de redireccionamiento de WAN y de llamada por desbordamiento tienen funciones parecidas y pueden confundirse. La intención de este apartado es ayudarle a decidir cuál de estas funciones le será útil y a encontrar la información necesaria para configurarlas.

En el capítulo "Configuración de la restauración de WAN" encontrará los mandatos de configuración de las tres funciones. Para obtener información adicional sobre las funciones de redireccionamiento de WAN y de llamada por desbordamiento, consulte el “La función de redireccionamiento de WAN” en la página 103.

Restauración de WAN

La restauración de WAN es la función más básica. Al utilizar esta función, se configura un enlace principal y uno secundario. En el caso de que el enlace principal diera un error, se arrancaría el enlace secundario, que asumiría las funciones del enlace principal. En el enlace secundario no se configura ninguna definición de protocolos, puesto que utiliza las del enlace principal.

Para la función de restauración de WAN:

- El enlace principal y el secundario están conectados.
- Sólo se puede configurar un enlace principal para que utilice un enlace secundario determinado.
- En el enlace secundario no se configura ninguna definición de protocolos (por ejemplo: direcciones de protocolos).
- El enlace principal puede ser una interfaz PPP serie o una interfaz PPP de multienlace. No puede ser una interfaz PPP de circuito de marcación.
- El enlace secundario debe ser una interfaz PPP de circuito de marcación o multienlace.
- Se debe habilitar la función WRS ejecutando el mandato **enable wrs**.
- Se debe habilitar la conexión entre los enlaces principal y secundario ejecutando el mandato **enable secondary-circuit**.

Nota: Si BRS está configurado para un enlace principal y éste es parte de una conexión entre el enlace principal y el secundario para la restauración de WAN, deberá configurar BRS para el enlace secundario. Lo normal, cuando se configura la función de restauración de WAN, es que el enlace secundario adopte la identidad del enlace principal. Sin embargo, esto no es

cierto para BRS; por lo tanto, BRS debe configurarse tanto para el enlace principal, como para el enlace secundario.

Redireccionamiento de WAN

La función de redireccionamiento de WAN es una función más avanzada. Al utilizar dicha función, se configura un enlace principal y uno alternativo. En el caso de que el enlace principal diera un error, se arrancaría el enlace alternativo. Los protocolos de direccionamiento (por ejemplo, RIP u OSPF) detectan la disponibilidad del nuevo enlace y ajustan las rutas utilizadas para reenviar paquetes.

Para la función de redireccionamiento de WAN:

- El enlace principal y el alternativo están conectados.
- Se pueden configurar varios enlaces principales de forma que utilicen el mismo enlace alternativo.
- Se deben configurar las definiciones de protocolos para el enlace alternativo.
- El enlace principal puede ser un enlace para el que se puedan configurar protocolos direccionables (por ejemplo, IP o IPX). Por ejemplo, el enlace principal puede ser una interfaz LAN, PPP, Frame Relay o una interfaz X.25 serie, o un circuito de marcación PPP o Frame Relay. Los siguientes tipos de interfaz no pueden ser enlaces principales: interfaces SDLC serie, interfaces SRLY serie y redes base como V.25bis y RDSI.
- El enlace alternativo puede ser un enlace para el que se puedan configurar protocolos direccionables (por ejemplo IP o IPX) , y el tipo de enlace de datos del enlace alternativo debe ser distinto del del enlace principal. Por ejemplo, el enlace alternativo puede ser una interfaz LAN, PPP, Frame Relay, o una interfaz X.25 serie, o un circuito de datos PPP o Frame Relay. Los siguientes tipos de interfaz no pueden ser enlaces alternativos: interfaces SDLC serie, interfaces SRLY serie, y redes base como V.25bis y RDSI.
- Si el enlace principal es un circuito de marcación, no puede ser un circuito de llamadas a petición. Para configurar un circuito de marcación de forma que no sea un circuito de llamadas a petición, debe configurarlo con el mandato **set idle 0** en el indicador de marcación `Circuit Config>`. Para obtener más información, consulte el apartado “Configuración y supervisión de circuitos de marcación”, en el *Access Integration Services Guía del usuario de software*.

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

  Nota: Los circuitos de marcación I.430/I.431 y T1/E1 canalizado, pueden utilizarse como WRS principal sin tener que configurarlos explícitamente.
- Se debe habilitar la función WRS ejecutando el mandato **enable wrs**.
- Se debe habilitar la conexión entre los enlaces principal y alternativo ejecutando el mandato **enable alternate-circuit**.
- Opcionalmente se pueden configurar las horas de estabilización, de estabilización de rutas y de inicio y fin de reversión, para controlar la reversión al enlace principal.
- Si el enlace alternativo es X.25, debería utilizar el mandato **national-personality set disconnect-procedure active** al configurar la interfaz X.25 del direccionador que tiene la función de redireccionamiento de WAN habilitada, y

el mandato **national-personality set disconnect-procedure passive** al configurar la interfaz X.25 del otro direccionador.

Llamada por desbordamiento

La función de llamada por desbordamiento es parecida a la de redireccionamiento de WAN, con la diferencia de que no es necesario que el enlace principal dé un error para arrancar el enlace alternativo. En cambio, se supervisa la utilización del enlace principal y, si se supera un umbral, se arranca el enlace alternativo. Además, no se cargan todos los protocolos en el enlace alternativo. En el enlace alternativo sólo se carga IP y el resto de protocolos siguen utilizando el enlace principal, a menos que se desactive.

Si el enlace principal se desactiva, el redireccionamiento de WAN toma el control y todos los protocolos configurados para la interfaz alternativa pueden empezar a detectar y utilizar rutas de la interfaz alternativa.

Para la llamada por desbordamiento:

- La llamada por desbordamiento utiliza la conexión entre los enlaces principal y alternativo de una conexión de un redireccionamiento de WAN.
- Se debe configurar una conexión de un redireccionamiento de WAN para poder utilizar la llamada por desbordamiento y se aplican todas las restricciones de la configuración del redireccionamiento de WAN.
- El enlace principal de una conexión de un redireccionamiento de WAN que utilizará la llamada por desbordamiento, debe ser Frame Relay.
- Para utilizar la llamada por desbordamiento, se debe utilizar el protocolo de direccionamiento OSPF.
- Se debe utilizar el mandato **enable dial-on-overflow** para configurar los umbrales de aumentar y de reducir, el intervalo de supervisión del ancho de banda y el tiempo mínimo que el enlace alternativo estará activo.
- Las horas de estabilización, de estabilización de rutas y de inicio y fin de reversión, no afectan al funcionamiento de la llamada por desbordamiento.

Para obtener más información sobre el redireccionamiento de WAN, consulte “La función de redireccionamiento de WAN” en la página 103.

Antes de empezar

Antes de configurar la restauración de WAN, debe disponer de:

1. Una interfaz serie principal (una línea cedida) configurada para PPP. Para el direccionador se puede utilizar cualquier interfaz serie.
2. Una interfaz con los circuitos de marcación asociados configurada para el direccionador. Como red base, se puede utilizar una interfaz RDSI o V.25bis.
3. Un circuito de marcación secundario configurado para establecer conexión si la interfaz principal se desactiva. Para configurar un circuito de marcación para que haga esto, establezca el temporizador de desocupado a cero ejecutando el mandato **set idle**, en el indicador de marcación `Circuit Config>`. Este mandato evita que el circuito de marcación sea un circuito de llamadas a petición.

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

   Nota: No configure direcciones de protocolos para la interfaz secundaria. Cuando el enlace secundario (circuito de marcación) está activo, utilizará las asignaciones de protocolos de la interfaz principal.

5. Un circuito de marcación secundario en el otro extremo del enlace, configurado sólo para recibir llamadas. Ejecute el mandato **set calls inbound** en el indicador `Circuit Config>`.

Procedimiento de configuración de la restauración de WAN

En este apartado se describen los pasos necesarios para configurar la restauración de WAN. Antes de empezar, ejecute el mandato **list device** en el indicador `Config>`, para obtener una lista de los números de interfaz de los distintos dispositivos.

Para configurar la restauración de WAN en el direccionador, siga los pasos siguientes :

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

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

2. Asigne un circuito de marcación secundario a la interfaz principal. Este es el circuito de reserva de la interfaz principal. 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 se acaba de añadir. Por ejemplo:

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

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

   ```
   WRS Config>enable wrs
   ```

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

Configuración del circuito de marcación secundario

Para configurar un circuito de marcación:

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

   ```
   Config> list device
   ```

   Si no se obtiene ninguna interfaz PPP de circuito de marcación, 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 desde el indicador `Config>` la interfaz secundaria (circuito de marcación), de forma que su tipo de enlace de datos sea el mismo que el de la interfaz principal (PPP):

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

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

   ```
   Config>
   network 3
   ```

4. Seleccione la interfaz de la red base del circuito de marcación. La red base puede ser V.25bis, ó RDSI.

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

5. Establezca el temporizador de desocupado a 0 (0=fijo) así:

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

6. Establezca uno de los extremos de la conexión de reserva para que reciba las llamadas (por ejemplo, el direccionador A):

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

7. Establezca el otro extremo de la conexión de reserva para que inicie las llamadas (por ejemplo, el direccionador B):

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

Notas:

1. No utilice el mandato **set calls both**. Al establecer los circuitos individualmente se evitarán colisiones entre intentos de conexión de entrada y de salida.
2. No configure ninguna dirección de reenvío (por ejemplo, IP, IPX, etc.) para el circuito de marcación. Las asignaciones de protocolos de la interfaz principal se utilizarán en la interfaz secundaria (circuito de marcación) cuando esté activa.
3. Para obtener instrucciones sobre cómo configurar la interfaz RDSI, consulte el apartado “Utilización de la interfaz RDSI”, en el *Access Integration Services Guía del usuario de software*.
4. Para obtener instrucciones sobre la configuración de la interfaz V.25bis, consulte el apartado “Utilización de la interfaz V.25bis”, en el *Access Integration Services Guía del usuario de software*.

Configuración y supervisión de la restauración de WAN

En este capítulo se describen los mandatos de configuración y de funcionamiento de la restauración de WAN. Consta de los apartados siguientes:

Nota: Consulte el apartado "Configuración y supervisión de circuitos de marcación", del *Access Integration Services Guía del usuario de software* para obtener más información sobre la configuración de circuitos de marcación. Un circuito de marcación puede utilizarse como interfaz si se configura el redireccionamiento de WAN.

Mandatos de configuración de la restauración de WAN, del redireccionamiento de WAN y de la llamada por desbordamiento

Los mandatos de configuración de la restauración de WAN le permiten crear o modificar la configuración de la interfaz de la restauración de WAN. En este apartado se ofrece un resumen de los mandatos de configuración de la restauración de WAN y, a continuación, se explican con más detalle.

La Tabla 8 lista los mandatos de configuración de la restauración de WAN y sus funciones. Entre los mandatos en el indicador `WRS Config>`. Para acceder al indicador `WRS Config>`, escriba **feature wrs** en el indicador `Config>`.

Tabla 8. Resumen de los mandatos de configuración de la 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 xxxii.
Add	Añade una correlación de principal a secundario (para la restauración de WAN) o principal a alternativo (para el redireccionamiento de WAN).
Disable	Inhabilita WRS, o una correlación de un único circuito secundario o alternativo.
Enable	Habilita WRS, o una correlación de un único circuito secundario o alternativo.
List	Muestra la configuración actual de la restauración de WAN.
Remove	Elimina una correlación principal a secundario o principal a alternativo, creada previamente con el mandato add.
Set	Establece los valores de los temporizadores de estabilización, estabilización de ruta y hora de reversión.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxiii.

Add

Utilice el mandato **add** para identificar un circuito de marcación secundario o alternativo, o una interfaz de enlace cedida para un enlace serie principal.

Sintaxis:

a**dd** alternate-circuit

secondary-circuit

alternate-circuit

El mandato **add alternate-circuit** enlaza una interfaz alternativa con una interfaz principal, para los propósitos del redireccionamiento de WAN. Se pueden asignar varias interfaces principales a una sola interfaz alternativa. El tipo del enlace alternativo no tiene por que ser el mismo que el del enlace principal (por ejemplo, el tipo del enlace alternativo puede ser un circuito PPP de marcación y el del enlace principal puede ser una línea Frame Relay cedida).

Ejemplo:

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

Alternate interface number

Es el número de la interfaz que se ha asignado antes como interfaz alternativa. Como interfaz alternativa se puede elegir entre una interfaz LAN, PPP, Frame Relay, una interfaz X.25 serie, o un circuito PPP de marcación o Frame Relay. El valor por omisión es 0.

Primary interface number

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

secondary-circuit

sl mandato **add secondary-circuit** enlaza una interfaz secundaria con una interfaz principal, para los propósitos de la restauración de WAN. Ambas interfaces deben haberse configurado previamente. Se puede asignar una sola interfaz secundaria a la interfaz principal 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 del circuito de marcación asignado previamente al añadir el dispositivo a la interfaz secundaria. Cualquier circuito PPP de marcación o interfaz PPP de multienlace puede ser una interfaz secundaria. El valor por omisión es 0.

Primary interface number

Es el número de interfaz de la interfaz principal asignado al añadir el dispositivo. Una interfaz principal puede ser cual-

quier línea alquilada definida previamente y que ejecute PPP. El valor por omisión es 0.

Disable

Utilice el mandato **disable** para inhabilitar la función de restauración de WAN, o para inhabilitar una conexión entre los enlaces principal y secundario para la restauración de WAN, o para inhabilitar una conexión entre los enlaces principal y alternativo para el redireccionamiento de WAN, o para inhabilitar la llamada por desbordamiento para una conexión entre los enlaces principal y alternativo.

Sintaxis:

disable alternate-circuit

dial-on-overflow

secondary-circuit

wrs

alternate-circuit *número-interfaz*

Inhabilita la conexión entre los enlaces principal y alternativo para el redireccionamiento de WAN.

Ejemplo:

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

Alternate interface number

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

dial-on-overflow *número-interfaz-alternativa*

Inhabilita la llamada por desbordamiento para todas las conexiones entre los enlaces principal y alternativo que utilizan un enlace alternativo determinado.

Ejemplo:

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

Alternate interface number

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

secondary-circuit *número-interfaz*

No permite que una interfaz secundaria restaure una interfaz principal asociada concreta, hasta que se ejecute el próximo mandato **enable secondary-circuit** en la consola WRS. Ambas interfaces deben haber sido previamente configuradas y enlazadas en la configuración WRS.

Ejemplo:

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

Secondary interface number

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

wrs Inhabilita globalmente en el direccionador la función de restauración de WAN. Esto significa que también se inhabilitan las funciones de redireccionamiento de WAN y de llamada por desbordamiento.

Enable

Utilice el mandato **enable** para habilitar la restauración de WAN, o para habilitar una conexión entre los enlaces principal y secundario para la restauración de WAN, o para habilitar una conexión entre los enlaces principal y alternativo para el redireccionamiento de WAN, o para habilitar la llamada por desbordamiento para una conexión entre los enlaces principal y alternativo.

Sintaxis:

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

dial-on-overflow

Habilita la llamada por desbordamiento y permite establecer parámetros para controlar el funcionamiento de la llamada por desbordamiento.

Ejemplo:

```
WRS>enable 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!
```

Primary interface number

Es el número de interfaz de la interfaz principal para la que se está habilitando la llamada por desbordamiento. El valor por omisión es 0.

add-threshold

Determina si se cargará una interfaz alternativa para obtener ancho de banda adicional. Este valor se expresa como un porcentaje de la velocidad de la línea configurada para la interfaz principal. El valor por omisión es el 90%.

drop-threshold

Determina cuando dejará de ser necesaria una interfaz alternativa que ofrece ancho de banda adicional. Este valor se

expresa como un porcentaje de la velocidad de la línea configurada para la interfaz principal. El valor por omisión es el 60%.

bandwidth monitoring interval
Determina con qué frecuencia se supervisará el ancho de banda de la interfaz principal para comprobar los valores *umbral de aumentar* y *umbral de reducir*. El valor por omisión es 15 segundos.

Minimum time to keep alternate up
Este período de tiempo debe ser lo suficientemente largo como para permitir que el direccionador establezca una ruta nueva cuando el tráfico IP del 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 principal para el enlace secundario indicado.

Ejemplo:

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

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

wrs Habilita la función de restauración de WAN en el direccionador. Esto significa que si las funciones de redireccionamiento de WAN y de llamada por desbordamiento están configuradas, también se habilitarán.

List

Utilice el mandato **list** para ver la información de configuración global de la función y la información de configuración de la llamada por desbordamiento, de las conexiones entre el enlace principal y el secundario para la restauración de WAN y de las conexiones entre el enlace principal y el alternativo para el redireccionamiento de WAN.

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 eliminar la correlación entre una interfaz alternativa o secundaria (de reserva) y la interfaz principal.

Sintaxis:

remove alternate-circuit

secondary-circuit

alternate-circuit *número-interfaz-alternativa número-interfaz-principal*

Elimina la correlación entre una interfaz alternativa (de reserva) y la interfaz principal para el redireccionamiento de WAN. Ambas interfaces deben haber sido previamente asignadas y enlazadas con el mandato **add alternate-circuit**.

número-interfaz-alternativa

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

número-interfaz-principal

Es el número de interfaz de la interfaz principal enlazada previamente a la interfaz 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-principal*

Elimina la correlación entre una interfaz secundaria (de reserva y la interfaz principal para la restauración de WAN. Ambas interfaces deben haber sido previamente asignadas y enlazadas con el mandato **add secondary-circuit**.

número-interfaz-secundaria

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

número-interfaz-principal

Es el número de interfaz de la interfaz principal enlazada previamente a la interfaz 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 del 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 utilizarán los enlaces que no tienen configuradas horas de estabilización y de primera estabilización.

first-stabilization

Establece el valor por omisión de la primera estabilización que utilizarán los enlaces que no tengan configurada una hora de primera estabilización.

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

stabilization

Establece el valor por omisión de estabilización que utilizarán los enlaces que no tengan configurada una hora de estabilización.

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

first-stabilization

Establece el número de segundos que esperará el direccionador durante la inicialización, antes de que el direccionamiento del enlace principal, si éste no está activo, se pase al enlace alternativo.

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 de la interfaz principal para la que se está estableciendo la primera estabilización. El valor por omisión es 0.

First primary stabilization time

Hora de estabilización de esta interfaz principal. El valor por omisión es 1.

routing-stabilization

Establece el valor de estabilización de ruta. Este parámetro define el número de segundos que, tanto el enlace principal como el enlace alternativo, permanecerán activos después de detectar que el enlace principal está activo y que el tiempo de estabilización, si se ha definido, se ha agotado. La hora de estabilización de ruta está definida de forma que los protocolos de direccionamiento, como OSPF o RIP, tengan tiempo suficiente para reconocer la disponibilidad de una ruta nueva. Sin el temporizador de estabilización de ruta, el tráfico podría ser interrumpido durante varios segundos, en el intervalo de tiempo que transcurre desde que se inhabilita la ruta alternativa hasta que se descubre la ruta principal.

Si el enlace alternativo estaba activo antes de la redirección, éste sigue activo y se hace caso omiso del temporizador de estabilización de ruta. Si el enlace alternativo se desactivó antes o durante la redirección, el enlace alternativo sigue desactivado y se hace caso omiso del temporizador de estabilización de ruta y del 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 configuradas 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 que deben transcurrir después de que se detecte por primera vez que el enlace principal está activo y antes de que empiece el proceso de reinicialización del direccionamiento en el enlace principal. Cuando se agota el tiempo de estabilización, se desactivará el enlace alternativo, a menos que se haya configurado el temporizador de estabilización de ruta. El temporizador de estabilización de ruta empezará a contar tan pronto como se agote el tiempo de estabilización y mantendrá activos los enlaces principal y alternativo el tiempo suficiente para mantener el tráfico del enlace alternativo hasta que los protocolos de direccionamiento, como OSPF y RIP, vuelvan a establecer la ruta en el enlace principal.

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 de la interfaz principal para la que se está definiendo la estabilización. El valor por omisión es 0.

Primary stabilization time

La hora de estabilización de la interfaz principal. El valor por omisión es 1.

start-time-of-day-revert-back

La hora del día en que el direccionador puede revertir a la ruta principal. El direccionador puede revertir a la interfaz principal en cualquier momento entre la hora de inicio y de fin de reversión. Sólo se revertirá a la interfaz principal si ésta 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 de la interfaz principal para la que se está estableciendo la primera estabilización. El valor por omisión es 0.

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

Este tiempo señala la hora de inicio de la ventana de reversión. El direccionador puede revertir a la interfaz principal en cualquier momento entre la hora de inicio y de fin de reversión. Sólo se revertirá a la interfaz principal si ésta está activa y se cumplen los parámetros de estabilización. El valor por omisión es 1.

stop-time-of-day-revert-back

Este tiempo señala la hora final de la ventana de reversión. El direccionador puede revertir a la interfaz principal en cualquier momento entre la hora de inicio y de fin de reversión. Sólo se revertirá a la interfaz principal si ésta 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 de la interfaz principal para la que se está estableciendo la primera estabilización. El valor por omisión es 0.

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

Este tiempo señala la hora final de la ventana de reversión. El direccionador puede revertir a la interfaz principal en cualquier momento entre la hora de inicio y de fin de reversión. Sólo se revertirá a la interfaz principal si ésta está activa y se cumplen los parámetros de estabilización. El valor por omisión es 1.

Acceso al proceso de supervisión de interfaces de la restauración de WAN

Para acceder al proceso de supervisión de interfaces de la restauración de WAN, escriba el mandato siguiente en el indicador GWCON (+):

```
+ feature wrs
```

Mandatos de supervisión de la restauración de WAN

Los mandatos de supervisión de la restauración de WAN (WRS) le permiten supervisar el estado de las conexiones entre los enlaces principal y secundario de la restauración de WAN, de las conexiones entre los enlaces principal y alternativo del redireccionamiento de WAN y de la llamada por desbordamiento. Las modificaciones del estado de funcionamiento de la restauración de WAN, del redireccionamiento de WAN y de la llamada por desbordamiento hechas desde la interfaz de supervisión, no tendrán efecto después de reinicializar el direccionador.

Acceda al indicador WRS escribiendo **feature wrs** en el indicador GWCON (+). La Tabla 9 muestra una lista de los mandatos de WRS y sus funciones, y en los apartados siguientes se explican con más detalle.

Tabla 9. Mandatos de supervisión de la 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 xxxii.
Clear	Borra las estadísticas de supervisión que se muestran con el mandato **list**.
Disable	Inhabilita el WRS, o un enlace secundario o alternativo individuales, o la llamada por desbordamiento.
Enable	Habilita el WRS, o un enlace secundario o alternativo individuales, o la llamada por desbordamiento.
List	Muestra la información de supervisión de uno o todos los circuitos alternativos o secundarios.
Set	Establece los valores de los temporizadores de estabilización, estabilización de ruta y hora de reversión.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiii.

Clear

Utilice el mandato **clear** para borrar las estadísticas de la restauración de WAN, redireccionamiento de WAN y llamada por desbordamiento, que se muestran al ejecutar el mandato **list**.

Sintaxis:

c**lear**

Nota: Este mandato borra el *Período de restauración más largo*, pero no borra el *Período de restauración más reciente*. En el ejemplo del mandato **list** puede verse una pantalla de ejemplo.

Disable

Utilice el mandato **disable** para inhabilitar totalmente la función de restauración de WAN, inhabilitar la restauración de una interfaz principal determinada a partir de su interfaz secundaria asociada, inhabilitar una interfaz alternativa, o inhabilitar la llamada por desbordamiento.

Sintaxis:

d**isable** alternate-circuit
dial-on-overflow
secondary-circuit
wrs

alternate-circuit

Inhabilita una conexión entre los enlaces principal y alternativo para el redireccionamiento de WAN. Pueden haber varias conexiones que utilicen el mismo enlace alternativo. Este mandato inhabilita todas las conexiones que utilizan 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 la llamada por desbordamiento para la conexión entre los enlaces principal y alternativo, sin cambiar el estado habilitado o inhabilitado del redireccionamiento de WAN para esta conexión. Si la llamada por desbordamiento está direccionando activamente, se interrumpirá cuando termine el próximo intervalo de supervisión.

secondary-circuit

Inhabilita la restauración de una interfaz principal concreta por parte de su interfaz secundaria asociada hasta que se ejecute el próximo mandato **restart**, **reload** o **enable secondary-circuit**. Ambas interfaces deben haber sido previamente configuradas y enlazadas en la configuración WRS.

Normalmente, en **talk 5** (GWCON), el mandato **disable** hace que la interfaz se inactive y permanezca inactiva. Sin embargo, esto no es cierto para la restauración de WAN. El mandato **disable** aplicado a la interfaz secundaria, no inhabilita la propia interfaz. Sólo inhabilita la llamada actual (o sea, hace que las llamadas activas se desconecten). Para inhabilitar la utilización del circuito secundario, deberá ejecutar el mandato **disable secondary-circuit** en el indicador de supervisión de la restauración de WAN e inhabilitar la interfaz secundaria en el indicador GWCON de mayor nivel.**Ejemplo:**

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

Secondary interface number

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

wrs Si se inhabilita WRS, se inhabilita en el direccionador la restauración de WAN, el redireccionamiento de WAN y la llamada por desbordamiento hasta la próxima ejecución del mandato **restart**, **reload** o **enable WRS**.

Enable

Utilice el mandato **enable** para habilitar la interfaz de la restauración de WAN, habilitar la restauración de un enlace principal a partir de un circuito secundario, habilitar un circuito alternativo, o habilitar la llamada por desbordamiento.

Sintaxis:

en**able** alternate-circuit

dial-on-overflow

secondary-circuit

wrs

alternate-circuit

Habilita las conexiones entre los enlaces principal y alternativo para el redireccionamiento de WAN, para todas las conexiones que utilicen el enlace 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 la llamada por desbordamiento y permite establecer parámetros para controlar la llamada por desbordamiento. Opcionalmente, permite que el protocolo IP se conecte inmediatamente con el circuito alternativo, como si se hubiera superado el umbral de aumentar.

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 principal para el enlace secundario indicado.

Ejemplo:

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

Secondary interface number

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

wrs Habilita en el direccionador la función de restauración de WAN. Para que funcione la restauración de WAN, el redireccionamiento de WAN o la llamada por desbordamiento, es necesario habilitar está función.

Set

Utilice el mandato **set** para establecer los parámetros del 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 utilizarán los enlaces que no tienen configuradas horas de estabilización y de primera estabilización.

Ejemplo:

```
WRS Config>set default ?
FIRST-STABILIZATION
STABILIZATION
```

first-stabilization

Establece el valor por omisión de la primera estabilización que utilizarán los enlaces que no tengan configurada una hora de primera estabilización.

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

stabilization

Establece el valor por omisión de estabilización que utilizarán los enlaces que no tengan configurada una hora de estabilización.

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

first-stabilization

Establece el número de segundos que esperará el direccionador durante la inicialización, antes de que el direccionamiento del enlace principal, si éste no está activo, se pase al enlace alternativo.

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 de la interfaz principal para la que se está estableciendo la primera estabilización. El valor por omisión es 0.

First primary stabilization time

Hora de estabilización de esta interfaz principal. El valor por omisión es 1.

routing-stabilization

Establece el valor de estabilización de ruta. Este parámetro define el número de segundos que, tanto el enlace principal como el enlace alternativo, permanecerán activos después de detectar que el enlace principal está activo y que el tiempo de estabilización, si se ha definido, se ha agotado. La hora de estabilización de ruta está definida de forma que los protocolos de direccionamiento, como OSPF o RIP, tengan tiempo suficiente para reconocer la disponibilidad de una ruta nueva. Sin el temporizador de estabilización de ruta, el tráfico podría ser interrumpido durante varios segundos, en el intervalo de tiempo que transcurre desde que se inhabilita la ruta alternativa hasta que se descubre la ruta principal.

Si el enlace alternativo estaba activo antes de la redirección, éste sigue activo y se hace caso omiso del temporizador de estabilización de ruta. Si el enlace alternativo se desactivó antes o durante la redirección, el enlace alternativo sigue desactivado y se hace caso omiso del temporizador de estabilización de ruta y del 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 configuradas 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 que deben transcurrir después de que se detecte por primera vez que el enlace principal está activo y antes de que empiece el proceso de reinicialización del direccionamiento en el enlace principal. Cuando se agota el tiempo de estabilización, se desactivará el enlace alternativo, a menos que se haya configurado el temporizador de estabilización de ruta. El temporizador de estabilización de ruta empezará a contar tan pronto como se agote el tiempo de estabilización y mantendrá activos los enlaces principal y alternativo el tiempo suficiente para mantener el tráfico del enlace alternativo hasta que los protocolos de direccionamiento, como OSPF y RIP, vuelvan a establecer la ruta en el enlace principal.

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 de la interfaz principal para la que se está definiendo la estabilización. El valor por omisión es 0.

Primary stabilization time

La hora de estabilización de la interfaz principal. El valor por omisión es 1.

start-time-of-day-revert-back

Establece la hora del día en que el direccionador podrá revertir a la ruta principal. El direccionador puede revertir a la interfaz principal en cualquier momento entre la hora de inicio y de fin de reversión. Sólo se revertirá a la interfaz principal si ésta 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 de la interfaz principal para la que se está estableciendo la primera estabilización. El valor por omisión es 0.

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

Este tiempo señala la hora de inicio de la ventana de reversión. El direccionador puede revertir a la interfaz principal en cualquier momento entre la hora de inicio y de fin de reversión. Sólo se revertirá a la interfaz principal si ésta está activa y se cumplen los parámetros de estabilización. El valor por omisión es 1.

stop-time-of-day-revert-back

Este tiempo señala la hora final de la ventana de reversión. El direccionador puede revertir a la interfaz principal en cualquier momento entre la hora de inicio y de fin de reversión. Sólo se revertirá a la interfaz principal si ésta 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 de la interfaz principal para la que se está estableciendo la primera estabilización. El valor por omisión es 0.

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

Este tiempo señala la hora final de la ventana de reversión. El direccionador puede revertir a la interfaz principal en cualquier momento entre la hora de inicio y de fin de reversión. Sólo se revertirá a la interfaz principal si ésta está activa y se cumplen los parámetros de estabilización. El valor por omisión es 1.

List

Utilice el mandato **list** para ver la información de supervisión de una o de todas las conexión entre los enlaces principal y secundario de la restauración de WAN, o de una o todas las conexiones entre los enlaces principal y alternativo del redireccionamiento de WAN.

Sintaxis:

list all

alternate-circuit

secondary-circuit

summary

all Proporciona información resumida, seguida por la información específica de 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
Número de veces que el enlace principal ha dado un error, haciendo que el direccionador intente activar un enlace secundario.

Completions
Número de intentos satisfactorios de restauración, en los que se ha activado y utilizado el enlace secundario.

Total packets forwarded
Número total de paquetes reenviados por la interfaz secundaria. Es la suma del número de paquetes reenviados en ambos sentidos, y el valor se acumulará en cada restauración satisfactoria, hasta que se ejecute el mandato de reiniciar o borrar las estadísticas de restauración.

Longest Completed Restoral Period
Este campo muestra en horas, minutos y segundos, el tiempo más largo que ha estado en funcionamiento la función de restauración, sin contar el tiempo de funcionamiento actual.

Total Overflow Attempts
Número de intentos debidos a un desbordamiento.

Completions
Número de intentos satisfactorios debidos a un desbordamiento, en los que se ha activado y utilizado el enlace secundario.

Longest Completed Overflow Period
Muestra en horas, minutos y segundos, el tiempo más largo que ha estado en funcionamiento la función de llamada por desbordamiento, sin contar el tiempo de funcionamiento actual.

Primary Net Interface
La interfaz que está siendo respaldada por la interfaz secundaria asociada.

Secondary Net Interface
El circuito de marcación que se está utilizando para respaldar la interfaz principal asociada.

Restoral Enabled
Indica que la restauración de esta interfaz principal está actualmente habilitada.

Restoral Active
Indica si la restauración está activa o no.

Current/Longest Duration
Indica en horas, minutos y segundos, el tiempo actual y el más largo de funcionamiento de la interfaz de red secundaria.

Primary Net Interface
La interfaz que está siendo respaldada por la interfaz alternativa asociada.

Alternate Net Interface
La interfaz alternativa que se está utilizando para respaldar la interfaz principal asociada.

Re-route/Overflow Enabled
Indica si las funciones de redireccionamiento y de desbordamiento están habilitadas o no.

Re-route/Overflow Active
Indica si las funciones de redireccionamiento y de desbordamiento están activas o no.

Recent Re-route Overflow Duration
Indica, en horas, minutos y segundos, el tiempo más reciente en que la interfaz de red alternativa ha sido redireccionada o desbordada.

Alternate-circuit
Proporciona valores totales para un circuito alternativo. Permite que el operador encargado de la supervisión, recupere el estado del redireccionamiento de WAN y las estadísticas asociadas para cada interfaz alternativa y sus interfaces principales asociadas.

Ejemplo:

```
WRS>li alt 7
Primary    1:FR/0 Frame Relay V.35/V.36
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 esta siendo respaldada por la interfaz alternativa asociada.

Alternate Interface
El circuito de marcación que se está utilizando para respaldar la interfaz principal asociada.

Reroute Enabled
Indica si el redireccionamiento de esta interfaz principal está actualmente habilitado.

Overflow Enabled
Indica si el desbordamiento de esta interfaz principal está actualmente habilitado.

Primary first stabilization
Número de segundos que se esperará el direccionador durante la inicialización antes de que el direccionamiento del enlace principal, si éste no está activo, se pase al enlace alternativo.

First stabilization
Número de segundos que deben transcurrir después de que se detecte por primera vez que el enlace principal está activo y antes de que se devuelva el direccionamiento del enlace alternativo al principal. El direccionamiento continuará utilizando el enlace alternativo hasta que el enlace principal permanezca activo durante este número de segundos.

Routing stabilization
Número de segundos que deben transcurrir después de que se devuelva el direccionamiento al enlace principal y antes de que se desactive el enlace alternativo. Durante este tiempo, ambos enlaces permanecerán activos. Este intervalo permite que protocolos de direccionamiento, como OSPF y RIP, tengan tiempo de reconocer que se dispone de una ruta a través de la interfaz principal.

Time-of-day revert back
Hora del día en que el direccionador puede revertir a la ruta principal. El direccionador puede revertir a la interfaz principal en cualquier momento entre la hora de inicio y de fin de reversión. Sólo se revertirá a la interfaz principal si ésta está activa y se cumplen los parámetros de estabilización. El valor por omisión es 0.

Restored times
Número de intentos de redireccionar la interfaz principal.

Overflow times
Número de intentos de llamada por desbordamiento.

secondary-circuit
Proporciona valores totales para cada circuito secundario. Permite que el operador encargado de la supervisión, recupere el estado de la restauración de WAN y las estadísticas asociadas para cada interfaz secundaria y sus interfaces principales asociadas.

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 respaldada por la interfaz secundaria asociada.

Secondary Interface
El circuito de marcación que se está utilizando para respaldar la interfaz principal asociada.

Secondary Enabled
Indica si la restauración de esta interfaz principal está actualmente habilitada.

Router Primary Interface State
Indica que el estado de la interfaz principal es uno de estos:

Up - Indica que el enlace está activo.

Down - Indica que el enlace está desactivado.

Disabled - Indica que el operador ha inhabilitado el enlace.

Not present - Indica que el enlace está configurado, pero que hay un problema de hardware.

Router Secondary Interface State
Indica que el estado de la interfaz secundaria asociada es uno de estos:

Up - Indica que el enlace está activo.

Down - Indica que el enlace está desactivado. También sucede cuando la red base del enlace secundario se inhabilita desde el indicador `Config>` o desde la consola del operador.

Available - Indica que el enlace está en modalidad de espera.

Testing - Indica que el enlace está en proceso de establecer una conexión.

Restoral Statistics:

Primary Restoral Attempts
Número de veces que el enlace principal ha dado un error, haciendo que el direccionador intente activar un enlace secundario.

Restoral Packets forwarded
Este campo indica el número total de paquetes reenviados.

Most Recent Restoral Period
Indica durante cuánto tiempo ha estado activo el enlace secundario, la última vez que se utilizó o durante la restauración actual.

summary Proporciona valores 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
Número de veces que el enlace principal ha dado un error, haciendo que el direccionador intente activar un enlace secundario.

Completions
Número de intentos satisfactorios de restauración en los que se ha activado y utilizado el enlace secundario.

Total packets forwarded
Número total de paquetes reenviados por la interfaz secundaria. Es la suma del número de paquetes reenviados en ambos sentidos. El valor se va acumulando cada período de restauración, hasta que se ejecute el mandato de reiniciar o borrar las estadísticas de restauración.

Longest restoral period
Este campo muestra en horas, minutos y segundos, el tiempo más largo que ha estado en funcionamiento la función de restauración, sin contar el tiempo de funcionamiento actual.

Primary Interface and State
La interfaz que está siendo respaldada por la interfaz secundaria asociada. Los estados válidos son:

Up - Indica que el enlace está activo.

Down - Indica que el enlace está desactivado.

Disabled - Indica que el operador ha inhabilitado el enlace.

Not present - Indica que el enlace está configurado, pero que hay un problema de hardware.

Secondary Interface and State

El circuito de marcación que se está utilizando para respaldar la interfaz principal asociada. Los estados válidos son:

Up - Indica que el enlace está activo.

Down - Indica que el enlace está desactivado. También sucede cuando la red base del enlace secundario se inhabilita desde el indicador `Config>` o desde la consola del operador.

Testing - Indica que el enlace está en proceso de establecer una conexión.

Available - Indica que el enlace está en modalidad de espera.

Reconfiguración dinámica de la restauración y el redireccionamiento de WAN

En este apartado se describe la reconfiguración dinámica (DR) y cómo afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

Las funciones de restauración y de redireccionamiento de WAN dan soporte al mandato **delete interface** de CONFIG (Talk 6) sin restricciones.

Mandato activate interface de GWCON (Talk 5)

Las funciones de restauración y de redireccionamiento de WAN dan soporte al mandato **activate interface** de GWCON (Talk 5), pero hay que tener en cuenta que:

- No se puede activar una interfaz principal de restauración de WAN si su interfaz secundaria está restaurando activamente otra interfaz principal.
- No se puede activar una interfaz principal de restauración de WAN si, antes de ejecutar el mandato **activate interface**, su interfaz secundaria era una interfaz principal de restauración de WAN, una interfaz principal de redireccionamiento de WAN, o una interfaz alternativa de redireccionamiento de WAN.
- No se puede activar una interfaz secundaria de restauración de WAN si su su interfaz principal está siendo restaurada por otra interfaz secundaria.
- No se puede activar una interfaz secundaria de restauración de WAN si, antes de ejecutar el mandato **activate interface**, su interfaz principal era una interfaz secundaria de restauración de WAN, una interfaz principal de redireccionamiento de WAN, o una interfaz alternativa de redireccionamiento de WAN.
- No se puede activar una interfaz principal de redireccionamiento de WAN si, antes de ejecutar el mandato **activate interface**, su interfaz alternativa se utilizaba de interfaz principal de redireccionamiento de WAN, de interfaz principal de restauración de WAN, o de interfaz alternativa de restauración de WAN.

- No se puede activar una interfaz alternativa de redireccionamiento de WAN si, antes de ejecutar el mandato **activate interface**, su interfaz principal era la interfaz principal de otra interfaz alternativa, una interfaz alternativa de redireccionamiento de WAN, una interfaz principal de restauración de WAN, o una interfaz secundaria de restauración de WAN.

El mandato **activate interface** de GWCON (Talk 5) da soporte a todos los mandatos específicos de la interfaz de las funciones de restauración y de redireccionamiento de WAN.

Mandato reset interface de GWCON (Talk 5)

Las funciones de restauración y de redireccionamiento de WAN no dan soporte al mandato **reset interface** de GWCON (Talk 5).

Mandatos de cambio temporal de GWCON (Talk 5)

Las funciones de restauración y de redireccionamiento de WAN permiten ejecutar los siguientes mandatos de GWCON que modifican temporalmente el estado operativo del dispositivo. Estos cambios se pierden si el dispositivo se reinicia, si se vuelve a cargar, o si se ejecuta un 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

La función de redireccionamiento de WAN

En este capítulo se describe la función de redireccionamiento de WAN. Consta de los apartados siguientes:

Visión general del redireccionamiento de WAN

El redireccionamiento de WAN le permite configurar una ruta alternativa de forma que si un enlace principal da un error, el direccionador iniciará una conexión nueva con el destino a través de la ruta alternativa. En el apartado "Visión general de las funciones de restauración de WAN, redireccionamiento de WAN y de llamada por desbordamiento" en la página 75, se da una explicación del restauración de WAN y de cómo trabajan juntos el redireccionamiento de WAN y la llamada por desbordamiento.

El proceso de redireccionamiento de WAN consiste en:

1. Detectar el error del enlace principal
2. Pasar al enlace alternativo
3. Detectar la recuperación del enlace principal
4. Revertir al enlace principal

El enlace alternativo puede ser cualquier enlace para el que se puedan configurar protocolos direccionables (por ejemplo, IP o IPX), y el tipo de enlace de datos del enlace alternativo debe ser distinto al del enlace principal. Por ejemplo, el enlace alternativo puede ser una interfaz LAN, o una interfaz PPP, Frame Relay, o X.25 serie, o un circuito PPP o Frame Relay de marcación. Estos tipos de interfaz no pueden ser enlaces alternativos: interfaces SDLC serie, interfaces SRLY serie, y redes base, como por ejemplo, V.25 bis y RDSI.

Nota: Si los enlaces principal o alternativo son circuitos de marcación, éste no debe configurarse para realizar llamadas a petición. Utilice el mandato **set idle 0** en el indicador `Circuit Config>`, para configurar el circuito de marcación de forma que no pueda realizar llamadas a petición. Para obtener más información, consulte el apartado "Configuración y supervisión de circuitos de marcación" en el *Access Integration Services Guía del usuario de software*.

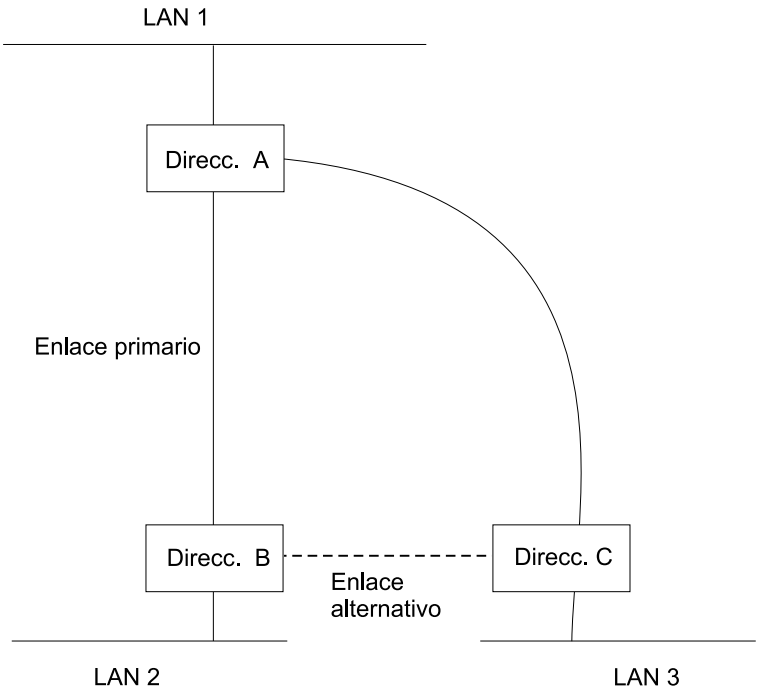


Figura 3. Redireccionamiento de WAN. Generalmente hay una conexión entre los direccionadores A y B y los direccionadores A y C. Si el enlace principal entre los direccionadores A y B da un error, el redireccionamiento de WAN establece un enlace alternativo entre los direccionadores B y C. De esta forma, los direccionadores A y B pueden comunicarse a través del direccionador C.

Llamada por desbordamiento

La llamada por desbordamiento permite utilizar una interfaz alternativa para el tráfico IP cuando la tasa de tráfico del enlace principal alcanza un umbral determinado. Esto significa que la interfaz principal no tiene porqué estar desactivada antes de que el enlace alternativo se active. Cuando el tráfico de la interfaz principal alcanza el umbral especificado, el direccionador activa el enlace alternativo. Para utilizar la llamada por desbordamiento, debe configurarse el redireccionamiento de WAN y la interfaz principal debe ser Frame Relay. IP es el único protocolo que puede conmutar a una interfaz alternativa realizando una llamada por desbordamiento. Además, si se utiliza la llamada por desbordamiento, debe utilizarse OSPF como protocolo IP de direccionamiento, en lugar de RIP.

Para obtener más información sobre la configuración de la llamada por desbordamiento, consulte el apartado “Mandatos de configuración de la restauración de WAN, del redireccionamiento de WAN y de la llamada por desbordamiento” en la página 81.

Supervisión del ancho de banda

Durante la configuración del redireccionamiento de WAN, puede especificarse un intervalo de supervisión del ancho de banda para la llamada por desbordamiento. Se supervisa la utilización del ancho de banda de recepción y trasmisión de la interfaz principal. Cuando el ancho de banda de la interfaz principal alcanza el umbral de *aumentar*, se emitirá una petición de redireccionamiento de WAN para activar la interfaz alternativa. Si el redireccionamiento de WAN logra activar la

interfaz alternativa, IP deja de direccionar por la interfaz principal y comienza a hacerlo por la interfaz alternativa.

Si el redireccionamiento de WAN no logra activar la ruta alternativa, intentará activar periódicamente la interfaz alternativa hasta que la utilización del ancho de banda de la interfaz principal caiga por debajo del umbral de *reducir*.

Cuando la utilización del ancho de banda de recepción y transmisión de la interfaz principal alcanza el umbral de *reducir* y se ha agotado el tiempo mínimo configurado que la interfaz alternativa estará activa, ésta se desactiva. Esto hace que IP deje de direccionar por la interfaz alternativa y empiece a utilizar la interfaz principal.

Los umbrales de aumentar y de reducir se especifican como un porcentaje de la velocidad configurada de la línea del enlace principal. La velocidad configurada de la línea no siempre coincide con la velocidad real del enlace. El volumen de tráfico del enlace en cada sentido se calcula por separado. Se cruza el umbral si el tráfico en cualquiera de los dos sentidos es mayor que el porcentaje especificado.

Configuración del redireccionamiento de WAN

A continuación se describen los pasos a seguir para configurar el redireccionamiento de WAN. En el próximo apartado se da un ejemplo de cómo realizar dichas tareas.

Para configurar el redireccionamiento de WAN, necesita:

1. Configurar el enlace principal.
2. Configurar el enlace alternativo.
3. Asignar el enlace alternativo al enlace principal. También puede especificar un período de estabilización para el enlace principal.

   Puede especificar una hora de reversión al enlace principal, lo que se producirá después de que se termine el período de estabilización (si se ha configurado). Esto permite que el enlace secundario permanezca activo hasta la hora especificada por el usuario y que se revierta al enlace principal durante las horas en que el tráfico es menos intenso.

   Nota: Los tipos de enlace de datos de los enlaces principal y alternativo, pueden ser diferentes. Los enlaces principal y alternativo pueden ser:

   - Una interfaz LAN.
   - Una interfaz PPP serie.
   - Una interfaz Frame Relay serie.
   - Una interfaz An X.25 serie.
   - Un circuito PPP de marcación.
   - Un circuito Frame Relay de marcación.

Ejemplo de configuración del redireccionamiento de WAN

La Figura 4 muestra el redireccionamiento de WAN utilizando un circuito Frame Relay de marcación sobre RDSI como enlace alternativo. Si el DLCI de Frame Relay entre los direccionadores A y C da un error, el redireccionamiento de WAN utilizará el circuito de marcación para establecer una conexión alternativa a través del direccionador D. Si uno de los enlaces principales entre una de las sucursales y las oficinas centrales da un error, el redireccionamiento de WAN establece una ruta alternativa hasta las oficinas centrales a través de otra sucursal.

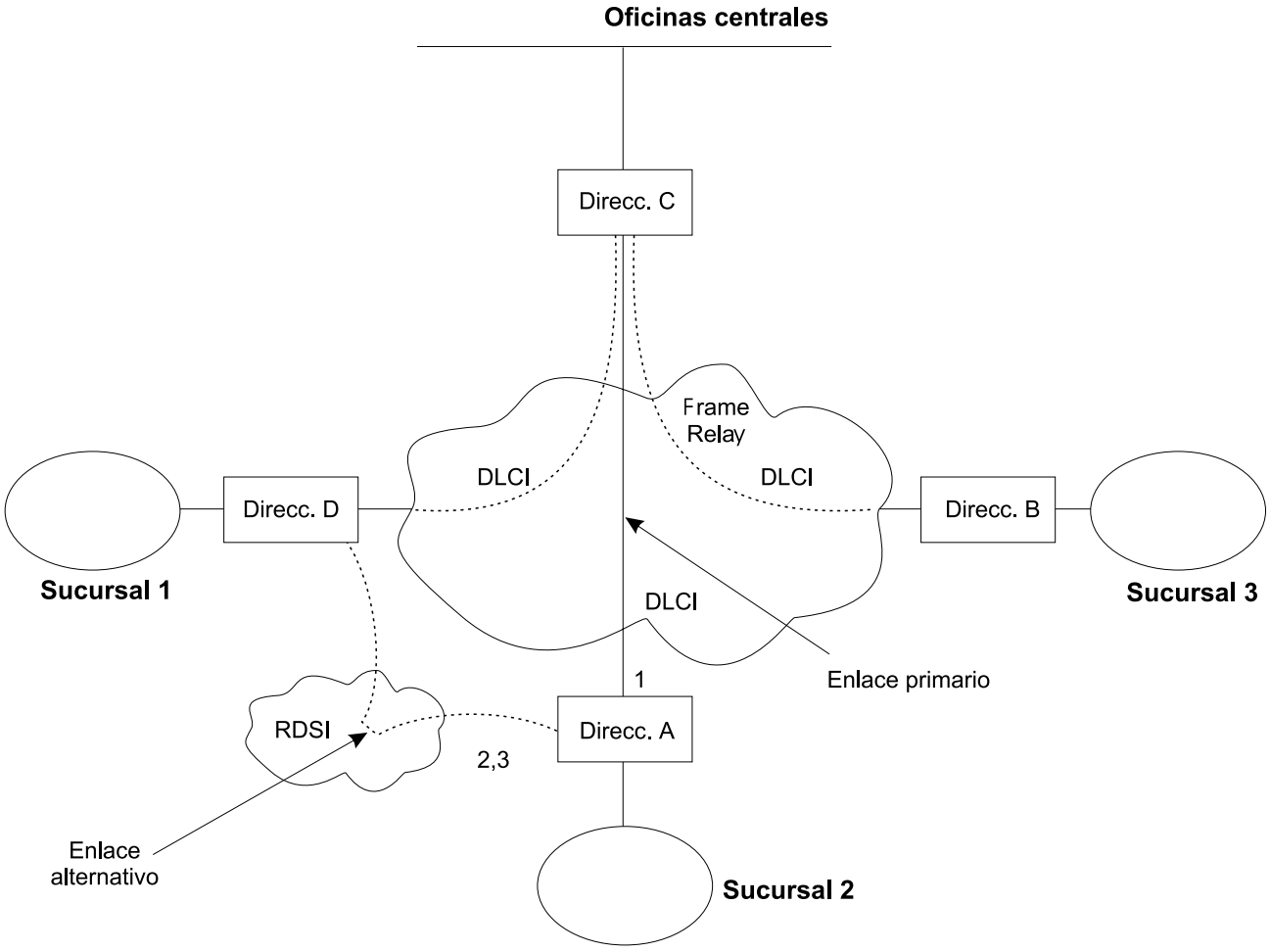


Figura 4. Ejemplo de configuración del redireccionamiento de WAN. Las sucursales utilizan Frame Relay para conectarse con las oficinas centrales.

En los apartados siguientes se describe cómo configurar el redireccionamiento de WAN en el direccionador A de la Figura 4. Se necesita:

- Configurar la interfaz Frame Relay principal (1) para que tenga un PVC obligatorio o un Grupo de PVC obligatorios, o habilitar la función Sin PVC para la interfaz Frame Relay.
- Configurar la interfaz RDSI (2) y su circuito de marcación Frame Relay (3).
- Asignar el circuito de marcación de forma que sea el enlace alternativo de la interfaz Frame Relay principal y ejecutar el mandato **set idle 0** en el indicador de marcación `Circuit Config>` para inhabilitar las llamadas a petición para este circuito.

- Opcionalmente, se puede asignar:
  - Un período de tiempo de estabilización para el enlace principal,
  - Una ventana de tiempo de reversión para el enlace principal.

A continuación se describen con más detalle estas tareas.

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 de la interfaz Frame Relay principal.

Para hacer que la interfaz FR principal se declare desactivada cuando pierda la conexión con otro u otros direccionadores, tiene tres opciones:

1. Habilitar la función Sin PVC. Si se habilita esta función, la interfaz FR se desactiva cuando no hay PVC activos.
2. Configurar un PVC como obligatorio, pero sin incluirlo en un grupo de PVC obligatorios. En este caso, la interfaz FR se desactiva cuando el PVC queda inactivo.
3. Configurar un conjunto de PVC como obligatorios y que además formen un grupo de PVC obligatorios. En este caso, la interfaz FR se desactiva cuando todos los PVC de un grupo de PVC obligatorios quedan inactivos.

Para configurar la interfaz Frame Relay principal, siga los pasos siguientes:

1. Si todavía no lo ha hecho, establezca en enlace de datos de la interfaz RDSI como Frame Relay.

   ```
   Config>set data-link frame relay
   Interface Number [0]? 2
   ```

2. Entrar en el proceso de configuración de Frame Relay.

   ```
   Config>network
   What is the network number [0]?2
   Frame Relay user configuration
   FR Config>
   ```

   Nota: Para configurar la interfaz Frame Relay principal, sólo hay que llevar a cabo *uno* de los dos pasos siguiente.

3. Añadir un PVC con el mandato **add permanent-virtual-circuit**.

   Para configurar el PVC como Obligatorio:

   Escriba **y** (sí) a la pregunta “Is circuit required for interface operation ?” (¿El circuito es obligatorio para el funcionamiento de la interfaz?).

   Para configurar el PVC como un miembro de un grupo de PVC obligatorios:

   a. Responda **y** (sí) a la pregunta “Does circuit belong to a Required PVC group ?” (¿El circuito pertenece a un grupo de PVC obligatorios?).

   b. A la pregunta “What is the group name ?” (¿Cuál es el nombre del grupo?), responda escribiendo un nombre de grupo.

   Si ya ha añadido algún PVC, utilice el mandato **change permanent-virtual-circuit** para configurar el PVC como obligatorio y para asignarlo a un Grupo de PVC obligatorios, según corresponda. Para obtener más información, consulte el apartado Utilización de interfaces Frame Relay en el *Access Integration Services Guía del usuario de software*.

```
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 []?grupo1
```

4. Si lo desea, habilite la función Sin PVC.

   Nota: Realice este paso *sólo* si se ha saltado el paso anterior.

   ```
   FR Config>enable no-pvc
   ```

Se pueden establecer parámetros adicionales para Frame Relay. Para obtener más información, consulte el apartado 'Utilización de Frame Relay' en el *Access Integration Services 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 los direccionadores A y D. Para obtener más información sobre cómo configurar las interfaces RDSI y los circuitos de marcación, consulte el apartado 'Utilización de la interfaz RDSI' en el *Access Integration Services Guía del usuario de software*.

A diferencia de lo que ocurre en la restauración de WAN, deben configurarse protocolos direccionables en el circuito de marcación, que se utilizarán como enlace alternativo. Si los protocolos direccionables no puede dejar de enviar paquetes de mantenimiento, el enlace alternativo establecerá una conexión incluso si el redireccionamiento no es necesario. En este caso, si sólo quiere utilizar el enlace alternativo como redireccionador, inhabilite el circuito de marcación. Para inhabilitar el circuito de marcación, ejecute el mandato **disable interface** en el indicador `Config>`.

Si la interfaz RDSI tiene asignados varios circuitos de marcación, podrá establecer prioridades para uno de ellos. Si todos los canales B tienen circuitos de marcación activos en la interfaz física y un circuito con una prioridad mayor recibe un paquete, se concluirá la conexión que tenga la prioridad más baja y el circuito con mayor prioridad establecerá una conexión.

Las prioridades que se pueden definir están comprendidas entre 0 y 15, donde 15 es el circuito de mayor prioridad y 0 es el de menor prioridad. La prioridad por omisión para los circuitos de marcación nuevos es de 8. Escriba **set priority** en el indicador `Circuit Config>` para cambiar la prioridad.

Asignación y configuración del enlace alternativo

Entre en el proceso de configuración del redireccionamiento de WAN para asignar el circuito de marcación como enlace alternativo para una interfaz LAN, una interfaz PPP, Frame Relay, o X.25 serie, o un circuito de marcación PPP o Frame Relay y, si así lo desea, para especificar los períodos de estabilización y la ventana de tiempo de reversión.

Hay tres tipos de períodos de estabilización:

- *El primer período de estabilización* es el tiempo que el direccionador espera a que la interfaz principal se active la primera vez que el direccionador intenta activarla. Si, después del primer período de estabilización, la interfaz principal no se ha activado, el redireccionamiento WAN activa el enlace alternativo.

- *El período de estabilización* es el tiempo que el direccionador espera para asegurarse de que el enlace principal es fiable antes de revertir del enlace alternativo al enlace principal.
- *El período de estabilización de direccionamiento* es el tiempo que el direccionador mantiene ambos enlaces, el principal y el alternativo, después de revertir del enlace alternativo al enlace principal. Este tiempo sirve para que protocolos de direccionamiento como OSPF o RIP reconozcan la disponibilidad de la ruta nueva a través del enlace principal antes de que se desactive el enlace alternativo.

La ventana de tiempo de reversión es la hora del día concreta en que el usuario quiere revertir al enlace principal después de que esté activado y que haya transcurrido el tiempo de estabilización configurado.

El usuario especifica las horas de inicio y parada de la ventana de reversión utilizando un reloj en formato de 24 horas. El enlace secundario se mantiene activo y no se desactiva hasta que se alcanza la hora inicial. Si la hora del día en que se activa el enlace principal ocurre entre las horas inicial y final (dentro de la ventana), la reversión al enlace principal se produce inmediatamente después de que se termine el tiempo de estabilización.

Para asignar y configurar el enlace alternativo, siga estos pasos:

1. Entre en el proceso de configuración de restauración de WAN.

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

2. Asigne el circuito de marcación como enlace alternativo de la interfaz Frame Relay principal.

```
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 definir el primer período de estabilización para una interfaz principal determinada, utilice el mandato **set first-stabilization-period**. Para definir un primer período de estabilización por omisión para todas las interfaces para las que no se ha especificado ningún período, 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 definir un período de estabilización para interfaces concretas, utilice el mandato **set stabilization-period**. Para definir un período de estabilización por omisión para todas las interfaces para las que no se ha especificado ningún período, 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 rutas. Para definir un período de estabilización de rutas para interfaces concretas, 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 tiempo de reversión.

   Para definir las horas inicial y final para ventanas de interfaces concretas, utilice los mandatos set start-time-of-day-revert-back y stop-time-of-day-revert-back. El valor por omisión es cero y significa que no hay ninguna ventana configurada. El reloj en formato de 24 horas empieza a la 1 a.m. y termina a medianoche, a las 24. Si las horas inicial y final son la misma (distintas de cero), el reversión se producirá exactamente a esa hora.

   A continuación se dan dos ejemplos de configuración de la ventana de reversión:

   a. Una hora inicial 23 y una hora final 3, dará una ventana de reversión de 11 p.m. a 3 a.m.

   b. Una hora inicial 1 y una hora final 5, dará una ventana de reversión de 1 a.m. a 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 función Network Dispatcher

En este capítulo se describe cómo utilizar la función Network Dispatcher y consta de los apartados siguientes:

Network Dispatcher utiliza una tecnología de reparto de carga desarrollada por IBM para determinar qué servidor es el más adecuado para recibir una nueva conexión. Se trata de la misma tecnología que utiliza el producto SecureWay® Network Dispatcher de IBM para Solaris, Windows NT® y AIX®.

Visión general de Network Dispatcher

La función Network Dispatcher aumenta el rendimiento de los servidores al reenviar las peticiones de sesiones TCP/IP a distintos servidores pertenecientes a un grupo de servidores, repartiendo la carga de las peticiones entre todos los servidores. El reenvío es transparente para los usuarios y las aplicaciones. Network Dispatcher es útil en aplicaciones de servidor, como por ejemplo e-mail, servidores World Wide Web, consultas a bases de datos distribuidas en paralelo y otras aplicaciones TCP/IP.

Network Dispatcher también puede utilizarse para repartir la carga del tráfico de una aplicación UDP sin información de estado entre un grupo de servidores.

Network Dispatcher puede ayudarle a maximizar el potencial de su sede, proporcionándole una herramienta poderosa, flexible y escalable para solucionar los problemas de puntas de demanda. En períodos de puntas de demanda, Network Dispatcher puede encontrar automáticamente el servidor óptimo para manejar las peticiones entrantes.

La función Network Dispatcher no utiliza un servidor de nombres de dominio para repartir la carga. Distribuye el tráfico entre los servidores mediante una combinación exclusiva de software de reparto de carga y de gestión. Network Dispatcher también puede detectar un servidor que esté dando errores y reenviar el tráfico a otros servidores que estén disponibles.

Todas las peticiones de los clientes que se envían a la máquina Network Dispatcher se reenvían al servidor seleccionado por Network Dispatcher como servidor óptimo, dependiendo de una serie de pesos establecidos dinámicamente.

Network Dispatcher calcula estos pesos basándose en cierto número de factores, entre los cuales está la cuenta de conexiones y la carga y la disponibilidad del servidor.

El servidor devuelve una respuesta al cliente sin la intervención de Network Dispatcher. Los servidores no necesitan ningún software adicional para comunicarse con Network Dispatcher.

La función Network Dispatcher es la clave para una gestión estable y eficiente de una red grande y escalable de servidores. Con Network Dispatcher puede enlazar varios servidores individuales en lo que aparenta ser un único servidor virtual. De esta forma, todo el mundo verá su sede como una sola dirección IP. Network Dispatcher funciona independientemente del servidor de nombres de dominio; todas las peticiones se envían a la dirección IP de la máquina Network Dispatcher.

Network Dispatcher permite que una aplicación de gestión basada en SNMP supervise el estado de Network Dispatcher al recibir estadísticas básicas y situaciones de alertas potenciales. En el apartado “Gestión de SNMP”, de la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 1* hallará más información.

Network Dispatcher consigue ventajas evidentes en el reparto de la carga del tráfico entre servidores agrupados, lo que redunda en una gestión estable y eficiente de su sede de Internet.

Reparto del tráfico TCP y UDP utilizando Network Dispatcher

El reparto de cargas se puede enfocar de muchas maneras. Algunos de esos enfoques permiten que los usuarios elijan un servidor distinto al azar en caso de que el primero vaya lento o no responda. Otro método es el de repartir la carga rotativamente, en el que el servidor de nombres de dominio elige un servidor para manejar las peticiones. Este enfoque es mejor, pero no tiene en cuenta la carga actual del servidor de destino, ni si está disponible.

Network Dispatcher puede repartir la carga de las peticiones de distintos servidores basándose en el tipo de petición, un análisis de la carga de los servidores o un conjunto configurable de pesos asignados por el usuario. Para gestionar cada tipo de reparto, Network Dispatcher dispone de los componentes siguientes:

Ejecutor Reparte la carga de las conexiones dependiendo del tipo de petición recibida. Los tipos de petición más corrientes son HTTP, FTP y Telnet. Este componente siempre está operativo.

Asesor Consulta a los servidores y analiza para cada uno los resultados obtenidos por cada protocolo. El asesor pasa esta información al ***gestor*** para establecer los pesos adecuados. El asesor es un componente opcional. Sin embargo, si no se utiliza un asesor, Network Dispatcher no será capaz de detectar si un servidor sufre una anomalía y continuará enviando conexiones nuevas a un servidor inactivo.

Network Dispatcher da soporte a asesores para FTP, HTTP, SMTP, NNTP, POP3 y Telnet, así como un asesor TN3270, que funciona con servidores TN3270 en los direccionadores IBM 2210, IBM 2212 e IBM 2216, y un asesor MVS™ que funciona con

Workload Manager (WLM) en sistemas MVS. WLM gestiona la carga de trabajo de un sólo ID de MVS. Network Dispatcher puede utilizar WLM para ayudar a repartir la carga de peticiones a los servidores MVS que ejecuten OS/390® V1R3 o posterior.

No existen asesores específicos para los protocolos UDP. Si tiene servidores MVS, puede utilizar el asesor del sistema MVS para proporcionar información de la carga del servidor. Además, si el puerto maneja tráfico TCP y UDP, puede utilizarse el asesor del protocolo TCP adecuado para proporcionar entrada al asesor para el puerto. Network Dispatcher utilizará esta entrada para repartir la carga del tráfico TCP y UDP del puerto.

Gestor Establece pesos para un servidor basándose en los elementos siguientes:

- Contadores internos del ejecutor
- Realimentación de los servidores proporcionada por los asesores de los protocolos
- Realimentación de un supervisor del sistema (asesor MVS).

El gestor es un componente opcional. Sin embargo, si no utiliza el gestor, Network Dispatcher repartirá la carga según un método de planificación rotativo basado en los pesos configurados para cada servidor.

Si utiliza Network Dispatcher para repartir la carga del tráfico UDP sin información de estado, deberá utilizar solamente servidores que respondan al cliente utilizando la dirección IP destino de la petición. Consulte “Configuración de un servidor para Network Dispatcher” en la página 121 para obtener una explicación más completa.

Alta disponibilidad de Network Dispatcher

La función base de Network Dispatcher tiene las características siguientes que, desde distintos puntos de vista, la convierten en el único punto en que se puede producir una anomalía:

- Examina todo el tráfico de entrada. Si algún paquete de una conexión existente utiliza una vía distinta a través de otro Network Dispatcher diferente para acceder a un servidor, éste, restablecerá inmediatamente la conexión.
- Hace un seguimiento de todas las conexiones establecidas y, aunque no las interrumpa, las entradas perdidas de la tabla de conexiones de Network Dispatcher provocarán el restablecimiento de una conexión.
- Aparece ante el direccionador de saltos anterior como el último salto y la finalización de la conexión.

Las características anteriores hacen que las anomalías siguientes sean críticas para el cluster:

- Si Network Dispatcher da un error por alguna razón, se perderán todas las tablas de conexiones, por lo que también se perderán todas las conexiones existentes entre el cliente y el servidor. Suponiendo que exista un segundo Network Dispatcher capaz de dirigir un cliente a los servidores, podrán activarse nuevas conexiones después de los retardos del protocolo de direccionamiento habituales, que pueden ser de varios minutos.

- Si la interfaz de Network Dispatcher configurada para el direccionador de IP anterior da un error, debe poderse obtener otra interfaz para el mismo Network Dispatcher, en cuyo caso, el direccionador de IP realizará la recuperación (utilizando el mecanismo de ARP para determinar la antigüedad, con un retraso de varios minutos), o se perderán todas las conexiones.
- Si se produce una anomalía en la interfaz de Network Dispatcher con los servidores, el direccionador de saltos anterior, supone que 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 error, que no son únicamente debidos a errores de Network Dispatcher, sino a errores producidos en sus proximidades, se perderán todas las conexiones existentes. Incluso con un Network Dispatcher de reserva en el que se estén ejecutando los mecanismos estándar de recuperación de IP, la recuperación es, en el mejor de los casos, lenta y sólo es aplicable a las conexiones nuevas. En el peor de los casos, las conexiones no se podrán recuperar.

Para mejorar la disponibilidad de Network Dispatcher, la función de alta disponibilidad de Network Dispatcher utiliza los mecanismos siguientes:

- Dos Network Dispatcher conectados a los mismos clientes y al mismo cluster de servidores y entre ellos.
- Un mecanismo de “latido” entre ambos Network Dispatcher capaz de detectar la anomalía de uno de los dos.
- Un criterio de accesibilidad que permita identificar los sistemas principales IP que pueden o que no pueden accederse desde cada Network Dispatcher.
- Sincronización de las bases de datos de Network Dispatcher (o sea, de las tablas de conexiones, de las tablas de accesibilidad y de otras bases de datos).
- Lógica para elegir el Network Dispatcher activo, que es el que está a cargo de un determinado cluster de servidores, y el Network Dispatcher en espera, que está continuamente sincronizado con ese cluster de servidores.
- Un mecanismo para tomar el control de IP rápidamente, cuando la lógica o un operador decide intercambiar el Network Dispatcher activo por el que está en espera.

Detección de anomalías

Además de los criterios básicos de detección de anomalías (pérdida de conexión entre los Network Dispatcher activo y en espera, detectada mediante los mensajes del mecanismo de Latido), hay otro mecanismo de detección de anomalías llamado “criterio de accesibilidad”.Cuando se configura la función Network Dispatcher, se suministra una lista de sistemas principales a los que cada uno de los Network Dispatcher debe poder acceder para funcionar correctamente. Los sistemas principales pueden ser direccionadores, servidores IP u otros tipos de sistemas principales. La accesibilidad al sistema principal se determina haciendo ping al sistema principal.

El intercambio tiene lugar si no pueden aceptarse los mensajes del mecanismo de latido, o si el Network Dispatcher activo ya no cumple el criterio de accesibilidad y el Network Dispatcher en espera es accesible. Para tomar una decisión en base a toda la información disponible, el Network Dispatcher activo envía regularmente al Network Dispatcher en espera sus posibilidades de accesibilidad. A continuación,

el Network Dispatcher en espera compara dichas posibilidades de accesibilidad con las suyas y decide si debe realizarse el intercambio.

Sincronización de bases de datos

Los Network Dispatcher principal y de reserva mantienen sincronizadas sus bases de datos mediante el mecanismo de "Latido". La base de datos de Network Dispatcher contiene las tablas de conexiones, las tablas de accesibilidad y otra información. La función Alta disponibilidad de Network Dispatcher utiliza un protocolo de sincronización de bases de datos que garantiza que ambos Network Dispatcher contengan las mismas entradas de la tabla de conexiones. La sincronización tiene en cuenta un margen de error conocido debido a los retardos en la transmisión. El protocolo realiza una sincronización inicial de las bases de datos y a partir de entonces mantiene la sincronización de las bases de datos mediante actualizaciones periódicas.

Estrategia de recuperación

En caso de que una máquina Network Dispatcher o una interfaz sufran una anomalía, el mecanismo de toma de control de IP dirigirá rápidamente todo el tráfico hacia el Network Dispatcher en espera. El mecanismo de sincronización de bases de datos garantiza que el Network Dispatcher en espera tendrá las mismas entradas que el Network Dispatcher activo, de manera que podrán mantenerse las conexiones cliente-servidor ya existentes.

Toma de control de IP

Nota: Las direcciones IP del cluster se supone que están en la misma subred lógica que el direccionador de saltos anterior (direccionador IP), a menos que las direcciones del cluster se anuncien.

El direccionador IP resolverá las direcciones del cluster mediante el protocolo ARP. Para realizar la toma de control de IP, el Network Dispatcher (en espera, pero pasando a ser el activo) emitirá una petición ARP a sí mismo, que se difundirá a todas las redes directamente conectadas pertenecientes a la subred lógica del cluster. El direccionador IP de saltos anterior actualizará sus tablas ARP (según se describe en la RFC 826) para enviar todo el tráfico de ese cluster al nuevo Network Dispatcher activo (antes en espera).

Configuración de Network Dispatcher

Hay varias formas de configurar Network Dispatcher para que dé soporte a su sede. Si la sede de Internet a la que se conectarán todos los clientes tiene un solo nombre de sistema principal, puede definir un único grupo de servidores y tantos puertos como se quiera para recibir las conexiones. Esta configuración se muestra en la Figura 5 en la página 116.

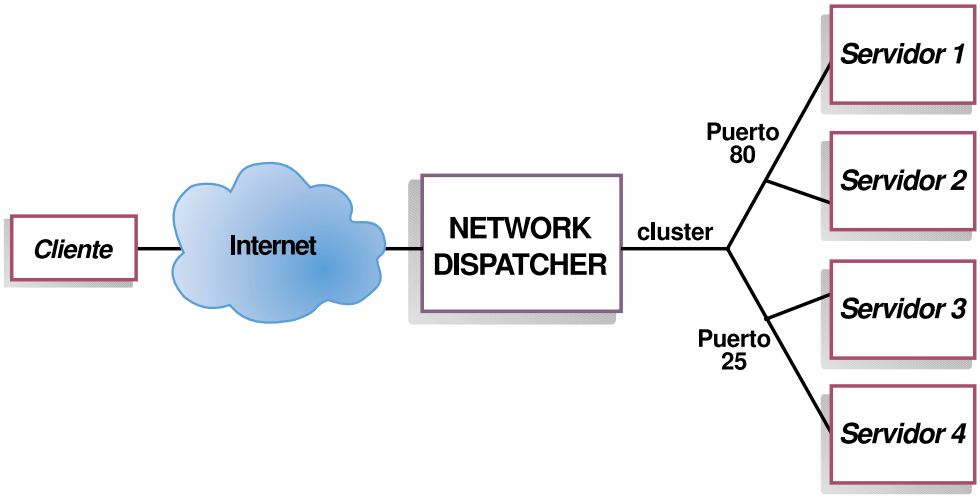


Figura 5. Ejemplo de Network Dispatcher configurado con un único grupo de servidores y dos puertos

En caso de que la sede hospede el contenido de varias empresas o departamentos que entren en la sede mediante URL distintos, sería necesario configurar Network Dispatcher de otra forma. En este caso, puede que interese definir un grupo de servidores para cada empresa o departamento, y tantos puertos como se quiera para recibir las conexiones en ese URL, tal y como se muestra en la Figura 6 en la página 117.

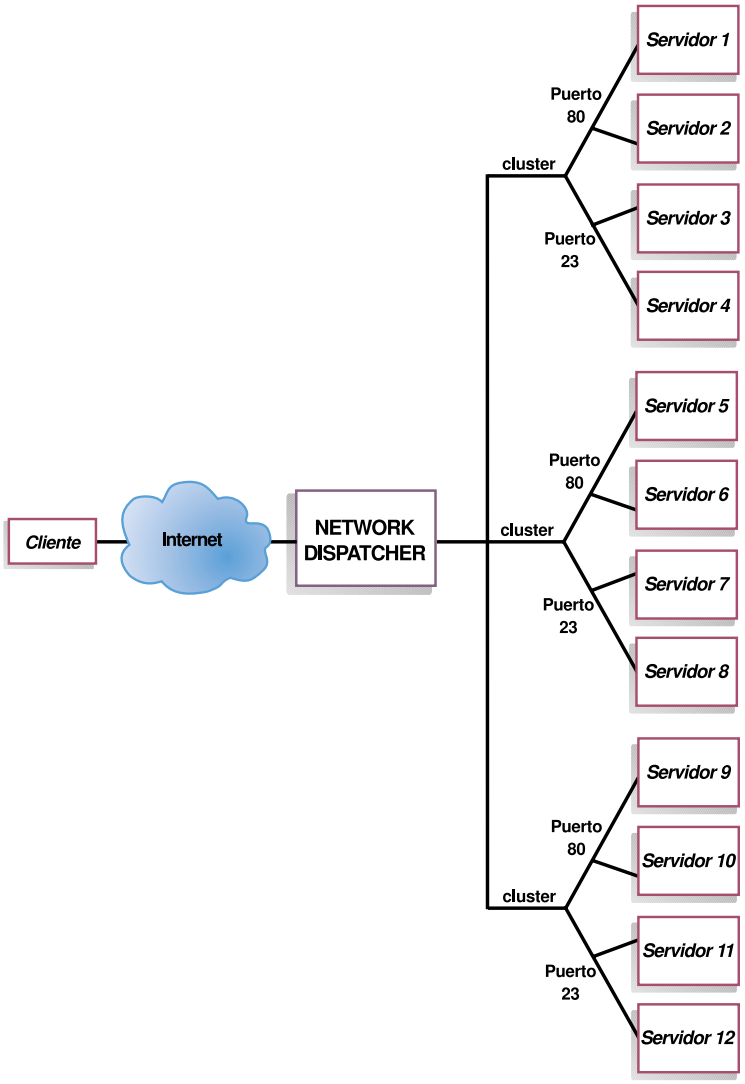


Figura 6. Ejemplo de Network Dispatcher configurado con tres grupos de servidores y tres URL

Sería conveniente configurar Network Dispatcher de una tercera forma si la sede de Internet fuera muy grande y dependiera de varios servidores dedicados para cada protocolo que se soporta. Por ejemplo, puede decidir tener servidores FTP independientes con líneas T3 directas para poder bajar archivos muy grandes. En este caso, puede que le interese definir un grupo de servidores para cada protocolo con un único puerto pero varios servidores, como se muestra en la Figura 7 en la página 118.

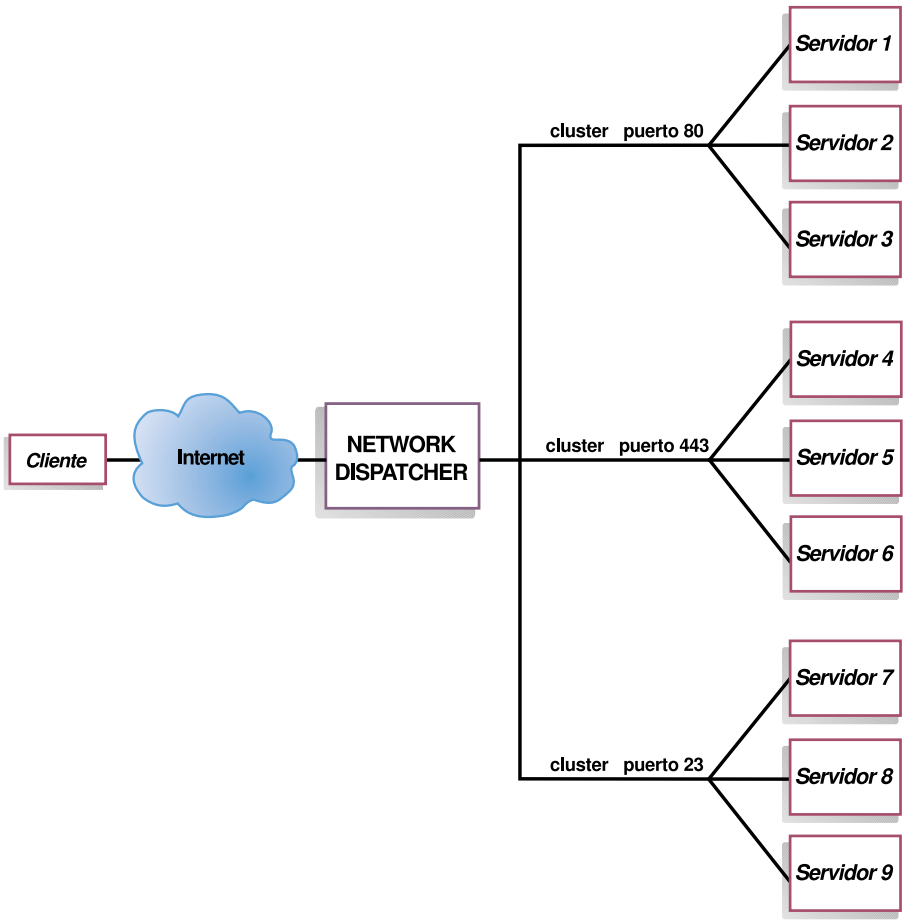


Figura 7. Ejemplo de Network Dispatcher configurado con tres grupos de servidores y tres puertos

Pasos para la configuración

Antes de configurar Network Dispatcher:

1. Asegúrese de que Network Dispatcher tiene interfaces directas con los servidores (es decir, cada máquina servidora debe estar conectada directamente a una subred que es local a la máquina Network Dispatcher). Puesto que la función Network Dispatcher sólo detecta el tráfico que va del cliente al servidor, los servidores pueden tener conexiones independientes con el direccionador de la empresa o con Internet, de manera que el tráfico saliente que va de los servidores a los clientes, puede eludir la máquina Network Dispatcher. Para permitir este tipo de conexiones salientes no es necesario realizar una configuración especial de Network Dispatcher.

   Si es importante que la disponibilidad de la red sea alta, en la Figura 8 en la página 119 se muestra una configuración de alta disponibilidad típica.

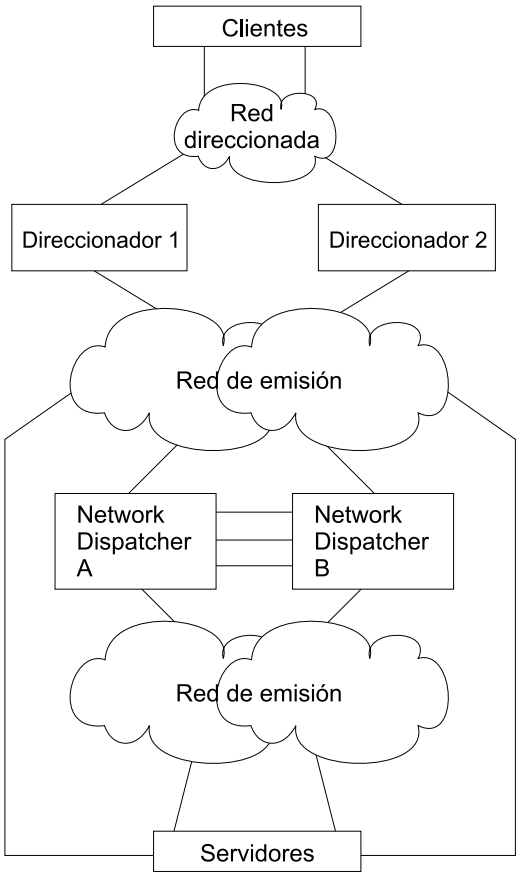


Figura 8. Configuración de alta disponibilidad de Network Dispatcher

2. Configure las interfaces de la máquina Network Dispatcher. Esto consiste en configurar todas las interfaces, las direcciones IP de todas las interfaces y los protocolos de direccionamiento que se vayan a utilizar. Network Dispatcher utiliza la dirección IP interna del direccionador, de manera que también debe configurarse mediante el mandato set internal-ip-address. La dirección IP interna no debe coincidir con la dirección de un grupo de servidores configurado en Network Dispatcher. Consulte el capítulo Configuración y supervisión IP de la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 1* para obtener más información sobre el mandato **set internal-ip-address**.
3. Vuelva a arrancar la máquina Network Dispatcher.

Configuración de Network Dispatcher para un IBM 2212

Para configurar Network Dispatcher para un IBM 2212:

1. En `talk 6`, acceda a la función Network Dispatcher ejecutando el mandato **feature ndr**.
2. Habilite el ejecutor y el gestor mediante los mandatos **enable executor** y **enable manager**.
3. Configure los clusters mediante el mandato **add cluster**. Si va a configurar las direcciones del cluster para que se anuncien, hallará más información en el apartado “Utilización de Network Dispatcher con el anuncio de direcciones del cluster” en la página 128. Si elige que Network Dispatcher no anuncie las direcciones del cluster, se deberán seleccionar direcciones del cluster que

formen parten de una subred que se anuncie y que sea local al direccionador Network Dispatcher. Normalmente será la subred en la que Network Dispatcher reciba el tráfico de los clientes proveniente del direccionador de saltos siguiente.

Nota: La direcciones IP del grupo de servidores no deben coincidir con la dirección IP interna del direccionador ni con ninguna de las direcciones IP de interfaces definidas en el direccionador. Si se está ejecutando Network Dispatcher y un servidor TN3270 en la misma máquina, la dirección del cluster puede coincidir con una dirección IP definida en la interfaz del bucle de retorno. Hallará más información en el apartado “Utilización de Network Dispatcher con el servidor TN3270” en la página 125.

4. Configure los puertos TCP y UDP de destino mediante el mandato **add port** para cada grupo de servidores de servidores que sirvan al protocolo correspondiente. Ejemplos de puertos son: 80 para HTTP, 20 y 21 para FTP y 23 para Telnet.
5. Configure los servidores con el mandato **add server**. Un servidor siempre está asociado con un puerto y un grupo de servidores. Un servidor puede servir a más de un puerto (es decir, un servidor puede definirse en varios puertos para el mismo grupo de servidores) y puede pertenecer a más de un grupo de servidores, si el sistema operativo del servidor da soporte a más de un alias.
6. Configure los asesores utilizando el mandato **add advisor**.

   Notas:

   a. Para el asesor MVS, no defina el valor Número de puerto (por omisión = 10007) para ningún grupo de servidores. El asesor MVS utiliza este número de puerto únicamente para comunicarse con WLM en los sistemas MVS.

   b. Para el asesor TN3270, se entran dos valores de puerto. El valor Número de puerto utilizado para la comunicación cliente-servidor (23, por omisión) debe definirse para los clusters adecuados. No defina el valor Puerto de comunicaciones (10008, por omisión) para ningún grupo de servidores. El asesor TN3270 utiliza el valor Puerto de comunicaciones solamente para reunir información sobre la carga de los servidores TN3270.
7. Mediante el mandato **enable advisor** habilite los asesores que se han configurado y mediante el mandato **set manager** modifique los porcentajes del gestor para incluir la entrada del asesor en los cálculos del peso.

si va a configurar Network Dispatcher para alta disponibilidad, siga los pasos siguientes. De lo contrario, ya se ha terminado la configuración.

Nota: Realice estos pasos primero en el Network Dispatcher principal y después en el de reserva. Para garantizar que la sincronización de las bases de datos sea la adecuada, debe habilitarse el ejecutor en el Network Dispatcher principal antes que en el de reserva.

8. Con el mandato **add backup**, configure si el Network Dispatcher es el principal o el de reserva y si el intercambio es manual o automático.
9. Configure todas las vías en las que se situará el mecanismo de latido entre los Network Dispatcher principal y de reserva, utilizando el mandato **add heartbeat**. Una vía se especifica definiendo las direcciones IP origen y destino.

Nota: Es obligatorio configurar más de una ruta para el latido entre los Network Dispatcher, para garantizar que no se interrumpa la comunicación de latidos entre las máquinas principal y de reserva si se produce una anomalía en una sola interfaz.

Si se dispone únicamente de una conexión LAN entre los dos Network Dispatcher, se puede establecer el segundo latido a través de una conexión LAN sencilla (por ejemplo, un cable cruzado utilizado directamente entre dos puertos Ethernet) o una conexión serie punto a punto (por ejemplo una conexión PPP próxima a través de un cable de módem nulo utilizando una dirección IP no numerada).

10. Con el mandato **add reach**, configure la lista de direcciones IP de los sistemas principales a los que debe poder acceder Network Dispatcher para garantizar un servicio completo. Normalmente suele consistir en un subconjunto de servidores, el direccionador de la empresa o una estación de administración. Debe configurarse al menos una dirección accesible por cada interfaz por la que Network Dispatcher envíe y reciba trafico.

La configuración se puede cambiar mediante los mandatos **set**, **remove** y **disable**. Consulte el “Configuración y supervisión de la función Network Dispatcher” en la página 133 para obtener más información sobre dichos mandatos.

Configuración de un servidor para Network Dispatcher

Para configurar un servidor para utilizarlo con Network Dispatcher:

1. Cambie el nombre al dispositivo bucle de retorno.

   Para que los servidores TCP y UDP funcionen, debe establecer (o mejor cambiarle el nombre) el dispositivo bucle de retorno (normalmente denominado ***lo0***) a la dirección del grupo de servidores. Network Dispatcher no modifica la dirección IP destino del paquete IP antes de reenviarlo a un servidor. Al establecer o cambiar el nombre del dispositivo bucle de retorno a la dirección del grupo de servidores, la máquina servidora aceptará paquetes dirigidos a la dirección del grupo.

   Es importante que el servidor utilice la dirección del grupo de servidores en lugar de su propia dirección IP para responder al cliente. Esto no tiene importancia con los servidores TCP, pero algunos servidores UDP utilizan sus propias direcciones IP cuando responden a las peticiones enviadas a la dirección del grupo. Cuando el servidor utiliza sus propias direcciones IP, algunos clientes descartarán la respuesta del servidor ya que no proviene de una dirección IP origen esperada. Debe utilizar solamente servidores UDP que utilicen la dirección IP destino de la petición cuando respondan al cliente. En este caso, la dirección IP destino de la petición es la dirección del cluster.

   Si el sistema operativo da soporte a alias de interfaz de red, como es el caso de AIX, Solaris o Windows NT, deberá usar la dirección del grupo de servidores como alias del dispositivo bucle de retorno. La ventaja de utilizar un sistema operativo que dé soporte a alias es que las máquinas servidoras pueden configurarse para que presten servicio a varias direcciones de grupos de servidores.

   Si el sistema operativo del servidor no da soporte a alias, como es el caso de HP-UX y OS/2, deberá definir ***lo0*** como dirección del grupo.

   Si el servidor es un sistema MVS ejecutando TCP/IP V3R2, deberá definir la dirección VIPA como dirección del grupo. Esta servirá como dirección del bucle

de retorno. La dirección VIPA no debe pertenecer a una subred que esté directamente conectada con el nodo MVS. Si el sistema MVS ejecuta TCP/IP V3R3, deberá usar la dirección del grupo de servidores como dirección del dispositivo bucle de retorno. Si utiliza la función de alta disponibilidad, deberá habilitar RouteD en el sistema MVS para que el mecanismo de toma de control de la función de alta disponibilidad funcione correctamente.

Nota: La lista de mandatos que aparecen en este capítulo se han probado en las versiones de los sistemas operativos 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 que corresponda a su sistema operativo, tal y como se muestra en la Tabla 10 en la página 123 para definir el dispositivo bucle de retorno o cambiarle el nombre.

Tabla 10. Mandatos para cambiar el nombre del dispositivo bucle de retorno (lo0) para Dispatcher

Sistema	Mandato
AIX	**ifconfig lo0 alias** *dirección_cluster* **netmask** *máscara_red*
HP-UX	**ifconfig lo0** *dirección_cluster*
Linux	**ifconfig lo:1** *dirección_cluster* **netmask** *máscara_red* **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 después en **Configuración**. 2. Pulse en **Panel de control** y efectúe una doble pulsación en **Red**. 3. Si todavía no lo ha hecho, añada el Controlador del adaptador de bucle de retorno de MS. a. En la ventana Red, pulse en **Adaptadores**. b. Elija el **Adaptador de bucle de retorno de MS** y pulse el botón **Aceptar**. c. Cuando se le solicite, inserte los discos o el CD de instalación. d. En la ventana Red, pulse en **Protocolos**. e. Elija el **Protocolo TCP/IP** y, a continuación, pulse en **Propiedades**. f. Elija el **Adaptador de bucle de retorno de MS** y pulse el botón **Aceptar**. 4. Establezca la dirección del bucle de retorno a la dirección del cluster. Acepte la máscara de subred por omisión (255.0.0.0) y no escriba ninguna dirección para la pasarela (gateway). **Nota:** Es posible que tenga que salir y volver a entrar en la Configuración de red antes de que aparezca el Controlador de bucle de retorno de MS en la Configuración TCP/IP.

OS/390	Configuración de un alias del bucle de retorno en el sistema OS/390.
	• En el miembro (archivo) de parámetros IP, un administrador tendrá que crear una entrada en la lista de direcciones de inicio. Por ejemplo:
	`HOME`
	`;Address Link`
	`192.168.252.11 tr0`
	`192.168.100.100 ltr1`
	`192.168.252.12 loopback`
	• Pueden definirse varias direcciones para el bucle de retorno
	• La dirección 127.0.0.1 se configura por omisión.

2. Compruebe si hay una ruta de más.

   En algunos sistemas operativos es posible que se cree un ruta por omisión que debe eliminarse.

   a. Compruebe la existencia de una ruta de más en Windows NT con este mandato: **route print**

   b. Compruebe la existencia de una ruta de más en todos los sistemas UNIX® y OS/2® con este mandato: **netstat -nr**

   c. Ejemplo de Windows NT: Después de escribir el mandato route print, se mostrará una tabla parecida a esta: (En este ejemplo se explica cómo

buscar y eliminar una ruta de más para el cluster 9.67.133.158 con una máscara de red por omisión 255.0.0.0.)

```
Rutas activas:
      Dirección de red          Máscara          Gateway         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 la dirección del cluster bajo la columna "Gateway". Si hay una ruta de más, la dirección del cluster aparecerá dos veces. En el ejemplo anterior, la dirección del cluster (9.67.133.158) aparece en la fila 2 y en la fila 8.

e. Busque la dirección de red correspondiente a las filas en las que aparece la dirección del cluster. Una de las rutas es necesaria y la otra debe eliminarse, ya que es ajena. La ruta de más que debe ser eliminada será aquella cuya dirección de red empiece con el primer dígito de la dirección del cluster, seguida de tres ceros. En el ejemplo anterior, la ruta de más es la de la fila dos, cuya dirección de red es 9.0.0.0:

```
 9.0.0.0        255.0.0.0     9.67.133.158     9.67.133.158     1
```

3. Elimine todas las rutas de más.

   En la Tabla 11 se muestran los mandatos de cada sistema operativo que sirven para eliminar las rutas de más.

Tabla 11. Mandatos para eliminar rutas en 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 eliminar rutas.
OS/2	No es necesario eliminar rutas.
Windows NT	**route delete** *dirección_red dirección_cluster* **Notas:** 1. Este mandato debe escribirse en el indicador de mandatos de MS-DOS. 2. En Windows NT, se debe eliminar la ruta de más cada vez que se reinicie el servidor. 3. Para no tener que eliminar manualmente la ruta de más cada vez que se reinicie el servidor, es útil crear e instalar un servicio con el Kit de recursos de Windows NT que elimine automáticamente la ruta de más cada vez que se reinicie el servidor.

Utilización de Network Dispatcher con el servidor TN3270

Network Dispatcher puede utilizarse con un cluster de direccionadores 2210, 2212, 2216 o Network Utilities haciendo funciones de servidor TN3270E para proporcionar servicios de servidor TN3270E en entornos 3270 grandes. El asesor TN3270 permite que Network Dispatcher reúna estadísticas de carga de los servidores TN3270E en tiempo real con el fin de lograr la mejor distribución posible entre los servidores TN3270E. Además de los servidores TN3270E externos al direccionador Network Dispatcher, uno de los servidores TN3270E del cluster puede ser interno (puede ejecutarse en el mismo direccionador que Network Dispatcher).

Claves para la configuración

La configuración de servidores TN3270E externos (es decir, servidores TN3270E que no se ejecutan en el mismo direccionador que Network Dispatcher) es básicamente la misma que la configuración de un servidor TN3270E autónomo. De hecho, al servidor TN3270E le es igual que el tráfico proveniente de los clientes se asigne en otra máquina. Sin embargo, hay que tener en cuenta determinadas cuestiones al configurar los servidores TN3270E externos si se utilizan con Network Dispatcher:

- Cuando se configura un servidor TN3270E, la dirección IP del servidor TN3270E también debe configurarse en la máquina servidora como una dirección de interfaz. Los clientes envían paquetes a la dirección IP del servidor TN3270E y la máquina servidora acepta los paquetes para entregarlos a una función local, en este caso, la función de servidor TN3270E. Si los servidores TN3270E se utilizan con Network Dispatcher, los clientes envían paquetes a la dirección IP del cluster de Network Dispatcher y Network Dispatcher reenvía los paquetes a los servidores sin cambiarlos, de manera que los paquetes lleguen a las máquinas servidoras con la misma dirección IP de destino que la dirección IP del cluster. Por lo tanto, la dirección IP del servidor TN3270 de cada servidor debe ser la misma que la dirección IP del cluster y la dirección IP del cluster, a su vez, debe estar definida en todas las máquinas servidoras como una dirección de interfaz (cualquier interfaz IP habilitada servirá) de forma que la máquina servidora aceptará los paquetes para entregarlos localmente a la función de servidor TN3270E.
- Debe asegurarse de que los protocolos de direccionamiento que se utilicen en los servidores TN3270E (es decir, OSPF o RIP) no anuncien la dirección del cluster. El direccionador Network Dispatcher debe “poseer” la dirección del cluster, en lo que concierne a la red del cliente.
- Si el tráfico que va del cliente a Network Dispatcher se transmite por la misma LAN que el tráfico que va del Network Dispatcher al servidor, deberá asegurarse de que los servidores no respondan a las peticiones ARP de la dirección del cluster, de modo que la dirección del cluster no puede definirse en la interfaz del servidor de esta LAN. Network Dispatcher debe ser el único que responda al protocolo ARP en la LAN (o en las LAN) en la que se recibe el tráfico de los clientes proveniente de la red. La dirección del cluster puede configurarse alternativamente en el servidor TN3270E como una dirección de interfaz de otra interfaz, o puede configurarse como la dirección IP interna del servidor TN3270E.
- Cada servidor TN3270E debe configurarse en Network Dispatcher con una dirección IP de servidor exclusiva. Esta es la dirección que Network Dispatcher

utiliza para localizar el servidor. Esta dirección también debe configurarse como una dirección de interfaz en el direccionador que haga funciones de servidor TN3270E. Si la dirección IP exclusiva del servidor no es de la subred local de la máquina Network Dispatcher, Network Dispatcher debe poder localizar el servidor mediante una ruta estática definida en la máquina Network Dispatcher o mediante protocolos de direccionamiento que anuncien la dirección IP exclusiva del servidor.

- Para evitar que las conexiones del TN3270 se eliminen prematuramente de la tabla de conexiones de Network Dispatcher cuando venza cierto tiempo de espera sin actividad del cluster, se debe configurar el temporizador keepalive del servidor TN3270E en la modalidad de marca de temporizador con un valor de tiempo de espera menor que el tiempo de espera sin actividad del cluster. El servidor TN3270E envía un mensaje al cliente y espera una respuesta que impida que la conexión se quede sin actividad.

Cuando el servidor TN3270E está en el mismo direccionador que Network Dispatcher, se aplica lo siguiente:

- Puesto que los paquetes enviados por el software de reparto de carga a un servidor TN3270E interno todavía tendrán la dirección del cluster como dirección IP de destino del paquete, la dirección IP del servidor TN3270E debe configurarse como la dirección del cluster.
- Si el servidor TN3270E es externo a la máquina Network Dispatcher, la dirección IP del servidor TN3270E debe definirse en el direccionador como la dirección IP interna o como una dirección de interfaz, de forma que el paquete pueda entregarse localmente a la función de servidor TN3270E. Sin embargo, el servidor TN3270E es interno al direccionador Network Dispatcher, la dirección IP del servidor TN3270E no debe definirse en el direccionador como la dirección IP interna ni como una dirección de interfaz. Si la dirección IP del servidor TN3270E (es decir, la dirección del cluster) está definida como la dirección IP interna o como una dirección de interfaz, Network Dispatcher no recibirá nunca los paquetes sino que irán directamente a la función de servidor TN3270E del direccionador.
- Cada servidor TN3270E debe configurarse en Network Dispatcher con una dirección IP de servidor exclusiva. Para un servidor TN3270E interno, hay que configurar la dirección IP exclusiva del servidor de manera que sea la misma que la dirección IP interna de la máquina Network Dispatcher.
- En las versiones anteriores a la V3.4, un servidor TN3270E se podía configurar para que Network Dispatcher pudiera acceder a él tanto interna como externamente, pero no simultáneamente, ni podía cambiar entre la modalidad principal y la de espera. Como resultado, al implementar una solución de alta disponibilidad de Network Dispatcher con servidores TN3270E internos en ambos direccionadores Network Dispatcher, el Network Dispatcher de un direccionador no podía repartir su carga con el servidor TN3270E del otro direccionador Network Dispatcher.

  A partir de la versión V3.4 de AIS, al implementar una solución de alta disponibilidad de Network Dispatcher con servidores TN3270E internos en ambos direccionadores Network Dispatcher, los servidores TN3270E internos pueden configurarse para que ambos Network Dispatcher puedan acceder a ellos. Sólo hay que añadir un bucle de retorno en ambos direccionadores Network Dispatcher y definir la dirección IP del servidor TN3270E (es decir, la dirección del cluster) para las interfaces de los dos bucles de retorno. Cuando Network

Dispatcher está en estado activo, la dirección del cluster de la interfaz del bucle de retorno se inhabilitará para que sea Network Dispatcher el que reciba los paquetes con destino a la dirección del cluster. Cuando Network Dispatcher está en estado de espera, la dirección del cluster de la interfaz del bucle de retorno se habilitará para que sea el servidor TN3270E el que reciba localmente los paquetes con destino a la dirección del cluster. De esta forma es como en una configuración de alta disponibilidad ambos Network Dispatcher pueden utilizar un servidor TN3270E interno.

La máquina Network Dispatcher activa debe ser la única máquina que responda a las peticiones ARP de la dirección del cluster. Puesto que la dirección del cluster está definida en ambas máquinas Network Dispatcher de la interfaz del bucle de retorno, el ARP por proxy debe inhabilitarse en ambas máquina Network Dispatcher para permitir que la máquina Network Dispatcher en espera siga respondiendo a peticiones ARP de la dirección del cluster.

La máquina Network Dispatcher activa también debe poseer la dirección del cluster por lo que respecta a la red cliente, de manera que la máquina Network Dispatcher en espera (que tiene la dirección del cluster definida en la interfaz del bucle de retorno) no pueda anunciar la dirección del cluster. Por omisión, RIP no anuncia rutas de sistemas principales (rutas cuya máscara es 255.255.255.255), pero si el anuncio de rutas de sistemas principales está habilitado, se debe definir la política de RIP de manera que se inhabilite específicamente el anuncio de la dirección del cluster.

En este ejemplo se muestra la política para impedir que RIP anuncie una dirección IP de cluster (que aquí se supone que es 10.0.0.1). Obsérvese que la segunda entrada de la política permite que RIP anuncie las demás rutas.

```
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 están habilitados el direccionamiento limítrofe de AS y la importación de rutas directas, u OSPF está habilitada en la interfaz del bucle de retorno, la dirección del cluster definida en la interfaz del bucle de retorno se anunciará y se deberá definir la política de OSPF de manera que se inhabilite específicamente el anuncio de la dirección del cluster.

En el ejemplo siguiente se muestra una política que impide que OSPF importe una dirección IP de cluster (que aquí se supone que es 10.0.0.1). Obsérvese

que la segunda entrada de la política permite que OSPF importe las demás rutas directas.

```
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 explicitas y Network Dispatcher

Se ha de ser muy cuidadoso con la definición explícita de LU en un entorno de Network Dispatcher. Una petición de sesión en una LU implícita o explícita puede ser despachada a cualquier servidor. Esto significa que la LU explícita tiene que definirse en todos los servidores, puesto que no se sabe con antelación a que servidor se despachará la sesión.

Utilización de Network Dispatcher con el anuncio de direcciones del cluster

El anuncio de direcciones del cluster permite configurar si los protocolos de direccionamiento de la máquina Network Dispatcher deben anunciar las direcciones del cluster definidas en Network Dispatcher o no. Las direcciones del cluster que no se van a anunciar deben ser direcciones que formen parte de una subred que se anuncie y que sea local a la máquina Network Dispatcher. Las direcciones del cluster configuradas para que se anuncien se anunciarán como direcciones de sistema principal y no han de formar parte de una subred que se anuncie. Anunciar direcciones del cluster resulta ventajoso en las situaciones que se describen a continuación:

- En el caso de tener varios servidores en distintos lugares geográficos que ofrezcan el mismo contenido y pretender que los clientes se conecten al lugar

más próximo en el que hay un servidor activo. Se puede lograr el objetivo configurando las mismas direcciones del cluster en todos los lugares en que hay servidores y anunciando estas direcciones desde todos esos lugares. Los protocolos de direccionamiento de la red dirigirán las conexiones de los clientes al lugar más próximo. Si el lugar más próximo está inactivo, la conexión se realizará con el siguiente lugar más próximo. Recuerde que los cambios en la red (que un direccionador o un enlace de red se desactive o se active) o los cambios en la disponibilidad de un servidor, pueden cambiar la condición del servidor más próximo incluso en medio de conexiones cliente-servidor ya existentes. Esto no es preocupante en el caso de conexiones fugaces, como las de HTTP, pero pueden ser más que preocupantes en el caso de conexiones longevas, como las de Telnet o TN3270.

- El anuncio de direcciones del cluster permite utilizar la alta disponibilidad de Network Dispatcher en una red ATM IP clásico. Cuando el Network Dispatcher en espera toma el control del Network Dispatcher activo, envía una petición ARP gratuita a todas las interfaces para lograr que el tráfico futuro con destino a la dirección del cluster se envíe a una dirección MAC nueva. Con ATM IP clásico, el servidor ARP se actualiza, pero no puede obligar a los clientes a que renueven sus antememorias. Las antememorias del cliente no se actualizarán hasta que expire el tiempo de espera de renovación configurado para el cliente. Este puede ser de varios minutos. Las conexiones de nuevos clientes que no tienen almacenada en antememoria la dirección ATM del Network Dispatcher principal, obtendrán inmediatamente la del Network Dispatcher de reserva, pero las conexiones ya existentes cuando se produzca la toma de control se perderán y no podrán restablecerse hasta que expire el tiempo de espera de renovación de ese cliente y se actualice la antememoria del cliente. Al definir las direcciones del cluster que no forman parte de la subred ATM con la del direccionador y anunciarlas, los protocolos de direccionamiento dirigirán el tráfico destinado a las direcciones del cluster al Network Dispatcher más cercano. El Network Dispatcher principal dejará de anunciar las direcciones del cluster cuando pase al estado inactivo y el que está en espera empezará a anunciar las direcciones del cluster cuando pase a se el Network Dispatcher activo.

Los protocolos de direccionamiento de la máquina Network Dispatcher deben configurarse correctamente antes de que puedan anunciar las direcciones del cluster:

- Para RIP, se debe habilitar la opción de enviar rutas de sistemas principales.
- Para OSPF, se debe habilitar el direccionamiento limítrofe de AS y la importación tanto de rutas directas como de subred.
- Para BGP, se debe verificar que el rango de direcciones de la política de origen incluye las direcciones del cluster que se anuncien y también se debe habilitar la opción classless-bgp.

Utilización de Network Dispatcher con antememoria del servidor Web

Deberá utilizar Network Dispatcher para definir un cluster y un puerto para la Antememoria del servidor Web. Al definir un puerto con modalidad *antememoria*, se le pedirá que configure la partición de antememoria. Para ver un ejemplo, consulte el mandato **add port** en “Configuración y supervisión de la antememoria del servidor Web” en la página 227. Los valores de configuración de una partición de antememoria pueden modificarse más adelante mediante el mandato **f webc** en el indicador `Config>`, que le permitirá ir directamente a la configuración de la función

antememoria del servidor Web. Consulte el “Utilización de la antememoria del servidor Web” en la página 185 y “Configuración y supervisión de la antememoria del servidor Web” en la página 227 para obtener más información sobre función de almacenamiento en antememoria del servidor Web.

Nota: La antememoria del servidor Web sólo se soporta en los direccionadores IBM 2212 que disponen de la tarjeta HPSC (High Performance System Card).

Utilización de Network Dispatcher con antememoria de clientes eNetwork Host On-Demand

Deberá utilizar Network Dispatcher para definir un cluster y un puerto para la antememoria de clientes Host On-Demand. Al definir un puerto con modalidad *hod client cache*, se le pedirá que configure la partición de antememoria. Se muestra un ejemplo del mandato **add port** en “Configuración de la antememoria de clientes Host On-Demand” en la página 168. Los valores de configuración de una partición de antememoria pueden modificarse más adelante ejecutando el mandato **f hod** en el indicador `Config>`, que le permitirá ir directamente a la configuración de la función de antememoria de clientes Host On-Demand. Para obtener más información sobre la función de antememoria de clientes Host On-Demand, consulte el “Configuración y supervisión de la antememoria de clientes IBM eNetwork Host On-Demand” en la página 167.

Nota: La antememoria de clientes eNetwork Host On-Demand sólo se soporta en los direccionadores IBM 2212 que disponen de la tarjeta HPSC (High Performance System Card).

Utilización de Network Dispatcher con antememoria SHAC (Scalable High Availability Cache)

Se puede utilizar Network Dispatcher con un grupo de antememorias de servidor Web para crear una antememoria SHAC (Scalable High Availability Cache). Una antememoria SHAC consta de una o dos máquinas Network Dispatcher (la segunda se utiliza como máquina de reserva de la primera), dos o más máquinas de antememoria de servidor Web y, por lo menos, un servidor final. En la Figura 9 en la página 131 se muestra un ejemplo de una configuración SHAC. La máquina Network Dispatcher reparte la carga del tráfico de los clientes entre las máquinas que realizan funciones de antememoria y estas sirven los archivos de la antememoria o los obtienen de los servidores finales, si no están almacenados en antememoria.

Network Dispatcher debe utilizarse en una máquina de antememoria de servidor Web (consulte el apartado “Utilización de Network Dispatcher con antememoria del servidor Web” en la página 129), ya que Network Dispatcher realmente está funcionando en la máquina Network Dispatcher y en todas las máquinas que realizan funciones de antememoria.

En la máquina Network Dispatcher se debe configurar el cluster y el puerto, y la modalidad del puerto debe establecerse como *extcache* para indicar que se encarga de repartir la carga de un conjunto de antememorias escalables externas. Consulte el mandato **add port** en la “Add” en la página 134. En el puerto, la máquinas que realizan funciones de antememoria se configuran como servidores. Como ocurre con otros servidores, las direcciones IP de la interfaz de las

antememorias se utilizan como direcciones IP del servidor exclusivas configuradas en la máquina Network Dispatcher. El asesor y el gestor son críticos para la SHAC. El asesor HTTP debe habilitarse en la máquina Network Dispatcher para todos los puertos para los que existan antememorias externas (es decir, cuya modalidad de puerto sea extcache). Las consultas del asesor se utilizar para determinar si las antememorias están en funcionamiento. El gestor debe habilitarse y los porcentajes del gestor debe establecerse de modo que incluyan la entrada del asesor en los cálculos del peso (es decir, hay que establecer el porcentaje del asesor a un valor mayor que 0).

Si se configura una antememoria como servidor en un cluster/puerto de la máquina Network Dispatcher, también se debe configurar el mismo cluster y puerto en la función Network Dispatcher de la máquina que hace funciones de antememoria. Los puertos definidos en las máquinas que hacen funciones de antememoria deben establecerse en la modalidad de antememoria y los servidores finales deben definirse como servidores para esos puertos. El asesor HTTP también debe ejecutarse en las máquinas que hacen funciones de antememoria para que sean capaces de determinar la carga y la disponibilidad del servidor final.

Observe que una máquina Network Dispatcher puede repartir la carga mejor que un cluster SHAC. Para obtener más información, consulte la “Función SHAC (Scalable High Availability Cache)” en la página 192.

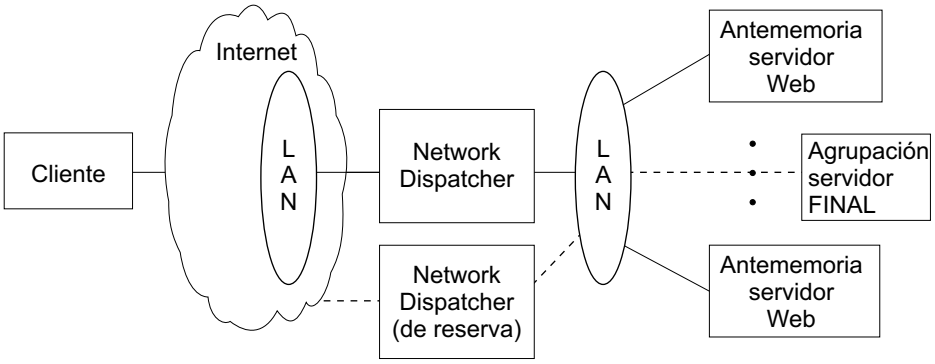


Figura 9. Servidores conectados a una red de área local

Configuración y supervisión de la función Network Dispatcher

En este capítulo se describen los mandatos de configuración y de funcionamiento de la función Network Dispatcher. Consta de los apartados siguientes:

Acceso a los mandatos de configuración de Network Dispatcher

Para acceder al entorno de configuración de Network Dispatcher:

1. Escriba **talk 6** en el indicador OPCON (*).
2. Escriba **feature ndr** en el indicador `Config >`.

Mandatos de configuración de Network Dispatcher

En la Tabla 12 se resumen los mandatos de configuración de Network Dispatcher y el resto del apartado se dedica a explicar los mandatos. Entre los mandatos en el indicador `NDR Config >`.

Tabla 12. Mandatos de configuración de 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 xxxii.
Add	Configura varios componentes del Network Dispatcher, incluyendo asesores, clusters, puertos y servidores.
Clear	Borra toda la configuración del Network Dispatcher.
Disable	Inhabilita los componentes ejecutor, gestor y de reserva del Network Dispatcher. También inhabilita asesores concretos.
Enable	Habilita los componentes ejecutor, gestor y de reserva del Network Dispatcher. También habilita asesores concretos.
List	Muestra toda la configuración del Network Dispatcher, o partes concretas de la configuración.
Remove	Elimina partes concretas de la configuración del Network Dispatcher.
Set	Cambia los parámetros de configuración de asesores, clusters, puertos, servidores o el gestor del Network Dispatcher.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxiii.

Add

Utilice el mandato **add** para configurar asesores, clusters, puertos, servidores y direcciones accesibles. Para la función de alta disponibilidad también puede configurar si este Network Dispatcher es el principal o el de reserva y qué direcciones IP utilizar para el mecanismo de latido y para la sincronización de bases de datos.

Sintaxis:

add advisor . . .

backup . . .

cluster . . .

heartbeat . . .

port . . .

reach . . .

server . . .

Advisor *nombre núm-puerto intervalo tiempo-espera puerto-com*

Especifica el nombre y el puerto de un asesor. Este parámetro también especifica con qué frecuencia reunirá información el asesor para un protocolo determinado y un período de tiempo, tras el que se considerará que el informe del asesor está obsoleto.

nombre Especifica el tipo de asesor. Escriba el número de asesor que le corresponde al tipo de asesor que se quiere añadir.

Tabla 13. Nombres y números de puerto del asesor

Número de asesor	Nombre de asesor	Número 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: de 0 a 8

Valor por omisión: 1

núm-puerto

Especifica el número de puerto del asesor.

Valores válidos: de 1 a 65535

Valores por omisión: Consulte la Tabla 13.

intervalo Especifica la frecuencia, en segundos, con que el asesor consulta a su protocolo para cada servidor. Transcurrida la mitad del intervalo sin obtener respuesta por parte del servidor, el asesor considera que el protocolo no está disponible.

Valores válidos: de 1 a 65535

Valor por omisión: 5

tiempo de espera
Especifica el intervalo de tiempo, en segundos, tras el cual se considera que el informe del asesor está obsoleto.

Para asegurarse de que el gestor no utiliza información desfasada en las decisiones que debe tomar sobre el reparto de la carga, el gestor no utilizará la información suministrada por el asesor cuya indicación de la hora sea anterior a la hora definida 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 no hará caso de los informes que debe utilizar. Por omisión, los informes del asesor no tienen tiempo de espera.

Lo normal es que se utilice este valor si se inhabilita un asesor. No confunda este parámetro con el tiempo de espera de la mitad del intervalo descrito antes, que tiene que ver con la falta de respuesta de un servidor.

Valores válidos: de 0 a 65535

Valor por omisión: 0, lo que significa que el informe del asesor nunca caducará.

puerto-com
Especifica el número de puerto utilizado por el asesor TN3270 para comunicarse con los servidores TN3270. Este parámetro es sólo de entrada para el asesor TN3270. Debe coincidir con el número de puerto del asesor establecido en la configuración del servidor TN3270.

Valores válidos: de 1 a 65535

Valor por omisión:

- Valor por omisión para TN3270:10008

Nota: Como el componente gestor es requisito previo para el funcionamiento del asesor, debe habilitarse el gestor antes de poder habilitar los asesores. Al configurar los pesos del servidor, utilizados para tomar decisiones sobre el reparto de la carga, también deberá definir los porcentajes del gestor para que el gestor tenga en cuenta las entradas de los asesores. Para que el asesor funcione correctamente, también se debe definir la dirección IP interna con el mandato **set internal-ip-address**. Consulte Configuración y supervisión IP, en *Configuración y supervisión de protocolos - Manual de consulta, 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 *cometido estrategia*

Especifica si este Network Dispatcher es el principal o el de reserva.

cometido Define si este es el Network Dispatcher principal o el de reserva. Utilice este mandato sólo si quiere tener una configuración redundante y si quiere ejecutar la función de alta disponibilidad. En este caso, también deberá configurar el mecanismo de latido (**add heartbeat**) y de accesibilidad (**add reach**).

Valores válidos: 0 ó 1

0 = principal

1 = de reserva

Valor por omisión: 0

estrategia

Especifica si Network Dispatcher volverá a la modalidad principal automática o manualmente. Si se produce una anomalía en el Network Dispatcher principal y pasa a modalidad de espera (lo que quiere decir que la función de toma de control de IP realizará una copia de seguridad) y a continuación vuelve a estar disponible, se convertirá automáticamente en el Network Dispatcher activo, si la estrategia se define como *automática*, tan pronto como las bases de datos se sincronicen. Si la estrategia se define como *manual*, el primer Network Dispatcher principal pasará a modalidad de espera y el operador deberá utilizar el mandato **switchover** en talk 5 para volver a activarlo. Consulte “Switchover” en la página 162.

Valores válidos: 0 ó 1

0 = automático

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-inactividad Anunciar-dirección-cluster Coste-ruta-anunciada*

Especifica la dirección IP de un cluster y la frecuencia con que el ejecutor realizará la recogida de basura de la base de datos del Network Dispatcher. Si se van a configurar las direcciones del cluster para que

se anuncien, hallará más información en el apartado “Utilización de Network Dispatcher con el anuncio de direcciones del cluster” en la página 128. Para las direcciones del cluster que no se van a configurar para que se anuncien, se deben elegir las direcciones del cluster que forman parte de una subred que se anuncie y que sea local a la máquina Network Dispatcher. Normalmente será la subred en la que el Network Dispatcher recibe el tráfico de los clientes proveniente del siguiente direccionador de salto.

Nota: La direcciones IP del cluster no deben coincidir con la dirección IP interna del direccionador ni con ninguna de las direcciones IP de interfaces definidas en el direccionador. Si se está ejecutando Network Dispatcher y un servidor TN3270 en la misma máquina, la dirección del cluster puede coincidir con una dirección IP definida en la interfaz del bucle de retorno. Hallará más información en “Utilización de Network Dispatcher con el servidor TN3270” en la página 125.

dirección Especifica la dirección IP del cluster.

Valores válidos: Cualquier dirección IP

Valor por omisión: 0.0.0.0

cuenta de FIN

Especifica el número de conexiones que deben estar en el estado FIN antes de que el ejecutor intente eliminar la información de conexión no usada de la base de datos del Network Dispatcher después de transcurrido el *tiempo de espera de FIN* o el definido en el *temporizador de inactividad*.

Valores válidos: de 0 a 65535

Valor por omisión: 4000

tiempo de espera de FIN

Especifica el número de segundos que una tarea puede permanecer en el estado de FIN antes de que el ejecutor intente eliminar la información de conexión no usada de la base de datos del Network Dispatcher.

Valores válidos: de 0 a 65535

Valor por omisión: 30

Temporizador de inactividad

Especifica el número de segundos que el ejecutor esperará que una conexión esté inactiva, antes de intentar eliminar la información de la conexión de la base de datos del Network Dispatcher.

Valores válidos: de 0 a 65535

Valor por omisión: 1500

Anunciar-dirección-cluster

Indica si la dirección del cluster debe anunciarse.

Valores válidos: yes o no

Valor por omisión: no

Coste-ruta-anunciada

Indica el coste de la ruta anunciada. Esta pregunta se realiza solamente si la respuesta a **Advertise cluster address** es *yes* (sí).

Valores válidos: de 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 del mecanismo de Latido. El mensaje del mecanismo de Latido se trasmitirá de la *dirección1*, perteneciente a este Network Dispatcher, a la *dirección2*, que pertenece al igual del Network Dispatcher.

Nota: Es obligatorio configurar más de una ruta para el latido entre ambos Network Dispatcher, para garantizar que no se interrumpa la comunicación de latidos entre las máquinas principal y de reserva si se produce una anomalía en una sola interfaz.

Si sólo se dispone de una conexión LAN entre los dos Network Dispatcher, se puede establecer el segundo latido a través de una conexión LAN sencilla (un cable cruzado utilizado directamente entre dos puertos Ethernet) o una conexión serie punto a punto (una conexión PPP próxima a través de un cable de módem nulo utilizando una dirección IP no numerada).

dirección1

Especifica la dirección IP de la interfaz de este Network Dispatcher desde la que se transmiten los mensajes del mecanismo de Latido.

Valores válidos: Cualquier dirección IP.

Valor por omisión: 0.0.0.0

dirección2

Especifica la dirección IP de la interfaz del igual del Network Dispatcher que recibe los mensajes del mecanismo de Latido. Esta dirección debe ser accesible 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 sus atributos.

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 IP cuya carga puede repartirse 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 de este puerto. Esto afecta a la diferencia que habrá en el número de peticiones que el ejecutor entregará 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 único cliente a un único servidor (llamado adherente), utilizará ftp pasivo (pftp), utilizará la antememoria del servidor Web (antememoria), las enviará a un conjunto de antememorias escalables externas (antememoria externa), utilizará la antememoria de clientes Host On-Demand, o no utilizará ningún protocolo particular para este cluster (ninguno).

Valores válidos: 0 - 5, donde:

- 0 = none (ninguna)
- 1 = sticky (adherente)
- 2 = pftp
- 3 = cache (sólo para dispositivos con HPSC)
- 4 = extcache (antememoria externa)
- 5 = hod client cache (sólo para dispositivos con HPSC)

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, 3=cache 4=extcache 5=hod client cache ]? 0
```

Notas:

1. Si se selecciona la modalidad de puerto 3 (`cache=3`), consulte el “Configuración y supervisión de la antememoria del servidor Web” en la página 227 para obtener más información sobre la antememoria del servidor Web.
2. Si se selecciona la modalidad de puerto 5 (`hod client cache=5`), consulte el “Configuración y supervisión de la antememoria de clientes IBM eNetwork Host On-Demand” en la página 167 para obtener más información sobre la antememoria del servidor Web.

reach *dirección*

Especifica las direcciones de sistema principal a las que el Network Dispatcher debe poder acceder para funcionar correctamente. Pueden ser la dirección de un servidor, de un direccionador, de una estación de administración o de otro sistema principal IP.

dirección Especifica la dirección IP 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 que pertenece el servidor.

Valores válidos: Cualquier dirección IP

Valor por omisión: 0.0.0.0

núm-puerto

Especifica el protocolo que ejecuta 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 concreto.

Valores válidos: de 0 hasta el valor del *peso-máx* especificado en el mandato add port.

Valor por omisión: peso-máx especificado en el mandato add port

estado-servidor

Especifica si el ejecutor debe considerar el servidor como disponible o como no disponible, cuando aquél empiece a procesar.

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 a la configuración de parámetros

En la Tabla 14 se listan los límites de las distintas opciones que pueden configurarse para un Network Dispatcher

Tabla 14. Límites a la configuración de parámetros

Parámetro	Límite (con HPSC)	Límite (sin HPSC)
Asesores	32 por cada 2212	8 por cada 2212
Clusters	100 por cada 2212	32 por cada 2212
Latidos	32 por cada 2212	8 por cada 2212
Puertos	32 por cluster	8 por cluster
Accesos	32 por cada 2212	8 por cada 2212
Servidores	128 por cada puerto configurado, 512 por cada número de puerto correspondiente a todos los clusters configurados para el 2212.	32 por cada puerto configurado, 128 por cada número de puerto correspondiente a todos los clusters configurados para el 2212.
Dirección IP del servidor exclusiva	32 por cada 2212	32 por cada 2212

Clear

Utilice el mandato **clear** para borrar toda la configuración del Network Dispatcher.

Sintaxis:

clear

Disable

Utilice el mandato **disable** para inhabilitar un componente del Network Dispatcher.

Sintaxis:

disable advisor . . .

backup

executor

manager

advisor *nombre núm-puerto*

Inhabilita un asesor del Network Dispatcher.

nombre Especifica el tipo de asesor. Escriba el número de asesor que le corresponde al tipo de asesor que se quiere inhabilitar.

Para obtener más información, consulte la Tabla 13 en la página 134.

Valores válidos: de 0 a 8

Valor por omisión: 0

núm-puerto

Especifica el número de puerto del asesor.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe escribir 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. Al inhabilitar el ejecutor se inhabilita la función Network Dispatcher.

Ejemplo:

```
disable executor
Executor is now disabled.
```

Nota: Al inhabilitar el ejecutor se parará el gestor, los asesores y la función de alta disponibilidad, en caso de que estuvieran ejecutándose.

manager Inhabilita el gestor del Network Dispatcher. El gestor es un componente opcional. Sin embargo, si no utiliza el gestor, Network Dispatcher repartirá la carga según un método de planificación rotativo, basado en los pesos actuales de los servidores.

Ejemplo:

```
disable manager
Manager is now disabled.
```

Nota: Puesto que el componente gestor es requisito previo para el funcionamiento de los asesores, si se inhabilita el gestor, se detendrá el funcionamiento de todos los gestores.

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 para el Network Dispatcher.

nombre Especifica el tipo de asesor. Escriba el número de asesor que le corresponde al tipo de asesor que se quiere habilitar.

Para obtener más información, consulte la Tabla 13 en la página 134.

Valores válidos: de 0 a 8

Valor por omisión: 0

núm-puerto

Especifica el número de puerto del asesor.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe escribir 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: Como el componente gestor es requisito previo para el funcionamiento del asesor, debe habilitarse el gestor antes de poder habilitar los asesores. Al configurar los pesos del servidor, utilizados para tomar decisiones sobre el reparto de la carga, también deberá definir los porcentajes del gestor para que el gestor tenga en cuenta las entradas de los asesores. Para que el asesor funcione correctamente, también se debe definir la dirección IP interna con el mandato **set internal-ip-address**. Consulte el capítulo Configuración y supervisión IP, de *Configuración y supervisión de protocolos - Manual de consulta, 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 función de reserva, deberá añadir al menos un latido

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.
```

Al habilitar el gestor por primera vez, se crea un registro del gestor con los valores por omisión siguientes:

Intervalo: 2 segundos

Ciclo de renovación: 2

Sensibilidad: 5 %

Corrección: 1.5

Porcentajes:

- **Activas:** 50%
- **Nuevas:** 50%
- **Asesor:** 0
- **Sistema:** 0

Consulte el mandato “Set” en la página 148 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 Muestra toda la información de configuración del Network Dispatcher. Esto incluye a los asesores, función de reserva, clusters, 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 Muestra la configuración de los asesores del Network Dispatcher.

backup Muestra la configuración de la función de reserva del Network Dispatcher.

cluster Muestra la configuración de los clusters del Network Dispatcher.

manager Muestra la configuración del gestor del Network Dispatcher.

port Muestra la configuración de los puertos del Network Dispatcher.

server Muestra la configuración de los servidores asociados con los clusters del Network Dispatcher.

Remove

Utilice el mandato **remove** para suprimir parte de la configuración de Network Dispatcher.

Sintaxis:

remove advisor . . .
backup
cluster . . .
heartbeat . . .
port . . .

reach . . .

server . . .

advisor *nombre núm-puerto*

Elimina un asesor determinado de la configuración de Network Dispatcher.

nombre Especifica el tipo de asesor. Escriba el número de asesor que le corresponde al tipo de asesor que se quiere eliminar.

Para obtener más información, consulte la Tabla 13 en la página 134.

Valores válidos: de 0 a 8

Valor por omisión: 0

núm-puerto

Especifica el número de puerto del asesor.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe escribir 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 función de reserva es requisito previo para las funciones de latido y de acceso, si se elimina la función de reserva, se detendrá el funcionamiento de las funciones de latido y de acceso.

Ejemplo: `remove backup`

cluster *dirección*

Elimina un cluster de la configuración de Network Dispatcher.

dirección Especifica la dirección IP del cluster.

Valores válidos: Cualquier dirección IP

Valor por omisión: 0.0.0.0

Nota: Al eliminar una dirección de cluster también se eliminan todos los puertos y servidores asociados con ese 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 latido de la configuración de Network Dispatcher.

dirección Especifica la dirección IP del Network Dispatcher de destino.

Valores válidos: Cualquier dirección IP

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 determinado de la configuración de 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 escribir un número de puerto.

Notas:

1. Al eliminar un puerto también se eliminarán todos los servidores asociados con dicho puerto.
2. Si la modalidad de puerto que se va a eliminar es la de antememoria, también se eliminará la configuración del proxy de la antememoria del servidor Web asociado.
3. Si la modalidad de puerto que se va a eliminar es la de la antememoria de clientes Host On-Demand, también se eliminará la configuración del proxy de la antememoria de clientes Host On-Demand.

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 el Network Dispatcher debe poder acceder.

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 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 escribir 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 ya existentes. 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 de un asesor.

nombre Especifica el tipo de asesor. Escriba el número de asesor que le corresponde al tipo de asesor que se quiere definir.

Para obtener más información, consulte la Tabla 13 en la página 134.

Valores válidos: de 0 a 8

Valor por omisión: 0

núm-puerto
Especifica el número de puerto del asesor.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe escribir un número de puerto.

intervalo Especifica la frecuencia con que el asesor consulta a su protocolo para cada servidor. Transcurrida la mitad del intervalo sin obtener respuesta por parte del servidor, el asesor considera que el protocolo no está disponible.

Valores válidos: de 0 a 65535

Valor por omisión: 5

tiempo de espera
Especifica el intervalo de tiempo, en segundos, tras el cual el asesor considera que el protocolo no está disponible.

Para asegurarse de que el gestor no utiliza información desfasada en las decisiones que debe tomar sobre el reparto de la carga, el gestor no utilizará la información suministrada por el asesor cuya indicación de la hora sea anterior a la hora definida 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 no hará caso de los informes que debe utilizar. Por omisión, los informes del asesor no tienen tiempo de espera.

Lo normal es que se utilice este valor si se inhabilita un asesor. No confunda este parámetro con el tiempo de espera de la mitad del intervalo descrito antes, que tiene que ver con la falta de respuesta de un servidor.

Valores válidos: de 0 a 65535

Valor por omisión: 0, lo que significa que se considera que el protocolo siempre está disponible.

puerto-com
Especifica el número de puerto utilizado por el asesor TN3270 para comunicarse con los servidores TN3270 . Este parámetro es sólo de entrada para el asesor TN3270 .

Valores válidos: de 1 a 65535

Valor por omisión:

- Valor por omisión para 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-inactividad*
Cambia la cuenta de FIN, el tiempo de espera de FIN y el temporizador de inactividad de un cluster en la configuración de Network Dispatcher.

dirección Especifica la dirección IP del cluster.

Valores válidos: Cualquier dirección IP

Valor por omisión: 0.0.0.0

cuenta de FIN
Especifica el número de conexiones que deben estar en el estado FIN antes de que el ejecutor intente eliminar la infor-

mación de conexión no usada de la base de datos del Network Dispatcher después de transcurrido el *tiempo de espera de FIN* o el definido en el *temporizador de inactividad*.

Valores válidos: de 0 a 65535

Valor por omisión: 4000

tiempo de espera de FIN
Especifica el número de segundos que han de transcurrir antes de que el ejecutor intente eliminar la información de conexión no usada de la base de datos de Network Dispatcher.

Valores válidos: de 0 a 65535

Valor por omisión: 30

Temporizador de inactividad
Especifica el número de segundos que una conexión puede permanecer inactiva, antes de que el ejecutor intente eliminar la información de la conexión de la base de datos de 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 porcentaje renovación sensibilidad corrección*
Define los valores que el gestor utiliza para determinar qué servidor satisfará mejor una petición.

intervalo Especifica, en segundos, el tiempo que transcurrirá antes de que el gestor actualice los pesos del servidor que utiliza el ejecutor para repartir las cargas de las conexiones.

Valores válidos: de 0 a 65535

Valor por omisión: 2

porcentaje
Especifica la importancia relativa de factores externos en las decisiones que toma el gestor sobre pesos. La suma de los porcentajes debe ser igual a 100. Los factores son los siguientes:

activo Número de conexiones activas en cada servidor TCP/IP, al que le sigue la pista el ejecutor.

Valores válidos: de 0 a 100

Valor por omisión: 50

nuevas Número de conexiones nuevas en cada servidor TCP/IP, conocido por el ejecutor.

Valores válidos: de 0 a 100

Valor por omisión: 50

asesor Entrada de los asesores de protocolo definida para Network Dispatcher.

Valores válidos: de 0 a 100

Valor por omisión: 0

sistema Entrada del asesor del sistema MVS proporcionada por la herramienta de supervisión del sistema WLM de MVS.

Valores válidos: de 0 a 100

Valor por omisión: 0

renovación

Especifica la frecuencia con que el gestor solicita al ejecutor que le informe sobre el estado. Este parámetro se especifica como un número de *intervalos*.

Valores válidos: de 0 a 100

Valor por omisión: 2

sensibilidad

Especifica el cambio en el porcentaje de los pesos de todos los servidores de un puerto, tras el cuál, el gestor actualiza los pesos que utiliza el ejecutor para repartir la carga de las conexiones.

Valores válidos: de 0 a 100

Valor por omisión: 5

corrección

Especifica un límite al peso que puede cambiar un servidor. La corrección minimiza la frecuencia con que se producen los cambios en la distribución de peticiones. Un índice de corrección más alto hará que los pesos cambien menos a menudo. Un índice de corrección más bajo hará que los pesos cambien más a menudo.

Valores válidos: valor decimal entre 1,0 y 42 949 673,00

Valor por omisión: 1,5

Nota: Sólo pueden especificarse dos números decimales.

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 el tipo de puerto, el peso máximo y la modalidad del puerto para un cluster y número de puerto determinados.

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 escribir un número de puerto.

tipo-puerto

Especifica el tipo de tráfico IP cuya carga puede repartirse en este puerto.

Valores válidos:

- 1 = TCP
- 2 = UDP
- 3 = ambos

Valor por omisión: 3

peso-máx

Especifica el peso para los servidores de este puerto. Esto afecta a la diferencia que habrá en el número de peticiones que el ejecutor entregará 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 único cliente a un único servidor (llamado adherente), utilizará ftp pasivo (pftp), utilizará la antememoria del servidor Web (antememoria), las enviará a un conjunto de antememorias escalables externas, utilizará la antememoria de clientes Host On-Demand, o no utilizará ningún protocolo para este cluster (ninguno).

Valores válidos:

- 0 = none (ninguna)
- 1 = sticky (adherente)
- 2 = pftp
- 3 = cache (sólo para dispositivos con HPSC)
- 4 = extcache (antememoria externa)
- 5 = hod client cache (sólo para dispositivos con HPSC)

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) [3]?
Max. weight (0-100) [20]? 30
Port mode (none=0, sticky=1, pftp=2, cache=3, extcache=4 hod client cache=5) [0]?
```

Notas:

1. Si se selecciona la modalidad de puerto 3 (cache=3), consulte el apartado “Configuración y supervisión de la antememoria del servidor Web” en la página 227 para obtener información.
2. Si se selecciona la modalidad de puerto 5 (hod client cache=5), consulte el apartado “Configuración y supervisión de la antememoria de clientes IBM eNetwork Host On-Demand” en la página 167 para obtener más información.

server *dirección-cluster núm-puerto dirección-servidor peso estado*

Cambia el estado y el peso de un servidor concreto de un cluster.

dirección-cluster

Especifica la dirección IP del cluster al que pertenece el 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 escribir 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 aquél empiece a procesar.

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 concreto.

Valores válidos: de 0 hasta el valor del *peso-máx* especificado en el mandato add port.

Valor por omisión: peso-máx especificado en el mandato add 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. Escriba **talk 5** en el indicador OPCON (*).
2. Escriba **feature ndr** en el indicador GWCON (+).

El Network Dispatcher también puede supervisarse mediante SNMP. Para obtener más información, consulte el apartado " Gestión SNMP", de la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 1*.

Mandatos de supervisión del Network Dispatcher

En la Tabla 15 se resumen todos los mandatos de supervisión del Network Dispatcher y el resto del apartado se dedica a explicar los mandatos. Entre los mandatos en el indicador `NDR >`.

Tabla 15. Mandatos de supervisión de 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 xxxii.
List	Muestra los atributos configurados actualmente para el asesor, clusters, puertos o servidores.
Quiesce	Especifica que no se deben enviar más peticiones de conexión a un servidor. Además, detiene temporalmente las funciones de latido y acceso.
Report	Muestra un informe sobre el asesor y el gestor.
Status	Muestra el estado actual de los contadores, clusters, puertos, servidores, asesor, gestor y función de reserva.
Switchover	Obliga a un Network Dispatcher que se está ejecutando en modalidad de espera a convertirse en el Network Dispatcher activo. Este mandato es necesario utilizarlo si se ha especificado que la modalidad de intercambio es manual.
Unquiesce	Permite al gestor del Network Dispatcher asignar un peso mayor que 0 a un servidor previamente desactivado en cada puerto para el que está configurado el servidor. Esta acción permite enviar nuevas peticiones de conexión 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 xxxiii.

List

Utilice el mandato **list** para visualizar información sobre el Network Dispatcher.

Sintaxis:

list advisor
cluster
port
server

advisor Muestra la configuración de los asesores del Network Dispatcher que están actualmente habilitados.

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 Muestra 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 Muestra 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 Muestra 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
```

En la página 161 podrá encontrar una descripción de la información mostrada por el mandato.

Quiesce

Utilice el mandato **quiesce** para parar temporalmente las funciones de latido o de acceso, o para especificar que no deben enviarse más peticiones de conexión a un servidor.

Sintaxis:

quiesce heartbeat
manager
reach

heartbeat *dirección*

Detiene la vía elegida para la función de latido. La *dirección* es la dirección IP del Network Dispatcher remoto al que envía mensajes de Latido este Network Dispatcher.

Ejemplo:

```
quiesce heartbeat
Remote Address [0.0.0.0]? 131.2.25.94
```

manager *dirección*

Especifica que no deben hacerse 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 que realiza el Network Dispatcher en la dirección especificada para determinar si es accesible, donde la *dirección* es la dirección IP que forma parte de los criterios de accesibilidad.

Ejemplo:

```
quiesce reach
Reach Address [0.0.0.0]? 131.2.25.92
```

Report

Utilice el mandato **report** para ver un informe sobre el asesor o sobre el gestor.

Sintaxis:

report advisor

manager

advisor *tipo núm-puerto*

Muestra un informe sobre un asesor determinado.

tipo El tipo de asesor. Escriba el número de asesor correspondiente al tipo de asesor. En la Tabla 13 en la página 134 se listan los tipos de asesores.

núm-puerto 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 que se muestra para las direcciones de los servidores representa:

≥0 Carga del servidor

-1 El asesor no puede ponerse en contacto con el servidor.

manager Muestra un informe sobre la información actual del gestor.

Ejemplo:

```
report manager

-----------------------------------
|  HOST TABLE LIST  |   STATUS    |
-----------------------------------
|  131.2.25.93      |    ACTIVE   |
|  131.2.25.94      |    ACTIVE   |
-----------------------------------
```

La información del informe indica lo siguiente:

Status Muestra el estado de la dirección del servidor.

Quiesce El servidor se ha desactivado.

Active El servidor no se ha desactivado.

```
-------------------------------------------------------------------------------
|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 del informe indica lo siguiente:

Weight El cálculo del peso total de este servidor.

- **Now** El peso anterior asignado al servidor.
- **New** El peso más reciente asignado al servidor.

Active % El porcentaje de la conexión activa que se utiliza para el cálculo del peso total del servidor. El valor de este parámetro se establece mediante el mandato **set manager proportions**. Consulte la página 150.

- **Wt** Es peso utilizado para el cálculo del peso total.
- **Connect** Número de conexiones activas del servidor.

New % El porcentaje de la conexión nueva que se utiliza para el cálculo del peso total del servidor. El valor de este parámetro se establece mediante el mandato **set manager proportions**. Consulte la página 150.

- **Wt** Es peso utilizado para el cálculo del peso total.
- **Connect** Número de conexiones nuevas del servidor.

Port % El porcentaje del asesor que se utiliza para el cálculo del peso total del servidor. El valor de este parámetro se establece mediante el mandato **set manager proportions**. Consulte la página 150.

- **Wt** Es peso utilizado para el cálculo del peso total.

Load La carga de este servidor según informa el asesor.

System % El porcentaje del supervisor del sistema, utilizado para calcular el peso total del servidor. El valor de este parámetro se establece mediante el mandato **set manager proportions**. Consulte la página 150.

Wt Es peso utilizado para el cálculo del peso total.

Load La carga de este servidor según informa el supervisor del sistema.

Status

Utilice el mandato **status** para obtener el estado de los asesores, función de reserva, contador, clusters, gestor, puertos y servidores.

Sintaxis:

status advisor
backup
cluster
counter
manager
ports
servers

advisor *nombre núm-puerto*

Obtiene el estado de un asesor determinado.

nombre Especifica el tipo de asesor. Escriba el número de asesor correspondiente al tipo de asesor. En la Tabla 13 en la página 134 se listan los tipos de asesores.

núm-puerto
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 determinado, 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
```

En la página 161 se pueden obtener definiciones de los campos mostrados.

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 determinado, donde:

dirección-cluster
: es la dirección IP del cluster.

núm-puerto
: es el número de puerto del 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 sobre el servidor indica lo siguiente:

Address Dirección IP del servidor

Weight Peso actualmente asignado a este servidor

Count Cuenta acumulada de las conexiones TCP y paquetes UDP

TCP Count Cuenta acumulada de conexiones TCP

UDP Count Cuenta acumulada de paquetes UDP

Active Número de conexiones TCP activas

FIN Conexiones TCP en estado FIN

Complete Conexiones TCP terminadas (detectado ACK después de FIN)

Status Estado configurado del servidor:

- **active** El servidor está activo.
- **down** El servidor está inactivo.
- **quiesced** El servidor está desactivado.
- **not responding** El servidor no responde al asesor.

Saved weight Peso del servidor anterior a que el servidor se marcara como inactivo

server *dirección*

Obtiene el estado de un servidor determinado, donde la *dirección* es la dirección IP del cluster al que 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 obligar a un Network Dispatcher que se está ejecutando en modalidad de espera a convertirse en el Network Dispatcher activo cuando la estrategia de intercambio es manual. Este mandato debe entrarse en el sistema principal donde se está ejecutando el Network Dispatcher que está en modalidad de espera.

Sintaxis:

sw**itchover**

Unquiesce

Utilice el mandato **unquiesce** para reiniciar un gestor o una función de latido o de acceso detenidos previamente con el mandato **quiesce**.

Sintaxis:

u**nquiesce** heartbeat

manager

reach

heartbeat *dirección*

Reinicia la vía para los mensajes de Latidos, donde *dirección* es la dirección IP del network dispatcher remoto al que este Network Dispatcher está enviando mensajes de Latidos.

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 que realiza el Network Dispatcher en la dirección especificada para determinar si es accesible, donde la *dirección* es la dirección IP que forma parte de los criterios de accesibilidad.

Ejemplo:

```
unquiesce reach
Reach address [0.0.0.0]? 20.3.4.5
```

Soporte de reconfiguración dinámica de Network Dispatcher

En este apartado se describe la reconfiguración dinámica (DR) y cómo afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

El mandato **delete interface** de CONFIG (Talk 6) no es aplicable a NDR. Network Dispatcher es una función y no está configurada como interfaz.

Mandato activate interface de GWCON (Talk 5)

El mandato **activate interface** de GWCON (Talk 5) no es aplicable a NDR. Network Dispatcher es una función y no está configurada como interfaz.

Mandato reset interface de GWCON (Talk 5)

El mandato **reset interface** de GWCON (Talk 5) no es aplicable a NDR. Network Dispatcher es una función y no está configurada como interfaz.

Mandatos de cambio inmediato de CONFIG (Talk 6)

NDR da soporte a los siguientes mandatos de CONFIG que cambian inmediatamente el estado operativo del dispositivo. Estos cambios se guardan y se mantienen si el dispositivo se reinicia, si se vuelve a cargar 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 **Nota:** Si la modalidad de puerto seleccionada es la antememoria de clientes del servidor Web o la antememoria de clientes Host On-Demand, los cambios en el proxy HTTP no son inmediatos.
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:** Si el ejecutor está inhabilitado, se eliminarán todos los clusters, puertos y servidores de las estructuras del código de ejecución, pero *NO de la memoria SRAM*. Si la modalidad de puerto que se ha eliminado era la antememoria de clientes del servidor Web o la antememoria de clientes Host On-Demand, se inhabilitarán todas las particiones de las antememorias de clientes del servidor Web o de la antememoria de clientes Host On-Demand y se cerrarán los proxies HTTP.
CONFIG, feature ndr, disable manager
CONFIG, feature ndr, enable advisor
CONFIG, feature ndr, enable backup
CONFIG, feature ndr, enable executor **Nota:** Si el ejecutor está habilitado y existen puertos de antememoria para los clientes del servidor Web o para los clientes de Host On-Demand, los cambios en los proxies HTTP y en las particiones no son automáticos ni inmediatos.
CONFIG, feature ndr, enable manager
CONFIG, feature ndr, remove advisor
CONFIG, feature ndr, remove backup
CONFIG, feature ndr, remove cluster **Nota:** Al eliminar un cluster todos los puertos y servidores asociados con ese cluster se eliminarán de las estructuras del código de ejecución y de la memoria SRAM. Si la modalidad del puerto eliminado era la de antememoria de clientes del servidor Web o la de antememoria de clientes Host On-Demand, el proxy HTTP también se desactivará y su memoria SRAM se borrará.
CONFIG, feature ndr, remove heartbeat

CONFIG, feature ndr, remove port **Nota:** Si la modalidad del puerto que se va a eliminar es la de la antememoria de clientes del servidor Web o la de la antememoria de clientes Host On-Demand, el proxy HTTP también se desactivará y su memoria SRAM se borrará.
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 **Nota:** Si la modalidad de este puerto era la de la antememoria de clientes del servidor Web o la de la antememoria de clientes Host On-Demand y ahora se va a establecer a otra distinta, los proxies HTTP de estos puerto se cerrarán y sus memorias SRAM se borrarán. Además, si el software operativo establece la modalidad del puerto de como cache o hod client cache, los cambios en el proxy HTTP no se realizarán inmediatamente.
CONFIG, feature ndr, set server

Mandatos no reconfigurables dinámicamente

Todos los parámetros de configuración de NDR pueden cambiarse dinámicamente.

Configuración y supervisión de la antememoria de clientes IBM eNetwork Host On-Demand

La antememoria de clientes Host On-Demand permite que los clientes Web se conecten con aplicaciones de sistemas principales SNA utilizando un programa de emulación de terminales basado en Java™, que conecta el cliente al sistema principal mediante TN3270. Una aplicación menos común de la función Host On-Demand es la utilización de Telnet para la emulación de terminales que no son TN3270. Soporta sesiones 3270, 5250, VT (VT52, VT100, VT220_7_BIT, VT220_8_BIT), y de pasarela CICS.

La dirección IP de los servidores Telnet tiene como valor por omisión la dirección del servidor Host On-Demand. Esto quiere decir que en la configuración más sencilla, el servidor TN3270E será externo al direccionador.

En una configuración más sofisticada, el administrador del servidor Host On-Demand configurará el servidor Host On-Demand especialmente para que su dirección de servidor Telnet de sesión común sea igual que la dirección del cluster de antememorias de clientes Host On-Demand (es decir, el o los direccionadores utilizados como servidores TN3270E). Este es el uso normal de la antememoria de clientes Host On-Demand previsto por sus creadores. En esta configuración, la dirección del cluster de Network Dispatcher tendrá varios puertos asociados: algunos para la función Host On-Demand y uno (normalmente el puerto 23) para la función TN3270E. En el capítulo “Utilización de la función Network Dispatcher” en la página 111 hallará más información sobre la configuración de TN3270E con Network Dispatcher. Desde el punto de vista del servidor Host On-Demand, éste está programado con una dirección de servidor Telnet arbitraria. Una sesión HOD puede estar programada para utilizar un servidor Telnet arbitrario, a menos que el navegador dé soporte a los applets firmados, suele ser así, pero consulte la publicación *eNetwork Host On-Demand, Versión 3.0, Guía del administrador*, número de documento de IBM SC10-3233, para ver cuáles son las disposiciones necesarias para OS/2. El servidor Host On-Demand utilizado para ofrecer capacidades de terminal a clientes es independiente de los servidores Telnet, que están directamente relacionados con los ordenadores con los que los clientes intentan comunicarse.

Por otro lado, para una configuración muy grande, puede añadirse cierto número de servidores TN3270E al puerto Telnet (puerto 23) dependientes de la configuración de Network Dispatcher. Para una configuración extremadamente grande, se pueden configurar más puertos como puertos Telnet, puesto que tanto la dirección IP y el puerto (por omisión, el 23) de un servidor Telnet, pueden configurarse en sesiones Host On-Demand. Solamente es necesario un servidor Host On-Demand para estas configuraciones de varios servidores Telnet que dan soporte a decenas de miles de usuarios.

Este soporte permite que un IBM 2212 actúe como servidor TN3270E para guardar en antememoria el applet de emulación de terminal y lo sirva a petición de los navegadores de los clientes. La primera vez que un cliente solicita el applet, se recupera del servidor Web y se almacena en la antememoria Host On-Demand. La antememoria servirá directamente las futuras peticiones del applet que realicen los clientes, eliminando la necesidad de recuperarlo de nuevo del servidor Web.

Para obtener información más detallada sobre la utilización de Host On-Demand desde un navegador cliente, consulte el capítulo titulado “En qué consisten los clientes Host On-Demand” de *eNetwork Host On-Demand, Versión 3.0, Guía del administrador*, número de documento de IBM SC10-3233.

Notas:

1. Las funciones de antememoria de clientes Host On-Demand y del servidor Web no pueden coexistir en una misma configuración.
2. La función Host On-Demand sólo funciona en la tarjeta HPSC (High Performance System Card).
3. Host On-Demand también da soporte a las conexiones con sistemas principales que no son SNA. Da soporte a sesiones 3270, 5250, VT (VT52, VT100, VT220_7_BIT, VT220_8_BIT) y de pasarela CICS.

En este capítulo se describe cómo configurar la función de la antememoria de clientes Host On-Demand y cómo utilizar los mandatos de supervisión de dicha función. Consta de los apartados siguientes:

Configuración de la antememoria de clientes Host On-Demand

La antememoria de clientes Host On-Demand debe utilizarse con Network Dispatcher. Antes de utilizar por primera vez la antememoria de clientes Host On-Demand, deberá:

1. Acceder a Network Dispatcher en `talk 6` desde el indicador `Config>` mediante el mandato **feature ndr**.
2. Habilitar el ejecutor
3. Añadir un cluster
4. Añadir los puertos siguientes:
   - Añadir el puerto 80 al cluster y establecerlo en la modalidad hod client cache. El puerto 80 es el puerto estándar del protocolo HTTP para la Web.
   - Añadir el puerto 8999 al cluster y aceptar los valores por omisión de todos los parámetros excepto el del número de puerto. El puerto 8999 es que utilizan los clientes para comunicarse con sus perfiles de grupo/usuario/sesión que están almacenados en el servidor Host On-Demand.
   - Se supone que el administrador del servidor Host On-Demand accederá al servidor Host On-Demand directamente, no a través de este IBM 2212, lo que es una ventaja de cara a la seguridad del sistema gracias al diseño de

Network Dispatcher, ya que los clientes solamente pueden acceder a los puertos configurados. Sin embargo, si esto resulta demasiado restrictivo, se puede añadir el puerto 8989 al cluster y aceptar los valores por omisión de los parámetros.

5. Añadir un servidor Host On-Demand y sólo uno. Si por razones administrativas inusuales se necesitaran más servidores Host On-Demand, repita todos los pasos anteriores desde el paso 4 en la página 168 para añadirlos como clusters exclusivos. El servidor debe añadirse a todos los puertos 80, 8999 y 8989 (si se utiliza).
6. Si interesa que el direccionador también sea el servidor TN3270E, siga el procedimiento descrito en "Utilización de la función Network Dispatcher" en la página 111, para configurar el puerto Telnet (23) que depende de la dirección del cluster y añada los servidores TN3270E a dicho puerto. También será necesario que el administrador del servidor Host On-Demand configure simultáneamente el servidor Host On-Demand para que utilice esta dirección Telnet alternativa.

A continuación podrá utilizar los mandatos de configuración y supervisión para modificar el entorno de la antememoria de clientes Host On-Demand.

Nota: Mientras que los cambios realizados en Network Dispatcher a través de Talk 6 modifican la configuración actual en funcionamiento, los cambios realizados en la antememoria de clientes Host On-Demand no modifican la configuración actual en funcionamiento a menos que se active explícitamente a través del mandato **activate** en Talk 6 o mediante la `función HOD Client Cache` de Talk 5. La excepción es que si el cluster o el puerto de un proxy HTTP se elimina mediante el mandato feature NDR de Talk 6, también se eliminará el proxy HTTP de la antememoria de clientes Host On-Demand de la configuración actual en funcionamiento.

Ejemplo:

```
Config>f ndr
NDR Config>enable executor
NDR Config>add cluster
Cluster Address [0.0.0.0]? 113.3.1.10
FIN count [4000]?
FIN time out [30]?
Stale timer [1500]?
Cluster 113.3.1.10 has been added.
Fincount has been set to 4000 for cluster 113.3.1.10
Fintimeout has been set to 30 for cluster 113.3.1.10
Staletimer has been set to 1500 for cluster 113.3.1.10
NDR Config>add port
Cluster Address [0.0.0.0]? 113.3.1.10
Port number [80]? 80
Port type(tcp=1, udp=2, both=3) [3]?
Max. weight (0-100) [20]?
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1 pftp=2 extcache=4 hod client cache=5) [0]? 5
Default server TCP connection timeout (Range 5-240 seconds) [120]?
Default client TCP connection timeout (Range 5-240 seconds) [120]?
Maximum partition size (1-4095 megabytes or 0 for no limit) [0]?
URL mask to identify Java applet [*.jar]?
      Default expiration time for Java applet
              (1-10080 minutes or 0 for no expiration) [60]?
Do you want to add a URL mask? [No]:

The Host On-Demand Client Cache partition has been successfully created.
Requested port has been added to cluster 113.3.1.10
Port Mode has been set to hod for port 80 in cluster 113.3.1.10
Maxweight has been set to 20 for port 80 in cluster 113.3.1.10
Port Type has been set to Both for port 80 in cluster 113.3.1.10
NDR Config>exit
```

Nota: Este ejemplo es parcial y solamente muestra la adición del puerto de la antememoria de clientes HOD (80) con su modalidad de puerto exclusiva y su menú de consola. El resto de la configuración sigue los ejemplos vistos en “Utilización de la función Network Dispatcher” en la página 111.

A continuación se ofrece una lista de los parámetros del ejemplo, descritos brevemente.

cluster-address Especifica la dirección IP del cluster.

Nota: Se supone que las direcciones IP del cluster están en la misma subred lógica que el direccionador de saltos anterior (direccionador IP).

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

FIN-count Especifica el número de conexiones que deben estar en el estado FIN antes de que el ejecutor intente eliminar la información de conexión no usada de la base de datos de Network Dispatcher después de transcurrido el *tiempo de espera de FIN* o el definido en el *temporizador de inactividad*.

Valores válidos: de 0 a 65535

Valor por omisión: 4000

FIN-timeout Especifica el número de segundos que una conexión puede permanecer en el estado de FIN antes de que el ejecutor intente eliminar la información de conexión no usada de la base de datos de Network Dispatcher.

Valores válidos: de 0 a 65535

Valor por omisión: 30

Stale-timer Especifica el número de segundos que una conexión puede permanecer inactiva antes de que el ejecutor intente eliminar la información de la conexión de la base de datos de Network Dispatcher.

Valores válidos: de 0 a 65535

Valor por omisión: 1500

port# Especifica el número de puerto del protocolo para este cluster.

Valores válidos: de 1 a 65535

Valor por omisión: 80

port-type Especifica los tipos de tráfico IP cuya carga puede repartirse en este puerto. Los tipos soportados son:

- 1 = TCP
- 2 = UDP
- 3 = ambos

Valores válidos: 1, 2, 3

Valor por omisión: 3

max-weight Especifica el peso máximo para los servidores de este puerto. Esto afectará al diferente número de peticiones que el ejecutor entregará a cada servidor.

Valores válidos: de 0 a 100

Valor por omisión: 20

port-mode Especifica si el puerto enviará todas las peticiones de un único cliente a un único servidor (llamado adherente), utilizará ftp pasivo (pftp), las enviará a un conjunto de antememorias escalables externas (antememoria externa), utilizará la función de antememoria de clientes Host On-Demand o no utilizará ningún protocolo concreto para este cluster (ninguno).

Valores válidos: 0,1,2,4,5, donde:

- 0 = none (ninguna)
- 1 = sticky (adherente)
- 2 = pftp
- 4 = extcache (antememoria externa)
- 5 = hod client cache (antememoria de clientes HOD)

Valor por omisión: 0

Default server TCP connection timeout Especifica el tiempo que transcurrirá antes de que finalice la conexión con un servidor.

Valores válidos: de 5 a 240 segundos

Valor por omisión: 120 segundos.

Default client TCP connection timeout Especifica el tiempo que transcurrirá antes de que finalice la conexión con un cliente.

Valores válidos: de 5 a 240 segundos

Valor por omisión: 120 segundos.

Do you want to modify the Host On-Demand Client Cache partition? Le permite modificar la configuración de la partición de la antememoria de clientes Host On-Demand.

Valores válidos: Yes o No

Valor por omisión: No

Maximum partition size Especifica la cantidad máxima de memoria que se asignará a esta partición de la antememoria de clientes Host On-Demand. Si este valor es superior a la cantidad de memoria disponible actualmente, se hará caso omiso del valor y no se impondrá ningún tamaño máximo de la partición.

Valores válidos: de 1 a 4095 Megabytes o 0 (sin máximo)

Valor por omisión: 0 (sin máximo)

URL mask to identify Java applets Especifica la máscara de URL utilizada para identificar los applets Java.

Valores válidos: cualquier máscara de URL

Valor por omisión: *.jar*

Default expiration time for Java applet Especifica el tiempo de caducidad que se aplicará a los applet Java.

Valores válidos: de 1 a 10080 minutos, o 0 si no caduca

Valor por omisión: 60

Do you want to add a URL mask? Especifica una máscara de URL nueva que se añadirá a la antememoria de clientes Host On-Demand. Las máscaras de URL permiten que el usuario incluya o excluya objetos individuales o grupos de objetos por su Localizador universal de recursos (URL).

Nota: Esta función no suele utilizarse con Host On-Demand, pero se explica aquí para que el tema esté completo. Existe una máscara de URL de interés; es la máscara de applet de Java, que se configura como parte de la partición. Esta máscara suele ser la única que debe configurarse; por lo que se recomienda que no utilice los mandatos add, delete, list, modify urlmask.

Valores válidos: Yes o No

Valor por omisión: No

Cuando se especifica una máscara de URL, se pueden utilizar caracteres comodín. Si se configura Network Dispatcher para la antememoria de clientes Host On-Demand o si se utilizan los mandatos **add** o **modify url** desde el indicador `HOD Client Cache`, se podrán utilizar caracteres comodín. Los caracteres utilizados como comodines son el * (asterisco) y el # (signo de número). Los comodines pueden utilizarse en cualquier posición del URL.

El signo * indica que o ningún carácter o cualquier número de caracteres forman parte del URL:

Ejemplo: *abc.html filtrará las máscaras de URL siguientes.

```
abc.html
finabc.html
defchtjqsprabc.html
```

El signo # representa un solo carácter.

Ejemplo: ab#.html filtrará las máscaras de URL siguientes.

```
abc.html
abf.html
abo.html
```

Debe utilizar Network Dispatcher para configurar el cluster y puerto iniciales de la función antememoria de clientes Host On-Demand. Una vez añadidos el cluster y el puerto, al configurar la *modalidad de puerto* como puerto de la antememoria de clientes Host On-Demand, podrá modificar y visualizar los parámetros de configuración de la antememoria de clientes Host On-Demand en el indicador `HOD Client Cache Config>`.

Consulte 139 para obtener más información sobre Network Dispatcher.

Acceso al entorno de configuración de la antememoria de clientes Host On-Demand

Para acceder al entorno de configuración de la antememoria de clientes Host On-Demand, escriba el mandato **f hod client cache** en el indicador `Config>`.

```
Config> f h
HOD Client Cache Config>
```

Mandatos de la antememoria de clientes Host On-Demand

En este apartado se describen los mandatos de configuración de la antememoria de clientes Host On-Demand. En la Tabla 16 se listan los mandatos de configuración de la antememoria de clientes Host On-Demand. Estos mandatos especifican los parámetros de la función antememoria de clientes Host On-Demand. Para activar las modificaciones, reinicie el direccionador o utilice el mandato **activate**.

Tabla 16. Resumen de los mandatos de configuración de la antememoria de clientes Host On-Demand.

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 xxxii.
Activate	Activa la partición de la antememoria de clientes Host On-Demand, utilizando la configuración más reciente.
Add	Añade una máscara de URL.
Delete	Suprime una máscara de URL o una partición.
List	Lista la información de la antememoria de clientes Host On-Demand.
Modify	Modifica la información de la antememoria de clientes Host On-Demand.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiii.

Activate

Utilice el mandato **activate** para inicializar la partición de la antememoria de clientes Host On-Demand, utilizando la configuración más reciente.

Sintaxis:

ac**tivate**

Ejemplo:

```
HOD Client Cache Config>act ?
ACTIVATE ALL initializes the Host On-Demand Client Cache partition, using
the latest configuration.
```

Add

Utilice el mandato **add** para añadir una máscara de URL.

Nota: Esta función no suele utilizarse con Host On-Demand.

Sintaxis:

add urlmask

Nota: Para añadir proxies y particiones, deberá utilizar Network Dispatcher y ejecutar los mandatos **add port** o **set port**.

Delete

Utilice el mandato **delete** para suprimir una máscara de URL o la partición.

Sintaxis:

delete partition
        urlmask

partition Suprime la partición de la antememoria de clientes Host On-Demand.

urlmask Nombre de la máscara de URL que se suprimirá de la antememoria de clientes Host On-Demand.

Nota: Las máscaras de URL normalmente no se añaden ni se suprimen con la antememoria de clientes HOD.

Ejemplo:

```
HOD Client Cache Config>del part
The HOD Client Cache partition number has been deleted.
```

Nota: Para suprimir un proxy debe utilizar la función Network Dispatcher y eliminar el puerto y el cluster asociados, o cambiar la modalidad de puerto a otra distinta de la antememoria de clientes Host On-Demand.

List

Utilice el mandato **list** para listar la información de la antememoria de clientes Host On-Demand.

Sintaxis:

list all
      external

partition
proxy
urlmask

all Lista la partición, todos los puertos, proxies y máscaras definidos en una antememoria de clientes Host On-Demand.

external Lista la información del gestor de control de antememoria externa.

Nota: El ECCM no suele utilizarse con la antememoria de clientes Host On-Demand.

partition Lista la partición de la antememoria de clientes Host On-Demand.

proxy Lista los proxies de la antememoria de clientes Host On-Demand.

urlmask Lista las máscaras de URL definidas en la antememoria de clientes Host On-Demand.

Ejemplo: list all

```
HOD Client Cache Config>list all
Host On-Demand Client Cache Partition
    Cluster address 113.3.1.10, Port 80

1 Host On-Demand Client Cache partition defined.
```

Ejemplo: list partition

```
HOD Client Cache Config>list pa
Host On-Demand Client Cache Partition
Maximum partition size    : Unlimited
URL mask to identify Java applets:   '*.jar'
      Default expiration time for Java applet:   60
Associated proxies (cluster port): (113.3.1.10 80)

1 Host On-Demand Client Cache partition defined.
```

Ejemplo: list proxy

```
HOD Client Cache Config>li pro
    1) Cluster address 113.3.1.10, Port 80, HOD Client Cache partition
HTTP proxy number [1]? 1
HTTP Proxy 1
HOD Client Cache Partition
Cluster Address           : 113.3.1.10
Port Number               : 80
Server Connection Timeout: 120 seconds
Client Connection Timeout: 120 seconds
```

Modify

Utilice el mandato **modify** para modificar la información de configuración de la antememoria de clientes Host On-Demand.

Sintaxis:

modify
external
partition
proxy
urlmask

external Cambia las características del gestor de control de antememoria externa.

Nota: Esta función no suele utilizarse con Host On-Demand.

partition Cambia las características de la partición de la antememoria de clientes Host On-Demand existente.

proxy Cambia las características de un proxy HTTP existente.

urlmask Cambia una máscara de URL ya existente.

Nota: Esta función no suele utilizarse con Host On-Demand.

Ejemplo: modify partition

```
HOD Client Cache Config>modify partition
Maximum partition size (1-4095 megabytes or 0 for no limit) [0]? 2000
URL mask to identify Java applet [*.jar]?
      Default expiration time for Java applet
               (1-10080 minutes or 0 for no expiration) [60]?
The Host On-Demand Client Cache partition has been modified.
```

Ejemplo: modify proxy

```
HOD Client Cache Config>mod proxy
    1) Cluster address 113.3.1.10, Port 80, HOD Client Cache partition
HTTP proxy number [1]? 1
Default server TCP connection timeout (Range 5-240 seconds) [120]? 200
Default client TCP connection timeout (Range 5-240 seconds) [120]?
The HTTP proxy has been modified.
```

Acceso al entorno de supervisión de la antememoria de clientes Host On-Demand

Para acceder al entorno de supervisión de la antememoria de clientes Host On-Demand, escriba el mandato **f hod client cache** en el indicador de configuración `t 5`.

```
+f h
```

Mandatos de supervisión de la antememoria de clientes Host On-Demand

En la Tabla 17 en la página 177 se listan los mandatos de supervisión de la antememoria de clientes Host On-Demand.

Tabla 17. Resumen de mandatos de supervisión de la antememoria de clientes Host On-Demand

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 xxxii.
Activate	Activa la información de la antememoria de clientes Host On-Demand, utilizando la configuración más reciente.
Clear	Borra todos los objetos de la partición de la antememoria de clientes Host On-Demand o borra las estadísticas de la antememoria de clientes Host On-Demand.
Enable	Habilita la partición de la antememoria de clientes Host On-Demand.
Delete	Suprime la partición, el proxy o un máscara de URL de la antememoria de clientes Host On-Demand.
Disable	Inhabilita la partición de la antememoria de clientes Host On-Demand.
List	Lista la información de la antememoria de clientes Host On-Demand.
Modify	Modifica la información de la antememoria de clientes Host On-Demand.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiii.

Activate

Utilice el mandato **activate** para activar la partición, o los proxies o un proxy en concreto de la antememoria de clientes Host On-Demand.

Sintaxis:

ac**tivate** all
external
partition
proxy

all Activa la partición de la antememoria de clientes Host On-Demand, todos los proxies definidos y el gestor de control de antememoria externa.

external Activa el gestor de control de antememoria externa.

partition Activa la partición de la antememoria de clientes Host On-Demand.

proxy Activa un proxy de la antememoria de clientes Host On-Demand.

Ejemplo: activate all

```
HOD Client Cache>act all
The Host On-Demand Client Cache partition must be disabled to reactivate it.
Do you wish to continue? [No]: y
```

Ejemplo: activate partition

```
HOD Client Cache>act pa
The Host On-Demand Client Cache partition must be disabled to reactivate it.
Do you wish to continue? [No]: y
Do you wish clear this partition? [No]: y
Do you wish to enable this partition? [Yes]: y
```

Ejemplo: activate proxy

```
HOD Client Cache>activate pr
    1) Cluster address 113.3.1.10, Port 80, HOD Client Cache partition
Enter proxy number: [1]? 1
You are trying to activate an existing proxy.
Doing this will cause the proxy to be terminated before
being reactivated.
Do you wish to continue? [No]: y
```

Clear

Utilice el mandato **clear** para borrar todos los objetos de la partición de la antememoria de clientes Host On-Demand, o para borrar las estadísticas.

Nota: Al borrar los objetos de la partición, no se borran las estadísticas de la partición.

Sintaxis:

cl**ear** partition
statistics

partition Borra todos los objetos de la partición.

statistics Borra las estadísticas existentes de la partición.

Ejemplo: clear partition

```
HOD Client Cache>clear pa
HOD Client Cache partition must be disabled to clear its contents.
Do you wish to continue? [No]: y
Do you wish to enable this partition? [Yes]: y
```

Enable

Utilice el mandato **enable** para habilitar la partición de la antememoria de clientes Host On-Demand.

Sintaxis:

e**nable** partition

Ejemplo:

```
HOD Client Cache>enable partition
```

Delete

Utilice el mandato **delete** para suprimir la partición de la antememoria de clientes Host On-Demand.

Sintaxis:

de**lete** partition

partition Suprime la partición de la antememoria de clientes Host On-Demand.

Ejemplo: delete partition

```
HOD Client Cache>delete partition
WARNING: This will delete partition and free all memory!
Do you wish to continue?  [No] : yes
HOD Client Cache>
```

Disable

Utilice el mandato **disable** para inhabilitar la partición de la antememoria de clientes Host On-Demand.

Sintaxis:

disable partition

Ejemplo:

```
HOD Client Cache>disable partition
```

List

Utilice el mandato **list** para visualizar la información de la antememoria de clientes Host On-Demand, todas las políticas y proxies, o una política o proxy en concreto.

Sintaxis:

list all
delete
depend
external
item
partition
policy
proxy

all Lista la partición de la antememoria de clientes Host On-Demand, todas las políticas y todos los proxies.

delete Lista los 100 últimos elementos suprimidos de la partición de la antememoria de clientes Host On-Demand.

depend Lista la tabla de dependencias de la partición.

external Lista la información del gestor de control de antememoria externa.

item Lista los elementos actuales de la partición de la antememoria de clientes Host On-Demand.

partition Lista la información de la partición de la antememoria de clientes Host On-Demand.

policy Lista la información de las políticas de la antememoria de clientes Host On-Demand.

proxy Lista la información de los proxies de la antememoria de clientes Host On-Demand.

Ejemplo: list all

```
HOD Client Cache>list all
HOD Client Cache Partition         Status: Enabled
     Cluster address: 113.3.1.10  Port 80
1 partition(s) active.
External Cache Manager Port: 83
         Connection timeout: 120 seconds
```

Ejemplo: list delete

```
HOD Client Cache>list delete

Delete Table
URL string -- hit count
======================
'/abc.html' -- 4
'/futbol.html' -- 2
'/tenis.html' -- 1
'/curling.html' -- 3
```

Ejemplo: list item

```
HOD Client Cache>list item

Current number of items:  5
URL String -- hit count
======================
'/' -- 2
'/archiv5k.html' -- 1
'/archiv4k.html' -- 1
'/archiv2k.html' -- 3
'/archiv1k.html' -- 1
```

Ejemplo: list partition

```
HOD Client Cache>list partition
HOD Client Cache Partition         Status: Enabled
     Cluster address: 113.3.1.10, Port 80
Partition size: Current - 0 bytes  Highest - 0 bytes   Maximum - Unlimited
Number of objects: Current - 0  Highest - 0 Maximum - Unlimited
Maximum object size: Unlimited
HOD Client Cache purge interval  : 600 minute(s)
Hit ratio: 0%
Total number of hits:  0
Cache Hit Bytes Served:  0
Breakdown of responses for the Cache Hits
 (note: this is based on whether the HTTP Proxy considered it a hit.
  So these count may not add up to the hit count above)
   Response 200(OK):                0
   Response 203(Non-Authoriative):  0
   Response 206(Partial Content):   0
   Response 300(Multiple Choices):  0
   Response 301(Moved Permanently): 0
   Response 304(Not Modified):      0
   Response 410(Gone):              0
Total number of misses:  0
Cache Miss Bytes Served:  0
Breakdown of responses for the Cache Misses
   Response 100 Range(Information):         0
   Response 200(OK):                        0
   Response 200 Range(Successful-not 200):  0
   Response 304(Not Modified):              0
   Response 300 Range(Redirection-not 304): 0
   Response 400 Range(Client Error):        0
   Response 500 Range(Server Error):        0
   Response other (not in the above):       0
Object Excluded (Object too large):        0
                (Object expired):          0
                (DONT CACHE header):       0
                (URL Mask excluded):       0
                (Image excluded):          0
                (Static object excluded):  0
                (Dynamic object excluded): 0
                (Cache disabled):          0
Total number of objects added via ECCM Interface: 0
Total number of objects not added via ECCM Interface but was attempted: 0
Total number of objects replaced via ECCM Interface: 0
```

Ejemplo: list policy

```
HOD Client Cache>list policy
URL mask to identify Java Applets: *.jar
     Default lifetime: 60 minute(s)
```

Ejemplo: list proxy

```
HOD Client Cache>list proxy
    1)   Cluster address 113.3.1.10, Port 80, HOD Client Cache Partition
Enter proxy number: [1]? 1
Proxy 1: assigned to the HOD Client Cache partition
Cluster address: 113.3.1.10     Port number: 80
Server Connection Timeout: 120 seconds
Client Connection Timeout: 120 seconds
Client connections: 0 current / 0 at highest point
Server connections: 0 current / 0 at highest point
Total cache hits: 0
Total cache misses: 0
Cache misses (object not in cache): 0
             (unsupported method):  0
             (can't send response): 0
             (non-cached request):  0
```

Modify

Utilice el mandato **modify** para modificar el gestor de control de antememoria externa.

Sintaxis:

m**odify** external

Soporte de reconfiguración dinámica de la antememoria de clientes Host On-Demand

En este apartado se describe la reconfiguración dinámica (DR) y cómo afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

La antememoria de clientes Host On-Demand no da soporte al mandato **delete interface** de CONFIG (Talk 6).

Mandato activate interface de GWCON (Talk 5)

El mandato **activate interface** de GWCON (Talk 5) no es aplicable a la antememoria de clientes Host On-Demand. La antememoria de clientes Host On-Demand es una función, no una interfaz.

Mandato reset interface de GWCON (Talk 5)

El mandato **reset interface** de GWCON (Talk 5) no es aplicable a la antememoria de clientes Host On-Demand. La antememoria de clientes Host On-Demand es una función, no una interfaz.

Mandatos de restablecimiento de componente de GWCON (Talk 5)

La antememoria de clientes Host On-Demand (HOD) da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos de la antememoria de clientes Host On-Demand (HOD):

Mandato GWCON, feature HOD, activate all

Descripción: Este mandato leerá todas las memorias SRAM de la antememoria de clientes Host On-Demand y hará que el entorno de ejecución actual sea el mismo.

Efecto en la red: Se interrumpirá la ejecución de todos los proxies que estén actualmente activos (es decir, se desactivarán todas las conexiones con los proxies). Si el gestor de control de antememoria externa estaba en funcionamiento, el dispositivo dejará de estar a la escucha de conexiones nuevas en el puerto actual (o sea, no se desactivarán las conexiones del puerto actual).

Limitaciones: No hay limitaciones.

El mandato **GWCON, feature HOD, activate all** da soporte a todos los mandatos de la antememoria de clientes Host On-Demand.

Mandato GWCON, feature HOD, activate partition

Descripción: Este mandato leerá todas las memorias SRAM de esta partición y hará que el entorno de ejecución actual de la partición sea el mismo.

Efecto en la red: Si la partición que se va a activar ya existe, se interrumpirá la ejecución de todos los proxies de esa partición (es decir, se desactivarán todas las conexiones con esos proxies).

Limitación:

La antememoria de clientes Host On-Demand ya debe estar activada (véase el mandato **CONFIG, feature HOD, activate**).

La tabla siguiente resume los cambios en la configuración de la antememoria de clientes Host On-Demand que se activan cuando se ejecuta el mandato **GWCON, feature HOD, activate partition**:

Mandatos cuyos cambios se activan al ejecutar el mandato GWCON, feature HOD, activate partition
CONFIG, feature HOD, add URLMASK
CONFIG, feature HOD, delete PARTITION
CONFIG, feature HOD, delete URLMASK
CONFIG, feature HOD, modify PARTITION
CONFIG, feature HOD, modify PROXY
CONFIG, feature HOD, modify URLMASK

Mandato GWCON, feature HOD, activate proxy

Descripción: Este mandato leerá todas las memorias SRAM de este proxy y hará que el entorno de ejecución actual del proxy sea el mismo.

Efecto en la red: Si el proxy que se va a activar ya existe, se interrumpirá su ejecución (es decir, se desactivarán todas las conexiones con ese proxy).

Limitaciones:

- La antememoria de clientes Host On-Demand ya debe estar activado (véase el mandato **CONFIG, feature HOD, activate**).

La tabla siguiente resume los cambios en la configuración de la antememoria de clientes Host On-Demand que se activan cuando se ejecuta el mandato **GWCON, feature HOD, activate proxy**:

Mandatos cuyos cambios se activan al ejecutar el mandato GWCON, feature HOD, activate proxy
CONFIG, feature HOD, modify PROXY

Mandato GWCON, feature HOD, activate external port

Descripción: Este mandato leerá todas las memorias SRAM del gestor de control de antememoria externa y hará que el entorno de ejecución actual del gestor de control de antememoria externa sea el mismo.

Efecto en la red: Si el gestor de control de antememoria externa estaba en funcionamiento, el dispositivo dejará de estar a la escucha de conexiones nuevas en el puerto actual (o sea, no se desactivarán las conexiones del puerto actual).

Limitaciones:

- La antememoria de clientes Host On-Demand ya debe estar activada (véase el mandato **CONFIG, feature HOD, activate**).

La tabla siguiente resume los cambios en la configuración de la antememoria de clientes Host On-Demand (HOD) que se activan cuando se ejecuta el mandato **GWCON, feature HOD, activate external port**:

Mandatos cuyos cambios se activan al ejecutar el mandato GWCON, feature HOD, activate external port
CONFIG, feature HOD, modify EXTERNAL

Mandatos activate de CONFIG (Talk 6)

La antememoria de clientes Host On-Demand (HOD) da soporte a los siguientes mandatos **activate** de CONFIG (Talk 6):

Mandato CONFIG, feature HOD, activate

Descripción: Cambia dinámicamente la antememoria de clientes Host On-Demand que está actualmente en funcionamiento, basándose en la memoria SRAM actual.

Efecto en la red: Se interrumpirá la ejecución de todos los proxies que estén actualmente activos (es decir, se desactivarán todas las conexiones con los proxies). Si el gestor de control de antememoria externa estaba en

funcionamiento, el dispositivo dejará de estar a la escucha de conexiones nuevas en el puerto actual (o sea, no se desactivarán las conexiones del puerto actual).

Limitaciones: Ninguno

El mandato **CONFIG, feature HOD, activate** da soporte a todos los mandatos de la antememoria de clientes Host On-Demand.

Mandatos de cambio temporal de GWCON (Talk 5)

La antememoria de clientes Host On-Demand (HOD) da soporte a los siguientes mandatos de GWCON que cambian temporalmente el estado operativo del dispositivo. Estos cambios se perderán si el dispositivo se reinicia, si se vuelve a cargar, o si se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
GWCON, feature HOD, modify external **Nota:** Este mandato cambiará el entorno de ejecución actual del gestor de control de antememoria externa. Si el gestor de control de antememoria externa estaba en funcionamiento, el dispositivo dejará de estar a la escucha de conexiones nuevas en el puerto actual (o sea, no se desactivarán las conexiones del puerto actual).
GWCON, feature HOD, delete partition **Nota:** Este mandato suprimirá la partición del entorno de ejecución actual.

Utilización de la antememoria del servidor Web

En este capítulo se describe la función de antememoria del servidor Web del 2212. Consta de los apartados siguientes:

Visión general de la antememoria del servidor Web

La función de almacenamiento en antememoria del servidor Web sólo está disponible para los modelos 2212 que disponen de la tarjeta HPSC. Es posible ampliar los modelos 2212 que no disponen de la tarjeta HPSC. Para obtener más información póngase en contacto con el representante de IBM Service.

La función de almacenamiento en antememoria del servidor Web almacena la páginas Web solicitadas con más frecuencia, para poder recuperarlas más rápidamente. La función de almacenamiento en antememoria del servidor Web guarda los elementos solicitados con más frecuencia más cerca de los clientes; esto libera recursos del servidor que está siendo utilizado actualmente como servidor de archivos y de conexiones de comunicaciones. La antememoria del servidor Web del 2212 permite acceder a gran velocidad a las páginas Web, reduciendo la actividad general de comunicaciones del sistema principal. La antememoria del servidor Web del 2212:

- Almacena las páginas Web estáticas y que no están protegidas
- Permite que los clientes y servidores HTTP accedan a la antememoria
- Permite que el usuario defina las políticas de llenado y anulación.
- Utiliza la función Network Dispatcher para repartir la carga de trabajo entre los servidores y permite la posibilidad de utilizar una antememoria de reserva.
- Proporciona una plataforma para futuras funciones de almacenamiento en antememoria controladas por el servidor.

  Nota: Las funciones de antememoria del servidor Web y de los clientes Host On-Demand no pueden coexistir en una configuración.

Todas las interfaces de red del 2212 que dan soporte a la conectividad TCP/IP, dan soporte a la conectividad entre la antememoria del servidor Web y los servidores y clientes HTTP.

La Figura 10 en la página 186 muestra cómo funciona Network Dispatcher sin la función de almacenamiento en antememoria del servidor Web.

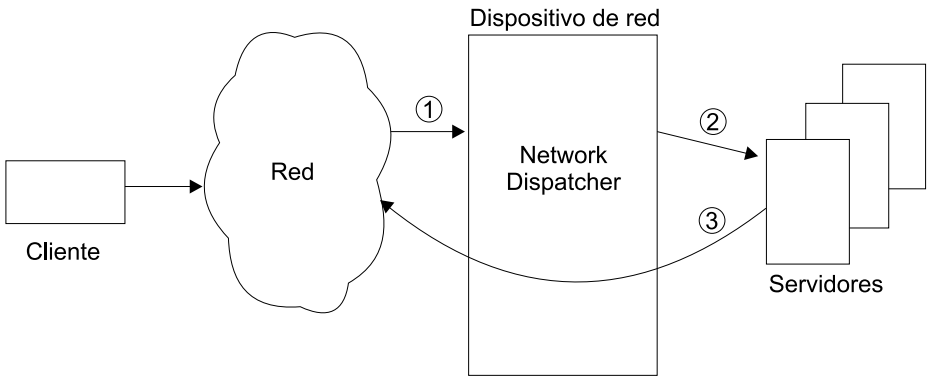


Figura 10. Network Dispatcher sin antememoria del servidor Web

1. Se solicita una dirección de cluster
2. Network Dispatcher reenvía la petición a los servidores
3. El servidor envía una respuesta al cliente.

La Figura 11 muestra cómo funciona Network Dispatcher con la función de almacenamiento en antememoria del servidor Web si la página solicitada no esta actualmente almacenada en antememoria. La función de almacenamiento en antememoria del servidor Web carga la respuesta en la antememoria si las políticas lo permiten.

Consulte el apartado “Utilización del proxy HTTP” en la página 190 para obtener más información sobre el proxy HTTP.

Una partición es una división del núcleo de la antememoria. Cada partición de la antememoria se configura independientemente, permitiendo que el dispositivo dé soporte a varias sedes.

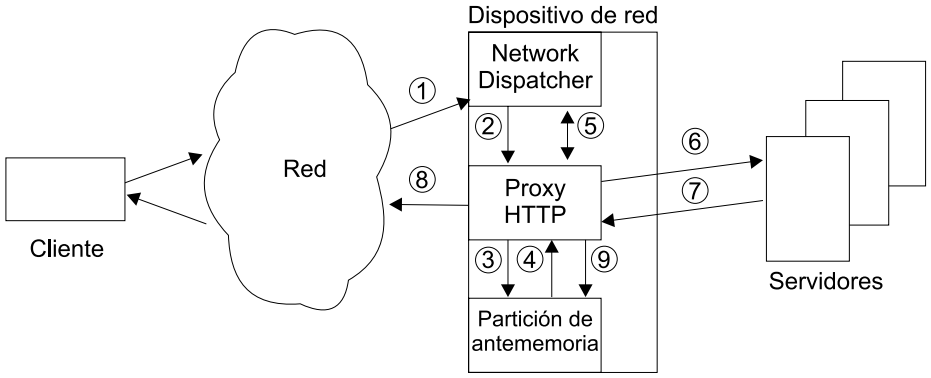


Figura 11. Network Dispatcher con antememoria del servidor Web y sin acierto en la antememoria

1. Llega una petición a la dirección del cluster
2. Network Dispatcher reenvía la petición al proxy HTTP si la partición está habilitada
3. El proxy HTTP busca en la partición de la antememoria
4. El proxy HTTP no encuentra la página solicitada en la partición de la antememoria

5. El proxy HTTP obtiene la información del servidor desde Network Dispatcher, si es necesaria para una nueva conexión
6. El proxy HTTP reenvía la petición al servidor. (Para la conexión TCP la dirección IP origen es la dirección de la interfaz de red del 2212. La dirección IP destino es la dirección IP de la interfaz del servidor).
7. El servidor envía la respuesta al proxy HTTP
8. El proxy HTTP envía la respuesta al cliente
9. El proxy HTTP carga la respuesta en la partición de la antememoria si las políticas lo permiten.

Es importante que el administrador comprenda que la dirección de destino de los paquetes destinados al servidor es la dirección del servidor y no la dirección del cluster, tal como se explica en el paso 6. La cuestión es importante si un servidor Web se configura en un sistema principal: si el servidor Web se configura para que esté a la escucha en una dirección IP concreta, esta dirección IP debe ser la dirección IP de la interfaz del servidor. En general, la interfaz del servidor tendrá asignado un conjunto de direcciones IP lógicas. Cuando el cluster de Network Dispatcher se configure para que utilice una dirección IP lógica del servidor, el servidor Web correspondiente debe configurarse para que esté a la escucha en esa dirección IP lógica. De ahí que un sistema principal (servidor) pueda tener varios servidores Web, cada uno a la escucha en una dirección IP lógica distinta. Network Dispatcher puede configurarse con clusters independientes por cada servidor Web. De esta forma, un sistema principal puede utilizarse para un determinado número de sedes Web. Además, hay que utilizar una partición de la antememoria diferente para cada servidor Web. Cuando los servidores Web residen en sistemas principales reproducidos, multiplique el número de sistemas principales reproducidos por el número de servidores Web para determinar el número de direcciones del servidor utilizadas.

Además, el número de direcciones del cluster debe unirse por medio de un alias a todas las direcciones de bucle de retorno del sistema principal; de esa manera, si una partición de la antememoria está inhabilitada, se podrá seguir accediendo al servidor Web, puesto que el Network Dispatcher pasa a la modalidad más sencilla del puerto, la modalidad cero (no se almacena nada en antememoria). Esta operación de emergencia sólo la pueden realizar los servidores conectados directamente; sin ellos, el direccionamiento resulta difícil, si no imposible.

La Figura 12 en la página 188 muestra cómo funciona Network Dispatcher con la función de almacenamiento en antememoria del servidor Web si la página solicitada está actualmente almacenada en antememoria.

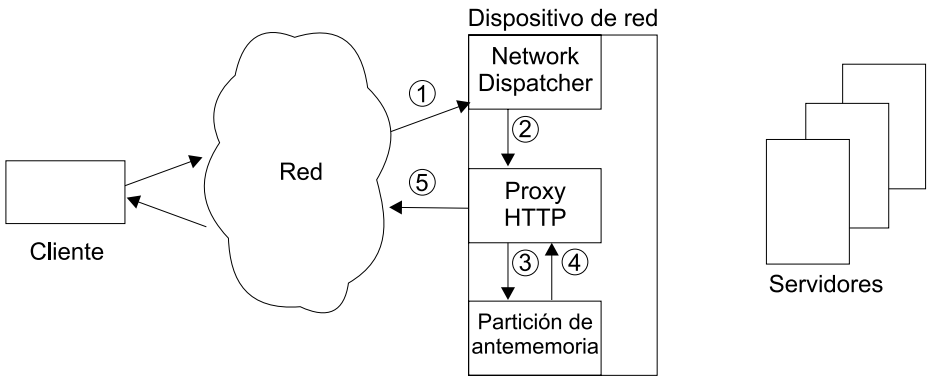


Figura 12. Network Dispatcher con antememoria del servidor Web y con acierto en la antememoria

1. Se solicita una dirección de cluster
2. Network Dispatcher reenvía la petición al proxy HTTP
3. El proxy HTTP busca en la partición de la antememoria
4. El proxy HTTP encuentra la página solicitada en la partición de la antememoria
5. El proxy HTTP devuelve la respuesta al cliente.

Almacenamiento en antememoria

La antememoria del servidor Web del 2212 tiene:

Almacenamiento en antememoria de páginas Web

El 2212 puede almacenar en antememoria objetos que solicita el servidor. Este método de almacenamiento en antememoria se conoce como almacenamiento transparente en antememoria. Puede utilizar `talk 6` para habilitar o inhabilitar el almacenamiento transparente en antememoria en una partición.

La alternativa al almacenamiento transparente en antememoria (automático) es el almacenamiento manual en antememoria. Es este caso, un agente externo utiliza el gestor de antememoria para almacenar en antememoria una página Web. Para obtener más información sobre la función de almacenamiento en antememoria Web controlada externamente, consulte el apartado “Visión general del gestor de control de antememoria externa” en la página 196.

Los objetos almacenados en antememoria inactivos se suprimen automáticamente. La antememoria del servidor Web del 2212 da soporte a servidores y clientes HTTP 1.0 y 1.1.

Políticas flexibles de almacenamiento en antememoria

Permite que los usuarios especifiquen si deben almacenarse en antememoria determinadas clases genéricas de objetos Web (imágenes, páginas estáticas que no son imágenes, páginas dinámicas). También se pueden especificar los tamaños máximos de los objetos y de las particiones de la antememoria. Además, los usuarios pueden especificar máscaras de URL para incluir o excluir explícitamente clases de objetos Web según convenga en su entorno.

Diagrama de flujo de las políticas de almacenamiento transparente en antememoria

1. ¿Están habilitados el almacenamiento en antememoria y el almacenamiento transparente en antememoria?
   - No - El objeto no se almacenará en antememoria.
   - Sí - Ir al paso 2
2. ¿El tamaño del objeto es menor o igual que el tamaño máximo?
   - No - El objeto no se almacenará en antememoria.
   - Sí - Ir al paso 3
3. ¿El objeto ha caducado?
   - No - Ir al paso 4
   - Sí - El objeto no se almacenará en antememoria.
4. ¿Van a utilizarse cabeceras HTTP y se ha utilizado una de ellas? **La cabecera HTTP utilizada es una cabecera de control de la antememoria que utiliza las directivas DO o DONT.**
   - Sí - ¿Se utilizan cabeceras HTTP y el objeto incluye una cabecera de control de la antememoria? Ir al paso 5.
5. ¿Las cabeceras HTTP contienen la directiva "DO"?
   - No - El objeto no se almacenará en antememoria.
   - Sí - Ir al paso 9.
6. ¿El URL está excluido por una máscara de exclusión?
   - Sí - El objeto no se almacenará en antememoria.
   - No - Ir al paso 7
7. ¿El URL está incluido mediante una máscara de inclusión?
   - Sí - Ir al paso 9.
   - No - Ir al paso 8
8. ¿El objeto es una imagen (.jpg o .gif)?
   - No - Ir al paso 9
   - Sí - ¿Son imágenes que pueden almacenarse en antememoria?
     - Sí - Ir al paso 11 en la página 190.
     - No - El objeto no se almacenará en antememoria.
9. ¿El objeto es estático y no es una imagen?
   - No - Ir al paso 10 en la página 190
   - Sí - ¿Son objetos estáticos distintos de imágenes y que pueden almacenarse en antememoria?
     - Sí - Ir al paso 11 en la página 190.
     - No - El objeto no se almacenará en antememoria.

10. El objeto es un objeto dinámico. ¿Los objetos dinámicos pueden almacenarse en antememoria?
    - Sí - Ir al paso 11.
    - No - El objeto no se almacenará en antememoria.
11. ¿Hay espacio en la partición para almacenar el objeto? **Los objetos que hace más tiempo que se han utilizado se eliminarán para dejar sitio al objeto.**
    - No - El objeto no se almacenará en antememoria.
    - Sí - El objeto se almacenará en antememoria.

Soporte de varias antememorias independientes
Se da soporte a un máximo de 16 particiones, lo que permite a un solo 2212 proporcionar servicios de almacenamiento en antememoria independientes para varios clusters. Las particiones de la antememoria son totalmente independientes. Cada partición de la antememoria posee contenido y políticas propios.

Conectividad total del servidor TCP/IP
Comunica los servidores y los clientes entre todas las interfaces de red del 2212 que dan soporte al conjunto de protocolos TCP/IP.

Reparto de la carga de los servidores finales (utilizando Network Dispatcher)
Utiliza Network Dispatcher para definir grupos de servidores y repartir la carga entre los servidores para acelerar la búsqueda de páginas Web que no se han encontrado en la antememoria.

Soporte de antememoria de reserva
Permite que los usuarios definan un segundo 2212 como antememoria del servidor de reserva. La antememoria del servidor de reserva puede funcionar como reserva "en frío" utilizando la función de Alta disponibilidad de Network Dispatcher. Hallará más información en “Alta disponibilidad de Network Dispatcher” en la página 113.

Nota: Al activarse, la antememoria del servidor de reserva está vacía. Para volver a llenar de páginas la antememoria del servidor de reserva deberá utilizar el almacenamiento transparente en antememoria (por ejemplo: peticiones de URL) o la función gestor de control de antememoria externa.

Utilización del proxy HTTP

Cada proxy HTTP representa una dirección o un puerto del cluster dedicado al almacenamiento en antememoria. Pueden existir varios proxies HTTP utilizando una partición de la antememoria.

El proxy HTTP maneja las peticiones recibidas de los clientes e intenta satisfacerlas desde su partición de la antememoria. Si el proxy HTTP puede satisfacer la petición, devolverá la respuesta al cliente. Si el proxy HTTP no puede satisfacer la petición, abrirá una conexión TCP con un servidor para intentar satisfacerla. Cuando el servidor responda a la petición del proxy HTTP, éste reenviará al cliente la respuesta del servidor. El proxy HTTP también decide si la respuesta del cliente debe almacenarse en antememoria. SI la respuesta debe almacenarse en antememoria, el proxy HTTP la pasa a la partición de la antememoria.

El proxy HTTP maneja las conexiones siguiendo estas directrices.

- El proxy HTTP intentará satisfacer solamente las peticiones de métodos GET y HEAD desde la antememoria. Las otras peticiones se enviarán al servidor sin modificaciones a través de una conexión TCP con el servidor que está conectado con la conexión TCP del cliente. Si ninguna conexión TCP está acoplada con la conexión TCP del cliente, se abrirá una nueva conexión TCP con el servidor y se acoplará con la conexión TCP del cliente.
- Los mensajes de todas las peticiones de métodos GET y HEAD que no puedan satisfacerse desde la partición de la antememoria, se enviarán al servidor sin modificaciones a través de la conexión TCP.
- Todas las respuestas recibidas del servidor se volverán a enviar al cliente sin modificaciones a través de la conexión TCP con el cliente.
- Únicamente se almacenarán en antememoria las respuestas del método GET. Se considera que las otras respuestas no deben almacenarse en antememoria. Las respuestas GET se almacenarán en antememoria solamente si el estado de la respuesta es aceptable, y la respuesta GET y junto con las políticas de almacenamiento en antememoria para la partición lo permiten.
  - Sólo se almacenarán en antememoria las respuestas con los códigos de estado siguientes: El proxy HTTP no permitirá que las cabeceras HTTP anulen esto.

    Códigos de estado:

    - 200 (ok)
    - 203 (non-authoritative)
    - 300 (multiple-choice)
    - 301 (moved permanently)
    - 410 (gone)
- Si se utilizan cabeceras HTTP en una petición GET, la cabecera de petición `If-Modified-Since` es la única que se utilizará para determinar si una entrada de la antememoria puede satisfacer la petición. No se utilizará ninguna otra cabecera condicional. La antememoria del servidor Web no utilizará identificadores de entidad para determinar si una entidad almacenada en antememoria puede utilizarse como respuesta.
- Se hace caso omiso de las directivas de las cabecera de `control de la antememoria` incluidas en las peticiones. Si la entidad no está en la partición de la antememoria, la petición se pasa al servidor.

  Nota: La antememoria del servidor Web es una ampliación del servidor y, por lo tanto, no utiliza la cabecera de `control de la antememoria` como las antememorias del proxy HTTP.
- Las respuestas dan soporte a las directivas de cabecera de antememoria "do", y "dont". Se hace caso omiso de las otras directivas. Las directivas "do" y "dont" son directivas nuevas que puede utilizar el servidor para informar a la antememoria del servidor Web de que almacene la entidad en antememoria o para que no lo haga.
- El proxy HTTP intenta satisfacer peticiones GET parciales desde la antememoria. Sin embargo, las respuestas GET parciales no se almacenan en la antememoria.

Nota: Si una petición GET parcial tiene más de diez rangos, se devolverá la respuesta completa.

- Se hará caso omiso de la cabecera `Host` de todos los mensajes HTTP, puesto que todas las peticiones de entrada deben ser para el mismo cluster de servidores.
- El proxy HTTP da soporte a conexiones HTTP continuas.

  Nota: Si se recibe una conexión continua de un cliente de nivel HTTP 1.0 y se devuelve respuesta desde la antememoria, se añadirá una cabecera `Connection` dependiendo de la petición. Por ejemplo, si el cliente quiere que la duración de la conexión sea larga, se mantendrá una conexión larga.
- El proxy HTTP no utilizará la antememoria para las peticiones que contengan la cabecera `Authorization`. No se almacenarán en antememoria las respuestas a dichas peticiones. Tampoco se almacenarán en antememoria las respuestas que tengan una cabecera `Proxy-Authorization`.
- El proxy HTTP será capaz de pasar a un comportamiento de transmisión a través de un túnel para una conexión HTTP, si tiene problemas analizando una petición o una respuesta de una conexión HTTP. El comportamiento de transmisión a través de un túnel para todos los análisis de mensajes y reenvía todas las peticiones del cliente al servidor y todas las respuestas del servidor al cliente.
- Si la partición de la antememoria está inhabilitada, todas las conexiones actuales y nuevas de clientes se reenviarán directamente al servidor final. Para que esta característica funcione, siga el procedimiento descrito en el apartado “Configuración de un servidor para Network Dispatcher” en “Utilización de la función Network Dispatcher” en la página 111.
- Si la partición de la antememoria está habilitada, la antememoria procesará todas las conexiones nuevas de clientes. Las conexiones ya existentes de clientes continuarán reenviando las peticiones directamente al servidor final.

Función SHAC (Scalable High Availability Cache)

La función SHAC (Scalable High Availability Cache) permite que un grupo de antememorias de servidor Web trabaje como una sola antememoria mayor. El número máximo de antememorias que pueden formar parte de un grupo es de dieciséis. Si se produce una anomalía en un miembro de la antememoria, se reduce la cantidad total de memoria disponible para almacenar datos en antememoria, en lugar de finalizar todas las funciones de almacenamiento en antememoria. En la Figura 17 en la página 196 encontrará un ejemplo de configuración.

Las antememorias individuales forman el espacio total de la antememoria. Si una antememoria deja de funcionar, las otras antememorias en funcionamiento continuarán almacenando en antememoria las páginas de entrada.

Las páginas Web de entrada se almacenan en las antememorias del grupo. Se distribuyen equitativamente entre las antememoria disponibles. Cada antememoria del grupo mantiene una tabla que hace un seguimiento del número de antememorias accesibles del grupo y de sus direcciones IP. Las tablas son idénticas para todas las antememorias del grupo. Las tablas utilizan un algoritmo llamado protocolo de rutinas para un conjunto de antememorias (CARP, Cache

Array Routine Protocol) para determinar en qué antememoria se guarda un URL determinado. La información de la tabla se obtiene del dispositivo Network Dispatcher e, indirectamente, de las antememorias que utilizan el asesor HTTP para realizar el seguimiento del estado de las antememorias de servidor Web del grupo. Las figuras siguientes demuestran las condiciones para localizar un URL utilizando la función SHAC.

La Figura 13 muestra la petición recibida de Network Dispatcher encontrada en la primera antememoria que ha recibido la petición.

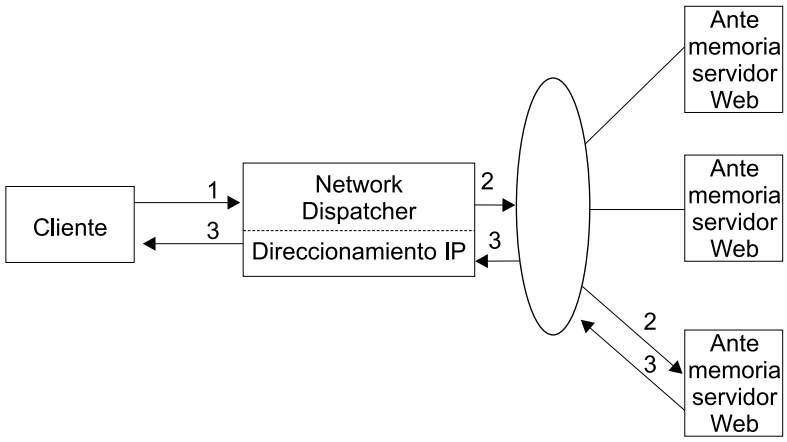


Figura 13. Encontrada petición hecha a la antememoria

1. Llega al Network Dispatcher una petición HTTP de una página Web realizada por un cliente.
2. El Network Dispatcher reenvía la petición a una de las antememorias de servidor Web. La antememoria recibe la petición y encuentra la página Web.
3. La antememoria envía la página Web directamente al cliente, eludiendo el Network Dispatcher.

La Figura 14 muestra una petición recibida de Network Dispatcher que no se ha encontrado en la primera antememoria, pero que el algoritmo CARP indica que el URL se guarda en otra antememoria.

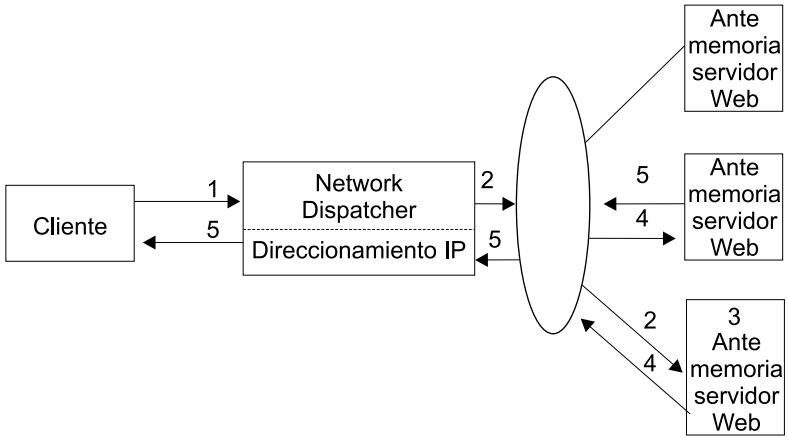


Figura 14. Petición reenviada a la antememoria responsable

1. Llega al Network Dispatcher una petición HTTP de una página Web realizada por un cliente.
2. Network Dispatcher reenvía la petición a una de las antememorias de servidor Web.
3. La antememoria recibe la petición y no encuentra la página Web. Entonces, la antememoria utiliza un algoritmo para localizar la antememoria responsable de la página Web.
4. A continuación, la petición se reenvía a la antememoria responsable de esta página Web.
5. La antememoria responsable de la página Web recibe la petición, encuentra la página Web y se la envía al cliente.

La Figura 15 muestra una petición recibida de Network Dispatcher que no se ha encontrado en la antememoria, pero el algoritmo CARP indica que la antememoria es responsable del URL.

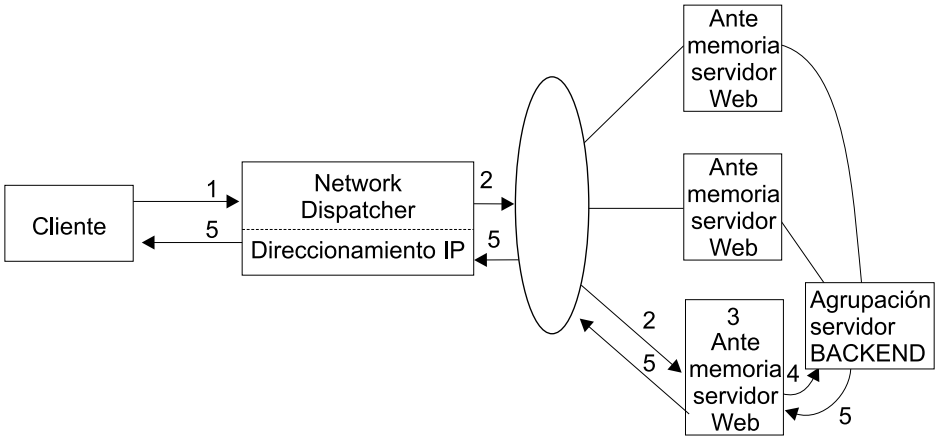


Figura 15. Petición reenviada al servidor final

1. Llega al Network Dispatcher una petición HTTP de una página Web realizada por un cliente.
2. Network Dispatcher reenvía la petición a una de las antememorias de servidor Web.
3. La antememoria recibe la petición y no encuentra la página Web. La antememoria utiliza un algoritmo para determinar cuál es la antememoria responsable de la página Web.
4. La antememoria envía la petición al servidor final.
5. El servidor final encuentra la página Web; dicha página se devuelve al cliente a través de la antememoria responsable de la página. Se almacenará en antememoria si ésta está configurada para almacenar la página en antememoria. Consulte el “Configuración y supervisión de la antememoria del servidor Web” en la página 227 para obtener información sobre la configuración.

La Figura 16 en la página 195 muestra una petición que no se ha encontrado en ninguna antememoria del grupo de antememorias.

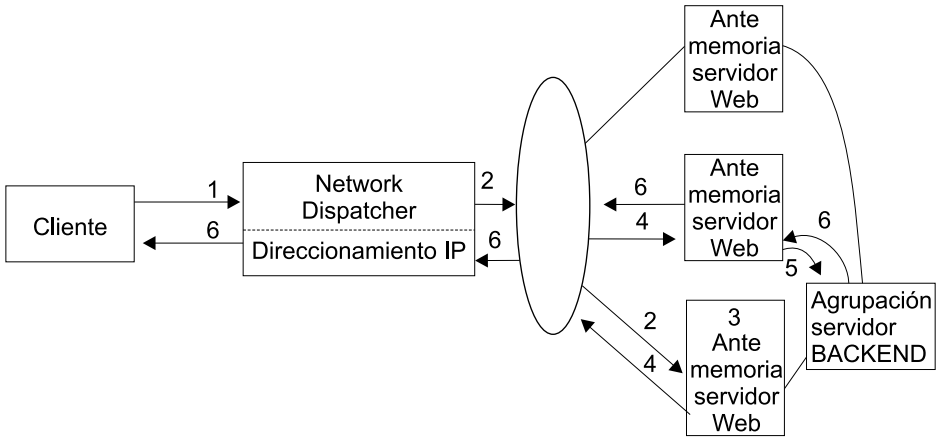


Figura 16. Petición reenviada a la antememoria responsable y no encontrada

1. Llega al Network Dispatcher una petición HTTP de una página Web realizada por un cliente.
2. Network Dispatcher reenvía la petición a una de las antememorias de servidor Web.
3. La antememoria recibe la petición y no encuentra la página Web. Entonces, la antememoria utiliza un algoritmo para localizar la antememoria responsable de la página Web. A continuación, la petición se reenvía a la antememoria responsable de esta página Web.
4. La antememoria responsable de la página Web recibe la petición y no encuentra la página Web.
5. La antememoria responsable de la página Web envía la petición a la agrupación de servidores finales.
6. El servidor final encuentra la página Web; dicha página se devuelve al cliente a través de la antememoria responsable de la página. Se almacenará en antememoria si ésta está configurada para almacenar la página en antememoria. Consulte el “Configuración y supervisión de la antememoria del servidor Web” en la página 227 para obtener información sobre la configuración.

Nota: En la Figura 15 en la página 194 y en la Figura 16 se comprende que todas las antememorias del grupo estén conectadas con todos los servidores finales de la agrupación para conseguir la máxima fiabilidad.

En la Figura 17 en la página 196 se muestra un ejemplo comprobado de la función SHAC con detallados parámetros de configuración utilizados junto con los descritos en los apartados “Utilización de Network Dispatcher con antememoria SHAC (Scalable High Availability Cache)” en la página 130, “Configuración y supervisión de la función Network Dispatcher” en la página 133 y “Configuración y supervisión de la antememoria del servidor Web” en la página 227. Se muestran las direcciones de la interfaz, internas, del cluster y la dirección IP del servidor, con sus máscaras de subred. También se muestran los mandatos de direccionamiento necesarios para las antememorias y el servidor final conectado al anillo 113.

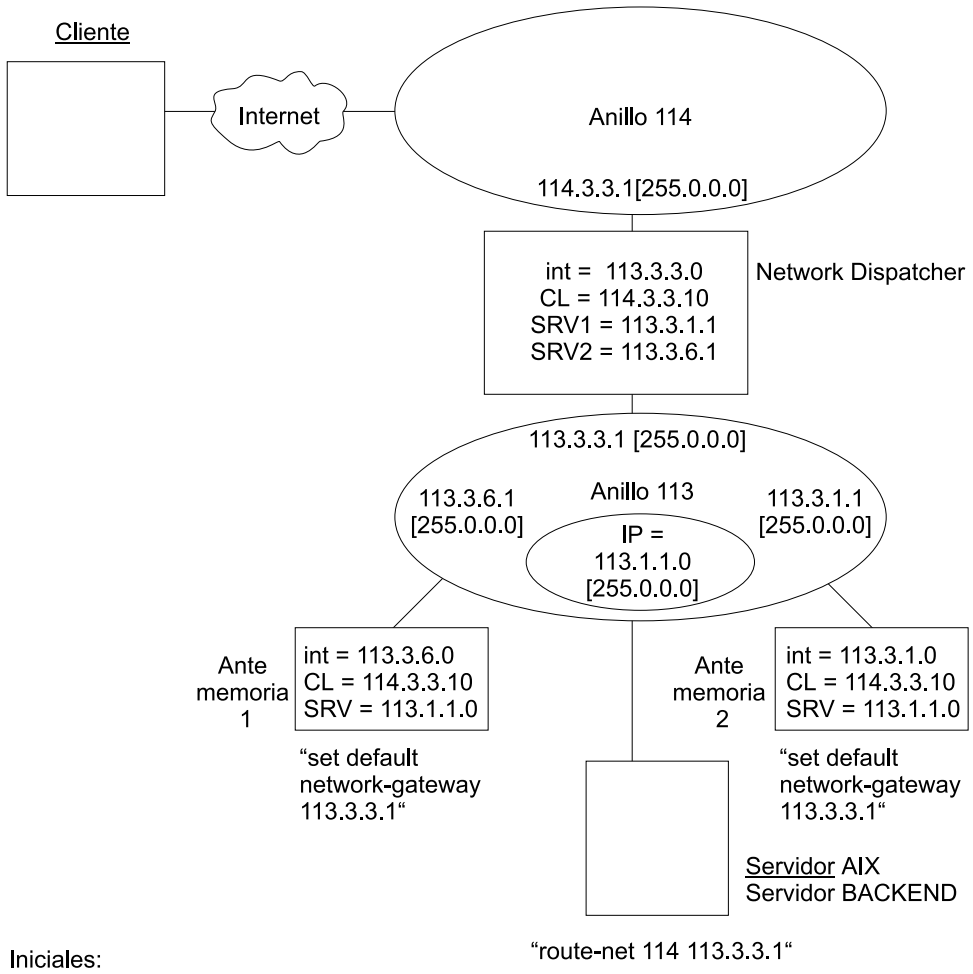


Figura 17. Dos antememorias con Network Dispatcher, un cliente y un servidor final.

Visión general del gestor de control de antememoria externa

El gestor de control de antememoria externa permite que los servidores Web controlen la antememoria del servidor Web y la antememoria del cliente Host On-Demand. El control se consigue a través de un puerto definido por el usuario para el gestor de control de antememoria externa (ECCM, External Cache Control Manager). El ECCM acepta mandatos de conexiones y de procesos con destino a una partición de este puerto. Los mandatos utilizan el protocolo de control de la antememoria externa (ECCP, External Cache Control Protocol). El ECCP utiliza formatos de vectores y subvectores para enviar mandatos de petición y mandatos de respuesta.

Un vector de mandatos puede solicitar varias funciones utilizando varios subvectores. Cada subvector representa una función diferente. El vector de mandatos indica en qué partición de la antememoria se aplicarán los mandatos, para lo que

debe especificar la dirección del cluster y el puerto de un proxy definido para esa partición.

El ECCP da soporte a las funciones siguientes:

- Añadir un objeto a una partición de la antememoria, así como suprimirlo
- Habilitar o inhabilitar una partición de la antememoria
- Modificar o listar las políticas aplicables a la partición de la antememoria
- Borrar o listar las estadísticas de la partición de la antememoria
- Borrar una partición de la antememoria (eliminar todos los objetos de la partición de la antememoria)
- Consultar la partición de la antememoria (buscar un objeto determinado)
- Añadir, suprimir, listar o borrar las máscaras de URL de una partición de la antememoria
- Modificar o listar la tabla de dependencias
- Anular objetos que utilizan dependencias.

Tabla de dependencias

El gestor de control de antememoria externa le permite crear una tabla de dependencias para cada partición de la antememoria. Esta tabla es particularmente útil cuando se trabaja con objetos dinámicos en la antememoria.

Nota: Almacenar objetos dinámicos en antememoria requiere que los objetos se actualicen cuando se modifica la información a partir de la que se crearon dichos objetos.

La información necesaria para crear la tabla de dependencias debe pasarse a la partición de la antememoria mediante la interfaz del gestor de control de antememoria externa.

La tabla de dependencias le ofrece la posibilidad de asignar una serie de dependencias a un conjunto de objetos URL (páginas Web almacenadas en antememoria). Estas dependencias se almacenan en tablas de dependencias de la antememoria del servidor Web mediante la interfaz del gestor de control de antememoria externa. La tabla de dependencias se utiliza para anular objetos de la partición de la antememoria que tienen esta dependencia cuando se modifica el origen del objeto. Sin una tabla de dependencias, habría que enviar un mandato de suprimir individual para cada objeto que se quisiera suprimir.

Ejemplo: las tres bases de datos siguientes contienen varios objetos.

```
basedatos1          basedatos2          basedatos3
---------           ---------           ---------
objeto_a            objeto_a            objeto_b
objeto_b            objeto_c            objeto_e
objeto_c            objeto_d
```

Supongamos que todas las páginas objeto_a a objeto_e están almacenadas en la antememoria. Si la base de datos 2 cambia, se puede enviar (a través de la interfaz del gestor de control de la antememoria) un mandato **invalid dependency basedatos2**. Como consecuencia, la antememoria del servidor Web suprimirá los objetos objeto_a, objeto_c y objeto_d de la partición de la antememoria.

Nota: Un objeto no tiene que estar en la partición de la antememoria para estar en la tabla de dependencias.

Autenticación del gestor de control de antememoria externa

El gestor de control de antememoria externa le permite controlas el acceso de los usuarios. Esto se consigue al solicitar a las conexiones de entrada una identificación de usuario y una contraseña. La identificación de usuario y la contraseña están ligadas con la identificación de usuario y la contraseña de conexión. Si el dispositivo está protegido por una contraseña y la conexión de entrada no tiene identificación de usuario ni contraseña o éstas no son válidas, se devolverá una respuesta de error y se cerrará la conexión. Si la identificación de usuario y la contraseña son válidas, el usuario podrá enviar mandatos a través de la interfaz.

Seguridad

La seguridad proporciona una forma de autenticar el usuario del ECCP. Se pueden configurar cuatro tipos de autenticación (RADIUS, TACACS, local o ninguno). No se proporciona el cifrado de datos. Cada mecanismo de cifrado (excepto ninguno) requiere tanto una identificación de usuario como su contraseña asociada. Esta información se envía al 2216 mediante vectores de autenticación. La identificación de usuario y la contraseña pueden tener de 1 a 8 bytes. La contraseña que se envía por la conexión del Control de la antememoria externa debe cifrarse mediante el método de cifrado DES. También se envía el número generador aleatorio de 8 bytes utilizado para el cifrado. La clave del cifrado no se envía a través de la conexión. En “Modify” en la página 237, hallará información sobre cómo configurar el puerto y los valores TCP.

Nota: Si el direccionador no está protegido mediante contraseña, se hará caso omiso del vector de autenticación.

Protocolo de control de la antememoria externa

El protocolo de control de la antememoria externa (ECCP) proporciona a los servidores finales la capacidad de controlar la antememoria del direccionador. Este control maximiza el rendimiento de la antememoria.

El ECCP es una interfaz construida en forma de protocolo que permite que los servidores añadan y supriman objetos así como que puedan modificar las políticas de la antememoria.

El gestor de control de antememoria externa se define en el direccionador (antememoria del servidor Web o antememoria de clientes Host On-Demand) para que acepte mandatos de conexiones y de procesos con destino a una partición de la antememoria.

Configuración

El gestor de control de antememoria externa se configura con los parámetros siguientes:

Puerto definido por el usuario: Número de puerto en el que el gestor de control de antememoria externa está a la escucha y acepta conexiones. Si se configura como 0, se supone que el gestor de antememoria externa está inhabilitado.

Valores válidos: de 0 a 65535

Valor por omisión: 0

Tiempo de espera máximo de TCP:

Valores válidos: de 5 a 240 segundos

Valor por omisión: 120

Clave de cifrado: La clave de cifrado se utilizará si el recuadro está protegido mediante contraseña. La clave de cifrado debe ser una serie de 16 caracteres hexadecimales (0-9,a-f,A-F).

Descripciones de las funciones del gestor de control de antememoria externa

En este apartado se describen las funciones del gestor de control de antememoria externa.

Añadir un objeto

Puede añadirse a la partición de la antememoria un objeto respuesta HTTP. El formato de los datos del objeto debe ser igual al de una respuesta HTTP. El gestor de control de antememoria externa analizará las cabeceras de la respuesta y extraerá la información necesaria. Es entonces cuando se añadirá el objeto a la antememoria.

La diferencia entre Añadir objeto y Añadir objeto (obligatoriamente) es que éste último mandato hará caso omiso de las cabeceras de control de antememoria que especifiquen DO o DONT. Se siguen utilizando las demás cabeceras que utiliza el proxy HTTP para determinar si almacenar en antememoria un objeto. Ambos mandatos Añadir objeto y Añadir objeto (obligatoriamente) sustituirán el objeto en la partición de la antememoria sin tener en cuenta la fecha.

Suprimir un objeto

Puede suprimirse de la antememoria un objeto HTTP. Se da el URL del objeto.

Utilización de la tabla de dependencias

La tabla de dependencias de una partición de la antememoria puede modificarse, listarse y utilizarse para anular objetos.

Para modificar la tabla de dependencias (añadir o eliminar dependencias), deben incluirse tanto la dependencia como el URL de la dependencia. Además, existen otras dos formas de modificar la tabla de dependencias. Una consiste en restaurar toda la tabla (es decir, eliminar todas las dependencias), o la URL de una dependencia (es decir, eliminar la URL de una dependencia de todas las dependencias). La otra consiste en efectuar un proceso de recogida de basura de la tabla de dependencias. El proceso de recogida de basura borra todos los URL de dependencias de la tabla de dependencias que no tengan ningún objeto con ese URL en la antememoria.

Hay varias maneras de listar la información de la tabla de dependencias. Puede recuperarse toda la tabla, todos los URL de dependencias de una dependencia concreta, o todas las dependencias que tienen un URL de una dependencia dada.

Los objetos pueden eliminarse (anularse) de la antememoria utilizando la tabla de dependencias. Se comprueba la tabla de dependencias utilizando la dependencia,. Se eliminarán de la partición de la antememoria, las URL de dependencias de esa dependencia.

Inhabilitar y habilitar una partición
Esta función permite cambiar el estado de la partición de la antememoria. Para poder utilizar el gestor de control de antememoria externa, la partición de la antememoria debe estar en el estado correcto. La partición de la antememoria debe estar inhabilitada para poder depurar los objetos que contiene.

Utilización de las políticas
Las políticas de una partición se pueden listar o modificar. Cada política puede aplicarse independientemente o para todo el grupo. Para modificar una política, debe pasarse el tipo de datos correcto correspondiente a esta política. Consulte el apartado “Formatos de los vectores del protocolo de control de la antememoria externa (ECCP)” en la página 201 (subvector de mandatos Política y subvector de respuesta Política) para saber los formatos de los datos dependiendo de cuál es la política.

Depurar la partición
Esta función permite eliminar todos los objetos de la partición de la antememoria. La partición de la antememoria debe estar inhabilitada para poder depurarla.

Consultar un objeto
Esta función permite ver si un objeto está en la partición de la antememoria. Además, si el objeto está en la partición de la antememoria y tiene una fecha de última modificación, se devuelve la fecha. Consulte el apartado “Formatos de los vectores del protocolo de control de la antememoria externa (ECCP)” en la página 201 (subvector de respuesta Consulta) para saber el formato de la fecha que se devuelve.

Utilización de las estadísticas
Esta función permite listar y restaurar (borrar) las estadísticas de la partición de la antememoria. Consulte el apartado “Formatos de los vectores del protocolo de control de la antememoria externa (ECCP)” en la página 201 (subvector de respuesta Estadísticas) para saber cuál es el formato de las estadísticas.

Utilización de una máscara de URL
Esta función permite listar y modificar las máscaras de URL de una partición de la antememoria. Cuando se utilice esta función, deberá incluirse el tipo de URL, de inclusión, de exclusión, dinámico o applet de la antememoria de clientes Host On-Demand. Se debe listar un tipo de URL. Esta función no funciona con varios tipos de URL.

Tiene la posibilidad de añadir una máscara de URL. Si la máscara de URL es de inclusión, dinámica o una máscara del applet de la antememoria de clientes Host On-Demand, debe incluirse el ciclo de vida. Al añadir una máscara dinámica se modificará la máscara de URL dinámica actual y al añadir una máscara del applet de la antememoria de clientes Host On-Demand, se modificará la máscara actual del applet de la antememoria de clientes Host On-Demand. Tiene la posibilidad de suprimir una máscara de URL. Esta función no es válida para la máscara URL dinámica o para la máscara del applet de la antememoria de clientes Host On-Demand. Tiene la posibilidad de restaurar todas las máscaras de URL de un tipo concreto. Restaurar una máscara de URL dinámica restaura la máscara de URL dinámica por omisión, y restaurar la máscara del applet de la antememoria de clientes Host On-Demand restaura la máscara del applet de la antememoria de clientes Host On-Demand por omisión.

Nota: La máscara dinámica se utiliza con imágenes de la antememoria del servidor Web y la máscara del applet de la antememoria de clientes Host On-Demand se utiliza con imágenes que tengan la función de antememoria de clientes Host On-Demand.

Formatos de los vectores del protocolo de control de la antememoria externa (ECCP)

Los clientes ECCP envían mandatos y reciben respuestas utilizando un formato de vector. El vector de autenticación es necesario si el recuadro está protegido mediante contraseña. Si el recuadro no está protegido mediante contraseña, se hará caso omiso del vector de autenticación si se recibe.

Formatos de los vectores

En este apartado se ofrecen las descripciones de los campos de los vectores.

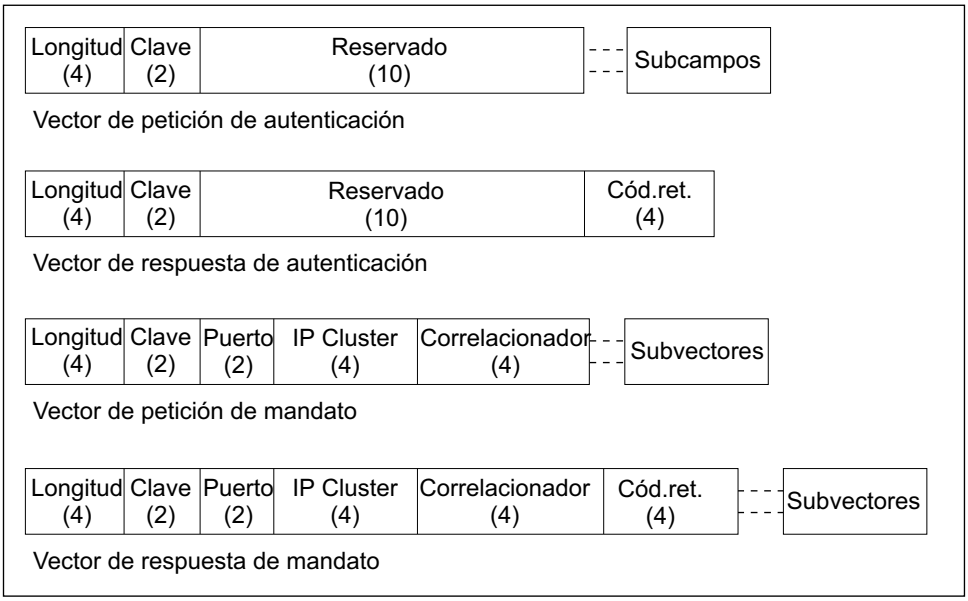


Figura 18. Vector de respuesta de mandatos

Longitud: Valor de 32 bits sin signo que representa la longitud (en bytes) de todo el vector, incluida la de los campos longitud y clave, así como la de los subvectores y subcampos. Los valores aceptables son:

- de 48 a 56 (vectores de petición de autenticación)
- 20 (vectores de respuesta de autenticación)
- de 24 a 4GB-4 (vectores de petición de mandatos)
- de 20 a 4GB-4 (vectores de respuesta de mandatos)

Clave: Valor de 16 bits sin signo que representa la clave del vector principal. Las claves del vector principal son:

- 0x4A00 (Vector de petición de autenticación)
- 0x4A01 (Vector de respuesta de autenticación)
- 0x4B00 (Vector de petición de mandatos)
- 0x4B01 (Vector de respuesta de mandatos)

IP del cluster: Dirección IP de 32 bits del cluster de la antememoria asociado con la partición de la antememoria de destino.

Puerto: Número de 16 bits del puerto del cluster de la antememoria asociado con la partición de la antememoria.

Correlacionador: Valor de 32 bits sin signo utilizado por el cliente ECCP para asociar la respuesta del mandato con la petición del mandato.

Código de retorno: Valor de 32 bits sin signo que representa el código de retorno. Sólo aparece en los vectores de respuesta.

Los vectores contienen uno o más subvectores. El vector de petición de autenticación requiere los subcampos nombre y contraseña. El vector de petición de mandatos contiene uno o más subvectores de mandatos. Si existen varios subvectores en el vector de petición de mandatos, existirán varios subvectores en el vector de respuesta de mandatos. Si se produce un error grave, se reflejará en el campo Código de retorno del vector de respuesta de mandatos.

Vector de petición de autenticación

El vector de petición de autenticación debe ser el primer vector de la Conexión del control de la antememoria externa, si el recuadro está protegido mediante contraseña. Si el recuadro no está protegido mediante contraseña, se hará caso omiso del vector.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x4A00

6-15 Reservado

Reservado para su futuro uso.

de 16 a (4n-1) Subcampo nombre.

de 4n a (4m-1) Subcampo contraseña.

Vector de petición de mandatos

El vector de petición de mandatos envía mandatos al gestor de control de antememoria externa. Si el recuadro está protegido mediante contraseña, el gestor de control de antememoria externa deberá recibir un vector de petición de autenticación válido antes de aceptar los mandatos.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x4B00

6-7 Puerto

Número de puerto del cluster de antememorias (proxy HTTP) asociado con la partición de la antememoria de destino.

8-11 Dirección IP del cluster

Dirección IP de un cluster de antememorias (proxy HTTP) asociado con la partición de la antememoria de destino.

12-15 Correlacionador

El correlacionador se utiliza para asociar las respuestas de mandatos con sus correspondientes peticiones de mandatos.

de 16 a (4n-1) Subvectores

Puede añadirse uno o más de los subvectores siguientes.

- Subvector de mandatos Añadir objeto (0x0100)
- Subvector de mandatos Añadir objeto (obligatoriamente) (0x0110)
- Subvector de mandatos Eliminar objeto (0x0400)
- Subvector de mandatos Dependencia (0x0A00)
- Subvector de mandatos Inhabilitar (0x0300)
- Subvector de mandatos Habilitar (0x0200)
- Subvector de mandatos Política (0x0500)
- Subvector de mandatos Depurar (0x0600)
- Subvector de mandatos Consulta (0x0700)
- Subvector de mandatos Estadísticas (0x0800)
- Subvector de mandatos Máscara de URL (0x900)

Vector de respuesta de autenticación

El vector de respuesta de autenticación se devuelve en respuesta a un vector de petición de autenticación.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x4A01

6-15 Reservado

Reservado para su futuro uso.

16-19 Código de retorno

Código de retorno del vector. Consulte el apartado “Códigos de retorno” en la página 224.

de 20 a (4n-1) Subvectores

Actualmente no existen subvectores para el vector de respuesta de autenticación.

Vector de respuesta de mandatos

El vector de respuesta de mandatos se devuelve en respuesta a un vector de petición de mandatos.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x4B01

6-7 Puerto

Número de puerto del cluster de antememorias (proxy HTTP) asociado con la partición de la antememoria de destino.

8-11 Dirección IP del cluster

Dirección IP de un cluster de antememorias (proxy HTTP) asociado con la partición de la antememoria de destino.

12-15 Correlacionador

El correlacionador se utiliza para asociar las respuestas de mandatos con sus correspondientes peticiones de mandatos.

16-19 Código de retorno

Código de retorno del vector. Consulte el apartado “Códigos de retorno” en la página 224.

de 20 a (4n-1) Subvectores

Se puede añadir el número de subvectores siguientes que se quiera, o no añadir ninguno.

- Subvector de respuesta Añadir objeto (0x0101)
- Subvector de respuesta Añadir objeto (obligatoriamente) (0x0111)
- Subvector de respuesta Eliminar objeto (0x0401)
- Subvector de respuesta Dependencia (0x0A01)
- Subvector de respuesta Inhabilitar (0x0301)
- Subvector de respuesta Habilitar (0x0201)
- Subvector de respuesta Política (0x0501)
- Subvector de respuesta Depurar (0x0601)
- Subvector de respuesta Consulta (0x0701)
- Subvector de respuesta Estadísticas (0x0801)
- Subvector de respuesta Máscara de URL (0x901)

Formatos de los subvectores

En este apartado se describen los formatos de los subvectores. Los subvectores tienen básicamente el mismo formato que el vector principal:

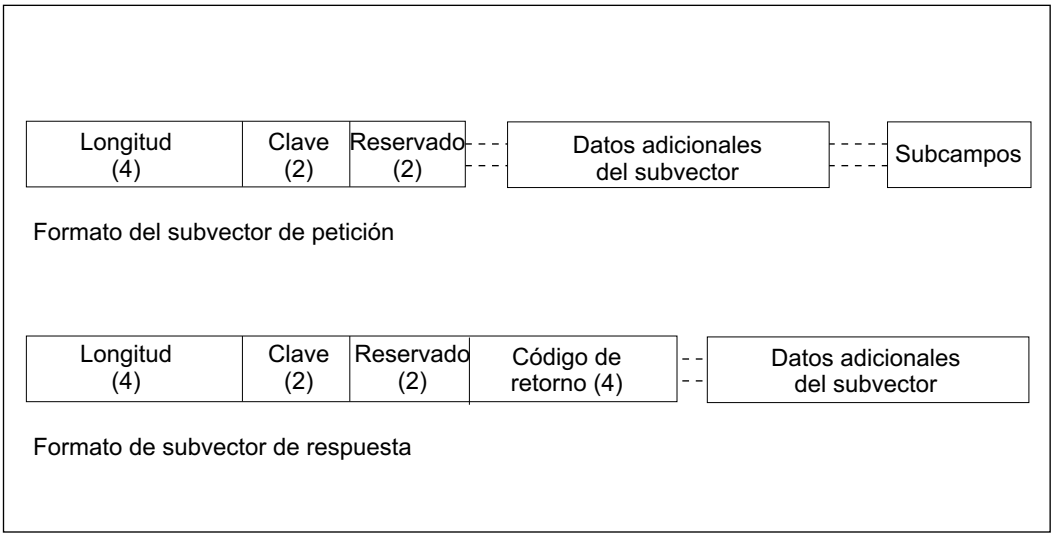


Figura 19. Formato de un subvector

Longitud: Valor de 32 bits sin signo que representa la longitud (en bytes) de todo el subvector, incluida la de los campos longitud y clave, así como la de los subcampos. El rango de valores aceptables está comprendido entre 6 y 4GB (no se comprueba el límite superior).

Clave: Valor de 16 bits sin signo que representa la clave del subvector. Las claves de los subvectores de petición son las siguientes:

- 0x0100 (Añadir un objeto Web)
- 0x0110 (Añadir un objeto Web, haciendo caso omiso de las cabeceras de control de la antememoria)
- 0x0200 (Habilitar el almacenamiento en la antememoria de la partición)
- 0x0300 (Inhabilitar el almacenamiento en la antememoria de la partición)
- 0x0400 (Eliminar un objeto Web)
- 0x0500 (Modificar o listar las políticas de la antememoria)
- 0x0600 (Eliminar todos los objetos Web de la partición)
- 0x0700 (Determinar si un objeto Web está en la partición)
- 0x0800 (Restaurar o listar las estadísticas de la antememoria)
- 0x0900 (Añadir, suprimir o listar las máscaras de URL)
- 0x0A00 (Añadir, suprimir, listar o restaurar dependencias)

Las claves de los subvectores de respuesta que se devuelven son las siguientes:

- 0x0101 (Añadir un objeto Web)
- 0x0111 (Añadir un objeto Web, haciendo caso omiso de las cabeceras de control de la antememoria)
- 0x0201 (Habilitar el almacenamiento en la antememoria de la partición)
- 0x0301 (Inhabilitar el almacenamiento en la antememoria de la partición)
- 0x0401 (Eliminar un objeto Web)
- 0x0501 (Modificar o listar las políticas de la antememoria)

- 0x0601 (Eliminar todos los objetos Web de la partición)
- 0x0701 (Determinar si un objeto Web está en la partición)
- 0x0801 (Restaurar o listar las estadísticas de la antememoria)
- 0x0901 (Añadir, suprimir o listar las máscaras de URL)
- 0x0A01 (Añadir, suprimir, listar o restaurar dependencias)

Reservado: Campo de 16 bits que actualmente no se utiliza.

Código de retorno: Valor de 32 bits sin signo que representa el código de retorno del subvector de petición. Sólo aparece en el subvector de respuesta.

Subvector de mandatos Añadir objeto: El subvector de mandatos Añadir objeto se utiliza para añadir un objeto Web a la partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0100

6-7 Reservado

de 8 a (4n-1) Subcampo URL

de 4n a (4m-1) Subcampo objeto

Subvector de mandatos Añadir objeto (obligatoriamente): El subvector de mandatos Añadir objeto (obligatoriamente) se utiliza para añadir un objeto Web a la partición de la antememoria. Se diferencia del subvector de mandatos Añadir objeto en que se hace caso omiso de las cabeceras de control de la antememoria del objeto.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0110

6-7 Reservado

de 8 a (4n-1) Subcampo URL

de 4n a (4m-1) Subcampo objeto

Subvector de mandatos Eliminar objeto: El subvector de mandatos Eliminar objeto se utiliza para eliminar un objeto Web de la partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0400

6-7 Reservado

de 8 a (4n-1) Subcampo URL

Subvector de mandatos Dependencia: El subvector de mandatos Dependencia se utiliza para modificar o listar la tabla de dependencias o para anular objetos utilizando la tabla de dependencias.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0A00

6-7 Reservado

8-9 Mandato

Mandato de dependencia a ejecutar.

0x0001 Obtener la tabla de dependencias (consulte el tipo de Dependencia de la dependencia)

0x0002 Añadir una dependencia o un URL de dependencias nueva a la tabla de dependencias

0x0003 Eliminar una dependencia o un URL de dependencias de la tabla de dependencias

0x0004 Restaurar la información de la tabla de dependencias (consulte el tipo de Dependencia de la dependencia)

0x0005 Anular un objeto según la dependencia

0x0006 Recoger la basura de la tabla de dependencias

10-11 Tipo de dependencia

Este campo se utiliza para identificar qué datos deben cambiarse. Estos datos se modifican utilizando el mandato Dependencia.

0x0000 No existe tipo de dependencia

0x0001 Utilizar el mandato en toda la tabla.

- Si el mandato es 0x0001 (Obtener) - obtiene toda la tabla.
- Si el mandato es 0x0004 (Restaurar) - borra toda la tabla.

0x0002 El mandato se aplica a la dependencia.

- Si el mandato es 0x0001 (Obtener) - obtiene todos los URL de la dependencia dada.
- Si el mandato es 0x0004 (Restaurar) - borra de la tabla una dependencia.

0x0003 El mandato se aplica al URL

- Si el mandato es 0x0001 (Obtener) - obtiene todas las dependencias del URL de dependencias.

- SI el mandato es 0x0004 (Restaurar) - borra de la tabla un URL de dependencias.

de 12 a (4n-1) Varios subcampos o ninguno.

Subcampo Dependencia
Nota: Este subcampo debe ser el primero, en caso de que se requieran ambos subcampos. Es obligatorio cuando se tienen estos tipos de mandatos Dependencia.

Mandato	Tipo de dependencia
0x0001	0x0002
0x0002	0x0000
0x0003	0x0000
0x0004	0x0002
0x0005	0x0000

Subcampo URL
Nota: Este subcampo debe ser el segundo, en caso de que se requieran ambos subcampos. Es obligatorio cuando se tienen estos tipos de mandatos Dependencia.

Mandato	Tipo de dependencia
0x0001	0x0003
0x0002	0x0000
0x0003	0x0000
0x0004	0x0003

Subvector de mandatos Inhabilitar: EL subvector de mandatos Inhabilitar se utiliza para inhabilitar una partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0300

6-7 Reservado

Subvector de mandatos Habilitar: El subvector de mandatos Habilitar se utiliza para habilitar una partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0200

6-7 Reservado

Subvector de mandatos Política: El subvector de mandatos Política le permite modificar una partición de la antememoria o listar la información de una partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0500

6-7 Reservado

8-9 Mandato

Mandato a ejecutar.

0x0001 Obtener la política

0x0002 Actualizar la política

10-11 Tipo de política

El tipo de política se utiliza para identificar los datos que deben cambiarse. A continuación, los datos se cambiarán utilizando el mandato Política.

0x0001 Almacenamiento transparente en antememoria

0x0002 Cabecera HTTP de control de la antememoria

0x0003 Almacenar en antememoria objetos dinámicos

0x0004 Almacenar en antememoria objetos imagen ("*.gif," "*.jpg")

0x0005 Almacenar en antememoria objetos estáticos

0x0006 Ciclo de vida por omisión de los objetos dinámicos

0x0007 Ciclo de vida por omisión de los objetos imagen

0x0008 Ciclo de vida por omisión de los objetos estáticos.

0x0009 Tiempo (en segundos) que transcurrirá entre cada recogida de basura.

0x000A Tamaño máximo de la partición (en MB).

0x000B Número máximo de objetos en la partición de la antememoria.

0x000C Tamaño máximo de un objeto de la partición de la antememoria.

0xFFFF Operar con todas las políticas.

Nota: Si el mandato es Obtener (0x0001), el subvector terminará aquí.

de 12 a (4n-1) Uno de los siguientes, dependiendo del tipo de política.

Si el tipo de política es 0x0001, 0x0002, 0x0003, 0x0004 ó 0x0005:

12-13 Establecer valor

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

14-15 Reservado

Si el tipo de política es 0x0006, 0x0007 ó 0x0008

12-15 El valor representa el ciclo de vida del objeto, en minutos.

El valor está comprendido entre 0 y 10.080, donde 0 indica que el objeto no caduca.

Si el tipo de política es 0x0009

12-15 Valor que representa el intervalo de depuración de la antememoria, en minutos.

El valor está comprendido entre 0 y 720, donde 0 indica que el proceso de recogida de basura está inhabilitado.

Si el tipo de política es 0x000A

12-13 Valor que representa el tamaño máximo de la partición, en MB. El valor está comprendido entre 0 y 4.095, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

14-15 Reservado

Si la política es 0x000B

12-15 Valor que representa el número máximo de objetos.

El valor está comprendido entre 0 y 100000, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

Si la política es 0x000C

12-15 Valor que representa el tamaño máximo de un objeto en la partición de la antememoria.

El valor está comprendido entre 512 y 300.000; si se especifica 0, significa que no existe límite.

Nota: El valor no se verifica.

Si la política es 0xFFFF

12-13 Almacenamiento transparente en antememoria (Establecer valor)

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

14-15 Cabecera HTTP de control de la antememoria (Establecer valor)

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

16-17 Almacenamiento en antememoria de objetos dinámicos (Establecer valor)

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

18-19 Almacenamiento en antememoria de objetos imagen (Establecer valor)

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

20-21 Almacenamiento en antememoria de objetos estáticos (Establecer valor)

- 0x0001 (Habilitado)

- 0x0002 (Inhabilitado)

22-23 Valor que representa el tamaño máximo de la partición, en MB.

El valor está comprendido entre 0 y 4.095, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

24-27 Valor que representa el número máximo de objetos.

El valor está comprendido entre 0 y 1.000.000, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

28-31 Valor que representa el tamaño máximo de un objeto en una partición de la antememoria.

El valor está comprendido entre 512 y 3.000.000; si se especifica 0, significa que no existe límite.

Nota: El valor no se verifica.

32-35 Valor que representa el ciclo de vida de un objeto dinámico, en minutos.

El valor está comprendido entre 0 y 10.080, donde 0 indica que el objeto no caduca.

Nota: El valor no se verifica.

36-39 Valor que representa el ciclo de vida de un objeto imagen, en minutos.

El valor está comprendido entre 0 y 10.080, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

40-43 Valor que representa el ciclo de vida de un objeto estático, en minutos.

El valor está comprendido entre 0 y 10.080, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

44-47 Valor que representa el intervalo de depuración de la antememoria, en minutos.

El valor está comprendido entre 0 y 720, donde 0 indica que debe habilitarse el proceso de recogida de basura.

Subvector de mandatos Depurar: El subvector de mandatos Depurar se utiliza para borrar todos los objetos de una partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0600

6-7 Reservado

Subvector de mandatos Consulta: El subvector de mandatos Consulta se utiliza para comprobar si un URL dado está en la partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0700

6-7 Reservado

de 8 a (4n-1) Subcampo URL

Subvector de mandatos Estadísticas: El subvector de mandatos Estadísticas se utiliza para obtener o restaurar las estadísticas de una partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0800

6-7 Reservado

8-9 Mandato

- 0x0001 - Obtiene las estadísticas de la partición de la antememoria.
- 0x0004 - Restaura las estadísticas de la partición de la antememoria.

10-11 Reservado

Subvector de mandatos Máscara de URL: El subvector de mandatos Máscara de URL se utiliza para listar o modificar las máscaras de URL asociadas con una partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0900

6-7 Reservado

8-9 Mandato

- 0x0001 - Obtiene las máscaras de URL definidas actualmente (consulte más adelante los tipos de URL para saber qué tipos de máscaras que se devuelven).
- 0x0002 - Añade la máscara de URL dada (consulte más adelante los tipos de URL para saber cuál es el tipo de máscara que se va a añadir).

- 0x0003 - Eliminar la máscara de URL dada (consulte más adelante los tipos de URL para saber cuál es el tipo de máscara que se va a eliminar).

  Nota: Suprimir la máscara de URL dinámica o la máscara del applet de clientes Host On-Demand, no es una función válida.

- 0x0004 - Restaurar todas las máscaras de URL del tipo de URL definido a continuación.

10-11 Tipo de URL

- 0x0001 - de inclusión
- 0x0002 - de exclusión
- 0x0003 - dinámico
- 0x0004 - applet de clientes Host On-Demand

12-15 Ciclo de vida

El valor está comprendido entre 0 y 10.080, donde 0 representa un objeto que no caduca. Sólo lo utiliza el mandato Añadir (0x0002), si el tipo de URL es de inclusión (0x0001), dinámico (0x0003) o el applet de clientes Host On-Demand (0x0004).

Nota: Si el mandato es Obtener (0x0001) o Borrar (0x0004), el subvector terminará aquí.

de 16 a (4n-1) Un subvector de mandatos URL.

Subvector de respuesta Añadir objeto: El subvector de respuesta Añadir objeto se utiliza para responder a un subvector de mandatos Añadir objeto (obligatoriamente).

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0101

6-7 Reservado

8-11 Código de retorno

Consulte los “Códigos de retorno” en la página 224.

Subvector de respuesta Añadir objeto (obligatoriamente): El subvector de respuesta Añadir objeto (obligatoriamente) se utiliza para responder a un subvector de mandatos Añadir objeto (obligatoriamente).

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0111

6-7 Reservado

8-11 Código de retorno

Consulte los “Códigos de retorno” en la página 224.

Subvector de respuesta Eliminar objeto: El subvector de respuesta Eliminar objeto se utiliza para responder a un subvector de mandatos Añadir objeto (obligatoriamente).

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0401

6-7 Reservado

8-11 Código de retorno

Consulte los “Códigos de retorno” en la página 224.

Subvector de respuesta Dependencia: El subvector de respuesta Dependencia se utiliza para responder a un subvector de mandatos Dependencia.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0A01

6-7 Reservado

8-11 Código de retorno

Consulte los “Códigos de retorno” en la página 224.

de 12 a (4n-1) Varios subcampos o ninguno.

```
Subcampo Dependencia
Nota: Este subcampo debe ir antes que los subcampos de mandatos
URL de la dependencia.
Es obligatorio cuando se tienen estos tipos de mandatos Dependencia.
Para obtener más información, consulte el
apartado "Subvector de mandatos Dependencia" en la página 207.

Mandato      Tipo de dependencia
 0x0001          0x0001          Nota: Los subcampos URL que vayan después
                                       del subcampo Dependencia son
                                       URL de dependencias de esa
                                       dependencia.
 0x0001          0x0003

Subcampo URL
Nota: Este subcampo debe ser el segundo, en caso de que se requieran ambos subcampos.
         Es obligatorio cuando se tienen estos tipos de mandatos Dependencia.

Mandato      Tipo de dependencia
 0x0001          0x0001          Nota: El subcampo Dependencia que va antes
                                       del subcampo URL indica el
                                       URL de la dependencia.
 0x0001          0x0002
```

Subvector de respuesta Inhabilitar: El subvector de respuesta Inhabilitar se utiliza para responder al subvector de mandatos Inhabilitar.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0301

6-7 Reservado

8-11 Código de retorno

Consulte los “Códigos de retorno” en la página 224.

Subvector de respuesta Habilitar: El subvector de respuesta Habilitar se utiliza para responder al subvector de mandatos Habilitar.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0201

6-7 Reservado

8-11 Código de retorno

Consulte los “Códigos de retorno” en la página 224.

Subvector de respuesta Política: El subvector de respuesta Política se utiliza para responder al subvector de mandatos Política.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0501

6-7 Reservado

8-11 Código de retorno

Consulte los “Códigos de retorno” en la página 224.

Si el subvector de mandatos Política era PUT (0x0002), el subvector terminará aquí.

de 12 a (4n-1) Uno de los siguientes, dependiendo del tipo de política del subvector de mandatos Política.

Si el tipo de política es 0x0001, 0x0002, 0x0003, 0x0004 ó 0x0005:

12-13 Establecer valor

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

14-15 Reservado

Si el tipo de política es 0x0006, 0x0007 ó 0x0008

12-15 El valor representa el ciclo de vida del objeto, en minutos.

El valor está comprendido entre 0 y 10.080, donde 0 indica que el objeto no caduca.

Si el tipo de política es 0x0009

12-15 Valor que representa el intervalo de depuración de la antememoria, en minutos.

El valor está comprendido entre 0 y 720, donde 0 indica que el proceso de recogida de basura está inhabilitado.

Si el tipo de política es 0x000A

12-13 Valor que representa el tamaño máximo de la partición, en MB. El valor está comprendido entre 0 y 4.095, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

14-15 Reservado

Si la política es 0x000B

12-15 Valor que representa el número máximo de objetos.

El valor está comprendido entre 0 y 100000, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

Si la política es 0x000C

12-15 Valor que representa el tamaño máximo de un objeto en la partición de la antememoria.

El valor está comprendido entre 512 y 300.000; si se especifica 0, significa que no existe límite.

Nota: El valor no se verifica.

Si la política es 0xFFFF

12-13 Almacenamiento transparente en antememoria (Establecer valor)

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

14-15 Cabecera HTTP de control de la antememoria (Establecer valor)

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

16-17 Almacenamiento en antememoria de objetos dinámicos (Establecer valor)

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

18-19 Almacenamiento en antememoria de objetos imagen (Establecer valor)

- 0x0001 (Habilitado)

- 0x0002 (Inhabilitado)

20-21 Almacenamiento en antememoria de objetos estáticos (Establecer valor)

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

22-23 Valor que representa el tamaño máximo de la partición, en MB.

El valor está comprendido entre 0 y 4.095, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

24-27 Valor que representa el número máximo de objetos.

El valor está comprendido entre 0 y 1.000.000, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

28-31 Valor que representa el tamaño máximo de un objeto en una partición de la antememoria.

El valor está comprendido entre 512 y 3.000.000; si se especifica 0, significa que no existe límite.

Nota: El valor no se verifica.

32-35 Valor que representa el ciclo de vida de un objeto dinámico, en minutos.

El valor está comprendido entre 0 y 10.080, donde 0 indica que el objeto no caduca.

Nota: El valor no se verifica.

36-39 Valor que representa el ciclo de vida de un objeto imagen, en minutos.

El valor está comprendido entre 0 y 10.080, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

40-43 Valor que representa el ciclo de vida de un objeto estático, en minutos.

El valor está comprendido entre 0 y 10.080, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

44-47 Valor que representa el intervalo de depuración de la antememoria, en minutos.

El valor está comprendido entre 0 y 720, donde 0 indica que debe inhabilitarse el proceso de recogida de basura.

Subvector de respuesta Depurar: El subvector de respuesta Depurar se utiliza para responder a un subvector de mandatos Depurar.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0601

6-7 Reservado

8-11 Consulte los “Códigos de retorno” en la página 224.

Subvector de respuesta Consulta: El subvector de respuesta Consulta se utiliza para comprobar si un URL dado está en la partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0701

6-7 Reservado

8-11 Código de retorno

Consulte los “Códigos de retorno” en la página 224.

Nota: Si el código de retorno no es correcto (no es 0x00000000), la respuesta terminará aquí.

12-39 Hora en que fue modificado por última vez el objeto, en formato GMT.

Nota: Este campo no existirá si el código de retorno no es 0x00000000 o si no lo conoce la Partición de la antememoria.

12-15 Segundos

16-19 Minutos

20-23 Horas

24-27 Meses desde enero (0-11)

28-31 Años desde 1900

32-35 Días desde el domingo (0-6)

36-39 Día del mes

Subvector de respuesta Estadísticas: El subvector de respuesta Estadísticas responde al subvector de mandatos Estadísticas.

0-3 Longitud

Toda la longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0801

6-7 Reservado

8-11 Código de retorno

Código de retorno del subvector.

12-

12-15 Número actual de bytes de la Partición de la antememoria. Sólo refleja los bytes de entidad y no incluye los bytes utilizados para almacenar las cabeceras o el control de la utilización de bloques.

16-19 Marca de nivel superior para el número de bytes de la Partición de la antememoria.

20-23 Número actual de objetos en la Partición de la antememoria.

24-27 Marca de nivel superior para el número de objetos de la Partición de la antememoria.

28-31 Número total de veces que se se han encontrado estos objetos en la Partición de la antememoria.

32-35 Número total de veces que no se se han encontrado estos objetos en la Partición de la antememoria.

36-39 Número de objetos que se han añadido a la Partición de la antememoria explícitamente por una máscara de URL de inclusión.

40-43 Número de objetos que no se han añadido a la Partición de la antememoria debido a que se ha desactivado el almacenamiento en antememoria.

44-47 Número de objetos que no se han añadido a la partición de la antememoria debido a que el objeto era demasiado grande.

48-51 Número de objetos que no se han añadido a la Partición de la antememoria debido a que se ha especificado la directiva DONT CACHE en la cabecera HTTP de control.

52-55 Número de objetos que no se han añadido a la Partición de la antememoria debido a que se han excluido explícitamente por la máscara de URL.

56-59 Número de objetos que no se han añadido a la Partición de la antememoria debido a que el objeto estaba inactivo.

60-63 Número de objetos que no se han añadido a la Partición de la antememoria debido a que el objeto imagen no se ha almacenado explícitamente en la antememoria.

64-67 Número de objetos que no se han añadido a la Partición de la antememoria debido a que el objeto estático no se ha almacenado explícitamente en la antememoria.

68-71 Número de objetos que no se han añadido a la Partición de la antememoria debido a que el objeto dinámico no se ha almacenado explícitamente en la antememoria.

72-75 Número de objetos depurados a causa de que la antememoria estaba llena o de que todas las particiones de la antememoria superaban la cantidad total permitida por la antememoria del servidor Web.

76-79 Número de objetos depurados a causa de que el ciclo de vida de los objetos ha finalizado.

80-83 Número de objetos depurados explícitamente, al dar su URL o al depurar toda la partición.

84-87 Número de objetos depurados a causa de la anulación de la dependencia.

88-91 Número de elementos suprimidos de la partición por la interfaz de control de la antememoria externa (suprimir).

92-95 Número de elementos añadidos a la partición por la interfaz de control de la antememoria externa.

96-99 Número de elementos que no ha añadido a la partición la interfaz de control de la antememoria externa, pero que se han intentado añadido.

100-103 Número de elementos sustituidos en la partición por la interfaz de control de la antememoria externa.

104-107 Número de respuestas 200 (OK) devueltas cuando se ha producido un acierto en la antememoria.

108-111 Número de respuestas 203 (Non_Authoritative) devueltas cuando se ha producido un acierto en la antememoria.

112-115 Número de respuestas 206 (Partial Content) devueltas cuando se ha producido un acierto en la antememoria.

116-119 Número de respuestas 300 (Multiple Choices) devueltas cuando se ha producido un acierto en la antememoria.

120-123 Número de respuestas 301 (Moved Permanently) devueltas cuando se ha producido un acierto de antememoria.

124- 127 Número de respuestas 304 (Not Modified) devueltas cuando se ha producido un acierto de antememoria.

128-131 Número de respuestas 410 (Gone) devueltas cuando se ha producido un acierto en la antememoria.

132-135 Número de respuestas de los números 100 (Informativas) devueltas cuando no se ha producido un acierto en la antememoria.

136-139 Número de respuestas 200 (OK) devueltas cuando no se ha producido un acierto en la antememoria.

140-143 Número de respuestas de los números 200 (Satisfactorias) devueltas cuando no se ha producido un acierto en la antememoria.

144-147 Número de respuestas 304 (Not Modified) devueltas cuando no se ha producido un acierto de antememoria.

148-151 Número de respuestas de los números 300 (Redirección) devueltas cuando no se ha producido un acierto en la antememoria (sin contar los mensajes 304).

152-155 Número de respuestas de los números 400 (Error del cliente) devueltas cuando no se ha producido un acierto en la antememoria.

156-159 Número de respuestas de los números 500 (Error del servidor) devueltas cuando no se ha producido un acierto en la antememoria.

160-163 Número de otras respuestas (distintas de las anteriores) devueltas cuando no se ha producido un acierto en la antememoria.

164-167 Número de bytes servidos al producirse un acierto en la antememoria (nota: no se cuentan las cabeceras HTTP).

168-171 Número de bytes servidos al no producirse un acierto en la antememoria (nota: no se cuentan las cabeceras HTTP).

Subvector de respuesta Máscara de URL: El subvector de respuesta Máscara de URL se utiliza para responder a un subvector de mandatos Máscara de URL.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0901

6-7 Reservado

8-11 Código de retorno

Código de retorno del subvector. Consulte los “Códigos de retorno” en la página 224.

de 12 a (4n-1) Varios subvectores URL o ninguno, si el subvector de mandatos Máscara de URL era Obtener (0x0001).

Formatos de los subcampos

En este apartado se ofrecen las descripciones de los subcampos.

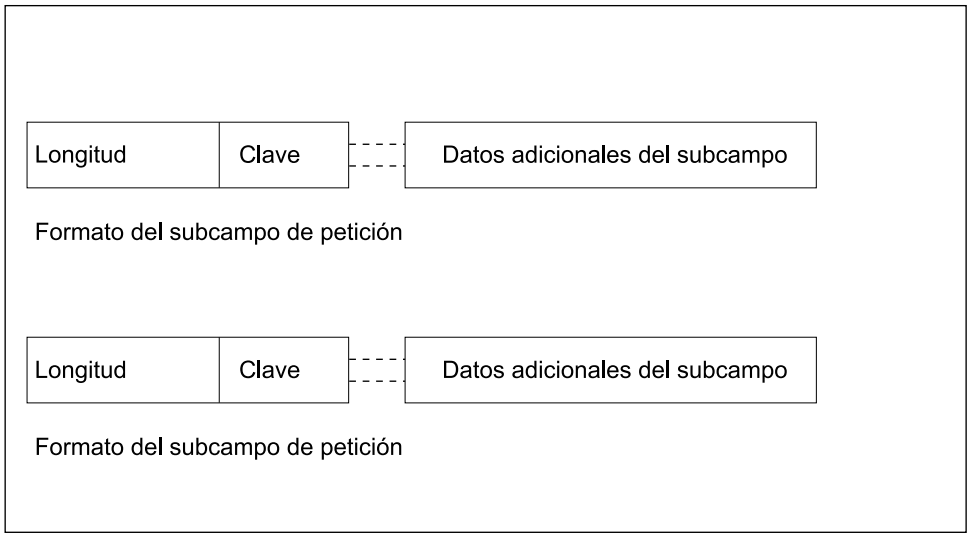


Figura 20. Formato de un subcampo

Longitud parcial: Valor de 32 bits sin signo que representa la longitud (en bytes) de todo el subcampo, incluida la de los campos longitud y clave, pero excluyendo

los bytes de relleno. Los subcampos se rellenan para que queden alineados con los límites de 4 bytes (palabra). El rango de valores aceptables es de 6 a 4GB.

Clave: Valor de 16 bits sin signo que representa la clave del subcampo. Las claves de los subcampos de mandatos son:

- 0x0010 (Localizador uniforme de recursos, después de desmantelar el protocolo "http:" y la dirección del recurso de Internet. Por ejemplo, el URL "http://192.9.200.50/archivo1.html" se enviaría como "/archivo1.html").
- 0x0020 (Objeto Web en formato de mensaje de respuesta HTTP)
- 0x0030 (Nombre de usuario del ECCP. El vector de autenticación necesita este subcampo).
- 0x0040 (Contraseña de usuario del ECCP. El vector de autenticación necesita este subcampo).
- 0x0050 (subcampo Dependencia)

Las claves de los subcampos de respuesta son:

- 0x0011 (Localizador uniforme de recursos, después de desmantelar el protocolo "http:" y la dirección del recurso de Internet).
- 0x0051 (subcampo Dependencia)

Reservado: Campo de 16 bits que actualmente no se utiliza.

Subcampo Dependencia: El subcampo Dependencia del subvector de respuesta Máscara de URL.

0-3 Longitud parcial

Longitud (en bytes) del subcampo, como se muestra en la Figura 20 en la página 221.

4-5 Clave

0x0050 - petición

0x0051 - respuesta

6-7 Reservado

de 8 a (4n-1) Dependencia y bytes de relleno

La dependencia debe tener una longitud de 1 a 50.

Subcampo Nombre: El subcampo Nombre del subvector de respuesta Máscara de URL.

0-3 Longitud

Longitud (en bytes) del subcampo, como se muestra en la Figura 20 en la página 221.

4-5 Clave

0x0030 - petición

6-7 Reservado

de 8 a (4n-1) Nombre y bytes de relleno

El nombre deber tener una longitud de 1 a 8.

Subcampo Objeto: El subcampo Objeto del subvector de respuesta Máscara de URL.

0-3 Longitud

Longitud (en bytes) del subcampo, como se muestra en la Figura 20 en la página 221.

4-5 Clave

0x0020 - petición

6-7 Reservado

de 8 a (4n-1) Objeto y bytes de relleno

El formato del objeto debe ser el de una Respuesta HTTP. Es una serie de caracteres.

Subcampo Petición de contraseña: El subcampo Petición de contraseña del subvector de respuesta Máscara de URL.

0-3 Longitud

Longitud (en bytes) del subcampo, como se muestra en la Figura 20 en la página 221.

4-5 Clave

0x0040

6-7 Reservado

8-15 El número generador utilizado para el cifrado (deben ser 8 bytes).

de 16 a (4n-1) Contraseña y bytes de relleno

La contraseña debe tener una longitud de entre 1 y 8 bytes y estar cifrada.

Subcampo Petición de URL: El subcampo Petición de URL del subvector de respuesta Máscara de URL.

0-3 Longitud

Longitud (en bytes) del subcampo, como se muestra en la Figura 20 en la página 221.

4-5 Clave

0x0010 - petición

0x0011 - respuesta

6-7 Reservado

de 8 a (4n-1) URL o máscara de URL y bytes de relleno

Esta URL o máscara de URL es un conjunto de caracteres que debe tener una longitud de entre 1 y 255 caracteres.

Códigos de retorno

Es importante comprobar los códigos de retorno de cada subvector de respuesta, además del código de retorno del vector de respuesta. El código de retorno del vector de respuesta se establecerá a un valor distinto de cero en caso de que se detecte un error grave, en cuyo caso, puede que no todos los subvectores de mandatos del vector de mandatos tengan su correspondiente subvector de respuesta.

Códigos de retorno y sus descripciones

0000 0000: La operación se ha realizado satisfactoriamente
0001 0000: No se ha encontrado el objeto
0002 0000: La partición de la antememoria ya está habilitada
0003 0000: La partición de la antememoria ya está inhabilitada
0004 0000: La partición de la antememoria no está habilitada
0005 0000: No se ha definido la partición de la antememoria
0006 0000: La partición de la antememoria está terminando
0007 0000: Es necesario un subcampo URL, pero no está presente
0008 0000: El intervalo de depuración proporcionado no es válido
0009 0000: Valor de configuración no soportado
000A 0000: Valor de mandato no soportado
000B 0000: Valor de tipo de política no soportado
000C 0000: Valor de tipo de URL no soportado
000D 0000: Clave de vector no soportada
000E 0000: Clave de subvector no soportada
000F 0000: Imposible analizar las cabeceras del objeto
0010 0000: Imposible obtener almacenamiento
0011 0000: Objeto demasiado grande para añadirlo a la partición
0012 0000: El formato del vector no es válido
0013 0000: El objeto no puede almacenarse en la antememoria
0014 0000: Detectado error de análisis HTTP
0015 0000: Es necesario un subcampo Objeto, pero no está presente
0016 0000: No se ha proporcionado ningún subcampo Dependencia o no es válido
0017 0000: Es necesario el vector de autenticación
0018 0000: No es necesario el vector de autenticación, por lo que se hará caso omiso
0019 0000: La dependencia no estaba en la tabla de dependencias
001A 0000: El URL de dependencias no estaba en la tabla de dependencias
001B 0000: Tipo de dependencia no soportado
001C 0000: No es correcto el identificador de usuario, la contraseña o el permiso para el ECC
001D 0000: No es correcto el tipo de máscara de URL para la carga de la imagen en el recuadro
FF01 yyyy: El mandato ha devuelto un error. Los últimos 2 bytes contienen información adicional.
- 0101: No se ha encontrado el objeto.
- 0102: El objeto no se ha podido almacenar en antememoria.
- 0103: El objeto ya existe en la partición.
- 0104: La inicialización de la partición ha dado un error, ya están activas el número máximo de particiones.
- 0105: La partición está activa.
- 0106: La partición no está activa.
- 0107: La partición está en un estado pendiente y no puede ejecutar el mandato. Espere unos segundos y vuelva a intentar ejecutar el mandato.
- 0108: No se ha definido la partición.
- 0109: Tipo de URL no soportado.
- 010A: El puntero de URL no es válido.
- 010B: El número de partición no es válido.
- 010C: Mandato de partición no soportado.

010D: El puntero de partición no es válido.
010E: El handle de la partición no hace referencia a una partición activa.
010F: El handle de la partición no hace referencia a una partición válida.
0110: Es necesario un puntero de política, pero no está presente.
0111: En necesario un puntero de estadísticas, pero no está presente.
0112: El intervalo de depuración es demasiado grande.
0113: La dependencia ya tiene URL.
0FFF: No está disponible el control de la antememoria externa.
FFF9: Imposible conseguir espacio de almacenamiento.
FFFA: Imposible conseguir un handle de partición.
FFFB: Es necesario un puntero SRAM de política, pero no está presente.
FFFC: Es necesario un puntero SRAM de partición, pero no está presente.
FFFD: Imposible asignar o inicializar el intervalo de vencimiento de la antememoria.
FFFE: Imposible asignar o inicializar la partición de la antememoria.
FFFF: Imposible asignar o inicializar el núcleo de la antememoria.

Configuración y supervisión de la antememoria del servidor Web

En este capítulo se describe cómo configurar la función antememoria del servidor Web y cómo utilizar los mandatos de supervisión de la antememoria del servidor Web. Consta de los apartados siguientes:

Configuración de la antememoria del servidor Web

La función de almacenamiento en antememoria del servidor Web del servidor Web debe utilizarse con Network Dispatcher. Antes de utilizar la antememoria del servidor Web por primera vez, deberá:

1. Acceder a Network Dispatcher en el indicador `Config>` de la consola `talk 6` mediante el mandato **feature ndr**.
2. Habilitar el ejecutor
3. Añadir un cluster
4. Añadir un puerto
5. Añadir uno o más servidores.

A continuación podrá utilizar los mandatos de configuración y de supervisión para modificar el entorno de la antememoria del servidor Web.

Nota: Mientras que los cambios realizados en Network Dispatcher mediante Talk 6 modifican la configuración en ejecución, los cambios realizados en la antememoria del servidor Web no modifican la configuración en ejecución, a menos que se activen explícitamente mediante el mandato **activate** en Talk 6 o mediante el mandato feature Webc de Talk 5. La excepción es que si el cluster o puerto de un proxy HTTP se elimina mediante el mandato feature NDR de Talk 6, también se eliminará de la configuración actualmente en ejecución el proxy HTTP de la antememoria del servidor Web.

Ejemplo:

```
Config>f ndr
NDR Config>enable executor
NDR Config>add cluster
Cluster Address [0.0.0.0]? 113.3.1.10
FIN count [4000]?
FIN time out [30]?
FIN stale timer [1500]?
Cluster 113.3.1.12 has been added.
Fincount has been set to 4000 for cluster 113.3.1.10
Fintimeout has been set to 30 for cluster 113.3.1.10
Staletimer has been set to 1500 for cluster 113.3.1.10
NDR Config>add port
Cluster Address [0.0.0.0]? 113.3.1.10
Port number [80]?
Port type (tcp=1, upd=2, both=3) [3]?
Max. weight (0-100) [20]?
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1 pftp=2 cache=3 extcache=4) [0]? 3
Do you want a new cache partition? [Yes]:
Enter cache partition [0]?
Default server TCP connection timeout (Range 5-240 seconds) [120]?
Default client TCP connection timeout (Range 5-240 seconds) [120]?
Maximum partition size (1-4095 megabytes or 0 for no limit) [0]?
Maximum number of objects (1-100000 or 0 for no limit) [0]?
Maximum object size (512-300000 bytes or 0 for no limit) [0]?
Do you want the cache enabled upon reboot? [Yes]:
 Default cache purge interval (1-720 minutes or 0 to disable) [10]
Enable transparent caching? [Yes]:
Check cache control headers? [Yes]:
Cache images? [Yes]:
      Default expiration time for images
              (1-10080 minutes or 0 for no expiration) [60]?
Cache non-image static objects? [Yes]:
      Default expiration time for non-image static objects
              (1-10080 minutes or 0 for no expiration) [60]?
URL mask to identify dynamic objects [*/cgi*]?
Cache dynamic objects? [No]:
Do you want to add a URL mask? [No]:

Cache partition number 1 has been successfully created.
Requested port has been added to cluster 113.3.1.10
Maxweight has been set to 20 for port 80 in cluster 113.3.1.10
NDR Config>add server
Cluster Address  [0.0.0.0] ? 113.3.1.10
Port number  [80] ? 80
Server Address  [0.0.0.0] ? 113.1.2.0
Server weight   [20] ?
Server state (down=0, up=1)  [1] ?
Server 113.1.2.0 has been added to the requested port(s) of cluster 113.3.1.10
Weight of server 113.1.2.0 has been set to 20 in port 80 of cluster 113.31.10
Server 113.1.2.0 has been set up.
NDR Config> exit
```

En la lista siguiente se describen brevemente los parámetros del ejemplo específicos de la antememoria del servidor Web.

cluster-address Especifica la dirección IP del cluster.

Nota: Las direcciones IP del cluster se supone que están en la misma subred lógica que las del direccionador de saltos anterior (direccionador IP), a menos que se estén anunciando las direcciones del cluster.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

FIN-count Especifica el número de conexiones que deben estar en el estado FIN antes de que el ejecutor intente eliminar la información de conexión no usada de la base de datos de Network Dispatcher después de transcurrido el *tiempo de espera de FIN* o el definido en el *temporizador de inactividad*.

Valores válidos: de 0 a 65.535

Valor por omisión: 4.000

FIN-timeout Especifica el número de segundos que una conexión puede permanecer en el estado de FIN antes de que el ejecutor intente eliminar la información de conexión no usada de la base de datos de Network Dispatcher.

Valores válidos: de 0 a 65.535

Valor por omisión: 30

Stale-timer Especifica el número de segundos que una conexión puede permanecer inactiva, después de que el ejecutor intente eliminar la información de la conexión de la base de datos de Network Dispatcher.

Valores válidos: de 0 a 65.535

Valor por omisión: 1500

port# Especifica el número de puerto del protocolo para este cluster.

Valores válidos: de 1 a 65.535

Valor por omisión: 80

port-type Especifica los tipos de tráfico IP cuya carga puede repartirse en este puerto. Los tipos soportados son:

- 1 = TCP
- 2 = UDP
- 3 = ambos

Valores válidos: 1, 2, 3

Valor por omisión: 3

max-weight Especifica el peso máximo para los servidores de este puerto. Esto afectara al diferente número de peticiones que el ejecutor entregará a cada servidor.

Valores válidos: de 0 a 100

Valor por omisión: 20

port-mode Especifica si el puerto enviará todas las peticiones de un único cliente a un único servidor (llamado adherente), utilizará ftp pasivo (pftp),utilizará la antememoria del servidor Web (antememoria), las enviará a un conjunto de antememorias escalables externas (antememoria externa), o no utilizará ningún protocolo concreto para este cluster (ninguno).

Valores válidos: de 0 a 4, donde:

- 0 = none (ninguna)
- 1 = sticky (adherente)

- 2 = pftp
- 3 = cache (antememoria)
- 4 = extcache (antememoria externa)

Valor por omisión: 0

Do you want a new cache partition? Especifica si quiere utilizar una partición de la antememoria ya existente o una nueva.

Valores válidos: Yes o No

Valor por omisión: Yes

Enter cache partition Especifica el número de la partición de la antememoria ya existente que se utilizará.

Valores válidos: Cualquier número de partición de la antememoria ya existente

Valor por omisión: 0

Default server TCP connection timeout Especifica el tiempo que transcurrirá antes de que finalice la conexión con un servidor.

Valores válidos: de 5 a 240 segundos

Valor por omisión: 120 segundos.

Do you want to modify cache partition? Le permite modificar la configuración de una partición de la antememoria ya existente.

Valores válidos: Yes o No

Valor por omisión: No

Default client TCP connection timeout Especifica el tiempo que transcurrirá antes de que finalice la conexión con un cliente.

Valores válidos: de 5 a 240 segundos

Valor por omisión: 120 segundos.

Maximum partition size Especifica la cantidad máxima de memoria que se asignará a esta partición de la antememoria. Si este valor es superior a la cantidad de memoria disponible actualmente, se hará caso omiso del valor y no se impondrá ningún tamaño máximo de la partición.

Valores válidos: de 1 a 4095 Megabytes o 0 (sin máximo)

Valor por omisión: 0 (sin máximo)

Maximum number of objects Especifica el número máximo de objetos que pueden almacenarse en una partición de la antememoria. Si el usuario escribe un 0, la partición de la antememoria estará limitada solamente por la cantidad de memoria disponible para la partición.

Valores válidos: de 1 a 100.000 ó 0 (sin límite)

Valor por omisión: 0 (sin límite)

Maximum object size Especifica el tamaño máximo de los objetos que se almacenarán en la antememoria. Loa objetos que superen este tamaño máximo nunca se almacenarán en la antememoria. Si se modifica el tamaño máximo de los objetos después de llenar la

antememoria, es posible que algunos objetos que ya estaban en la antememoria tengan temporalmente un tamaño superior al máximo que se ha definido.

Valores válidos: de 512 a 300.000 bytes o 0 (sin tamaño máximo)

Valor por omisión: 0 (sin tamaño máximo)

Do you want the cache enabled upon reboot? Especifica si una partición de la antememoria debe habilitarse automáticamente o sólo cuando lo solicite explícitamente el usuario. Las particiones de la antememoria configuradas para que se habiliten inmediatamente se habilitan automáticamente cuando se vuelve a arrancar el 2212. Las particiones de la antememoria que no están configuradas para habilitarse inmediatamente seguirán estando disponibles, pero inhabilitadas, hasta que el usuario habilite la partición desde la consola `talk 5` de la antememoria del servidor Web.

Valores válidos: Yes o No

Valor por omisión: Yes

Default cache purge interval Especifica el intervalo de depuración por omisión de la antememoria.

Valores válidos: de 1 a 720 minutos o 0 (inhabilitado)

Valor por omisión: 10 minutos

Enable transparent caching? Especifica si las respuestas del servidor a objetos que no se han encontrado (no encontrados en la antememoria) deben almacenarse automáticamente en la antememoria. La alternativa es utilizar ECCP para manipular la antememoria.

Valores válidos: Yes o No

Valor por omisión: Yes

Check cache control headers? Permite que un servidor especifique a la antememoria del servidor Web si la respuesta se puede elegir para ser almacenada en antememoria.

Valores válidos: Habilitado o Inhabilitado

Valor por omisión: Inhabilitado

Cache images? Especifica si los archivos de imágenes (*.gif o *.jpg) deben almacenarse en antememoria.

Valores válidos: Yes o No

Valor por omisión: Yes

Default expiration time for images

Valores válidos: de 1 a 10.080 minutos, o 0 (ninguna)

Valor por omisión: 60 minutos

Cache non-image static objects? Especifica si datos estáticos que no son imágenes (archivos que no contenga la máscara */cgi* y archivos que no terminen en .jpg o .gif) deben almacenarse en antememoria.

Valores válidos: Yes o No

Valor por omisión: Yes

Default expiration time for non-image static objects

Valores válidos: de 1 a 10.080 minutos, o 0 (ninguna)

Valor por omisión: 60 minutos

URL mask to identify dynamic objects Especifica la máscara de URL que se utilizará para identificar objetos dinámicos.

Valores válidos: cualquier máscara de URL

Valor por omisión: */cgi*

Cache dynamic objects? Especifica si deben almacenarse en la antememoria los objetos dinámicos. Los objetos dinámicos son objetos que construye el servidor al recibir la petición del objeto y que reconstruye a cada nueva petición, hayan cambiado o no los datos.

Valores válidos: Yes o No

Valor por omisión: No

Do you want to add a URL mask? Especifica una máscara de URL nueva que se añadirá a la antememoria. Las máscaras de URL permiten que el usuario incluya o excluya objetos individuales o grupos de objetos por su Localizador universal de recursos (URL).

Valores válidos: i o e

Valor por omisión: i

Cuando se especifica una máscara de URL, se pueden utilizar caracteres comodín. Al configurar Network Dispatcher para la Antememoria del servidor Web o al utilizar los mandatos **add** o **modify url** desde el indicador `f webc`, pueden utilizarse caracteres comodín. Los caracteres utilizados como comodines son el * (asterisco) y el # (signo de número). Los comodines pueden utilizarse en cualquier posición del URL.

El * indica que cualquier número de caracteres puede formar parte de ese URL, incluso ninguno.

Ejemplo: *abc.html filtrará las máscaras de URL siguientes.

```
abc.html
finabc.html
defchtjqsprabc.html
```

El signo # representa un solo carácter.

Ejemplo: ab#.html filtrará las máscaras de URL siguientes.

```
abc.html
abf.html
abo.html
```

En el ejemplo siguiente se selecciona la modalidad de puerto 3 (`cache=3`) y no se añade ninguna partición de la antememoria nueva.

```
NDR Config>add port
Cluster Address  [0.0.0.0] ? 113.3.1.11
Port number  [80] ?
Max. weight (0-100)  [20] ?
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1 pftp=2 cache=3 extcache=4)  [0] ? 3
Do you want a new cache partition?  [Yes] : n
Enter cache partition  [0] ? 0
Maximum TCP segment size  (Range 512-32768 bytes)  [4096] ?
Default server TCP connection timeout (Range 5-240 seconds) [120] ?
Default client TCP connection timeout (Range 5-240 seconds)  [120] ?
Do you want to modify cache partition [0]?  No :
Requested port has been added to cluster 113.3.1.11
Maxweight has been set to 20 for port 80 in cluster 113.3.1.11
```

Nota: En el ejemplo siguiente se selecciona la modalidad de puerto 3 (`cache=3`) y se añade una partición de la antememoria nueva.

```
NDR Config>add port
Cluster Address [0.0.0.0]? 113.3.1.10
Port number [80]?
Port type(tcp=1, udp=2, both=3) [3]?
Max. weight (0-100) [20]?
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1 pftp=2 cache=3 extcache=4) [0]? 3
Do you want a new cache partition? [Yes]: y
Default server TCP connection timeout (Range 5-240 seconds) [120]?
Default client TCP connection timeout (Range 5-240 seconds) [120]?
Maximum partition size (1-4095 megabytes or 0 for no limit) [0]?
Maximum number of objects (1-100000 or 0 for no limit) [0]?
Maximum object size (512-300000 bytes or 0 for no limit) [0]?
Do you want the cache enabled upon reboot? [Yes]:
 Default cache purge interval (1-720 minutes or 0 to disable) [10]?
Enable transparent caching? [Yes]:
Check cache control headers? [Yes]:
Cache images? [Yes]:
      Default expiration time for images
              (1-10080 minutes or 0 for no expiration) [60]?
Cache non-image static objects? [Yes]:
      Default expiration time for non-image static objects
              (1-10080 minutes or 0 for no expiration) [60]?
URL mask to identify dynamic objects [*/cgi*]?
Cache dynamic objects? [No]:
Do you want to add a URL mask? [No]:

Cache partition number 0 has been successfully created.
Requested port has been added to cluster 113.3.1.10
Maxweight has been set to 20 for port 80 in cluster 113.3.1.10
Port Type has been set to Both for port 85 in cluster 113.3.1.10
NDR Config>
```

Para configurar el cluster y el puerto iniciales de la función de almacenamiento en antememoria del servidor Web, debe utilizarse Network Dispatcher. Una vez añadidos el cluster y el puerto, al configurar la *modalidad de puerto* como puerto de la antememoria, podrá modificar y visualizar los parámetros de configuración del almacenamiento en Antememoria del servidor Web en el indicador `WEBC Config>`.

Consulte la página 139 para obtener más información sobre Network Dispatcher.

Acceso al entorno de la antememoria del servidor Web

Para acceder al entorno de configuración de la antememoria del servidor Web, escriba el mandato siguiente en el indicador Config>.

```
Config> feature webc
WEBC Config>
```

Mandatos de la antememoria del servidor Web

En este apartado se describen los mandatos de configuración de la antememoria del servidor Web. En la Tabla 18 se listan los mandatos de configuración de la antememoria del servidor Web. Estos mandatos especifican los parámetros de la función antememoria del servidor Web. Para activar los cambios, reinicie el direccionador.

Tabla 18. Resumen de mandatos de configuración de la antememoria del servidor Web

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 xxxii.
Activate	Activa o vuelve a activar las particiones de la antememoria utilizando la configuración más reciente.
Add	Añade una máscara de URL.
Delete	Suprime una máscara de URL o una partición.
List	Lista la información del almacenamiento en antememoria.
Modify	Modifica la información del almacenamiento en antememoria.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxiii.

Activate

Utilice el mandato **activate** para inicializar todas las particiones de la antememoria, utilizando la configuración más reciente.

Sintaxis:

ac**tivate**

Ejemplo:

```
WEBC Config>act ?
ACTIVATE all initializes cache partitions, using
the latest configuration.
```

Add

Utilice el mandato **add** para añadir una máscara de URL.

Sintaxis:

ad**d** urlmask

Ejemplo:

```
WEBC Config>add url
Partition number [0]?
New URL mask []? *mascaranueva*
Include or Exclude from cache (i or e) [i]? i
Set default expiration time?  [No]:y
Default expiration time
        (1-10080 minutes or 0 for no expiration) [0]? 20
The URL mask has been added to cache partition number 0.
```

Nota: Para añadir proxies y particiones, deberá utilizar Network Dispatcher y ejecutar los mandatos **add port** o **set port**.

partition number Número de partición que se añadirá a la partición.

Valores válidos: cualquier número de partición válido

Valor por omisión: 0

new URL mask Nombre de la máscara de URL que se añadirá.

Valores válidos: Cualquier máscara de URL válida

Valor por omisión: ninguno

include or exclude from cache Especifica si el URL debe incluirse en la antememoria o excluirse de ella.

Valores válidos: i o e

Valor por omisión: i

default expiration time Especifica la hora de vencimiento por omisión, en minutos. Un cero indica que no tiene hora de vencimiento.

Valores válidos: de 0 a 10.080 minutos

Valor por omisión: 0 (sin hora de vencimiento)

Delete

Utilice el mandato **delete** para suprimir de la base de datos de configuración una máscara de URL o una partición.

Sintaxis:

de**lete** partition
urlmask

partition Número de la partición que se suprimirá de una antememoria.

urlmask Nombre de la máscara de URL que se suprimirá de una antememoria.

Ejemplo:

```
WEBC Config>delete url
Partition number [0]? 0
URL masks defined : 5
    1: EXCLUDE '*index*'
    2: EXCLUDE '*comp*'
    3: INCLUDE '*tmp*'
      Default expiration time: 1 minutes
    4: INCLUDE '*stat*'
        Default expiration time: 5 minutes
    5: INCLUDE '*html*'
      Default expiration time: 1000 minutes (16 hrs 40 mins)
URL mask number [1]? 5
The URL mask for cache partition number 0 has been deleted.
```

Nota: Se deben suprimir todos los proxies que utilizan una partición antes de suprimir la partición. Para suprimir un proxy deberá utilizar la función realizar una conversión "proxy" y eliminar el puerto y el cluster asociados, o cambiar la modalidad de puerto a otra distinta de la de antememoria.

partition number Número de partición que se suprimirá de la partición.

Valores válidos: cualquier partición válida

Valor por omisión: 0

URL mask number Número de la máscara de URL que se suprimirá.

Valores válidos: cualquier número de máscara de URL válido.

Valor por omisión: 1

List

Utilice el mandato **list** para listar la información de la antememoria del servidor Web.

Sintaxis:

list all / external / partition / proxy / urlmask

all List todos los puertos, particiones, proxies y máscaras definidos en una antememoria.

external Lista la información del Gestor de control de la antememoria externa.

partition Lista los números de partición de una antememoria.

proxy Lista los proxies definidos en una antememoria.

urlmask Lista las máscaras de URL definidas en una antememoria.

Ejemplo: list all

```
WEBC Config>list all
Cache Partition 0
    Cluster address 113.3.1.10, Port 80

1 cache partition(s) defined.
```

Ejemplo: list external

```
WEBC Config>list ext
External Cache manager : Enabled
Port number            : 82
TCP timeout            : 120 seconds
```

Ejemplo: list partition

```
WEBC Config>list part
Cache Partition 0
Maximum partition size         : 1 MB
Maximum number of objects      : Unlimited
Maximum object size:           : Unlimited
Activate on reboot             : Enabled
Cache purge interval           : 10 minutes
Dynamic URL mask               : '*/cgi*' "
Transparent caching: Enabled
Check cache control headers        : Disabled
Cache images                       : Disabled
Cache non-image static objects: Enabled
      Default expiration time      : 60 minutes (1 hrs 0 mins)
Cache dynamic objects: Disabled
Associated proxies (cluster port)  : (113.3.1.10 80)

1 cache partition(s) defined.
```

Ejemplo: list url

```
WEBC Config>list url
Partition number [0]?
URL masks defined : 5
    1: EXCLUDE '*index*'
    2: EXCLUDE '*comp*'
    3: INCLUDE '*tmp*'
      Default expiration time: 1 minutes
    4: INCLUDE '*stat*'
      Default expiration time: 2 minutes
    5: INCLUDE '*html*'
      Default expiration time: 1000 minutes (16 hrs 40 mins)
```

Modify

Utilice el mandato **modify** para modificar la información de la Antememoria del servidor Web.

Sintaxis:

modify external
partition
proxy
urlmask

external Le permite modificar el Gestor de control de la antememoria externa.

partition Le permite modificar una partición.

proxy Le permite modificar el proxy

urlmask Le permite modificar la máscara de URL.

Ejemplo: modify external

```
WEBC Config>mod ext
External cache manager port number(0 to disable) [82]?
TCP connection timeout (Range 5-240) seconds) [120]? 20
Do you want to modify the encryption key:? [No]? Y
Encryption key should be 16 characters long.
Encryption key (16 characters) in Hex (0-9, a-f, A-F):
Encryption Key again (16 characters) in Hex (0-9, a-f, A-F):
The external cache manager has been modified.
```

external cache manager port number Especifica el número de puerto del gestor de control de la antememoria externa que se va a modificar.

Valores válidos: de 0 a 255

Valor por omisión: 82

TCP connection timeout Especifica la conexión TCP del gestor de control de la antememoria externa que se va a modificar.

Valores válidos: de 5 a 240 segundos

Valor por omisión: 120

do you want to modify the encryption key Especifica si se ha de modificar o no la clave de cifrado.

Valores válidos: yes o no

Valor por omisión: no

encryption key Clave de cifrado para el gestor de control de la antememoria externa que se va a modificar. La clave de cifrado debe ser una serie de 16 caracteres hexadecimales.

Valores válidos: caracteres hexadecimales (0-9, a-f, A-F)

Valor por omisión: ninguno

Ejemplo: modify partition

```
WEBC Config>modify partition
Partition number [0] ?
Maximum partition size (1-255 megabytes or 0 for no limit) [0]? 200
Maximum number of objects (1-100000 or 0 for no limit)[0]? 5000
Maximum object size (512-300000 bytes or 0 for no limit)[0]? 250000
Do you want the cache enabled upon reboot? [Yes]:
 Default cache purge interval (1-720 minutes or 0 to disable) [10]? 20
Enable transparent caching? [Yes]:
Check cache control headers? [Yes]:
Cache images? [Yes]:
      Default expiration time for images
              (1-10080 minutes or 0 for no expiration) [60]?
Cache non-image static objects? [Yes]:
      Default expiration time for non-image static objects
              (1-10080 minutes or 0 for no expiration) [60]?
URL mask to identify dynamic objects [*/cgi*]? *dyn*
Cache dynamic objects? [No]: y
Cache partition number 0 has been modified.
```

partition number Número de la partición que se modificará.

Valores válidos: cualquier número de partición válido

Valor por omisión: 0

maximum partition size Tamaño máximo de la partición que se modificará. Un cero indica que no existe límite.

Valores válidos: de 1 a 255 megabytes o 0 para indicar que no existe límite

Valor por omisión: 0

maximum number of objects Número máximo de objetos en la partición que se modificará. Un cero indica que no existe límite.

Valores válidos: de 0 a 100.000 ó 0 para indicar que no hay límite

Valor por omisión: 0

maximum object size Tamaño máximo de los objetos de la partición que se va a modificar. Un cero indica que no existe límite.

Valores válidos: de 512 a 300.000 ó 0 para indicar que no hay límite

Valor por omisión: 0

do you want the cache enabled upon reboot Especifica si se ha de habilitar o no la antememoria después de volver a arrancar.

Valores válidos: yes o no

Valor por omisión: yes

default cache purge interval Especifica el intervalo de depuración por omisión de la antememoria. Un cero inhabilita el intervalo de depuración por omisión de la antememoria.

Valores válidos: de 1 a 170 minutos o 0 para inhabilitarlo

Valor por omisión: 10

enable transparent caching Especifica si se ha de habilitar o no el almacenamiento transparente en antememoria. La alternativa es utilizar ECCP para manipular la antememoria.

Valores válidos: yes o no

Valor por omisión: yes

check cache control headers Especifica si se han de comprobar o no las cabeceras de control de la antememoria.

Valores válidos: yes o no

Valor por omisión: yes

cache images Especifica si se han de almacenar las imágenes en antememoria.

Valores válidos: yes o no

Valor por omisión: yes

Default expiration time for images Especifica la hora de vencimiento por omisión de las imágenes. Un cero indica que no existe hora de vencimiento.

Valores válidos: de 1 a 10.080 ó 0 para indicar que no existe hora de vencimiento.

Valor por omisión: 60

cache non-image static objects Especifica si se han de almacenar en antememoria los objetos estáticos que no son imágenes.

Valor por omisión: yes

Valores válidos: yes o no

Default expiration time for non-image static objects Especifica la hora de vencimiento por omisión de los objetos estáticos que no son imágenes. Un cero indica que no existe hora de vencimiento.

Valores válidos: de 1 a 10.080 ó 0 para indicar que no existe hora de vencimiento.

Valor por omisión: 60

url mask to identify dynamic objects Especifica la máscara de URL que se utilizará para identificar objetos dinámicos.

Valores válidos: cualquier máscara de url válida

Valor por omisión: */cgi*

cache dynamic objects Especifica si se han de almacenar en antememoria los objetos dinámicos.

Valores válidos: yes o no

Valor por omisión: no

Ejemplo: modify url

```
WEBC Config>modify url
Partition number [0]?
URL masks defined : 5
    1: EXCLUDE '*index*'
    2: EXCLUDE '*comp*'
    3: INCLUDE '*tmp*'
      Default expiration time: 1 minutes
    4: INCLUDE '*stat*'
      Default expiration time: 2 minutes
    5: INCLUDE '*html*'
      Default expiration time: 1000 minutes (16 hrs 40 mins)
URL mask number  [1] ? 4
New URL mask *stat*?
Include or Exclude from cache (i or e) [i]?
Set default expiration time?  Yes :
Default expiration time
        (1-10080 minutes or 0 for no expiration) [2]? 5
URL mask number 4 has been modified.
```

partition number Especifica el número de partición del URL que se va a modificar.

Valores válidos: cualquier número de partición válido

Valor por omisión: 0

url mask number Especifica el número de la máscara de URL que se va a modificar.

Valores válidos: cualquier número de máscara de URL válido.

Valor por omisión: 1

new url mask *stat*

Valores válidos: yes o no

Valor por omisión: yes

include or exclude from cache Especifica si incluir o no, o excluir o no el URL modificado en la antememoria.

Valores válidos: i o e

Valor por omisión: i

set default expiration time Especifica si se ha de establecer o no la hora de vencimiento por omisión.

Valores válidos: yes o no

Valor por omisión: yes

default expiration time Especifica la hora de vencimiento por omisión, en minutos. Un cero indica que no hay hora de vencimiento.

Valores válidos: de 1 a 10.080 minutos ó 0 para indicar que no hay hora de vencimiento.

Valor por omisión: 0

Acceso al entorno de supervisión de la antememoria del servidor Web

Para acceder al entorno de supervisión de la antememoria del servidor Web, escriba el mandato **f webc** en el indicador de configuración `t 5`.

```
t 5>f webc
```

Mandatos de supervisión de la antememoria del servidor Web

La Tabla 19 lista los mandatos de supervisión de la antememoria del servidor Web. Todos los mandatos funcionan en el sistema en ejecución y no modifican la base de datos de configuración. El mandato **activate** utiliza la información de la configuración.

Tabla 19. Resumen de los mandatos de supervisión de la antememoria del servidor Web

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 xxxii.
Activate	Activa o vuelve a activar las particiones de la antememoria utilizando la configuración más reciente.
Clear	Borrar una partición o las estadísticas de una partición.
Enable	Habilita una partición.
Delete	Suprime una partición, proxy o máscara de URL del sistema en ejecución.
Disable	Inhabilita una partición.
List	Lista la información del almacenamiento en antememoria.
Modify	Modifica la información del almacenamiento en antememoria.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiii.

Activate

Utilice el mandato **activate** para activar todas las particiones de las antememorias del servidor Web, o una partición o un proxy determinados.

Sintaxis:

ac**tivate** all
external
partition
proxy

all Activa o vuelve a activar todas las particiones definidas de la antememoria.

external Activa el Gestor de control de la antememoria externa.

partition Activa o vuelve a activar una partición de una antememoria.

proxy Activa o vuelve a activar un proxy de una antememoria.

Ejemplo: activate all

```
WEBC>act all
Cache partitions, must be disabled to reactivate them.
Do you wish to continue? [No]: y
WEBC>
```

Ejemplo: activate Proxy

```
WEBC>act pr

    1) Cluster address 113.3.1.10, Port 80, Cache partition 0
    2) Cluster address 113.3.1.10, Port 81, Cache partition 0
Enter proxy number:  1 ? 1
You are trying to activate an existing proxy.
Doing this will cause the proxy to be terminated before
being reactivated.
Do you wish to continue? [No]: yes
```

Clear

Utilice el mandato **clear** para borrar una partición o las estadísticas de una partición.

Nota: Al borrar los objetos de la partición, no se borran las estadísticas de la partición.

Sintaxis:

clear partition
statistics

partition Borra todos los objetos de la partición.

statistics Borra las estadísticas existentes de la partición.

Ejemplo:

```
WEBC>clear partition
Enter partition number: [0]?
Cache partition 0 must be disabled to clear its contents.
Do you wish to continue? [No]: yes
Do you wish to enable this partition? [Yes]: yes
```

partition number Especifica el número de partición que se va a borrar.

Valores válidos: cualquier número de partición válido

Valor por omisión: 0

Enable

Utilice el mandato **enable** para habilitar una partición del sistema en ejecución.

Sintaxis:

enable partition

Ejemplo:

```
WEBC>enable partition
Enter partition number: [0]?
```

partition number Número de la partición que se va a habilitar.

Valores válidos: cualquier número de partición válido

Valor por omisión: 0

Delete

Utilice el mandato **delete** para suprimir una partición del sistema en ejecución. Se suprimirán todos los proxies que utilicen la partición. No se realizará ningún cambio en la base de datos de configuración ni para los proxies ni para las particiones.

Sintaxis:

de**lete** partition

partition Suprime una partición de la antememoria.

Ejemplo:

```
WEBC>delete partition
Enter partition number: [0]? 0
WARNING: This will delete partition 0 and free all memory!
Do you wish to continue?  [No] : yes
WEBC>
```

partition number Especifica el número de la partición que se va a suprimir.

Valores válidos: cualquier número de partición válido

Valor por omisión: 0

Disable

Utilice el mandato **disable** para inhabilitar una partición en el sistema en ejecución.

Sintaxis:

d**isable** partition

partition Inhabilita una partición.

Ejemplo:

```
WEBC>disable partition
Enter partition number: [0]?
```

partition number Especifica el número de la partición que se va a inhabilitar.

Valores válidos: cualquier número de partición válido

Valor por omisión: 0

List

Utilice el mandato **list** para visualizar la información de todos los almacenamientos de Antememorias del servidor Web, de una partición, de una política o de un proxy.

Sintaxis:

l**ist** all
delete
depend
external
item
partition
policy
proxy

all Lista todas las particiones, políticas y proxies de una antememoria.

delete Lista los 100 últimos elementos suprimidos de la partición de la antememoria.

depend Lista la tabla de dependencias de la partición.

external Lista la información del Gestor de control de la antememoria externa.

item Lista los elementos y el contador de aciertos actuales de la partición de la antememoria.

partition Lista la información sobre una partición de la antememoria.

policy Lista la información sobre las políticas de la antememoria.

proxy Lista la información sobre un proxy de la antememoria.

Ejemplo:

```
WEBC>list all
Cache Partition 0        Status: Enabled
     Cluster address: 113.3.1.10  Port 80
1 partition(s) active.
External Cache Manager Port: 82
         Connection Timeout: 120 seconds
```

Ejemplo:

```
WEBC>list delete
Enter partition number: [0]? 0
Delete Table
URL String -- hit count
=======================
'/abc.html' -- 4
'/futbol.html' -- 2
'/tenis.html' -- 1
'/curling.html' -- 3
```

Ejemplo:

```
WEBC>list depend
Enter partition number: [0]?

Dependency table for Partition 0
------------------------------------
dep: tenis_info
   count of URLs: 2
   URLs:
         tenis_schedule.html
         tenis_roster.html
dep: futbol_info
   count of URLs: 2
   URLs:
         futbol_schedule.html
         futbol_roster.html
dep: roster
   count of URLs: 2
   URLs:
         futbol_roster.html
         tenis_roster.html
dep: schedule
   count of URLs: 2
   URLs:
         futbol_schedule.html
         tenis_schedule.html
```

Ejemplo:

```
WEBC>list item
Enter partition number: [0]? 0
Current number of items: 5
URL String -- hit count
======================
'/' -- 2
'/archiv5k.html' -- 1
'/archiv4k.html' -- 1
'/archiv2k.html' -- 3
'/archiv1k.html' -- 1
```

Ejemplo:

```
WEBC>li partition 0
Cache Partition 0        Status: Enabled
     Cluster address: 113.3.1.10, Port 80
     Cluster address: 113.3.1.10, Port 81
Partition size: Current - 0 bytes  Highest - 0 bytes  Maximum - Unlimited
Number of objects: Current - 0  Highest - 0  Maximum - Unlimited
Maximum object size: Unlimited
Cache purge interval: 10 minute(s)
Hit ratio: 0%
Total number of hits:  0
Cache Hit Bytes Served: 0
Breakdown of responses for the Cache Hits
 (note: this is based on whether the HTTP Proxy considered it a hit.
  So these counts may not add up to the hit count above)
   Response 200(OK):                0
   Response 203(Non-Authoriative):  0
   Response 206(Partial Content):   0
   Response 300(Multiple Choices):  0
   Response 301(Moved Permanently): 0
   Response 304(Not Modified):      0
   Response 410(Gone):              0
Total number of misses:  0
Cache Miss Bytes Served:  0
Breakdown of responses for the Cache Misses
 (note: this is based on whether the HTTP Proxy got the response
  back through it. In the case of multiple boxes working together
  as a big cache these counts will not add up to the total misses
  if a handoff was done)
   Response 100 Range(Information):         0
   Response 200(OK):                        0
   Response 200 Range(Successful-not 200):  0
   Response 304(Not Modified):              0
   Response 300 Range(Redirection-not 304): 0
   Response 400 Range(Client Error):        0
   Response 500 Range(Server Error):        0
   Response other (not in above):           0
Object Excluded (Object too large):        0
                (Object expired):          0
                (DONT CACHE header):       0
                (URL Mask excluded):       0
                (Image excluded):          0
                (Static object excluded):  0
                (Dynamic object excluded): 0
                (Cache disabled):          0
Total number of objects added via ECCM Interface: 0
Total number of objects not added via ECCM Interface but was attempted: 0
Total number of objects replaced via ECCM Interface: 0
```

Ejemplo:

```
WEBC>li pol
Enter partition number: [0]?
Transparent caching: Enabled
Cache Control Headers: Enabled
Cache images:                   Enabled
     Default lifetime: 0 minute(s)
Cache non-image static objects: Enabled
     Default lifetime: 0 minute(s)
Cache dynamic objects: Disabled
Dynamic URL mask: *dyn*
URL masks defined:
  1: EXCLUDE *index*
  2: EXCLUDE *comp*
  3: INCLUDE *tmp*
      Default expiration time: 1 minutes
  4: INCLUDE *stat*
      Default expiration time: 2 minutes
  5: INCLUDE *html*
      Default expiration time: 1000 minutes (16 hrs 40 mins)
```

Ejemplo: proxy que forma parte de un conjunto de antememorias SHAC (Scalable High Availability Cache).

```
WEBC>li pr
    WEBC>li pr
    1)   Cluster address 113.3.3.10, Port 80, Cache Partition 0
    2)   Cluster address 113.3.3.20, Port 80, Cache Partition 0
Enter proxy number: [1]? 1
Proxy 1: assigned to cache partition 0
Cluster address: 113.3.3.10     Port number: 80
Server Connection Timeout: 120 seconds
Client Connection Timeout: 120 seconds
Client connections: 0 current / 2 at highest point
Server connections: 0 current / 2 at highest point
Total cache hits: 0
Total cache misses: 649
Cache misses (object not in cache): 649
             (unsupported method):  0
             (can't send response): 0
             (non-cached request):  0
This Proxy is part of a cache group
  Source IP address for group is: 113.3.3.1
  There are currently 2 Cache(s) in this group
  Below are the Caches in the group:
  113.3.1.1
  113.3.6.1
```

Ejemplo: proxy que no forma parte de un conjunto de antememorias SHAC.

```
WEBC>li pr
    1)   Cluster address 113.3.1.10, Port 80, Cache Partition 0
    2)   Cluster address 113.3.1.10, Port 81, Cache Partition 0
Enter proxy number:  [1]?
Proxy 1: assigned to cache partition 0
Cluster address: 113.3.1.10     Port number: 80
Server Connection Timeout: 240 seconds
Client Connection Timeout: 240 seconds
Client connections: 0 current / 0 at highest point
Server connections: 0 current / 0 at highest point
Total cache hits: 0
Total cache misses: 0
Cache misses (object not in cache): 0
             (unsupported method):  0
             (can't send response): 0
             (non-cached request):  0
             (invalidation):        0
```

Modify

Utilice el mandato **modify** para modificar el Gestor de control de la antememoria externa.

Sintaxis:

m**odify** external

Ejemplo: modify external

```
WEBC Config>mod ext
External cache manager port number(0 to disable) [82]?
TCP connection timeout (Range 5-240) seconds) [120]? 20
Do you want to modify the encryption key:? [No]? Y
Encryption key should be 16 characters long.
Encryption key (16 characters) in Hex (0-9, a-f, A-F):
Encryption Key again (16 characters) in Hex (0-9, a-f, A-F):
```

external cache manager port number

TCP connection timeout

do you want to modify the encryption key

encryption key

Soporte de reconfiguración dinámica de la antememoria del servidor Web

En este apartado se describe la reconfiguración dinámica (DR) y cómo afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

La antememoria del servidor Web no da soporte al mandato **delete interface** de CONFIG (Talk 6).

Mandato activate interface de GWCON (Talk 5)

El mandato **activate interface** de GWCON (Talk 5) no es aplicable a la antememoria del servidor Web. La antememoria del servidor Web es una función, no una interfaz.

Mandato reset interface de GWCON (Talk 5)

El mandato **reset interface** de GWCON (Talk 5) no es aplicable a la antememoria del servidor Web. La antememoria del servidor Web es una función, no una interfaz.

Mandatos de restablecimiento de componente de GWCON (Talk 5)

La antememoria del servidor Web da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos de la antememoria del servidor Web:

Mandato GWCON, feature WEBC, activate all

Descripción: Este mandato leerá todas las memorias SRAM de la antememoria del servidor Web y hará que el entorno de ejecución actual sea el mismo.

Efecto en la red: Se interrumpirá la ejecución de todos los proxies que estén actualmente activos (es decir, se desactivarán todas las conexiones con los proxies). Si el gestor de control de antememoria externa estaba en funcionamiento, el 2212 dejará de estar a la escucha de conexiones nuevas en el puerto actual (o sea, no se desactivarán las conexiones del puerto actual).

Limitaciones:

La antememoria del servidor Web ya debe estar activada (véase el mandato **CONFIG, feature webc, activate**).

El mandato **GWCON, feature webc, activate all** da soporte a todos los mandatos de la antememoria del servidor Web.

Mandato GWCON, feature WEBC, activate partition

Descripción: Este mandato leerá todas las memorias SRAM de esta partición y hará que el entorno de ejecución actual de la partición sea el mismo.

Efecto en la red: Si la partición que se va a activar ya existe, se interrumpirá la ejecución de todos los proxies de esa partición (es decir, se desactivarán todas las conexiones con esos proxies).

Limitaciones:

- La antememoria del servidor Web ya debe estar activada (véase el mandato **CONFIG, feature webc, activate**).

En la tabla siguiente se resumen los cambios en la configuración de la antememoria del servidor Web que se activan al ejecutar el mandato **GWCON, feature webc, activate partition**:

Mandatos cuyos cambios se activan al ejecutar el mandato GWCON, feature webc, activate partition
CONFIG, feature webc, add urlmask
CONFIG, feature webc, delete partition
CONFIG, feature webc, delete urlmask
CONFIG, feature webc, modify partition
CONFIG, feature webc, modify proxy
CONFIG, feature webc, modify urlmask

Mandato GWCON, feature WEBC, activate proxy

Descripción: Este mandato leerá todas las memorias SRAM de este proxy y hará que el entorno de ejecución actual del proxy sea el mismo.

Efecto en la red: Si el proxy que se va a activar ya existe, se interrumpirá su ejecución (es decir, se desactivarán todas las conexiones con ese proxy).

Limitación:

La antememoria del servidor Web ya debe estar activada (véase el mandato **CONFIG, feature webc, activate**).

En la tabla siguiente se resumen los cambios en la configuración de la antememoria del servidor Web que se activan al ejecutar el mandato **GWCON, feature webc, activate proxy**:

Mandatos cuyos cambios se activan al ejecutar el mandato GWCON, feature webc, activate proxy
CONFIG, feature webc, modify proxy

Mandato GWCON, feature WEBC, activate external port

Descripción: Este mandato leerá todas las memorias SRAM del gestor de control de antememoria externa y hará que el entorno de ejecución actual del gestor de control de antememoria externa sea el mismo.

Efecto en la red: Si el gestor de control de antememoria externa estaba en funcionamiento, el 2212 dejará de estar a la escucha de conexiones nuevas en el puerto actual (o sea, no se desactivarán las conexiones del puerto actual).

Limitación:

La antememoria del servidor Web ya debe estar activada (véase el mandato **CONFIG, feature webc, activate**).

En la tabla siguiente se resumen los cambios en la configuración de la antememoria del servidor Web que se activan al ejecutar el mandato **GWCON, feature webc, activate external port**:

Mandatos cuyos cambios se activan al ejecutar el mandato GWCON, feature webc, activate external port
CONFIG, feature webc, modify external

Mandatos activate de CONFIG (Talk 6)

La antememoria del servidor Web da soporte a los siguientes mandatos **activate** de CONFIG (Talk 6):

Mandato CONFIG, feature WEBC, activate

Descripción: Cambia dinámicamente la antememoria del servidor Web actualmente en ejecución basándose en la memoria SRAM actual.

Efecto en la red: Se interrumpirá la ejecución de todos los proxies que estén actualmente activos (es decir, se desactivarán todas las conexiones con los proxies). Si el gestor de control de antememoria externa estaba en funcionamiento, el 2212 dejará de estar a la escucha de conexiones nuevas en el puerto actual (o sea, no se desactivarán las conexiones del puerto actual).

Limitaciones: Ninguna.

El mandato **CONFIG, feature webc, activate** da soporte a todos los mandatos de la antememoria del servidor Web.

Mandatos de cambio temporal de GWCON (Talk 5)

La antememoria del servidor Web da soporte a los siguientes mandatos de GWCON que cambian temporalmente el estado operativo del dispositivo. Estos cambios se perderán si el dispositivo se reinicia, si se vuelve a cargar, o si se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
GWCON, feature webc, modify external **Nota:** Este mandato cambiará el entorno de ejecución actual del gestor de control de antememoria externa. Si el gestor de control de antememoria externa estaba en funcionamiento, el 2212 dejará de estar a la escucha de conexiones nuevas en el puerto actual (o sea, no se desactivarán las conexiones del puerto actual).
GWCON, feature webc, delete partition **Nota:** Este mandato suprimirá la partición del entorno de ejecución actual.

Configuración y supervisión del subsistema de codificación

Las funciones de compresión de y de cifrado de datos se agrupan en el Subsistema de codificación (ES, Encoding Subsystem). El Subsistema de codificación permite que las interfaces o protocolos accedan a los dispositivos de codificación y se activa automáticamente al activar un enlace de compresión o cifrado. En la plataforma 2212, los dispositivos de codificación son el Adaptador de compresión y cifrado (CEA, Compression/Encryption Adapter) y el dispositivo software. El dispositivo software consiste en un software operativo que realiza la compresión y el cifrado. Cuando se utiliza el dispositivo software, los algoritmos de compresión y cifrado se ejecutan en el procesador del direccionador. No es necesario cambiar la configuración por omisión para utilizar el CEA o el dispositivo software.

Puede supervisarse la actividad del ES escribiendo **feature es** desde el indicador de supervisión (Talk 5).

Los parámetros de configuración del ES permiten limitar la cantidad de memoria que utilizará el dispositivo software del ES. La configuración por omisión permite que el ES disponga de tanta memoria como necesite. Para limitar el uso de la memoria, ejecute el mandato **set**, después de **feature es**, en el proceso de configuración (Talk 6).

Este capítulo consta de los apartados siguientes:

Configuración del subsistema de codificación

Los parámetros de configuración del ES permiten controlar el número de sesiones de compresión y cifrado que podrá manejar simultáneamente el dispositivo software de codificación. El dispositivo software de codificación consiste esencialmente en una colección de bibliotecas de compresión y cifrado que se ejecutan en el procesador del direccionador. Una sesión consiste en una conexión dúplex a través de una interfaz determinada configurada para que utilice las funciones de compresión o de cifrado.

Nota: Los parámetros de configuración del ES influyen solamente sobre el dispositivo software de codificación, no sobre el CEA.

En general, la codificación de datos es una operación que consume muchos recursos del procesador. Al limitar el número de sesiones de codificación, se puede controlar hasta cierto punto el impacto de la codificación de datos en el rendimiento del direccionador. Por ejemplo, si el direccionador tiene 20 interfaces de marcación configuradas para que utilicen la función de compresión y se ha determinado que comprimir con más de 10 interfaces a la vez produce un efecto negativo en el rendimiento del direccionador, debe establecerse que el número máximo de sesiones de compresión es de 10. Esto permite que 10 de las 20 interfaces utilicen la función de compresión.

Las necesidades de memoria del dispositivo software de codificación también son una razón para limitar el número de sesiones. Cada sesión de compresión utiliza aproximadamente 30 KB de la memoria del direccionador y una sesión de cifrado utiliza aproximadamente 2 KB. Si el ES utiliza demasiada memoria, otras funciones podrán sufrir restricciones de memoria¡a y el rendimiento del direccionador se verá afectado negativamente. Consulte el apartado “Consideraciones” en la página 262 para obtener más información.

Se puede establecer el número mínimo o máximo de sesiones del ES haciendo constar el número de sesiones o especificando un número o uno de los valores *unlimited (ilimitado)*, *default (por omisión)*. Los valores *unlimited* y *default* tienen el mismo significado: ambos permiten que el direccionador dé soporte a todas las sesiones que se activen para cifrado o compresión, mientras no se agote la memoria.

Nota: Ninguno de los parámetros de configuración del ES (Talk 6) pueden reconfigurarse dinámicamente. Para activar los valores de los parámetros después de cambiarlos, deberá reiniciar o volver a cargar el direccionador.

En el proceso de configuración (Talk 6), escriba **feature es** en el indicador `Config>` para acceder a los mandatos de configuración del ES. Aparecerá el indicador `ES Config>`. En la Tabla 20 se listan los mandatos.

Tabla 20. 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 xxxii.
List	Muestra la configuración 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 xxxiii.

List

Utilice el mandato **list** para visualizar la configuración 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 y compresión de datos.

Sintaxis:

s**et** 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 de software.

software minimum compression-sessions *n, unlimited o default*
Establece el número mínimo de sesiones de compresión disponibles para las interfaces. El direccionador reserva este número de sesiones de forma que siempre estarán disponibles.

Valor por omisión: 0

Valores válidos: de 0 a *unlimited*; alternativamente, *default*

software maximum compression-sessions *n, unlimited o default*
Establece el número máximo de sesiones de compresión disponibles para las interfaces. Una vez se activa este número, no se podrán activar más sesiones.

Valor por omisión: 0

Valores válidos: de 0 a *unlimited*; alternativamente, *default*

software minimum encryption-sessions *n, unlimited o default*
Establece el número mínimo de sesiones de cifrado disponibles para las interfaces. El direccionador reserva este número de sesiones de forma que siempre estarán disponibles.

Valor por omisión: 0

Valores válidos: de 0 a *unlimited*; alternativamente, *default*

software maximum encryption-sessions *n, unlimited o default*
Establece el número máximo de sesiones de cifrado disponibles para las interfaces. Una vez se activa este número, no se podrán activar más sesiones.

Valor por omisión: 0

Valores válidos: de 0 a *unlimited*; alternativamente, *default*

Supervisión del subsistema de codificación

En el proceso de supervisión, escriba **feature es** en el indicador `+` para acceder a los mandatos de supervisión del ES. Aparecerá el indicador `ES Monitor>`. En la Tabla 21 en la página 254 se listan los mandatos disponibles.

Tabla 21. 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 xxxii.
List	Muestra información detallada sobre los puertos, los circuitos, los dispositivos, la configuración y el estado del ES, o muestra un resumen.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiii.

List

Utilice el mandato **list** para mostrar información sobre el ES. En el apartado en el que se describe el mandato **list summary**, se da un ejemplo de la salida del mandato **list**, en que aparece información sobre los puertos, los dispositivos y el estado del ES.

Sintaxis:

list ports
circuits
devices
config
status
summary

ports El mandato **list ports** lista los puertos de codificación creados por los 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 las funciones de compresión o cifrado están configuradas a través de la interfaz Net 1 PPP, se asociará un puerto con dicha interfaz. El campo QLen muestra la suma de todas las peticiones de compresión o de cifrado pendientes para todos los circuitos asociados con el puerto. Un cliente, como por ejemplo el protocolo PPP configurado para una interfaz determinada, presenta una petición al ES cuando asigna para codificación un almacenamiento intermedio de datos concreto.

El campo Status muestra *Idle (Desocupado)* si no hay ningún petición en la cola del puerto o *Busy (Ocupado)* o *Waiting (En espera)*, si las peticiones se están procesando o están en la cola del puerto.

circuits El mandato **list circuits** muestra los circuitos definidos por los clientes del sistema de codificación. Cada circuito corresponde a una conexión dúplex. Los datos cifrados o comprimidos en un extremo se descifran o descomprimen en el otro.

Por omisión, sólo se mostrarán los circuitos activos. Utilice el mandato **list circuits all** para incluir los circuitos activos e inactivos.

Para cada circuito encontrado, se mostrarán el puerto y el usuario, igual que en el mandato **list ports**. Además, se mostrarán dos líneas de información; una línea Tx para el circuito de salida y una línea Rx para el circuito de entrada. El identificador del circuito es un número arbitrario

suministrado por el cliente, para que pueda identificar todos los circuitos que cree. Para los circuitos Frame Relay, este número corresponde al identificador del circuito Frame Relay de enlace de datos (DLCI) asociado. Los enlaces Punto a punto sólo crean un circuito, identificado siempre por el número *1*.

Además, también se muestran los siguientes elementos:

Dev Número que representa el dispositivo de codificación que atiende esa corriente. Es 1 cuando la codificación la realiza el software utilizando la CPU y 2 cuando la codificación la realiza el adaptador de compresión y cifrado.

Cmpr Campo que muestra el algoritmo de compresión o descompresión que está activo para esta corriente. Si es *LZC*, significa que se está utilizando el método de compresión STAC-LZC; si es *MPPC*, se está utilizando el método PPC, de Microsoft®. Se añadirá un asterisco (*) al nombre del algoritmo, si la corriente opera en modalidad sin información de estado. La modalidad sin información de estado es una modalidad en la que no se mantiene la historia de los paquetes de datos después de procesarlos, al contrario de lo que ocurre en la modalidad continua, en la que se mantiene la historia de cada paquete que se ha manejado para poder manejar el siguiente. Por ejemplo, en la modalidad de compresión continua, el codificador mantiene almacenada en una antememoria información sobre los paquetes anteriores, con el fin de poder comprimir los paquetes actuales.

Encr Campo que muestra el algoritmo de cifrado o descifrado que se está utilizando. Es *DES* para el algoritmo DES estándar, *3DES* para el algoritmo Triple DES o *RC4* si se utiliza el algoritmo RC4, de RSA'. Se añadirá un asterisco (*) al nombre del algoritmo, si la corriente esta funcionando en modalidad sin información de estado. Esto tiene importancia en el algoritmo RC4, pero apenas significa nada para los algoritmos DES/3DES. Obsérvese que el nombre que aparece corresponde al algoritmo de cifrado básico utilizado, no al formato de encapsulado utilizado por el cliente. Por ejemplo, el protocolo PPP da soporte a dos métodos de encapsulado: DESE (RFC 1969) que utiliza el algoritmo de cifrado DES, y MPPE (método no estándar de Microsoft), que utiliza el RC4.

QLen Este parámetro muestra el número de paquetes de salida que esperan en la cola de la corriente a ser codificados o decodificados. Obsérvese que este número sólo muestra los paquetes que realmente se han enviado al ES para ser procesados. Algunos clientes pueden poseer sus propias colas y, desde ellas, enviar al sistema de codificación sólo unos pocos paquetes cada vez.

Status Una rápida ojeada al estado de las corrientes. No es extraño ver que todas las corrientes estén en espera y que ninguna esté ocupada. Ver alguna corriente en estado ocupado significaría haber atrapado la actividad de la cola durante una

ventana de tiempo muy pequeña del ciclo de proceso. Los estados posibles son:

Idle No hay paquetes en la cola de esta corriente

Busy En este momento, el sistema está procesando paquetes de esta corriente (lo que quiere decir que el elemento en cabeza de la cola está siendo procesado por el motor de codificación en este momento).

Waiting Las peticiones están pendientes, pero actualmente no se está procesando ninguna de esa corriente.

devices El mandato **list devices** lista los dispositivos de codificación que el sistema tiene disponibles. Un dispositivo de codificación generalmente se refiere a un adaptador de compresión y cifrado. El software que se utiliza cuando no se dispone de un acelerador hardware, está implementado como dispositivo virtual y también aparecerá en está lista como dispositivo *Host Software (Software del sistema principal)*. Este mandato tiene dos formas: **list devices** y **list device n**. La primera genera un listado que es un resumen breve de todos los dispositivos reconocidos por el sistema. La segunda genera un listado detallado de un determinado dispositivo n, donde n es el número de la unidad. La unidad 1 representa el software del sistema principal, que es un dispositivo de codificación virtual, y la unidad 2 representa el adaptador de compresión y cifrado. Puede utilizarse un asterisco (*) en lugar del número n, en cuyo caso, se generará un listado para ambas unidades.

config El mandato **list config** muestra los parámetros actuales de configuración. Estos son los parámetros que se leen de la memoria no volátil cuando el direccionador se reinicia o se vuelve a cargar. La información que se muestra es idéntica a la que se muestra por el mandato de configuración (Talk 6) **list config**.

status El mandato **list status** muestra el estado del sistema de codificación, y consiste en varios distintivos globales de estado y en varias estadísticas sobre el sistema. Estas son las descripciones de los campos que se muestran con el mandato **list status**:

Last Error
Último código de error devuelto a los clientes del sistema de codificación. Sirve con propósitos de depuración y debe utilizarse solamente por personal del servicio técnico.

Internal Condition flags
Este campo muestra determinadas condiciones internas, definidas en la lista siguiente:

Ready El sistema está en funcionamiento y es operativo. Esta es la condición normal.

Not Working
El sistema de codificación no está operativo a causa de un error interno.

No Devices Available
Indica que no hay dispositivos disponibles para realizar la codificación. Esta condición no debería

producirse, ya que si no existe un codificador hardware, la codificación la llevará a cabo software interno.

Out of Memory
El sistema ha intentado asignar memoria y no ha podido. Esta condición indica que el direccionador se está quedando sin memoria RAM y que el sistema de codificación se está viendo afectado negativamente.

Number of Ports
Campo que indica el número de clientes que ha establecido por su cuenta algún puerto en el ES. En el mandato **list ports** se ofrece la definición de puerto.

Number of Circuits
En el mandato **list circuits** se ofrece una definición de circuito.

Global Request pool size
Número de almacenamientos intermedios de peticiones asignados y libres. Se utiliza aproximadamente un almacenamiento intermedio de peticiones por cada paquete codificado. Si el número de almacenamientos intermedios libres es menor que el número de asignados, significa que el proceso de codificación está en marcha.

Total # of Requests processed
Valor que muestra el número total de almacenamientos intermedios procesados por el motor de codificación. Este número se corresponde aproximadamente con el número total de paquetes comprimidos o cifrados por todos los clientes del sistema desde la última vez que se reinició o se volvió a cargar el direccionador.

summary Este mandato muestra 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
------ --------------------------  ---------  ----------
     2 Hardware Accelerator/0        2/1     Ready
     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 codificación

En este apartado se describe la reconfiguración dinámica (DR) y cómo afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

El subsistema de codificación no da soporte al mandato **delete interface** de CONFIG (Talk 6).

Mandato activate interface de GWCON (Talk 5)

El mandato **activate interface** de GWCON (Talk 5) no es aplicable al subsistema de codificación. Los parámetros de configuración del ES determinan la cantidad de memoria que se le asignará al ES durante el arranque y no no está asociado con ninguna interfaz.

Mandato reset interface de GWCON (Talk 5)

El mandato **reset interface** de GWCON (Talk 5) no es aplicable al subsistema de codificación. Los parámetros de configuración del ES determinan la cantidad de memoria que se le asignará al ES durante el arranque y no no está asociado con ninguna interfaz.

Mandatos no reconfigurables dinámicamente

Los subsistemas de codificación no permiten cambiar dinámicamente ninguno de sus parámetros de configuración.

Configuración y supervisión de la compresión de datos

En este capítulo se trata de la compresión de datos en un 2212 sobre las interfaces Frame Relay y PPP. Consta de los apartados siguientes:

La compresión de datos está soportada para las 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 efectivo de las interfaces de red del dispositivo. Está pensado para utilizarlo principalmente en enlaces WAN de baja velocidad.

La compresión de datos en el dispositivo está soportada para las interfaces PPP y Frame Relay.

- Para interfaces PPP, la compresión está implementada según el Protocolo de control de compresión (CCP), definido en el documento RFC 1962 del Comité de Ingeniería de Internet. El CCP proporciona los mecanismos básicos utilizados para la negociación del uso de la compresión y un medio para elegir entre varios protocolos de compresión.

  El dispositivo ofrece dos protocolos de compresión: el protocolo Stac-LZS, definido en el documento RFC 1974; y el protocolo de compresión punto a punto de Microsoft (MPPC, Microsoft Point-to-Point Compression), descrito la RFC 2118. Ambos están basados en algoritmos de compresión de Stac Electronics.
- Para interfaces Frame Relay, la compresión está implementada según el FRF.9, el *Acuerdo de implementación de compresión de datos a través de Frame Relay* desarrollado por el Comité técnico del foro de debate sobre Frame Relay. El FRF.9 describe un Protocolo de compresión de datos (DCP), modelado a partir del CCP de la interfaz PPP y, de forma similar, proporciona un medio para negociar varios algoritmos y opciones de compresión. El dispositivo soporta la "modalidad 1" de negociación del DCP. El FRF.9 también describe una "modalidad 2" más general, pero no está soportada. La propia compresión se realiza mediante el mismo motor de compresión que se utiliza para el protocolo Stac-LZS de la interfaz PPP.

Conceptos de la compresión de datos

La compresión de datos en el dispositivo proporciona un medio de aumentar el rendimiento de los enlaces de una red, al hacer un uso más eficiente del ancho de banda disponible para un enlace. El principio básico subyacente es sencillo: representar el flujo de datos que pasa por un enlace de la forma más compacta que sea posible, de manera que el tiempo necesario para transmitirlo sea el menor posible, dada una velocidad establecida para el enlace.

La compresión de datos puede realizarse en varias capas del modelo de red. En un extremo, las aplicaciones pueden comprimir los datos antes de transmitirlos a sus iguales en cualquier lugar de la red, mientras que en el otro extremo, los dispositivos pueden realizar la compresión en la capa de enlace de datos, trabajando únicamente con la corriente de bits que pasa entre dos nodos. La forma en que se realiza la compresión y su eficacia depende de muchos factores, como por ejemplo en qué capa de red se realiza la compresión, cuál es el conocimiento intrínseco que tienen el compresor y el descompresor de los datos que van a comprimirse, el algoritmo de compresión que se ha escogido o el tipo de datos a comprimir. Normalmente, la mejor compresión la consigue la capa de aplicación; por ejemplo, una aplicación de transmisión de archivos puede permitirse el lujo de disponer de todo el archivo de datos antes de realizar la compresión, y puede poder probar varios algoritmos de compresión para ver con cuál se logra una mejor compresión de los datos de ese archivo en particular. Aunque así se puede conseguir una compresión excelente para este tipo de aplicación, no se resuelve el problema de comprimir el flujo de tráfico general que circula por una red, puesto que la mayoría de aplicaciones de red no comprimen los datos que generan.

La compresión en el dispositivo tiene lugar en una capa de red mucho más baja, como es la capa de enlace de datos. En el dispositivo, la compresión se efectúa sobre los paquetes individuales que se transmiten por un enlace. La compresión se realiza en tiempo real, a medida que los paquetes se envían a través del dispositivo: el remitente comprime un paquete justo antes de enviarlo y el descompresor lo descomprime tan pronto como lo recibe. Esta operación es transparente para los protocolos de red de las capas superiores.

Nociones básicas sobre compresión de datos

Un compresor de datos reconoce la información “redundante” en los datos y genera un conjunto de datos distinto que contiene la menor redundancia posible. La información “redundante” es aquella información que puede derivarse y volver a crearse a partir de los datos actualmente disponibles. Por ejemplo, el funcionamiento de un compresor puede consistir en reconocer patrones de caracteres repetidos en una corriente de datos, y sustituirlos por una secuencia de código más corta que represente a ese patrón. Si el compresor y el descompresor se ponen de acuerdo en cuáles son esas secuencias de código, entonces el descompresor siempre podrá volver a crear los datos originales a partir de los datos comprimidos.

A esta correlación entre las secuencias de datos originales y las secuencias correspondientes a la salida comprimida se la conoce normalmente como ***diccionario de datos***. Estos diccionarios pueden definirse estáticamente (información disponible por el compresor y por el descompresor, basada en la experiencia) o pueden generarse dinámicamente, basándose generalmente en la información que se va a comprimir. Los diccionarios estáticos pueden aplicarse en la mayoría de entornos en los que la naturaleza de los datos a procesar es limitada, conocida, y no son muy efectivos si se usan con compresores de uso general. La mayoría de sistemas de compresión utilizan diccionarios dinámicos, incluidos los diccionarios utilizados en el dispositivo. En un 2212, los diccionarios de datos se basan en el paquete que se procesa actualmente y en los posibles paquetes vistos antes, pero no se puede “ver por anticipado” en la corriente de datos, como sucede cuando la compresión se realiza en otras capas. En los sistemas en que el diccionario de datos se crea dinámicamente y está basado solamente en los datos vistos antes, al diccionario normalmente se le conoce como ***historia***. Los términos historia y dic-

cionario de datos se utilizarán indistintamente en el resto del capítulo, aunque debe entenderse que en otros entornos una historia es una forma específica de diccionario de datos.

El hecho de que el dispositivo utilice diccionarios dinámicos y de que el compresor y el descompresor deban mantener sincronizados sus diccionarios, significa que la compresión de datos se realiza en una corriente de datos que pasa entre dos extremos. De ahí que la compresión en el direccionador sea un proceso orientado a la conexión, donde los extremos de la conexión son, a su vez, el compresor y el descompresor. Cuando se arranca el proceso de compresión en la corriente, ambos extremos restablecen sus diccionarios de datos a un estado inicial conocido y, después, van actualizando dicho estado a medida que se reciben datos.

La compresión puede efectuarse para cada paquete individual, con lo que las historias se restablecerán antes de procesar cada paquete. Sin embargo, lo normal es que los diccionarios de datos no se restablezcan entre paquetes, lo que quiere decir que las historias se basan no sólo en el contenido del paquete actual, sino también en el contenido de los paquetes vistos antes. Esto suele mejorar la eficacia global de la compresión, puesto que aumenta la cantidad de datos que utiliza el compresor para buscar redundancias a eliminar. Un ejemplo sería el caso de un sistema principal que está “haciendo ping” a otro sistema principal con IP: se envía una serie de paquetes y, generalmente, cada paquete nuevo es casi idéntico al anterior. El compresor puede tener pocas posibilidades a la hora de comprimir el primer paquete, pero reconocerá que cada uno de los paquetes siguientes son muy parecidos al último que se ha enviado y creará versiones muy comprimidas de dichos paquetes.

Puesto que las historias del compresor y del descompresor varían con cada paquete recibido, los mecanismos de descompresión son sensibles a los paquetes perdidos, corrompidos o reordenados. Los protocolos de compresión empleados por el dispositivo incluyen mecanismos de señalización de forma que el compresor y el descompresor puedan detectar una pérdida de sincronización y se vuelvan a sincronizar entre ellos, lo que puede ser necesario si un paquete se pierde debido a un error de transmisión. Generalmente, esto se consigue incluyendo un número de secuencia en cada paquete, que el descompresor comprobará para asegurarse de que está recibiendo todos los paquetes y de que los está recibiendo en orden. Si detecta un error, él mismo se restablecerá a un estado inicial conocido, enviará un señal al compresor para que haga lo mismo y, a continuación, esperará (descartando todos los paquetes que lleguen comprimidos) hasta que el compresor le envíe un acuse de recibo conforme él también se ha restablecido.

La compresión en un enlace suele realizarse con datos que se transmiten en ambos sentidos del enlace. Normalmente, en cada extremo de la conexión funciona tanto un compresor como un descompresor, que se comunican con sus análogos del otro extremo de la conexión, como se muestra en la Figura 21 en la página 262. La salida (compresión) se ejecuta independientemente de la entrada (descompresión). Es posible que se utilicen algoritmos de compresión totalmente diferentes en cada sentido del enlace. Al establecer la conexión de un enlace, el protocolo de control de compresión del enlace negociará con su igual para determinar los algoritmos de compresión que se utilizarán para la conexión. Si los dos extremos no pueden ponerse de acuerdo sobre los protocolos de compresión a utilizar, no se realizará ninguna clase de compresión y el enlace funcionará normalmente (los paquetes se enviarán sin comprimir).

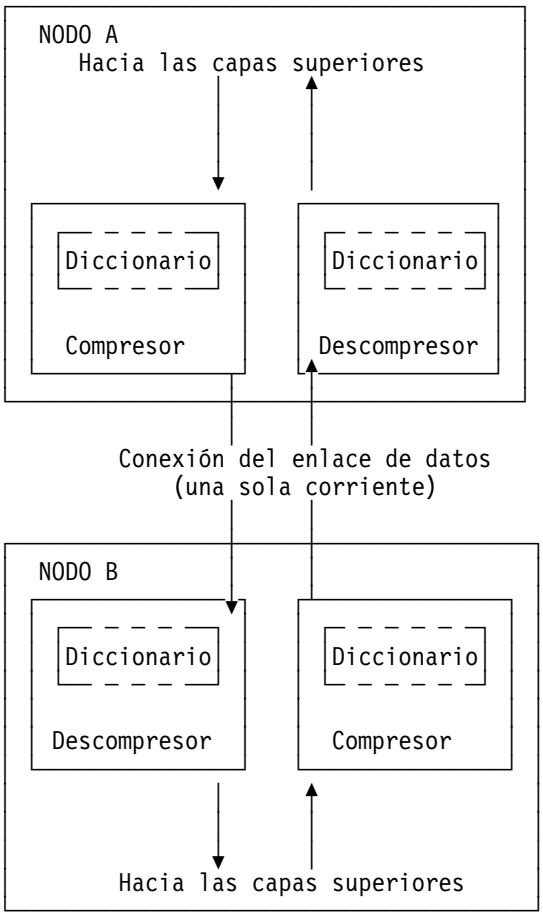


Figura 21. Ejemplo de compresión de datos bidireccional con diccionarios de datos

En realidad, una corriente representa una conexión entre un proceso de compresión específico en un extremo del enlace y un proceso de descompresión asociado en el otro extremo del enlace, lo que es más preciso que decir que es simplemente una “conexión” entre dos nodos; es posible que un protocolo de compresión sofisticado pueda dividir el flujo de datos entre dos sistemas principales en varias corrientes, comprimiendo cada una de forma independiente. Por ejemplo, el CCP de la interfaz PPP es capaz de negociar la utilización de varias historias a través de un solo enlace PPP, aunque el direccionador no dé soporte a esto.

Consideraciones

Tomar la decisión de utilizar o no utilizar compresión de datos no siempre es fácil. Hay varios factores que deben tenerse en cuenta antes de habilitar la compresión en una conexión.

Carga de la CPU

La compresión de datos es un procedimiento que requiere muchos cálculos. A medida que la cantidad de datos procesados aumenta (por unidad de tiempo), más carga de trabajo recae sobre el procesador del dispositivo. Si la carga se vuelve demasiado grande, el rendimiento del dispositivo se degradará (para todas las interfaces de red, no sólo para las que estén utilizando compresión).

En realidad, el dispositivo contiene varios procesadores y utiliza multiproceso asimétrico (por ejemplo, los controladores de E/S del enlace trabajan conjuntamente

con el procesador principal), de forma que el efecto de la carga del procesador no siempre podrá medirse inmediatamente. Puesto que la operación de compresión puede solaparse con la transmisión de los paquetes, la carga puede, de hecho, ser totalmente transparente y no plantear ningún problema. No obstante, es posible que el procesador del dispositivo se sobrecargue y que se degrade el rendimiento.

Como norma general, la compresión sólo debe habilitarse en enlaces WAN de baja velocidad (probablemente sólo en enlaces de hasta 64 kbps, la velocidad típica de un enlace de marcación RDSI). El ancho de banda total para los datos comprimidos en todos los enlaces probablemente deberá limitarse a unos pocos cientos de kbps. No es una buena idea ejecutar la compresión en todos los canales de un adaptador de acceso primario RDSI.

Los parámetros del subsistema de codificación permiten limitar el número de conexiones que ejecutarán concurrentemente la compresión. Pueden habilitarse más interfaces para compresión que las que se están ejecutando realmente. Cuando se alcanza el número máximo de conexiones activas que utilizan compresión, las conexiones adicionales sencillamente no negociarán el uso de la compresión, al menos hasta que no concluya un enlace que ya esté utilizando compresión.

Ocupación de la memoria

Otra cuestión a tener en cuenta cuando se configura la compresión son las necesidades de memoria. Las historias de compresión y descompresión ocupan una cantidad de memoria importante, que es un recurso limitado del dispositivo. El algoritmo Stac-LZS, por ejemplo, necesita unos 16 KB para una historia de compresión y unos 8 KB para una historia de descompresión. Este problema aumenta ya que deben existir historias para cada conexión que se establezca: una historia de compresión se sincroniza con su historia de descompresión correspondiente en un direccionador igual. Para un enlace PPP, esto implica una historia de compresión y una historia de descompresión (suponiendo que la compresión de datos se ejecute bidireccionalmente en el enlace). Para un enlace Frame Relay, pueden existir tantas historias como se necesiten, un par para cada conexión virtual (DLCI) que se establezca.

Al arrancar, el dispositivo crea una agrupación de historias de compresión y descompresión. Siempre se asignan a pares y se conocen como ***sesiones de compresión*** (una sesión es simplemente una historia de compresión emparejada con una historia de descompresión). Técnicamente, la compresión y la descompresión son funciones independientes, pero en la práctica, la compresión casi siempre se ejecuta bidireccionalmente, así que, para simplificar el funcionamiento, la memoria se gestiona y se configura en términos de sesiones más que de historias individuales. Puesto que cada algoritmo de compresión tiene necesidades de memoria distintas, tanto para la compresión como para la descompresión, para poder manejar el caso peor se asigna un tamaño de sesión de aproximadamente 30 KB. La agrupación de sesiones de compresión se llena según las opciones configuradas en el subsistema de codificación. Consulte el “Configuración y supervisión del subsistema de codificación” en la página 251 para obtener más detalles.

Cuando el dispositivo intente establecer una conexión de compresión en un enlace, empezará por reservar una sesión de la agrupación de sesiones asignadas. Si no hay sesiones disponibles, la compresión no se efectuará en esta conexión. El

direccionador intentará iniciar la compresión en esta conexión más adelante, cuando haya sesiones disponibles.

El número de sesiones de compresión asignadas es un parámetro configurable. Al establecer el número de sesiones asignadas, se limita la cantidad de memoria utilizada y el número máximo de conexiones que pueden funcionar simultáneamente con compresión. Limitar el número de conexiones que pueden funcionar simultáneamente con compresión permite controlar el problema de la carga de la CPU.

Contenido de los datos

Debe tenerse en cuenta la naturaleza real de los datos que se van a transmitir antes de habilitar la compresión para esa conexión. La compresión funciona mejor con ciertos tipos de datos que en otros. Los paquetes que contienen mucha información casi idéntica (por ejemplo, el conjunto de paquetes generados por un mandato “ping” de IP) normalmente se pueden comprimir muy bien. Una colección aleatoria típica de texto y datos binarios que se transmita por un enlace se suele poder comprimir en una proporción que va de 1,5:1 a 3:1. Algunos datos sencillamente no pueden comprimirse. En particular, los datos que ya se han comprimido, raramente podrán comprimirse más. De hecho, los datos que ya se han comprimido antes, puede que se expandan al enviarlos al motor de compresión.

Si se sabe por adelantado que la mayor parte del flujo de datos que pasará por una conexión consistirá en datos comprimidos, se recomienda no habilitar la compresión para esta conexión. Un ejemplo de esto es una conexión con un sistema principal que esté configurado fundamentalmente como sede de archivos FTP, donde todos los archivos disponibles para ser transmitidos están almacenados en el sistema principal en algún formato comprimido.

Compresión en la capa de enlace

Un último factor a tener en cuenta es la naturaleza del enlace de red entre los dos sistemas principales. La compresión puede realizarse en una capa incluso más baja que la de las interfaces hardware del dispositivo. En concreto, el hardware y el firmware de muchos módems modernos incorporan mecanismos de compresión de datos. Si la compresión se va a realizar en el enlace, en la capa más baja (fuera del dispositivo), lo mejor será no habilitar la compresión de datos en el dispositivo para esta interfaz. Como ya se ha mencionado, comprimir una corriente de datos ya comprimidos no suele ser efectivo y, de hecho, puede degradar ligeramente el rendimiento. A menos que haya una razón concreta para creer que el direccionador hará un mejor trabajo de compresión que el hardware del enlace, lo mejor es dejar que sea éste último el que realice la compresión.

Configuración y supervisión de la compresión de datos para enlaces PPP

El 2212 utiliza el protocolo de control de compresión (CCP) para PPP para negociar la utilización de la compresión en un enlace. El CCP proporciona un mecanismo general para negociar la utilización de un protocolo de compresión determinado, incluso, posiblemente, la utilización de protocolos distintos en cada sentido del enlace y varias opciones específicas del protocolo. El software soporta los protocolos Stac-LZS y MPPC, de forma que el igual también debe dar soporte al menos a uno de estos algoritmos para que la negociación sobre la compresión de datos entre los dos nodos sea satisfactoria. Los dos nodos también deben

ponerse de acuerdo sobre las opciones específicas del algoritmo para que funcione la compresión.

Configuración de la compresión de datos para enlaces PPP

Para configurar la compresión de datos para enlaces PPP:

1. Habilite el protocolo CCP para el enlace con el mandato **enable ccp**. Esto permite que el enlace negocie qué tipo de compresión utilizar con el otro nodo. En la negociación se acuerda el algoritmo de compresión que se utilizará, así como las opciones específicas del protocolo.
2. Seleccione los algoritmos de compresión que pueden negociarse, utilizando el mandato **set ccp algorithms**.
3. Establezca los parámetros negociables para cada algoritmo de compresión, utilizando el mandato **set ccp options**.

Se puede visualizar la configuración actual de compresión con el mandato **list ccp**.

En la Tabla 22 se listan los mandatos disponibles y la Figura 22 en la página 266 es un ejemplo de cómo configurar la compresión para un enlace PPP. Para obtener descripciones detalladas de estos mandatos, consulte el apartado 'Mandatos de configuración punto a punto', de la publicación *Access Integration Services Guía del usuario de software*.

Tabla 22. Mandatos de configuración de la compresión de datos para 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 del algoritmo de compresión.
set ccp algorithms	Especifica una lista de algoritmos de compresión, ordenados por prioridad.
list ccp	Muestra 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 22. Ejemplo de configuración de la compresión para un enlace PPP

Notas:

1. El mandato de red selecciona la interfaz de red para el enlace PPP. Si el enlace es un circuito de marcación PPP, deberá utilizar el mandato **encapsulator** para acceder al menú de configuración PPP.
2. Si se habilita CCP y no establece ningún algoritmo para el enlace, el software configurará automáticamente el enlace para que utilice los protocolos STAC y MPPC, como si se hubiera entrado el mandato **set ccp algorithms stac mppc**.

   Si se establecen varios algoritmos, el orden de los algoritmos determinará su preferencia a la hora de negociar con ellos para el enlace.

   Si ejecuta el mandato **set ccp algorithms none**, el software inhabilitará automáticamente la compresión para el enlace.

   Si MPPE y CCP están habilitados, el algoritmo de compresión es MPPC.

Supervisión de la compresión de datos para enlaces PPP

La compresión se supervisa de la misma forma que los otros componentes PPP. En el apartado ‘Acceso a la interfaz del proceso de supervisión’, de la publicación *Access Integration Services Guía del usuario de software*, se describe cómo acceder al entorno de la consola PPP y se describen detalladamente los mandatos. En la Tabla 23 en la página 267 se listan los mandatos relativos a la compresión. En la Figura 23 en la página 267 se muestra un ejemplo de listado con información sobre la compresión para una interfaz PPP.

Tabla 23. Mandatos de supervisión de la compresión de datos para PPP	
Mandato	**Función**
list control ccp	Lista el estado del CCP y de las opciones negociadas.
list ccp	Lista las estadísticas de los paquetes del CCP.
list cdp o **list compression**	Lista las estadísticas de los datagramas comprimidos.

```
+ 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 23. Supervisión de la compresión para una interfaz PPP

Configuración y supervisión de la compresión de datos para enlaces Frame Relay

Después de configurar los parámetros de compresión globales y de habilitar la compresión para la interfaz, deberá establecer los parámetros para cada uno de los circuitos (PVC) de la interfaz Frame Relay. Cada circuito definido para la interfaz puede tener habilitada la compresión y cada circuito que negocie satisfactoriamente la utilización de la compresión utilizará una sesión de compresión de la agrupación global. También puede inhabilitar la compresión para la interfaz, lo que quiere decir que ningún circuito de la interfaz será elegible para transportar tráfico de datos comprimidos.

Configuración de la compresión de datos para enlaces Frame Relay

Para configurar la compresión de datos para enlaces FR:

1. Habilite la compresión para la interfaz ejecutando el mandato **enable compression**. Esto habilita el enlace para que negocie la compresión con el otro nodo.
2. Habilite la compresión para cada nuevo PVC que vaya a transportar datos comprimidos con el mandato **add permanent-virtual-circuit**. Se pueden cambiar los circuitos PVC existentes utilizando el mandato **change permanent-virtual-circuit**.

Se puede visualizar la configuración actual de compresión ejecutando los mandatos **list lmi** o **list permanent-virtual-circuit**.

En la Tabla 24 en la página 270 se listan los mandatos disponibles para configurar la compresión para un enlace Frame Relay y la Figura 24 en la página 269 es un ejemplo de configuración de un enlace Frame Relay. Hallará más información en el apartado "Mandatos de configuración de Frame Relay", de la publicación *Access Integration Services Guía del usuario de software*.

```
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 24. Ejemplo de configuración de la compresión para un enlace Frame Relay

Tabla 24. Mandatos de configuración de la compresión de datos	
Mandato	**Acción**
add permanent-virtual-circuit *número*	Utilícelo para habilitar la compresión de datos en un PVC concreto definido para una interfaz.
change permanent-virtual-circuit *número*	Utilícelo para establecer si un PVC específico comprimirá datos o no.
disable compression	Inhabilita la compresión de datos.
enable compression	Habilita la compresión de datos.
list lmi	Muestra la configuración actual de la interfaz.
list permanent	Muestra información resumida sobre los circuitos.

Nota: Si se habilita la compresión para circuitos huérfanos, se reducirá el número de sesiones de compresión disponibles para los PVC nativos en el dispositivo.

Si se habilita la compresión para una interfaz Frame Relay que ya tiene habilitada la compresión, el software le pedirá si quiere cambiar los parámetros de compresión de la interfaz, como se muestra en el ejemplo siguiente. Se puede cambiar la compresión de la interfaz sin inhabilitar la compresión.

Ejemplo de cambio de la compresión para 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 para enlaces Frame Relay

La compresión se supervisa de la misma forma que los otros componentes de Frame Relay. En el apartado “Mandatos de supervisión de Frame Relay”, de la publicación *Access Integration Services Guía del usuario de software* se describe cómo acceder al entorno de la consola Frame Relay y se describen detalladamente los mandatos. En la Tabla 25 en la página 271 se listan los mandatos relativos a la compresión. En “Ejemplo: Supervisión de la compresión para una interfaz o circuito Frame Relay” en la página 271 se muestra un ejemplo de listado con información sobre la compresión para una interfaz Frame Relay.

Tabla 25. Mandatos de supervisión de la compresión de datos para Frame Relay	
Mandato	**Se muestra**
list lmi	Muestra el estado actual de la interfaz.
list permanent	Muestra información resumida sobre los circuitos.
list circuit	Muestra el estado actual de un circuito.

Ejemplo: Supervisión de la compresión para 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 la autenticación local o remota

La autenticación es el proceso de determinar quién es un determinado usuario (o entidad). Autenticar el acceso de los usuarios para el protocolo PPP en el 2212 aumenta la flexibilidad de la gestión de perfiles de usuario en lo que se refiere a los protocolos PPP de autenticación: PAP, MSCHAP, CHAP y SPAP. Consulte el apartado 'Protocolos de autenticación PPP', de la publicación *Access Integration Services Guía del usuario de software*, para obtener información adicional sobre cómo configurar los protocolos PAP, MSCHAP, CHAP y SPAP.

La autenticación puede configurarse localmente o puede configurarse para consolidar la configuración de usuarios utilizando servidores de autenticación disponibles en la red para atender a las peticiones de autenticación provenientes de toda la red. El IBM 2212 implementa un sistema de autenticación que se mantiene de forma local, así como los protocolos de servidor de autenticación siguientes:

- Radius
- TACACS
- TACACS+

Utilización de la seguridad de autenticación, autorización y contabilidad (AAA)

La seguridad de autenticación, autorización y contabilidad (AAA) consiste en protocolos configurables que permiten controlar el acceso a los servicios. Se puede configurar la AAA para que realice la autenticación de forma local o remota.

Los protocolos de seguridad pueden configurarse para los siguientes funciones:

- Enlaces PPP
- Inicio de sesión de usuarios (inicio de sesión Telnet o Consola)
- Túneles

La configuración se realiza definiendo un servidor principal y uno secundario. La información del servidor se configura y almacena de forma independiente de la configuración AAA. El nombre del perfil del servidor que se utilizará se proporciona durante la configuración.

La contabilidad no puede realizarse localmente bajo ninguna circunstancia y debe ser Radius o TACACS+.

La autorización sólo puede realizarse localmente o mediante autenticación remota, utilizando Radius o TACACS+.

¿Qué es la seguridad AAA?

La seguridad AAA es el nombre del sistema de seguridad de este dispositivo. Consta de:

Autenticación

Proceso de identificación de un usuario. La autenticación utiliza un nombre y una contraseña para permitir el acceso.

Autorización
Proceso de determinación de los servicios a los que un usuario puede acceder.

Contabilidad
Proceso por el que se registra cuándo un usuario ha iniciado o finalizado una sesión. Existen dos tipos de registros de contabilidad.

Registros de inicio
Indican que se va a iniciar un servicio.

Registros de finalización
Indican que un servicio ha finalizado.

Utilización de PPP

Pueden configurarse las funciones siguientes para el protocolo punto a punto (PPP):

- Autenticación
- Autorización
- Contabilidad

Cada función puede tener su propio protocolo de seguridad, que se configurará independientemente.

- La configuración del protocolo de autenticación no afecta a los de autorización o contabilidad.
- La configuración del protocolo de autorización no afecta a los de autenticación o contabilidad.
- La configuración del protocolo de contabilidad no afecta a los de autenticación o autorización.
- Si se configura la seguridad AAA como remota, la autenticación, la autorización y la contabilidad se establecerán como remotas.
- Si se configura la seguridad AAA como local, la autenticación y la autorización se establecerán como locales. Ni la autenticación ni la autorización se pueden inhabilitar.

Consulte los mandatos de configuración del protocolo punto a punto, en *Access Integration Services Guía del usuario de software* para obtener más información sobre los mandatos de configuración PPP que pueden utilizarse en este entorno.

Protocolos válidos de seguridad PPP

Estos son los protocolos válidos de seguridad PPP:

Métodos de autenticación
Local, RADIUS, TACACS+, TACACS

Métodos de autorización
Local, RADIUS, TACACS+

Métodos de contabilidad
RADIUS, TACACS+

Tabla 26. Establecer protocolos de seguridad PPP

Acción	Autenticación	Autorización	Contabilidad
set AAA local	local	local	hacer caso omiso
set AAA remote	remota	remota	remota
set AUTHENT local	local	hacer caso omiso	hacer caso omiso
set AUTHOR local	hacer caso omiso	local	hacer caso omiso
set AUTHENT remote	remota	hacer caso omiso	hacer caso omiso
set AUTHOR remote	hacer caso omiso	remota	hacer caso omiso
set ACCOUNTING remote	hacer caso omiso	hacer caso omiso	remota
disable ACCOUNTING	hacer caso omiso	hacer caso omiso	inhabilitada

Utilización del inicio de sesión

La configuración del inicio de sesión AAA puede ser remota o local. Si se quiere que la autenticación sea local, la autorización también deber ser local. Si se elige la autenticación remota, la autorización también deber ser remota. No está permitido que la contabilidad sea local, así que si la autenticación y la autorización son locales, la contabilidad debe inhabilitarse.

Atención:

Si un servidor remoto de autenticación no responde, es posible utilizar un id de usuario y una contraseña de inicio de sesión locales si está habilitada la opción login-of-last-resort. Esto permite realizar un único intento de inicio de sesión local en caso de que la autenticación remota no se realice en el tiempo especificado. Además, si la opción tech-support-bypass está habilitada, se pueden utilizar el id y la contraseña del soporte técnico para iniciar la sesión y la petición no se transmitirá al servidor de autenticación.

Si se utiliza la autenticación remota, es importante especificar un nivel de privilegios. Los usuarios que se conecten pueden escribir un id de usuario y una contraseña correctas, pero si no se especifica ningún privilegio no se puede acceder a la consola. Se pueden establecer tres niveles de privilegios: de administrador, de operador y de supervisor. Para RADIUS, utilice el atributo SERVICE-TYPE número 6 o añada el número de atributo de proveedor 216. Consulte el apartado Apéndice A, “Atributos de la seguridad AAA remota” en la página 707 para obtener más detalles sobre los atributos de RADIUS.

Si se configura la autenticación remota, se puede establecer la autorización para que utilice el protocolo de autorización remota Radius o TACACS+, y se puede establecer la contabilidad para que utilice Radius o TACACS+.

- Si se configura la seguridad AAA como local, la autenticación y la autorización se establecerán como locales, y la contabilidad se inhabilitará.

- Si se configura la seguridad AAA como remota, la autenticación, la autorización y la contabilidad se establecerán como remotas.
- Si se configura el protocolo de autenticación como local, el protocolo de autorización se establecerá automáticamente como local, y se inhabilitará la contabilidad.
- Si se configura el protocolo de autenticación como remoto, el protocolo de autorización se establecerá automáticamente como remoto solamente si está establecido como local y no se tendrá en cuenta el protocolo de contabilidad.
- Si se configura el protocolo de autorización como remoto, el protocolo de autenticación se establecerá automáticamente como remoto solamente si está establecido como local, y no se tendrá en cuenta el protocolo de contabilidad.
- Si se configura el protocolo de contabilidad como remoto, los protocolos de autenticación y de autorización se establecerán automáticamente como remotos solamente si están establecidos como locales.
- Inhabilitar el protocolo de contabilidad, no afecta a los protocolos de autenticación o de autorización.
- No está permitido inhabilitar la autenticación ni la autorización.

Protocolos válidos de seguridad de inicio de sesión y administración

Estos son los protocolos válidos de seguridad de inicio de sesión y de administración:

Métodos de autenticación y autorización
Local, RADIUS, TACACS Plus

Métodos de contabilidad
RADIUS, TACACS Plus

Tabla 27. Establecer protocolos de seguridad de inicio de sesión

Acción	Autenticación	Autorización	Contabilidad
set AAA local	local	local	inhabilitada
set AAA remote	remota	remota	remota
set AUTHENT local	local	local	inhabilitada
set AUTHOR local	local	local	inhabilitada
set AUTHENT remote	remota	remota, si es local; si no, hacer caso omiso	hacer caso omiso
set AUTHOR remote	remota, si es local; si no, hacer caso omiso	remota	hacer caso omiso
set ACCOUNTING remote	remota, si es local; si no, hacer caso omiso	remota, si es local; si no, hacer caso omiso	remota
disable ACCOUNTING	hacer caso omiso	hacer caso omiso	inhabilitada

Utilización de túneles

Establezca la autenticación de túneles igual que la autorización de túneles. Si se establece la autenticación de túneles como local o como remota, se podrá habilitar la contabilidad. El servidor de autorización y de autenticación debe ser el mismo.

La configuración de túneles para contabilidad se aplica a los túneles IPSec. La autenticación y la autorización de túneles no se aplica a los túneles IPSec. No se puede habilitar la autenticación ni la autorización para los túneles IPSec utilizando AAA.

Protocolos válidos de seguridad de túneles

Estos son los protocolos válidos de seguridad de túneles:

Métodos de autenticación y autorización
Local, RADIUS

Métodos de contabilidad
RADIUS, TACACS Plus

Tabla 28. Establecer protocolos de seguridad de túneles

Acción	Autenticación	Autorización	Con-tabilidad
set AAA local	local	local	hacer caso omiso
set AAA remote	remota	remota	remota
set AUTHENT local	local	local	hacer caso omiso
set Author local	local	local	hacer caso omiso
set AUTHENT remote	remota	remota	hacer caso omiso
set AUTHOR remote	remota	remota	hacer caso omiso
set ACCOUNTING remote	hacer caso omiso	hacer caso omiso	remota
disable ACCOUNTING	hacer caso omiso	hacer caso omiso	inhabilitada

Reglas sobre las contraseñas

La autenticación local le permite utilizar una contraseña para controlar el acceso en el inicio de sesión. La contraseña puede comprobarse con alguna o con todas las reglas siguientes.

Nota: Las reglas siguientes atañen solamente al inicio de sesión de usuarios PPP y no al inicio de sesión de consola.

- Que tenga un número mínimo de caracteres. Defina el número de caracteres obligatorios.
- Que contenga al menos un carácter alfabético.
- Que contenga al menos un carácter no alfabético.
- Que contenga un carácter no numérico en la primera posición.

- Que contenga un carácter no numérico en la última posición.
- Que no contenga más de tres caracteres consecutivos idénticos a los utilizados en la contraseña anterior.
- Que no contenga más de dos caracteres consecutivos.
- Que la identificación de usuario no forme parte de la contraseña.
- Que sea diferente de las tres contraseñas anteriores.
- Que se cambie después de cierto número de días. Defina el número de días que tendrán que transcurrir entre cada cambio de contraseña.
- Que se bloquee después de un número determinado de intentos de inicio de sesión erróneos. Defina el número de intentos erróneos.

Explicación de los servidores de autenticación

Un ***servidor de autenticación*** es un servidor de la red dedicado a validar identificaciones de usuario y contraseñas para la red. Si se configura un dispositivo para realizar la autenticación mediante un servidor de autenticación y el dispositivo recibe un paquete de un protocolo de autenticación, el dispositivo envía una identificación de usuario y una contraseña al servidor para su autenticación. Si la identificación de usuario y la contraseña son correctas, el servidor responde positivamente. El dispositivo podrá comunicarse con el remitente de la petición. Si el servidor no encuentra la identificación de usuario ni la contraseña recibidas del dispositivo, le responderá negativamente. El dispositivo rechazará la sesión de la que recibió la petición de autenticación.

Soporte de identificación de seguridad

El 2212 puede autenticar clientes de acceso telefónico que utilicen la identificación de seguridad con un servidor ACE/Server de Security Dynamics. El servidor ACE/Server utiliza los métodos TACACS, TACACS+ o RADIUS para autenticar el cliente. Configure el cliente de acceso telefónico como los demás clientes de acceso telefónico del 2212.

El cliente de acceso telefónico iniciará la sesión como siempre, pero utilizará el código de paso de la identificación de seguridad como contraseña. El código de paso de la identificación de seguridad consiste en un número PIN de 4 a n dígitos, seguido del número de identificación de seguridad proporcionado por la tarjeta de señas. (El número máximo de dígitos del PIN depende del servidor). La identificación de usuario y la contraseña podrían ser los siguientes:

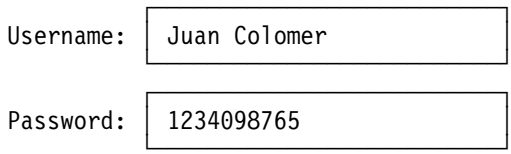


Figura 25. Nombre de usuario y código de paso de la identificación de seguridad

Cuando el servidor ACE/Server autentica el inicio de sesión, es posible que solicite la seña siguiente del cliente. La seña siguiente es la seña siguiente de la tarjeta de señas. El número máximo de dígitos de la seña siguiente depende de la tarjeta de señas de identificación de seguridad que esté utilizando el cliente. El cliente podrá entrar el código de paso y la seña siguiente cuando se le solicite la contraseña,

utilizando el formato `código de paso*seña`, tal como se muestra en el ejemplo siguiente:

```
Username: Juan Colomer

Password: 1234098765*111111
```

Figura 26. Código de paso de la identificación de seguridad con la seña siguiente

Nota: Cuando el servidor solicita que el cliente entre la seña siguiente, el cliente deberá:

1. Entrar el PIN
2. Esperar una nueva seña de la tarjeta y entrar la seña
3. Escribir un * seguido de la seña siguiente de la tarjeta

El administrador del servidor ACE/Server configura las condiciones que harán que el servidor solicite la seña siguiente o un PIN nuevo.

Los clientes de acceso telefónico deben utilizar SPAP para poder recibir alertas del sistema de autenticación cuando sea necesario que entren la seña siguiente. Si el cliente no utiliza SPAP y no puede conectarse, deberá intentar entrar un código de paso nuevo utilizando el formato `código de paso*seña`. Si el cliente sigue sin poder conectarse, podría haber algún otro problema entre el cliente y el servidor ACE/Server.

Limitaciones de la identificación de seguridad

Existen las limitaciones siguientes:

- No se da soporte a los métodos de cifrado Security Dynamics Inc. (SDI) ni DES.
- No se da soporte a la función “New PIN” de la identificación de seguridad.
- TACACS no da soporte a las funciones “New PIN” ni “Next-Token”. El cliente puede especificar una seña siguiente al iniciar la sesión, pero el servidor no la utilizará.
- No se da soporte a los clientes configurados para utilizar devolución de llamada.
- Si se utiliza CHAP con TACACS o TACACS+, establezca en 0 el intervalo de repetición de identificación del CHAP.
- No utilice CHAP si se está utilizando la autenticación RADIUS y la identificación de seguridad.
- Los clientes conseguirán los mejores resultados utilizando TACACS+ y SPAP.
- No se da soporte a los clientes DIALs de Windows 3.1 con autenticación mediante identificación de seguridad que utilice multienlace.
- Si se utiliza la autenticación mediante identificación de seguridad, lo más recomendable es utilizar el software de cliente más reciente (por ejemplo, Windows 95 u OS/2).

Configuración de la autenticación

Este capítulo describe los mandatos operativos y de configuración para la autenticación. Consta de los apartados siguientes:

- "Acceso al indicador de configuración de la autenticación"
- "Mandatos de configuración de la autenticación"
- "Reconfiguración dinámica del sistema de autenticación (AAA)" en la página 303

Acceso al indicador de configuración de la autenticación

Para acceder al indicador `AAA Config>`:

1. Escriba **talk 6** en el indicador `*`.
2. Escriba **feature auth** en el indicador `Config>`.

Mandatos de configuración de la autenticación

En la Tabla 29 se listan los mandatos disponibles desde el indicador `AAA Config >`.

Tabla 29. Mandatos de configuración de la autenticación

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 xxxii.
Disable	Inhabilita varias opciones de AAA.
Enable	Habilitar varias opciones de AAA.
List	Muestra los parámetros de configuración de AAA.
Login	Configura AAA para el inicio de sesión.
Nets-info	Muestra información acerca de la autenticación PPP.
Password-rules	Configura las reglas de contraseña (habilita o inhabilita).
PPP	Configura AAA para PPP.
Servers	Configura servidores AAA individuales remotos.
Set	Configura los parámetros de autenticación 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 xxxiii.

Disable

Utilice el mandato **disable** para inhabilitar la opción de contabilidad elegida.

Sintaxis:

disable accounting
ipsec-accounting
login-last-resort
tech-support-bypass

unauthent-accounting

accounting
Indica que se va a inhabilitar la contabilidad de AAA.

ipsec-accounting
Indica que se va a inhabilitar la contabilidad de IPSec.

login-last-resort
Indica que se va a inhabilitar el último recurso de conexión.

tech-support-bypass
Indica que se va a inhabilitar la opción de eludir la autenticación utilizando los datos del soporte técnico.

unauthent-accounting
Indica que se va a inhabilitar la contabilidad de usuarios no autenticados. No se contabilizarán las sesiones PPP que se activan sin autenticar el usuario porque no está habilitada la autenticación PPP. No se transmitirán los registros inicial y final.

Enable

Utilice el mandato **enable** para habilitar la opción de contabilidad seleccionada.

Sintaxis:

en**able** accounting
ipsec-accounting
login-last-resort
tech-support-bypass
unauthent-accounting

accounting
Indica que se va a habilitar la contabilidad de AAA.

ipsec-accounting
Indica que se va a habilitar la contabilidad de IPSec.

login-last-resort
Indica que se va a habilitar el último recurso de conexión. En caso de que se supere un determinado tiempo de espera durante la transmisión de información de autenticación a un servidor de autenticación remoto, aparecerá un indicador que permitirá que un usuario autenticado localmente pueda conectarse.

tech-support-bypass
Indica que se va a habilitar la opción de eludir la autenticación utilizando los datos del soporte técnico.

unauthent-accounting
Indica que se va a habilitar la contabilidad de usuarios no autenticados.

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

En los siguientes ejemplos se muestran las salidas típicas para distintas opciones 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 el inicio de sesión.

La Tabla 30 lista los submandatos disponibles con el mandato **login**.

Tabla 30. Submandatos de login

Mandato	Función
Disable	Inhabilita la contabilidad para el inicio de sesión.
List	Muestra los parámetros de configuración de AAA para el inicio de sesión.
Set	Establece los parámetros de configuración de AAA para el 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 autenticación.

Sintaxis:

login set aaa
accounting
authentication
authorization

aaa *tipoaut*
Establece el tipo de autenticación, autorización y contabilidad. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuarios mantenida localmente.

remote Establece el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuarios remota.

id-servidor
Especifica el identificador de la base de datos remota.

accounting *tipoaut*
Establece el tipo de contabilidad. *Tipoaut* es uno de los siguientes:

remote Establece el tipo de autenticación para utilizar una base de datos de usuarios remota.

id-servidor
Especifica el identificador de la base de datos remota.

authentication *tipoaut*
Establece el tipo de autenticación. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autenticación para utilizar una base de datos de usuarios mantenida localmente.

remote Establece el tipo de autenticación para utilizar una base de datos de usuarios remota.

id-servidor
Especifica el identificador de la base de datos remota.

authorization *tipoaut*
Establece el tipo de autorización. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autorización para utilizar una base de datos de usuarios mantenida localmente.

remote Establece el tipo de autorización para utilizar una base de datos de usuarios remota.

id-servidor
Especifica el identificador de la base de datos remota.

Nets-info

Utilice el mandato **nets-info** para visualizar el protocolo de autenticación PPP configurado en cada interfaz PPP.

Sintaxis:

n**ets-info**

Password-rules

Utilice el mandato **password-rules** para configurar la contraseña (habilitar o inhabilitar).

La Tabla 31 lista los submandatos disponibles con el mandato **password-rules**.

Tabla 31. Submandatos de login

Mandato	Función
Disable	Inhabilita una regla de contraseña.
Enable	Habilita una regla de contraseña.
List	Muestra el estado actual de las reglas de contraseña (habilitado o inhabilitado).

Disable

Utilice el mandato **password-rules disable** para inhabilitar cualquiera o todas las reglas de contraseña.

Sintaxis:

pa**ssword-rules disable** all

compare-ident-prev

change-days

first-non-numeric

ident-chars

last-non-numeric

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 se solicite un cambio de contraseña.

Valores válidos: del 0 al 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

minimum-length
El número mínimo de caracteres necesario para tener una contraseña válida.

Valores válidos: del 1 al 31

Valor por omisión: 8

maximum-length
El número máximo de caracteres que puede contener una contraseña.

Valores válidos: del 1 al 31

Valor por omisión: 8

one-alpha
Al menos uno de los caracteres de la contraseña debe ser alfanumérico.

one-nonalpha
Al menos uno de los caracteres de la contraseña debe ser numérico.

prev-three
La contraseña no puede ser igual que una 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 cualquiera o todas las reglas de contraseña. Consulte el mandato **disable** para ver una lista con las descripciones de las reglas de contraseña.

Sintaxis:

pa**ssword-rules enable** all

compare-ident-prev

change-days

first-non-numeric

ident-chars

last-non-numeric

minimum-length

one-alpha

one-nonalpha

prev-three

userid-contained

List

Utilice el mandato **password-rules list** para visualizar el estado actual de las reglas de contraseña (habilitado o inhabilitado).

Sintaxis:

pa**ssword-rules list**

PPP

Utilice el mandato **ppp** para configurar AAA para PPP.

La Tabla 32 lista los submandatos disponibles con el mandato **ppp**.

Tabla 32. Submandatos de PPP

Mandato	Función
Disable	Inhabilita la contabilidad para PPP.
List	Muestra 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:

pp**p 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 *tipoaut*
Establece el tipo de autenticación, autorización y contabilidad. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuarios mantenida localmente.

remote Establece el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuarios remota.

id-servidor
Especifica el identificador de la base de datos remota.

accounting *tipoaut*
Establece el tipo de contabilidad. *Tipoaut* es uno de los siguientes:

remote Establece el tipo de autenticación para utilizar una base de datos de usuarios remota.

id-servidor
Especifica el identificador de la base de datos remota.

authentication *tipoaut*
Establece el tipo de autenticación. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autenticación para utilizar una base de datos de usuarios mantenida localmente.

remote Establece el tipo de autenticación para utilizar una base de datos de usuarios remota.

id-servidor
Especifica el identificador de la base de datos remota.

authorization *tipoaut*
Establece el tipo de autorización. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autorización para utilizar una base de datos de usuarios mantenida localmente.

remote Establece el tipo de autorización para utilizar una base de datos de usuarios remota.

id-servidor
Especifica el identificador de la base de datos remota.

Servers

Utilice el mandato **servers** para configurar servidores remotos individuales de AAA.

La Tabla 33 lista los submandatos disponibles con el mandato **servers**.

Tabla 33. Submandatos de Server

Mandato	Función
Add	Añade un perfil de servidor remoto de AAA.
Change	Cambia un perfil de servidor remoto.
Delete	Suprime un perfil de servidor remoto.
Lists	Muestra la información de perfil de servidor de AAA.

Add

Utilice el mandato **servers add** para añadir un perfil de servidor remoto.

Sintaxis:

ser**vers add** nombre

radius Establece el tipo de autenticación para utilizar el protocolo RADIUS del servidor de autenticación.

Se pueden establecer valores para los siguientes parámetros:

accounting-level
Indica qué nivel de información de contabilidad se va a grabar. Los niveles superiores graban toda la información listada para los niveles inferiores.

Rango: de 0 a 10

Valor por omisión: 0

>**0** Graba información de:

- INBYTES_AH
- OUTBYTES_AH
- INBYTES_ESP
- OUTBYTES_ESP

>**1** Graba información de:

- INPKTS_AH
- OUTPKTS_AH
- INPKTS_ESP
- OUTPKTS_ESP

>**2** Graba información de:

- INBYTES_BAD
- OUTBYTES_BAD
- INPKTS_BAD
- OUTPKTS_BAD

>**3** Graba información de:

- INPKTS_BAD_AH
- OUTPKTS_BAD_AH
- INPKTS_BAD_ESP
- OUTPKTS_BAD_ESP

>**4** Graba información de:

- INPKTS_BAD_AH_RPLY
- INPKTS_BAD_ESP_RPLY

accounting-port
Indica el puerto de contabilidad del servidor RADIUS.

Rango: de 1 a 10000

Valor por omisión: 1646

authentication-port
Indica el puerto de autenticación del servidor RADIUS.

Rango: de 1 a 1000

Valor por omisión: 1645

author-authent
Especifica si se deben transferir los atributos de autorización durante la autenticación.

Valores válidos: yes, no

Valor por omisión: yes

account-for-packets
Indica si se deben enviar la cuenta de paquetes al parar la contabilidad.

Valores válidos: yes, no

Valor por omisión: yes

key-for-encryption:
Especifica la clave de cifrado.

Valores válidos: Cualquier serie de caracteres alfanumérica de hasta 32 caracteres.

Valor por omisión: Ninguno.

primary-server-address:
Especifica la dirección del servidor de autenticación primario.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

retries

Valores válidos: del 1 al 100

Valor por omisión: 3

retry-interval

Valores válidos: del 1 al 60

Valor por omisión: 3

secondary-server-address:
Especifica la dirección del servidor de autenticación secundario.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

tacacs Establece el tipo de autenticación para utilizar el protocolo TACACS del servidor de autenticación.

Se pueden establecer valores para los siguientes parámetros:

primary-server-address:
Especifica la dirección del servidor de autenticación primario.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

retries

Valores válidos: del 1 al 100

Valor por omisión: 3

retry-interval

Valores válidos: del 1 al 60

Valor por omisión: 3

secondary-server-address:
Especifica la dirección del servidor de autenticación secundario.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

tacacsplus
Establece el tipo de autenticación para utilizar el protocolo TACACS+ del servidor de autenticación.

Se pueden establecer valores para los siguientes parámetros:

encryption:
Especifica si se utilizará el cifrado.

Valores válidos: yes, no

Valor por omisión:

key-for-encryption:
Especifica la clave de cifrado que se utilizará.

Valores válidos: Cualquier valor de 16 dígitos hexadecimales

Valor por omisión:

primary-server-address:
Especifica la dirección del servidor de autenticación primario.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

privilege-level

Valores válidos: del 0 al 15

Valor por omisión: 0

restarts Establece el número de reinicios. Este parámetro no incluye los reinicios de tiempo excedido y se refiere a los reinicios solicitados por el servidor.

Valores válidos: del 0 al 3200

Valor por omisión: 0

time-to-connect
La cantidad de tiempo permitida para obtener la autenticación del servidor.

Valores válidos: del 1 al 60

Valor por omisión: 9

secondary-server-address:
Especifica la dirección del servidor de autenticación 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 ver las descripciones de perfil de servidor remoto.

Sintaxis:

ser**vers change** radius

tacacs

tacacsplus

Consulte el mandato **servers add** para ver las descripciones de perfil de servidor remoto.

Delete

Utilice el mandato **servers delete** para suprimir un perfil de servidor remoto. Consulte el mandato **add** para ver las descripciones de perfil de servidor remoto.

Sintaxis:

ser**vers delete** radius

tacacs

tacacsplus

Consulte el mandato **servers add** para ver las descripciones de perfil de servidor remoto.

List

Utilice el mandato **servers list** para visualizar la información de perfil de servidor de AAA.

Sintaxis:

ser**vers list** all

names

profile

Set

Utilice el mandato **set** para establecer los parámetros para el inicio de sesión, PPP y el túnel L2TP.

Sintaxis:

s**et** aaa

accounting

authentication

authorization

aaa *tipoaut*

Establece el tipo de autenticación, autorización y contabilidad. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuarios mantenida localmente.

remote Establece el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuarios remota.

id-servidor

Especifica el identificador de la base de datos remota.

accounting *tipoaut*

Establece el tipo de contabilidad para el inicio de sesión, PPP y el túnel. *Tipoaut* es uno de los siguientes:

options Permite entrar opciones de contabilidad.

bytes Indica que la contabilidad se llevará a nivel de byte.

incoming Indica que se llevará la contabilidad de los bytes entrantes.

enable Habilita la contabilidad para las opciones especificadas.

disable Inhabilita la contabilidad para las opciones especificadas.

outgoing Indica que se llevará la contabilidad de los bytes salientes.

enable Habilita la contabilidad para las opciones especificadas.

disable Inhabilita la contabilidad para las opciones especificadas.

packets Indica que la contabilidad se llevará a nivel de paquete.

incoming Indica que se llevará la contabilidad de los paquetes entrantes.

enable Habilita la contabilidad para las opciones especificadas.

disable Inhabilita la contabilidad para las opciones especificadas.

outgoing Indica que se llevará la contabilidad de los paquetes salientes.

enable Habilita la contabilidad para las opciones especificadas.

disable Inhabilita la contabilidad para las opciones especificadas.

remote Establece el tipo de autenticación para utilizar una base de datos de usuarios remota.

id-servidor
Especifica el identificador de la base de datos remota.

authentication *tipoaut*
Establece el tipo de autenticación para el inicio de sesión, PPP y el túnel. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autenticación para utilizar una base de datos de usuarios mantenida localmente.

remote Establece el tipo de autenticación para utilizar una base de datos de usuarios remota.

id-servidor
Especifica el identificador de la base de datos remota.

authorization *tipoaut*
Establece el tipo de autorización para el inicio de sesión, PPP y el túnel. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autorización para utilizar una base de datos de usuarios mantenida localmente.

remote Establece el tipo de autorización para utilizar una base de datos de usuarios remota.

id-servidor
Especifica el identificador de la base de datos remota.

Tunnel

Utilice el mandato **tunnel** para configurar AAA para el túnel L2TP.

La Tabla 34 lista los submandatos disponibles con el mandato **tunnel**.

Tabla 34. 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 los parámetros de 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 *tipoaut*

Establece el tipo de autenticación, autorización y contabilidad. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuarios mantenida localmente.

remote Establece el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuarios remota.

id-servidor
Especifica el identificador de la base de datos remota.

accounting *tipoaut*

Establece el tipo de contabilidad. *Tipoaut* es uno de los siguientes:

remote Establece el tipo de autenticación para utilizar una base de datos de usuarios remota.

id-servidor
Especifica el identificador de la base de datos remota.

authentication *tipoaut*

Establece el tipo de autenticación. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autenticación para utilizar una base de datos de usuarios mantenida localmente.

remote Establece el tipo de autenticación para utilizar una base de datos de usuarios remota.

id-servidor
Especifica el identificador de la base de datos remota.

authorization *tipoaut*

Establece el tipo de autorización. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autorización para utilizar una base de datos de usuarios mantenida localmente.

remote Establece el tipo de autorización para utilizar una base de datos de usuarios remota.

id-servidor
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 podrá acceder a los siguientes mandatos.

Tabla 35. 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 xxxii.
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 perfiles 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 xxxiii.

Add

Utilice el mandato **user profiles add** para añadir el perfil de usuario de un usuario remoto a la base de datos local de usuarios PPP o para dar un acceso de túnel igual mediante una red IP al direccionador.

Sintaxis:

add ppp-user

tunnel

ppp-user Añade el perfil de usuario de un usuario remoto a la base de datos de usuarios PPP. Puede añadir hasta 500 usuarios. Añada un usuario PPP para cada direccionador remoto o cliente DIALs que se puede conectar al dispositivo que está configurando.

Consulte el apartado Add en el capítulo “El proceso CONFIG (CONFIG - Talk 6) y los mandatos” de la publicación *Access Integration Services 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
   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 Da a un igual acceso de túnel al direccionador mediante una red IP. El igual queda entonces autorizado a iniciar en el direccionador sesiones de PPP por túnel.

Consulte el apartado Add del capítulo “Configuración del proceso CONFIG” de la publicación *Access Integration Services 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 perfiles 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
1 record displayed.
```

List Especifica cómo acceder a la información de la lista.

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 se ha habilitado o no se ha habilitado el cifrado.

Status Lista si se ha habilitado o no se ha habilitado el estado.

Login attempts
Lista el número de veces que el usuario ha intentado iniciar la sesión.

Login failures
Lista el número de intentos fallidos de inicio de sesión.

Report

Utilice el mandato **report** para generar un informe de perfiles de usuario PPP.

Sintaxis:

report addresses
all
callback
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
1 record displayed.
```

```
User profile config> report callback
PPP user name      Callback type        Phone Number
-----------------  -------------------  --------------------
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*

Reconfiguración dinámica del sistema de autenticación (AAA)

En este apartado se describe la reconfiguración dinámica (DR) y cómo afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

AAA no da soporte al mandato **delete interface** de CONFIG (Talk 6).

Mandato activate interface de GWCON (Talk 5)

AAA no da soporte al mandato **activate interface** de GWCON (Talk 5).

Mandato reset interface de GWCON (Talk 5)

AAA no da soporte al mandato **reset interface** de GWCON (Talk 5).

Mandatos de cambio inmediato de CONFIG (Talk 6)

AAA da soporte a los siguientes mandatos de CONFIG que permiten modificar inmediatamente el estado operativo del dispositivo. Estos cambios se guardan y se mantienen si el dispositivo se reinicia, si se vuelve a cargar 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:** Entra en vigor en la siguiente secuencia de conexión.
CONFIG, feature authentication, enable tech-support-bypass
CONFIG, feature authentication, disable tech-support-bypass **Nota:** Entra en vigor en la siguiente secuencia de conexión.
CONFIG, feature authentication, enable unauthent-accounting
CONFIG, feature authentication, disable unauthent-accounting

Mandatos no reconfigurables dinámicamente

La tabla siguiente describe los mandatos de configuración de AAA que no pueden modificarse dinámicamente. Para activarlos es necesario reiniciar o volver a cargar 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 los protocolos de cifrado

El objetivo del cifrado es transformar datos a un formato no legible para asegurar la confidencialidad. Los datos ***cifrados*** deben ser descifrados para obtener los datos originales.

El 2212 da soporte a:

- El algoritmo de cifrado RC4 con claves de 40 y 128 bits para el cifrado de punto a punto de Microsoft (MPPE, Microsoft Point-to-Point Encryption) en interfaces PPP.
- El algoritmo DES-CBC (Data Encryption Standard in Cipher Block Chaining Mode) con claves de 56 bits para el soporte del Protocolo de control de cifrado PPP tal como se describe en los documentos RFC 1968 y 1969.
- El algoritmo comercial CDMF (Commercial Data Masking Facility) que utiliza claves de 40 bits para el cifrado de Frame Relay. Este algoritmo está patentado.
- Frame Relay utiliza también el DES triple y una clave de 128 bits.

Cifrado PPP mediante el protocolo ECP

El protocolo ECP (Encryption Control Protocol) se utiliza en el direccionador para negociar el uso del cifrado en los enlaces punto a punto que se comunican mediante el protocolo PPP. El protocolo ECP proporciona un mecanismo generalizado para negociar los algoritmos de cifrado y descifrado que se utilizarán en un enlace PPP. Se pueden negociar distintos algoritmos de cifrado en cada dirección del enlace PPP.

Un método de cifrado y descifrado se denomina ***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, puesto que el cifrado en una sola dirección supone un riesgo para la seguridad. El enlace se terminará cuando ECP no pueda negociar los algoritmos de cifrado en ambas direcciones.

Configuración del cifrado ECP para PPP

Para configurar el dispositivo para que utilice el cifrado en la capa de enlace de datos, deberá:

1. Establecer las claves de cifrado para los dispositivos remotos y las interfaces PPP remotas.

   Establecer la clave de cifrado para el dispositivo remoto mediante el mandato **add ppp-user** en el indicador `Config>`. Consulte el mandato **Add** del capítulo "Configuración del proceso CONFIG" de la publicación *Access Integration Services Guía del usuario de software* para obtener una descripción de la sintaxis y las opciones del mandato.

   Establecer la clave de cifrado para la interfaz PPP local con el mandato **enable ecp** (consulte el mandato `PPP Config>` **enable** de talk 6 en la publicación *Access Integration Services Guía del usuario de software*).

2. Configure los enlaces individuales PPP para utilizar ECP (Encryption Control Protocol) con el mandato **enable ecp** en el indicador `PPP Config>`.
3. Habilite 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 el cifrado. Para obtener información acerca de:

- La inhabilitación del cifrado, consulte el mandato `PPP Config>` **disable ecp** en la publicación *Access Integration Services Guía del usuario de software*.
- El cambio de la clave y contraseña de cifrado del usuario, consulte el mandato `Config>` **change ppp-user** en la publicación *Access Integration Services Guía del usuario de software*.
- El listado de estados de cifrado, consulte el mandato `PPP Config>` **list ecp** en la publicación *Access Integration Services Guía del usuario de software*.
- El establecimiento del nombre de dispositivo, consulte el mandato `PPP Config>` **set name** en la publicación *Access Integration Services Guía del usuario de software*.

Supervisión del cifrado ECP para PPP

Puede supervisar los distintos valores de cifrado de las interfaces:

1. Accediendo al indicador de supervisión con el mandato **talk 5**.
2. Seleccionando la interfaz que desea supervisar con el mandato **network**. Este mandato le coloca en el indicador `PPP n>`, donde *n* representa el número de red. Consulte el apartado “Configuración y supervisión de las interfaces del Protocolo punto a punto” de la publicación *Access Integration Services Guía del usuario de software* para obtener instrucciones acerca del uso del mandato **network**.

Desde este indicador podrá:

- Listar el estado actual del cifrado, la negociación de cifrado más reciente, el tiempo transcurrido desde el cambio de estado del cifrado y los algoritmos que utilizan los encriptadores. (Consulte el mandato **list control ecp** de la publicación *Access Integration Services Guía del usuario de software*.)
- Listar los paquetes de control del cifrado recibidos y transmitidos en la interfaz. (Consulte el mandato **list ecp** en la publicación *Access Integration Services 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 *Access Integration Services Guía del usuario de software*.)

Cifrado de punto a punto de Microsoft (MPPE)

El cifrado de punto a punto de Microsoft (MPPE, Microsoft Point-to-Point Encryption) permite a las estaciones de trabajo Windows conectadas de forma remota y denominadas clientes de acceso telefónico a redes (DUN) de Microsoft, cifrar los datos que se transmiten a través de un enlace PPP entre ellas y el 2212. MPPE se puede utilizar también para cifrar los datos que se transmiten a través de un enlace PPP de direccionador a direccionador. MPPE se negocia siempre en ambas direcciones.

MPPE utiliza algoritmos de claves secretas para realizar el cifrado. En estos algoritmos se utiliza la misma clave tanto para el cifrado como para el descifrado. Esta clave no la configura el usuario, sino que la genera el proceso de negociación MPPE entre las estaciones de trabajo de envío y recepción. Para utilizar MPPE, deberá configurar el protocolo MS-CHAP (Microsoft Challenge/Handshake Authentication Protocol).

Si la interfaz PPP se autentica con MS-CHAP, el direccionador pasa a una "modalidad de Microsoft" en la que negociará sólo MPPC si se ha habilitado la compresión y sólo MPPE si se ha habilitado el cifrado. En la "modalidad de Microsoft", el direccionador pasa por alto la lista de prioridad de los algoritmos de compresión e inhabilita la negociación ECP.

Configuración de MPPE

Para configurar MPPE, deberá seguir estos pasos para cada interfaz:

1. Configure MS-CHAP. En la publicación *Access Integration Services Guía del usuario de software*, consulte los apartados "MS-CHAP (Microsoft PPP CHAP Authentication)" y "Configuración y supervisión de las interfaces del Protocolo punto a punto" para obtener información acerca del uso y configuración de MS-CHAP.
2. Si está configurando una conexión de direccionador a direccionador, establezca el nombre de la interfaz PPP local con el mandato **set name** (consulte el mandato `PPP Config>` **set name** en la publicación *Access Integration Services Guía del usuario de software*).
3. Si quiere utilizar la compresión de datos, habilite MPPC utilizando el mandato **enable ccp** de talk 6 en el indicador `PPP Config>`. MPPE no necesita la compresión de datos.
4. Habilite MPPE. Utilice el mandato **enable mppe** en el indicador `PPP Config>` (consulte el mandato `PPP Config>` **enable** en la publicación *Access Integration Services Guía del usuario de software*).
5. Reinicie el direccionador para activar la configuración.

También puede inhabilitar MPPE y listar las opciones de MPPE.

- Utilice el mandato **disable mppe** de talk 6 en el indicador `PPP Config>` para inhabilitar MPPE.
- Utilice el mandato **list ccp** de talk 6 en el indicador `PPP Config>` para listar las opciones de MPPE que se han configurado.

Supervisión de MPPE

Active el indicador `PPP>` tal como se describe en el apartado "Supervisión del cifrado ECP para PPP" en la página 306. Utilice el mandato **list mppe** para ver las estadísticas de MPPE y el mandato **list control ccp** para ver el estado de MPPE. En el apartado "Configuración y supervisión de las interfaces del Protocolo punto a punto" de la publicación *Access Integration Services Guía del usuario de software* encontrará ejemplos de la salida de estos mandatos.

Configuración del cifrado en las interfaces de Frame Relay

Nota: Frame Relay utiliza un esquema de cifrado patentado.

El cifrado de datos está soportado en todas las interfaces en las que haya habilitado el cifrado. Puede configurar circuitos individuales de una interfaz habilitada para el cifrado con el fin de cifrar o no cifrar según se desee.

Para configurar el dispositivo para utilizar el cifrado en enlaces de Frame Relay:

1. Acceda al indicador de configuración de Frame Relay con el mandato **talk 6**.
2. Seleccione la interfaz de Frame Relay que desea que tenga activado el cifrado con el mandato **net** #
3. Habilite el cifrado en la interfaz de Frame Relay utilizando el mandato **enable encryption**. Consulte los mandatos de configuración de Frame Relay en la publicación *Access Integration Services Guía del usuario de software*.
4. Añada circuitos virtuales permanentes con posibilidad de cifrado y defina la clave de cifrado para cada PVC utilizando el mandato **add permanent-virtual-circuit**. Consulte los mandatos de configuración de Frame Relay en la publicación *Access Integration Services Guía del usuario de software*.
5. Repita los pasos del 1 al 4 para cada interfaz con posibilidad de cifrado que configure.

Nota: Si el cifrado está activado para un circuito virtual permanente de FR, los datos no fluirán por el circuito a menos que se negocie satisfactoriamente el cifrado con el dispositivo que se encuentre en el otro extremo del circuito virtual. No se da soporte al cifrado para los circuitos huérfanos, ya que se debe configurar el PVC para introducir 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 acerca de

- La inhabilitación del cifrado en una interfaz, consulte el mandato de configuración de Frame Relay **disable encryption** en la publicación *Access Integration Services Guía del usuario de software*.
- El cambio de los valores de cifrado para un PVC, consulte el mandato de configuración de Frame Relay **change permanent-virtual-circuit** en la publicación *Access Integration Services Guía del usuario de software*.
- El listado de estados de cifrado, consulte los mandatos de configuración de Frame Relay **list all,**, **list lmi** y **list permanent-virtual-circuit** en la publicación *Access Integration Services Guía del usuario de software*.

Supervisión del cifrado en las interfaces de Frame Relay

Puede supervisar los distintos valores de cifrado de las interfaces:

1. Accediendo al indicador de supervisión con el mandato **talk 5**.
2. Seleccionando la interfaz que desea supervisar con el mandato **network** #. Este mandato le coloca en el indicador `FR x>`.

Desde este indicador, puede listar el estado de cifrado actual de una interfaz, un PVC o un circuito. Consulte el mandato de supervisión de Frame Relay **list** en la publicación *Access Integration Services Guía del usuario de software*.

Utilización de la función de política

En este capítulo se describe cómo interactúa la función de política con otros componentes software del direccionador para tomar decisiones acerca de la QoS, la seguridad o ambas. También se describen los conceptos y mandatos de configuración específicos relacionados con la función de política. Esta función permite la utilización de un servidor de directorios LDAP como depósito central para la información de la política. También se describen los conceptos y pasos de configuración necesarios para habilitar las funciones de LDAP. Los siguientes temas tratan estos conceptos, la manera como los direccionadores aplican las políticas e incluye ejemplos.

Visión general de la función de política

La función de política facilita la gestión del tráfico IPv4 en una red. Se pueden configurar políticas para reglas de filtro muy simples (descartar o pasar) o para casos de seguridad y QoS complejos. La combinación de políticas determina la forma en que los direccionadores manejan el tráfico IPv4 en una red.

Decisión y aplicación de una política

La implementación de políticas en esta familia de direccionadores constituye la base para la toma de decisiones de políticas y la forma de aplicarlas. A estos conceptos a menudo se les denomina punto de decisión de política (PDP) y punto de aplicación de la política (PEP).

La base de datos de políticas, que reside en la memoria del direccionador, consta del conjunto de políticas cargado desde la configuración local y las políticas que se han leído del LDAP. La base de datos de políticas se crea en las situaciones siguientes:

- Recarga o reinicio del dispositivo
- Ejecución del mandato de supervisión **reset database**
- Renovación automática
- Petición de conjunto de SNMP

La base de datos de políticas sirve como PDP y consta de un conjunto de políticas que determinan la manera en que los componentes relacionados con la función de política manejan los paquetes. Cuando como resultado de una política se toma una decisión (basada en la hora, información del paquete IP o información especifica del protocolo como puede ser la identificación), la decisión se pasa al componente de aplicación (PEP) para que lleve a cabo la acción. La Figura 27 en la página 310 muestra la relación de estos componentes.

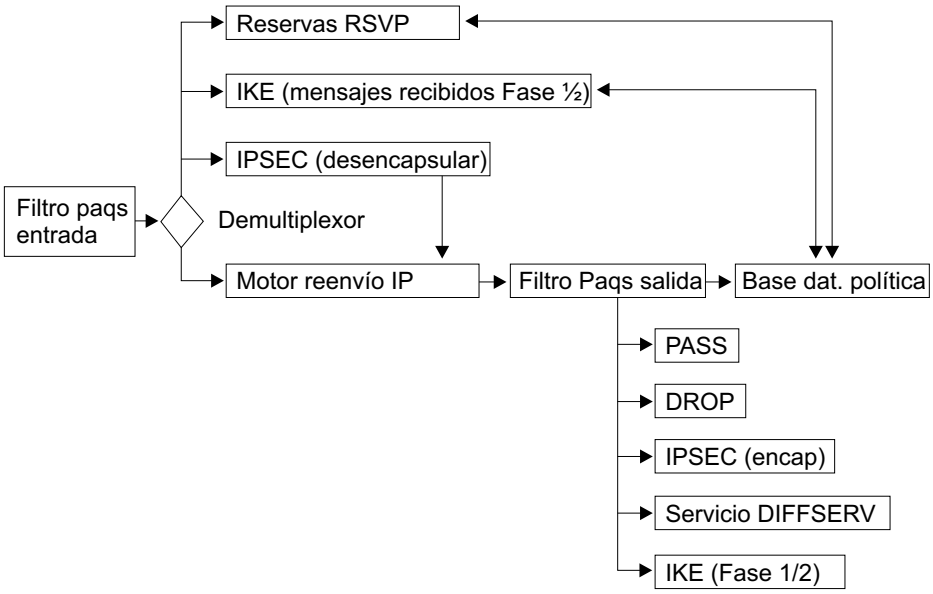


Figura 27. Flujo de paquetes IP y base de datos de políticas

Decisión de política y flujo de paquetes

Los paquetes IP deben pasar el filtro de paquetes de entrada antes de llevar a cabo ninguna otra acción. Si el filtro de paquetes de entrada contiene alguna regla, puede que se lleve a cabo alguna acción en el paquete. Si hay una coincidencia con un filtro que excluye el paquete o si no se da ninguna coincidencia con el filtro de paquetes de entrada, el paquete se descarta.

Si el paquete pasa el filtro de paquetes de entrada, va a un filtro de demultiplexado que comprueba si el paquete tiene un destino local. En ese caso, pasará a otros módulos según el tipo de paquete. 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 se debe tomar.

Si el paquete no tiene un destino local, se entrega al motor de reenvío y se toma una decisión de direccionamiento. Si esta decisión no descarta el paquete (el direccionamiento basado en la política puede decidir descartarlo), éste va al filtro de paquetes de salida. Si el paquete de salida contiene reglas de filtro, puede ser que se le aplique una conversión de dirección (NAT), que se pase, o que se descarte. Si no hay reglas de filtro, el paquete se pasa. Si hay reglas de filtro y no se da ninguna coincidencia, el paquete se descarta. Si el paquete pasa el filtro de paquetes de salida, el motor IP consulta la base de datos de políticas para determinar si se deben llevar a cabo otras acciones en el paquete.

Nota: Si se han habilitado filtros de paquetes de entrada y de salida para una o varias interfaces y se espera que los paquetes que debe controlar la base de datos de políticas atraviesen estas interfaces, debe existir una regla de filtro que incluya estos paquetes en los filtros de paquetes de entrada y de salida para que no se descarten antes de consultar la base de datos de políticas. Se recomienda utilizar la base de datos de políticas para configurar todas las reglas de pasar y descartar, en lugar de utilizar los filtros de paquetes.

Consultas de políticas de IP

Cuando el motor de reenvío de IP consulta la base de datos de políticas, se pueden devolver los siguientes tipos de combinaciones de decisiones:

- No se ha encontrado ninguna coincidencia—pasar el paquete
- Se ha encontrado una coincidencia—descartar el paquete
- Se ha encontrado una coincidencia—pasar el paquete
- Se ha encontrado una coincidencia—proteger el paquete en el túnel IPSec x
- Se ha encontrado una coincidencia—proteger el paquete en el túnel IPSec x de IKE negociado
- Se ha encontrado una coincidencia—iniciar las negociaciones de ISAKMP para las fases 1 y 2, descartar el paquete
- Se ha encontrado una coincidencia—proporcionar DiffServ QoS x, proteger el paquete con IPSec

Consultas de políticas de IPSec

Si IPSec recibe un paquete, primero debe desencapsularlo y decidir después si ha llegado en el túnel IPSec correcto (denominado a veces comprobación de conformidad). Para ello consulta la base de datos de políticas que devuelve los siguientes tipos de decisiones:

- Comprobación de conformidad pasada—reenviar el paquete
- Comprobación de conformidad anómala—descartar el paquete

Decisiones de políticas de IKE

Es posible que IKE consulte la base de datos de políticas y reciba las decisiones de políticas de IP de la *fase 1* que aparecen en la Tabla 36.

Tabla 36. Consultas de fase 1 de IKE y decisiones recibidas

Tipo de consulta	Decisión
Mensaje 1 (modalidad principal)	No se ha encontrado ninguna coincidencia, descartar el paquete
Mensaje 1 (modalidad principal)	Se ha encontrado una coincidencia, negociar con la política x de la fase 1
Mensaje 5 (modalidad principal)	No se ha encontrado ninguna coincidencia, detener las negociaciones con el igual, descartar el paquete
Mensaje 5 (modalidad principal)	No se ha encontrado ninguna coincidencia, detener las negociaciones con el igual, descartar el paquete
Mensaje 5 (modalidad principal)	Se ha encontrado una coincidencia, la política x coincide, finalizar la fase 1
Mensaje 5 (modalidad principal)	Se ha encontrado una coincidencia, la política y coincide, detener la fase 1 actual e iniciar la fase 1 nueva con la política nueva
Mensaje 1 (modalidad agresiva)	No se ha encontrado ninguna coincidencia, descartar el paquete
Mensaje 1 (modalidad agresiva)	Se ha encontrado una coincidencia, la política x coincide

Es posible que IKE consulte la base de datos de políticas y reciba las decisiones de políticas de IP de la *fase 2* que aparecen en la Tabla 37 en la página 312.

Tabla 37. Consultas de fase 2 de IKE y decisiones recibidas

Tipo de consulta	Decisión
Mensaje 2 (responder)	No se ha encontrado ninguna coincidencia, descartar el paquete
Mensaje 2 (responder)	Se ha encontrado una coincidencia, negociar con la política x

Decisiones de políticas de RSVP

Si un paquete es un mensaje de control de RSVP, RSVP consulta la base de datos de políticas para determinar si debe aceptar o rechazar la reserva. Si se acepta, RSVP determina los atributos de la reserva que se deben limitar, según la política. Las políticas de la base de datos de políticas pueden controlar la duración de la reserva, la cantidad de ancho de banda que se debe asignar y el retardo mínimo que se debe garantizar.

Objetos de política

Una política consta de un perfil, que contiene un conjunto de atributos de paquete sobre los que se toman decisiones, acciones que se deben tomar si los atributos de un paquete coinciden con los de un perfil, y un período de validez durante el cual se toman las decisiones y se aplican las acciones. Estos elementos se detallan en los siguientes temas:

Las partes que forman una política son objetos definidos diferenciados. Los objetos de política pueden hacerse referencia entre sí y, como grupo de elementos relacionados, forman una política. Al separar la información de configuración en objetos diferenciados separados, muchos de ellos se pueden reutilizar en definiciones de políticas múltiples, lo que ahorra tiempo y reduce las tareas de mantenimiento. En los temas siguientes se describen con detalle los objetos de política individuales.

Política

El objeto de política describe las condiciones que hay que comprobar y, si se da alguna de esas condiciones, las acciones que se deben aplicar. La política hace referencias explícitas al período de validez y al perfil. Para que la política sea válida, estas referencias son obligatorias. La política también debe hacer referencia explícita a una o varias de las siguientes acciones: un objeto de túnel IPSec con claves manuales, una acción IPSec, una acción ISAKMP, una acción RSVP o una acción DiffServ. Son combinaciones válidas:

- Túnel IPSec con claves manuales
- Acción IPSec para descartar paquetes
- Acción IPSec para pasar paquetes (sin seguridad)
- Acción IPSec para proteger paquetes, acción ISAKMP
- Acción DiffServ (descartar)
- Túnel IPSec con claves manuales y acción DiffServ (pasar)
- Acción IPSec para proteger paquetes, acción ISAKMP, acción DiffServ (pasar)
- Acción RSVP
- Acción RSVP y acción DiffServ (pasar)

Nota: En estas combinaciones no puede existir ningún túnel manual IPSec en la misma definición de política que una acción IPSec (túnel IPSec de IKE negociado) y no se debe asociar ninguna acción RSVP con ningún tipo de acción IPSec. Si se asocia una acción IPSec para proteger paquetes con una política, también deberá asociar una acción ISAKMP con la política.

Cada política tiene también un número de prioridad asociado (cuanto mayor es el número del atributo de prioridad, más alta es la prioridad). La prioridad determina si una política prima sobre otra política. Generalmente, sólo hay que establecer si dos o más perfiles de política entran en conflicto de alguna manera. La política que tenga un perfil más específico deberá tener una prioridad superior. Por ejemplo, suponga que una política especifica que el tráfico de la subred A a la subred B se debe proteger con IPSec (DES) y otra política especifica que el tráfico del punto a′ (un sistema principal concreto de la subred A) a la subred B se debe proteger con IPSec (3DES). La política más específica (de a′ a B) debería tener una prioridad superior a la política de A a B.

Una buena idea es designar valores de prioridad iniciales que se diferencien en 5 o más dígitos, lo que ofrece espacio para especificar luego valores de prioridad adicionales para las políticas que entren en conflicto. Cada política tiene también un atributo habilitado que determina si se debe habilitar cuando se carga en la base de datos de políticas. Si se encuentra una coincidencia de política durante la búsqueda en una base de datos de políticas, pero está inhabilitada, se aplicará la siguiente política más específica.

Mediante el mandato de supervisión **check-consistency** se puede iniciar una comprobación de coherencia y de conflictos tanto dentro de una sola política como entre todas las políticas definidas. Con este mandato no se pretenden resolver los problemas, pero sirve para identificarlos de forma que el administrador pueda tomar medidas para resolverlos. En el apartado “Mandatos de supervisión de políticas” en la página 379 hallará más detalles sobre el mandato.

Perfil

El perfil determina la información que se debe utilizar para seleccionar una política concreta. El perfil consta de información sobre la dirección de origen, la dirección de destino, el protocolo y el puerto de origen y de destino.

Nota: Cuando se definen políticas para IPSec/ISAKMP, cada pasarela que proporciona seguridad debe tener una política para definir la asociación de seguridad. El perfil de cada pasarela debe asociar el origen con el destino y el destino con el origen. El perfil de una política de IPSec debe especificar la dirección de origen, así como el tráfico que se debe encapsular en el túnel y la dirección de destino que debe encontrarse en el extremo final del túnel.

También se puede seleccionar según el byte de tipo de servicio (TOS) y la dirección IP de entrada y salida. Por omisión, un paquete recibido en cualquier interfaz de entrada y que sale por cualquier interfaz de salida se compara con los otros selectores. En algunos casos, se puede necesitar la flexibilidad de especificar exactamente las interfaces a las que debe llegar el paquete y la interfaz de la que debe salir. Si se quiere así, se deben añadir objetos consistentes en pares de interfaces y asociar el nombre de grupo de los objetos con el perfil. Se pueden asignar objetos consistentes en pares de interfaces a un grupo dándoles el mismo nombre. Esto permite especificar combinaciones del tipo "cualquier paquete que

llegue a direccIPx y salga de una interfaz *O* cualquier paquete que llegue en una interfaz y salga de direccIPx". Esto es particularmente útil si se define una regla de descarte general para una interfaz pública.

Par de interfaces: Identifica la interfaz de salida y la interfaz de entrada. Especifica las direcciones IP de la interfaz para esta selección. El valor 255.255.255.255 incluye cualquier interfaz.

Si se quiere utilizar el perfil para seleccionar una política IPSec/ISAKMP, se tiene la opción de especificar el ID local que se enviará 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 extremo final del túnel local para el tráfico de IPSec/IKE y la lista de ID remota es *Any*. También se puede especificar el nombre de dominio totalmente calificado (FQDN), FQDN de usuario e ID de clave. Normalmente, esto es suficiente porque todas las negociaciones de ISAKMP de la fase 1 se autentican con certificados públicos o claves previamente compartidas. Sin embargo, en algunas situaciones de acceso remoto en las que la política es utilizar comodines para las direcciones de destino, se recomienda especificar una lista de usuarios de acceso remoto a los que se les permitirá el acceso a los recursos de la red.

Estos usuarios se siguen autenticando mediante los métodos de autenticación de ISAKMP normales, pero la base de datos de políticas da un paso más al asegurarse de que el igual envía el ID local que coincide con uno de los ID especificados en el grupo de usuarios remotos del perfil de la política. Esto es obligatorio si una autoridad certificadora (CA) pública administra certificados para todo el mundo y el administrador de la red sólo quiere que tenga acceso un grupo concreto de estos usuarios (por ejemplo, los empleados de la empresa). El grupo de usuarios remotos consiste en una lista de usuarios que pertenecen al mismo grupo. Estos usuarios se especifican añadiendo uno o más *USUARIOS*. Un grupo de usuarios puede hacer que el nombre de grupo sea el mismo para cada usuario. Este grupo también se puede asociar opcionalmente con un perfil.

Período de validez

El período de validez especifica la duración de la política: el año, los meses, los días y las horas en que es válida. Esta flexibilidad permite que el administrador de la red especifique cuándo es válida una política, por ejemplo “siempre” o “sólo este año”, durante los meses de enero, febrero y marzo, de lunes a viernes, o de 9 de la mañana a 5 de la tarde. Cuando una política de la base de datos de políticas deja de ser válida, se aplicará la siguiente política más específica. De esta forma, se puede definir una política que especifique que se proteja todo el tráfico de la subred A a la subred B, de lunes a viernes, y de 9 de la mañana a 5 de la tarde, y que en cualquier otro momento se descarte todo el tráfico de la subred A a la subred B. En este caso, la primera política debe tener una prioridad más alta (que se especifica cuando se escribe el mandato de supervisión **add policy**).

Acción DiffServ

La acción DiffServ describe la calidad del servicio (QoS) que se proporcionará a los paquetes que coincidan con una política que especifique una acción DiffServ. Se puede configurar la acción DiffServ para que descarte paquetes. También se puede utilizar para correlacionar paquetes en calidades de servicio relativas. Se puede configurar el ancho de banda asignado como un porcentaje del ancho de banda de salida o como un valor absoluto en kbps. Se debe especificar si será la cola garantizada (AF)/optimizada o la cola preferente (EF) la que proporcione la asignación de ancho de banda. Para obtener más información sobre estas colas y

cómo se definen, consulte los apartados “Utilización de la función de servicios diferenciados” en la página 449 y “Configuración y supervisión de la función de servicios diferenciados” en la página 457.

La acción DiffServ también especifica cómo marcar el elemento de código (byte TOS) para el tráfico de EF y AF, antes de enviarlo a la interfaz de salida. El tráfico de EF y AF se mide, y el que no satisface determinados criterios, se vigila. El tráfico de EF que no satisface determinados criterios se descarta y, opcionalmente, el byte DS del tráfico de AF que no satisface dichos criterios se vuelve a marcar mediante el método del marcador de tres colores, TCM (Three Color Marker). El marcado, la medición y la vigilancia de paquetes permite que el direccionador central de una red en que está habilitada la función DiffServ, clasifique los paquetes basándose en elementos de código DS y que controle la congestión descartando primero el tráfico que no satisfaga determinados criterios. Esto ayuda a que en las redes en que está habilitada la función DiffServ la velocidad de transmisión del tráfico preferente sea mayor y el retardo menor.

Acción RSVP

RSVP especifica si se deben permitir o denegar los flujos de RSVP si se produce una reserva de RSVP y la petición de reserva coincide con el perfil de la política. Si permite la reserva, la acción RSVP también especifica la duración permitida de la reserva, el ancho de banda y, si se quiere, una referencia a la acción DiffServ. La referencia a la acción DiffServ permite al RSVP determinar cómo marcar el byte 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 el QoS hasta el límite de RSVP y luego marcar el byte TOS adecuadamente para que la red DiffServ pueda aplicar el ancho de banda correcto.

Acción IPSec

La acción IPSec puede especificar una acción de descarte, pase o protección. Si la acción es de descarte, todos los paquetes que coincidan con esta política se descartarán. Si la acción es de pase sin seguridad, se autoriza el pase a todos los paquetes. Si la acción es de pase con seguridad, todos los paquetes se protegen mediante la asociación de seguridad (SA) especificada por la acción. La acción IPSec también contiene las direcciones IP de los extremos final del túnel IPSec y las SA de IKE.

Las propuestas de IPSec a las que hace referencia la acción IPSec determinan los atributos de SA. La acción IPSec puede especificar varias propuestas de IPSec que se envían y comprueban en el orden en que se han especificado. Tener varias propuestas en una acción IPSec permite que la configuración contenga todas las combinaciones de seguridad aceptables, por lo que se reduce el número de potenciales discrepancias de configuración entre pasarelas VPN.

Propuesta de IPSec

La propuesta de IPSec contiene la información acerca de qué transformación de ESP o AH (o ambas) proponer o comprobar durante las negociaciones de ISAKMP de la fase 2. Si se necesita un reenvío secreto perfecto (un cálculo Diffie Hellman nuevo), la propuesta de IPSec identifica el grupo DH que se debe utilizar. Las transformaciones a las que hace referencia la propuesta de IPSec se envían o comprueban en el orden en que se han especificado. La primera transformación de ESP o AH de la lista debe ser la más apropiada. Si hay más de una en la lista, ambas se comparan con la lista de transformaciones del igual para encontrar una coincidencia. Si ninguna de las transformaciones configuradas coinciden con la

lista del igual, la negociación falla. La propuesta de IPSec puede listar una combinación de transformaciones de AH y ESP, pero las únicas combinaciones válidas son:

- Lista sólo de AH (modalidad de túnel o transporte)
- Lista sólo de ESP (modalidad de túnel o transporte)
- Lista de AH (modalidad de transporte) y lista de ESP (modalidad de túnel)

Transformación de IPSec

Los atributos de la transformación de IPSec contienen información acerca de los parámetros de cifrado de IPSec y de autenticación y también especifican con qué frecuencia se renovarán las claves. La transformación es AH (sólo autenticación) o ESP (cifrado, autenticación o ambas) y puede configurarse para que funcione en modalidad de túnel o de transporte.

Acción ISAKMP

La acción ISAKMP especifica la información de gestión de claves para la fase 1. Especifica si las negociaciones de la fase 1 deben empezar en modalidad principal (proporciona protección de identidad) o en modalidad agresiva. También especifica si la asociación de seguridad de la fase 1 se debe negociar al iniciar el dispositivo o a petición. La acción ISAKMP también debe hacer referencia a una o más propuestas de ISAKMP. La primera referencia debe ser para la propuesta de ISAKMP más aceptable.

Propuesta de ISAKMP

La propuesta de ISAKMP especifica los atributos de cifrado y autenticación de la asociación de seguridad de la fase 1. También especifica el grupo de Diffie Hellman que se debe utilizar para generar las claves y la duración de la asociación de seguridad de la fase 1. Se debe seleccionar el método de autenticación de la propuesta de ISAKMP. Este puede ser la modalidad de certificados públicos o de claves previamente compartidas.

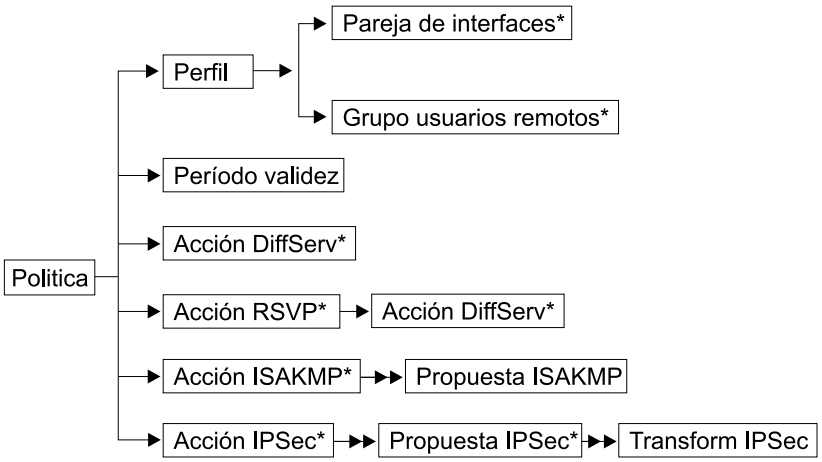
Usuario

Se debe configurar un USUARIO para cualquier política que utilice una negociación de ISAKMP con clave previamente compartida como método de autenticación. La configuración de USUARIO identifica la clave previamente compartida que se debe utilizar para el igual ISAKMP. El objeto de usuario contiene la información de identificación para un igual ISAKMP remoto, es decir la dirección IP, FQDN, ID de clave o FQDN de usuario y el método que el usuario quiere utilizar para la autenticación. Se puede seleccionar una modalidad de certificados o de clave previamente compartida. Si se selecciona la modalidad de clave previamente compartida, también se ha de especificar si se debe escribir en ASCII o en hexadecimal, y el valor de la clave. Los USUARIOS se pueden agrupar asignándolos al mismo nombre de grupo. Este grupo también se puede asociar opcionalmente con un perfil de políticas para llevar a cabo una búsqueda de política más estricta para la fase 1.

Túnel IPSec con claves manuales

El túnel IPSec con claves manuales es una configuración estática de los parámetros de cifrado y autenticación. No se realiza ninguna negociación para el túnel, de manera que los dos iguales deben tener exactamente la misma configuración. Las claves realmente forman parte de esta configuración y deben coincidir en ambos lados del túnel. Puesto que no se realiza ninguna negociación en esta modalidad, las claves no se renuevan nunca. Para obtener más información sobre los túneles IPSec con claves manuales, consulte la descripción de la función IPSec en el “Utilización de la seguridad IP” en la página 389.

La Figura 28 muestra la relación entre los objetos de configuración de una política.



Notas:

1. La flecha → indica una referencia simple.
2. La flecha →► 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 pasa al túnel seguro.

Figura 28. Relación de los objetos de configuración de una política

Interacción entre LDAP y la base de datos de políticas

La familia de direccionadores permite que un servidor LDAP (Lightweight Directory Access Protocol) sea el depósito de información de la política (la base de datos de políticas). LDAP es un protocolo que permite buscar y modificar información en un servidor de directorios. LDAP es una versión simplificada del estándar X.500. Los direccionadores dan soporte a la posibilidad de buscar (pero no de modificar) información en el servidor de directorios. El agente de búsqueda de políticas del direccionador recupera toda la información de políticas del servidor de directorios que se refiere a ese dispositivo. Todos los servidores LDAP que funcionan en LDAP versión 2 ó 3 funcionan con la implementación en el direccionador. Una ventaja importante de utilizar un servidor de directorios para almacenar información de políticas, en comparación con los métodos más tradicionales de configuración almacenada localmente, es la posibilidad de realizar un cambio en un lugar y que ese cambio se aplique a todos los dispositivos de la red ampliada. Esto incluye a los dispositivos del dominio administrativo, así como a los dispositivos que están dentro de los límites públicos de la red.

Por ejemplo, suponga que tiene una definición de transformación de IPSec que reside en el directorio. Si quiere cambiar la política de cifrado corporativa de DES a 3DES, normalmente deberá realizar un cambio en la configuración de todos los dispositivos que estén dentro del límite de la red. Si utiliza el directorio para distribuir las políticas, sólo deberá cambiar una transformación de IPSec. Después, todos los dispositivos de la red que tengan habilitada la función de política deberá volver a crear la base de datos. Otro ejemplo: suponga que tiene que cambiar una acción DiffServ denominada “GoldService” para aumentar el valor de ancho de banda del 40% al 45%. El servidor LDAP y la infraestructura de políticas permiten que estos tipos de cambios de la configuración se adapten mejor a nuevas situaciones y reducen las discrepancias en la configuración.

El administrador de la red también puede aprovechar la posibilidad de renovar la base de datos automáticamente cada día a una hora concreta. Para seleccionar esta opción, escriba el mandato **set refresh** de la función de política. También se puede especificar si se quiere habilitar la renovación y, en ese caso, la hora en se quiere que se renueve la base de datos. Esta opción es útil para efectuar cambios automatizados. Por ejemplo, suponga que debe añadir una política nueva para que el departamento de ventas de EE.UU. pueda hablar con el departamento de desarrollo de Japón a través de Internet y que las pasarelas de seguridad son SG1 y SG2. Sólo tiene que entrar esta información en el directorio y, a medianoche, las pasarelas SG1 y SG2 efectuarán automáticamente este cambio si tienen habilitada la renovación automática.

Después de leer correctamente la información de políticas del servidor LDAP, puede que quiere almacenar en antememoria esta información en un almacenamiento persistente del dispositivo. A continuación, se puede elegir leer siempre la información almacenada en antememoria, eliminando por consiguiente el tiempo necesario para interrogar el servidor LDAP. También se puede elegir que el motor de búsqueda de políticas sea el que lea la copia almacenada en antememoria, en caso de que el servidor LDAP no estuviera disponible cuando se solicite una renovación. Para obtener más información, consulte los mandato de supervisión **cache-ldap-plcys** y **flush-cache** del capítulo “Mandatos de supervisión de políticas” en la página 379 y el mandato de configuración **enable ldap** del capítulo “Mandatos de configuración del servidor de políticas de LDAP” en la página 374.

El motor de búsqueda de políticas LDAP le permite especificar el nivel de seguridad que se utilizará al crear la base de datos de políticas. Estas opciones de seguridad se definen con el mandato **set default** de la función de política. Las opciones son:

- Pasar todo el tráfico durante la búsqueda (valor por omisión).
- Descartar todo el tráfico *excepto* las peticiones de búsqueda de políticas de LDAP y los resultados.
- Descartar todo el tráfico *excepto* las solicitudes de búsqueda de políticas de LDAP y los resultados protegidos por IPSec.

En algunas situaciones, es suficiente definir una de las dos primeras opciones. Sin embargo, si el tráfico LDAP tiene que atravesar la infraestructura pública, se debe proteger y autenticar la información seleccionando la tercera opción. Si se hace así, se deben seleccionar las opciones de cifrado y autenticación de las fases 1 y 2. También se debe escribir las direcciones IP de los extremos final del túnel (servidores LDAP principal y secundario). Este túnel IKE/IPSec de rutina de carga se

negociará antes de que se envíe el tráfico LDAP. Esta función permite establecer la configuración que aparece en la Figura 29 en la página 319.

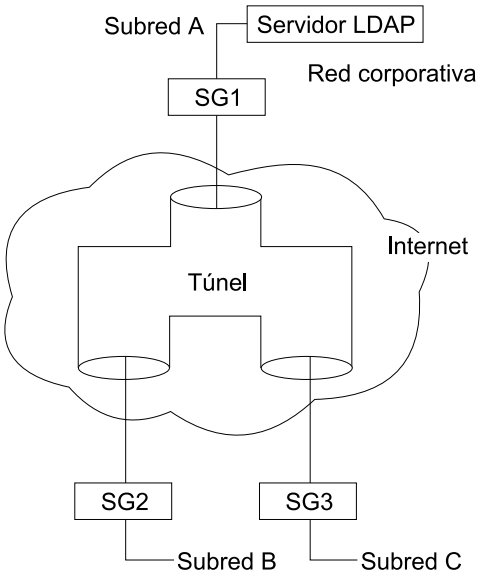


Figura 29. Protección del tráfico a través de Internet

Esta figura muestra un servidor LDAP de la subred A de la red corporativa. SG1, SG2 y SG3 buscan sus políticas en el servidor LDAP. La búsqueda de políticas para SG2 y SG3 se produce a través de Internet y está protegida mediante IPSec.

La información de configuración que necesita la base de datos de políticas para recuperar satisfactoriamente las políticas del directorio es:

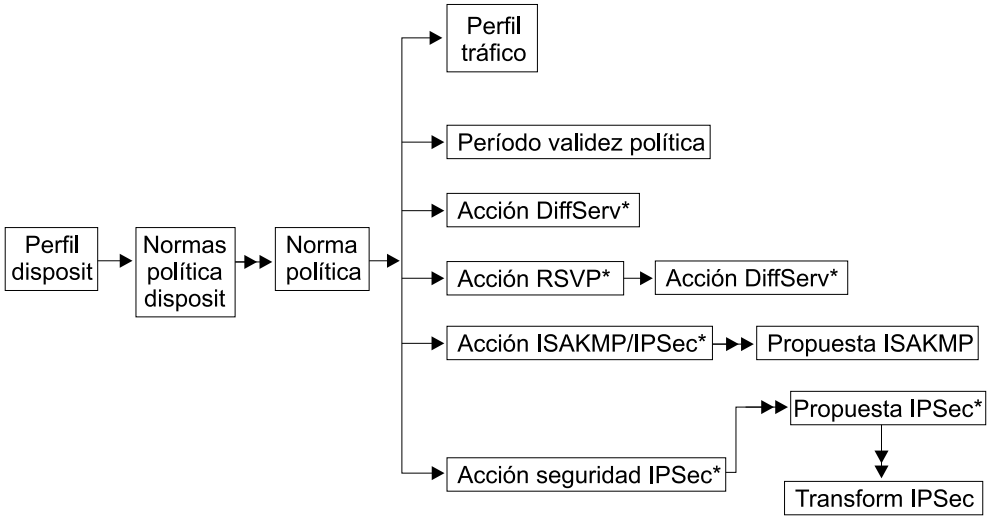
- Dirección IP del servidor principal (también se puede configurar un servidor secundario de reserva)
- Número de puerto en el que el servidor está a la escucha (nota: no se da soporte a SSL y TLS)
- El nombre de usuario y la contraseña son obligatorias
- Nombre base distinguido del objeto DeviceProfile para este direccionador o clase de direccionadores.
- Información de políticas por omisión

Cuando haya introducido esta información de configuración, la próxima vez que se renueve la base de datos de políticas se intentará conseguir la información de políticas al servidor de directorios. la base de datos de políticas permite una combinación de políticas configuradas localmente y reglas leídas del servidor LDAP. Si se dos reglas entran en conflicto y tienen la misma prioridad, la regla leída en la configuración local prima sobre la regla leída en el servidor de directorios.

Esquema de política

El esquema de LDAP es el conjunto de reglas e información que conforman las definiciones de clase y atributo que determinan el contenido de las entradas del directorio. Generalmente, el esquema de LDAP se graba en una sintaxis de ASN1, similar a las MIB del SNMP. El esquema de política al que da soporte esta familia de direccionadores es un trabajo que incluye algunos esfuerzos por desarrollar estándares realizados por el IETF. Se basa en el seguimiento realizado al trabajo

de desarrollo de estándares realizado por los grupos de trabajo de IPSec y de políticas del IETF y el del grupo de trabajo de políticas del DMTF. El esquema de política coincide en gran manera con los objetos de configuración existentes en la función de política del direccionador. Se pueden consultar encontrar los archivos de definición del esquema de política y los de configuración del servidor LDAP accediendo al URL: **http://www.networking.ibm.com/support**. Seleccione el producto de direccionador que desee y el enlace *Downloads*. La Figura 30 muestra la estructura global del esquema de política.



Notes:

1. La flecha → indica una referencia simple.
2. La flecha →→ 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 pasa al túnel seguro.

Figura 30. Estructura del esquema de política

DeviceProfile y DevicePolicyRules son dos objetos clave en el esquema de política. Habilitan el agente de búsqueda de políticas para localizar las políticas necesarias para el dispositivo. DeviceProfile contiene información acerca de la dirección IP administrativa del dispositivo y una referencia a DevicePolicyRules preceptiva. Se pueden agrupar dispositivos en objetos DeviceProfile o que cada dispositivo de la red tenga su propio DeviceProfile. La opción que se elija dependerá de si hay más de un dispositivo en la red que deba obtener el mismo conjunto de reglas. Esto no suele ser así para las pasarelas de seguridad, puesto que todas tienen un extremo final de túnel distinto. Para los dispositivos que no son de QoS, es probable que todos los dispositivos de un grupo lean el mismo conjunto de políticas.

El objeto DevicePolicyRules se recupera según el valor del DeviceProfile que se obtiene para el dispositivo. Una vez recuperado el objeto DevicePolicyRules, se puede recuperar la lista de PolicyRules para ese dispositivo. Si no se encuentra un objeto o si se detecta un error durante la comprobación de coherencia de un objeto, se cancela la búsqueda y se visualizan los mensajes en 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 manejarlas:

- Suprimir todas las políticas leídas localmente y volver a una regla de descartar todo o pasar todo.
- Mantener todas las políticas leídas localmente. Especifique esta opción con el mandato **set default** de la función de política.

En cualquier caso, se vuelve a intentar la búsqueda pasado el intervalo de reintentos configurado. Si no se puede conectar con el servidor LDAP principal, se intenta hacerlo con el servidor secundario después de 5 intentos. Si no se puede conectar con el servidor secundario, se vuelve a intentar con el servidor principal después de 5 intentos. Puede especificar el intervalo de reintentos con el mandato **set ldap retry-interval** de la función de política. Si falla una búsqueda debido a la latencia de la red, se puede cambiar el tiempo de espera por omisión de la búsqueda, que es de 3 segundos, mediante el mandato **set ldap search-timeout** de la función de política.

Generación de reglas

Configure una política para especificar cómo quiere que funcione la red. El direccionador convierte la información de políticas en un conjunto de reglas que compara con los flujos de tráfico. Antes, esto se hacía de forma manual definiendo los filtros de paquetes de entrada y salida para cada patrón de tráfico. La base de datos de políticas lo elimina, porque sólo deberá configurar una sola política.

La mayor parte del trabajo se realiza de forma interna cada vez que se construye la base de datos de políticas. En algunos casos, un direccionador convierte una política directamente en una sola regla. En el caso de ISAKMP/IPSec, convierte una política en cinco reglas. Son necesarias cinco reglas para dar cuenta de las direcciones del tráfico (entrada y salida) y para los flujos de control que se producen durante las negociaciones de IKE de las fases 1 y 2. La relación entre políticas y reglas es la siguiente:

Una política DiffServ → Una regla DiffServ

Una política RSVP → Una regla RSVP

Una política ISAKMP/IPSec → Cinco reglas ISAKMP/IPSec

Ejemplo: Proteja el tráfico de la subred A a la subred B; los extremos finales del túnel son SGa y SGb.

1. Entrada de fase 1 (Profile = SGb to SGa, Proto UDP, Src Port 500, Dst Port 500): Esta regla es necesaria para filtrar las negociaciones de fase 1 de entrada del igual ISAKMP remoto si el dispositivo funciona como responder ISAKMP.
2. Salida de fase 1 (Profile = SGa to SGb, Proto UDP, Src Port 500, Dst Port 500): Esta regla es necesaria para filtrar la información de fase 1 necesaria si el tráfico inicia las negociaciones de fase 1 de ISAKMP. En este caso, el dispositivo funciona como iniciador de ISAKMP.
3. Entrada de fase 2 (Profile = SGb to SGa, Proto UDP, Src Port 500, Dst Port 500): Esta regla es necesaria para filtrar el tráfico de fase 2 de

entrada del igual ISAKMP remoto. Este tráfico es el resultado del igual remoto que inicia una negociación inicial o renovación de fase 2. No es necesaria ninguna regla de salida de fase 2, puesto que el tráfico de salida (regla 5) siempre inicia las negociaciones si hace falta.

4. Tráfico hacia el túnel protegido (Profile = Subnet A to Subnet B): Esta regla es necesaria para colocar el tráfico no protegido en un túnel de seguridad. Si no se ha negociado la asociación de seguridad, se recopila también la regla de fase 1 e IKE inicia las fases 1 y 2. Cuando se han establecido los SA, los paquetes que coinciden con esta regla se entregan a IPSec para la encapsulación y transmisión.
5. Tráfico del túnel protegido (Profile = Subnet B to Subnet A): Esta regla es necesaria para asegurar que los paquetes que deberían haber llegado en un túnel protegido han llegado realmente en éste. Si el IPSec no ha desencapsulado el paquete y encuentra esta regla, se descarta el paquete. Esta regla maneja el tráfico que se cuela en la red.

Un túnel IPSec con claves manuales → Dos reglas IPSec

Ejemplo: Proteja el tráfico de la subred A a la subred B; los extremos finales del túnel son SGa y SGb.

1. Tráfico hacia el túnel protegido (Profile = Subnet A to Subnet B): Esta regla es necesaria para colocar el tráfico no protegido en un túnel de seguridad. Es un túnel configurado estáticamente para que esté siempre disponible y los paquetes que coinciden con esta regla se dirigen directamente a IPSec para la encapsulación y transmisión.
2. Tráfico del túnel protegido (Profile = Subnet B to Subnet A): Esta regla es necesaria para asegurar que los paquetes que deberían haber llegado en un túnel protegido han llegado realmente en éste. Si el IPSec no ha desencapsulado el paquete y encuentra esta regla, se descarta el paquete. Esta regla maneja el tráfico que se cuela en la red.

Se pueden ver estar reglas mediante el mandato de supervisión **list rule** de la función de política.

Ejemplos de configuración

Los siguientes ejemplos muestran cómo utilizar la función de política para configurar los direccionadores de una red. Primero, acceda a la función de política::

```
* talk 6
Config>feature policy
IP Network Policy configuration
```

Política IPSec/ISAKMP con QoS

Puede entrar la información de políticas de dos formas distintas. La primera es definir los objetos de política individuales y agruparlos después. Para utilizar este método, defina primero las transformaciones de IPSec y luego la propuesta de IPSec (que se refiere a las transformaciones de IPSec). Luego defina la acción IPSec (que se refiere a propuesta de IPSec) y así sucesivamente hasta que haya definido completamente la política. Con la Figura 31 en la página 323 como refe-

rencia, este método se inicia a la derecha de los objetos de política y funciona hasta la izquierda.

La segunda posibilidad, que es más fácil, es definir primero las opciones de política de un nivel superior y, según se le indique, entrar las definiciones para los objetos de política individuales según corresponda. Después de la Figura 31 se incluye un ejemplo de procedimiento de configuración que utiliza 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 ha definido anteriormente un objeto que cumpla sus necesidades, puede volver a utilizarlo en vez de crear una definición nueva. Por ejemplo, si se ha configurado un período de validez para allTheTime para una política anterior, puede utilizarlo. El siguiente procedimiento muestra todo el proceso, pero no muestra la reutilización de la información de políticas definida anteriormente. Para ver un ejemplo del uso de la información definida anteriormente, consulte el apartado “Política de sólo IPSec/ISAKMP” en la página 334.

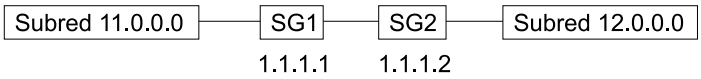


Figura 31. Configuración de IPSec/ISAKMP con QoS

El caso de configuración de política descrito en el siguiente texto es desde la perspectiva de SG1. La sentencia de política es:

Proteja el tráfico de la subred 11 a la subred 12 cuyos extremos finales del túnel son SG1 y SG2, y proporcione un QoS para el tráfico de este túnel mediante la acción GoldService de DiffServ.

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 ningún perfil configurado, por lo que debe definir uno nuevo.

```
List of Profiles:
        0: New Profile

Enter number of the profile for this policy [0]?
```

3. Definición de perfil nuevo; en este caso el tráfico que nos interesa es el de la subred 11 a 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 terminado con la definición del perfil y vuelto al menú de configuración de la política.

```
List of Profiles:
        0: New Profile
        1: trafficFrom11NetTo12Net

Enter number of the profile for this policy [1]? 1
```

5. No hay ningún período de validez configurado, 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. Cuestiones de configuración del período de validez; en este ejemplo el período de validez es de 9 de la mañana a 5 de la tarde, de lunes a viernes, todos los meses 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 terminado con la definición del período de validez y vuelto al menú de configuración de la 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. Defina siempre una acción IPSec nueva porque el extremo final del túnel será siempre distinto. Las excepciones son si hay varios túneles entre las dos pasarelas, y en las configuraciones de acceso remoto con comodines donde el extremo final del túnel es desconocido.

```
IPSEC Actions:
        0: New IPSEC Action

Enter the Number of the IPSEC Action [0]?
```

9. Menú de acción 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 ninguna propuesta de IPSec configurada, por lo que debe definir una nueva. Tenga en cuenta que cuando se haya definido la propuesta de IPSec, se puede volver a utilizar en las múltiples acciones IPSec.

```
List of IPSEC Proposals:
        0: New Proposal

Enter the Number of the IPSEC Proposal [0]?
```

11. Configure la 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 ninguna transformación de ESP configurada, por lo que debe definir una nueva. Cuando haya definido la transformación de ESP, cualquier propuesta de IPSec puede volver a utilizarla.

```
List of ESP Transforms:
        0: New Transform

Enter the Number of the ESP transform [0]? 0
```

13. Configure la transformación 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 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 IPSec protegida, por lo que debe identificar una acción ISAKMP para las negociaciones de la fase 1. No hay ninguno definido, debe entrar uno nuevo. En la mayoría de los casos, son suficientes una propuesta y una acción ISAKMP para todas las políticas de seguridad.

```
ISAKMP Actions:
        0: New ISAKMP Action

Enter the Number of the ISAKMP Action [0]?
```

18. Configure la acción 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 ninguna propuesta ISAKMP configurada, por lo debe crear una nueva.

```
List of ISAKMP Proposals:
        0: New Proposal
```

20. Configure la 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 acción 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 la 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. Configure la acción DiffServ.

    Si la acción DiffServ es para la cola garantizada:

```
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 DiffServ es para la cola preferente:

```
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 la 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 se han habilitado DiffServ o IPSec, se le advierte que antes de que se aplique la política, debe habilitar DiffServ, IPSec o ambos (la función DiffServ o 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 es añadir una definición de perfil de USUARIO para el igual ISAKMP remoto. Este paso no es necesario si las negociaciones ISAKMP deben autenticar el igual con certificados públicos. Sin embargo, en el ejemplo anterior hemos elegido la clave previamente compartida como método de autenticación, por lo que hay que identificar el usuario y entrar la clave previamente compartida que esperamos que utilice el igual.

```
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 han finalizado. Si desea configurar DiffServ, IPSec, o cualquier red o configuración de IP, debe hacerlo antes de que el túnel IPSec funcione. El siguiente ejemplo de mandato list muestra la configuración que se acaba de realizar. Para activar estos cambios, vuelva a cargar el dispositivo o escriba el mandato de supervisión **reset database** de la función 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
 ------  --------------  ---------------  ---------------  -----  --------
```

Política de sólo IPSec/ISAKMP

Un ejemplo de procedimiento de configuración, que sigue a la Figura 32 y utiliza valores que corresponden a los de la figura, utiliza el método de izquierda a derecha y muestra cómo crear sobre el ejemplo de procedimiento anterior volviendo a utilizar la información que ha creado la anterior.

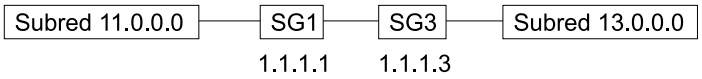


Figura 32. Configuración de IPSec y utilización de una definición anterior

El caso de configuración de política descrito en el siguiente texto es desde la perspectiva de SG1. La sentencia de política en este caso es:

Proteja el tráfico de la subred 11 a la subred 13 (sólo el tráfico TCP) cuyos extremos finales del túnel son SG1 y SG3, y no proporcione ningún 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 definida anteriormente.

```
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]:
```

Descartar todo el tráfico público (regla de filtro)

Este ejemplo de política muestra cómo configurar una regla de descarte sencilla para la interfaz pública que descarta todo el tráfico que no está protegido mediante el IPSec. Esta regla es muy general y **debe** tener la menor prioridad de todas las reglas configuradas.

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 perfil nuevo que incluya todo el tráfico de entrada o salida de la interfaz pública (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. Puesto que la información de origen o destino (o ambas) se han separado con un comodín, debe especificar las interfaces de las que espera que llegue y salga el tráfico.

```
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 entra a través de la interfaz pública. Déle el mismo nombre que al 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 período de validez que especifique `all the time`.

```
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 acción IPSec nueva para descartar 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 motor de búsqueda de políticas LDAP

Este ejemplo muestra cómo configurar y habilitar el motor de búsqueda de políticas LDAP En este ejemplo hay dos directorios LDAP (uno principal y uno secundario) con direcciones IP de 11.0.0.2 y 13.0.0.1 respectivamente. Los dos están a la escucha en el puerto 389 de TCP y el dispositivo debe enlazarse con el servidor LDAP como cn=router, password miContraseña. La entrada base en el árbol del directorio para las políticas del direccionador es cn=RouterDeviceProfile,o=ibm,c=us.

Nota: Actualmente, los servidores LDA primario y secundario deben estar a la escucha en el mismo puerto y tener las mismas credenciales de autenticación para el direccionador. El DeviceProfile debe ser el mismo para el direccionador de los dos servidores de directorios.

Este ejemplo muestra también cómo establecer la política por omisión para que las comunicaciones de LDAP estén protegidas a través del IPSec. Este ejemplo utiliza una clave previamente compartida para la autenticación de ISAKMP, y SHA y 3DES para los parámetros de autenticación y cifrado para las fases 1 y 2. El extremo inicial del túnel es 1.1.1.4 para el dispositivo que lleva a cabo la búsqueda de políticas de LDAP y los extremos finales del túnel son 1.1.1.1 para el servidor LDAP 11.0.0.1 y 1.1.1.3 para el servidor LDAP 13.0.0.1.

1. Configure y habilite el motor de búsqueda de políticas 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 miContraseña
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:                   miContraseña


        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 momento, está listo para gestionar los direccionadores de la red con la función de política. Para obtener información detallada sobre los mandatos utilizados para configurar los parámetros de política necesarios como perfiles, propuestas, transformaciones y acciones, consulte los apartados “Mandatos de configuración de políticas” en la página 353, “Mandatos de configuración del servidor de políticas de LDAP” en la página 374 y “Mandatos de supervisión de políticas” en la página 379.

Ejemplo de configuración rápida de política

El mandato **qconfig** disponible en la función de política permite añadir rápidamente una política basada en un caso de cuatro disponibles. Se le harán unas sencillas preguntas. Dependiendo de las respuestas, se generarán unos objetos de política u otros. El mandato **qconfig** saca partido de las plantillas de políticas predefinidas para minimizar las preguntas que es necesario realizar para determinar la configuración. No se pueden cambiar los objetos de política mediante el mandato **qconfig**; sólo sirve para añadir políticas rápidamente. Consulte el apartado “Mandatos de configuración de políticas” en la página 353 para obtener más información sobre este mandato.

El ejemplo siguiente reproduce el ejemplo de IPSec/ISAKMP descrito al principio del capítulo. Brevemente, el objetivo es proteger y autenticar el tráfico que va de la subred 11.0.0.0 a la subred 12.0.0.0 con SG1 y SG2. Además, al tráfico protegido por esas pasarelas de seguridad se le debe ofrecer un QoS. En este ejemplo, el QoS es AF11 y se elige un tipo de 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

Los objetos de política siguientes se han definido previamente. Estos objetos representan las configuraciones más habituales y se pretende que puedan utilizarse para muchas configuraciones de políticas. Estas definiciones de objetos de política predefinidos con el mandato **qconfig** proporcionan una forma fácil de añadir políticas en la configuración de una red. Las plantillas predefinidas no pueden cambiarse ni suprimirse. Si se quiere cambiar un objeto, deberá copiarlo con el mandato **copy**, y especificar un nombre nuevo. Una vez copiado, podrá cambiar la copia. Si se actualiza a un release nuevo o a una versión PTF del código y las plantillas se han modificado, será necesario ejecutar el mandato de configuración **refresh-templates** de la función de política para obtener las plantillas más recientes; de lo contrario, continuarán utilizándose las definiciones originales.

Existen los siguientes objetos predefinidos de la función política:

Períodos de validez

Se han predefinido los siguientes objetos de períodos de validez:

```
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 DiffServ

Se han predefinido los siguientes objetos de acciones DiffServ:

```
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 IPSec

Se han predefinido los siguientes objetos de acciones IPSec:

```
IPSECAction Name = ipsecDropTraffic
        Action   = Drop

IPSECAction Name = ipsecPassTrafficClear
        Action   = Clear
```

Propuestas de IPSec para la fase 2 de IKE

Se han predefinido los siguientes objetos de propuesta de IPSec 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 siguientes objetos de transformaciones de IPSec:

```
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 ISAKMP

Se han predefinido los siguientes objetos de acciones ISAKMP:

```
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 siguientes objetos de propuestas de ISAKMP:

```
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 función de política

Este capítulo describe los mandatos de política y LDAP proporcionados por la función de política para configurar y utilizar los dispositivos de direccionador de una red. Incluye los siguientes apartados:

Acceso al indicador de configuración de políticas

Para entrar los mandatos de configuración de políticas:

1. Entre **talk 6** en el indicador OPCON (*).
2. Entre **feature policy** en el indicador Config>.

Aparecerá el indicador Policy config>. Ahora puede entrar los mandatos de configuración de políticas.

Mandatos de configuración de políticas

Estos mandatos le permiten configurar la información contenida en las políticas. La Tabla 38 resume los mandatos de configuración de políticas y el resto de este apartado los describe detalladamente. Escriba estos mandatos en el indicador Policy config>. Puede entrar el mandato y las opciones en una línea o entrar sólo el mandato y responder a las indicaciones. Para ver una lista de las opciones del mandato válidas, en lugar de escribir el mandato con las opciones, escríbalo con un interrogante.

Tabla 38. Mandatos de configuración de políticas

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 xxxii.
Add	Añade la información utilizada para crear una política.
Change	Cambia la información que constituye 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	Muestra la información de una política.
Qconfig	Le permite añadir una política basada en plantillas predefinidas.
refresh-templates	Permite instalar o eliminar las plantillas más recientes de la versión del código que se está ejecutando en una plataforma dada. Esto facilita cambiar entre distintos releases y niveles de PTF.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxiii.

Add

Utilice el mandato **add** para añadir información en 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 acerca de las selecciones de DiffServ-action que se deben aplicar. Consulte los apartados “Utilización de la función de servicios diferenciados” en la página 449 y “Configuración y supervisión de la función de servicios diferenciados” en la página 457 para obtener más detalles.

name El nombre exclusivo de la acción DiffServ para la política.

permission level Especifica si el direccionador debe reenviar los paquetes que coincidan con esta acción DiffServ.

1
Permitir

2
Denegar

Valor por omisión: 2

queue number La cola donde se colocan los paquetes de salida que coinciden con esta acción DiffServ.

1
Preferente (EF)

2
Garantizada (AF)/Optimizada

Valor por omisión: 2

bwshare type El tipo de asignación de compartimento de ancho de banda.

1
Absoluto (en kbps)

2
Porcentaje (del total de ancho de banda de salida)

Valor por omisión: 2

bwshare Ancho de banda (en kbps o como porcentaje del ancho de banda de salida) asignado a este servicio.

Reenvío garantizado

Assured forwarding class Indica la clase de reenvío garantizado para los paquetes de salida que coinciden con esta acción DiffServ.

1
Byte DS de la clase AF1

2
Byte DS de la clase AF2

3
Byte DS de la clase AF3

4
Byte DS de la clase AF4

5
Clase nueva

Assured forwarding policing type Indica el tipo de vigilancia AF para los paquetes de salida que coinciden con esta acción DiffServ.

1
TCM de una tasa, no sensible a los colores

2
TCM de una tasa, sensible a los colores

3
TCM de dos tasas, no sensible a los colores

4
TCM de dos tasas, sensible a los colores

5
Ninguno

Parámetros de TCM de una tasa

Committed information rate (CIR) Especifica la tasa de información comprometida.

Committed burst size (CBS) Especifica el tamaño de ráfagas comprometido.

Excess burst size (EBS) Especifica el tamaño de ráfagas en exceso.

Notas:

1. Especifique la CIR en bytes de paquetes IP por segundo. Se 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 manera que al menos uno de ellos sea mayor que cero. Se recomienda que el valor del CBS o del EBS que sea mayor que cero, sea mayor o igual que el tamaño del paquete IP más grande posible de la corriente.

Parámetros de TCM de dos tasas

Committed information rate (CIR) Especifica la tasa de información comprometida.

Committed burst size (CBS) Especifica el tamaño de ráfagas comprometido.

Peak information rate (PIR) Especifica la tasa de información pico.

Peak burst size (PBS) Especifica el tamaño de ráfagas pico.

Notas:

1. Especifique la CIR y la PIR en bytes de paquetes IP por segundo. Se incluye la cabecera IP, pero no la cabecera específica del enlace. El valor de la PIR deber ser igual o mayor que el de la CIR.
2. Especifique el CBS y el PBS en bytes. Ambos deben configurarse con valores mayores que cero, y mayores o iguales que el tamaño del paquete IP más grande posible de la corriente.

Reenvío acelerado

transmitted ds-byte mask Máscara que se debe aplicar a los bytes de ds transmitidos para el reenvío acelerado. Este valor indica qué bits del byte DS de un paquete se deben cambiar cuando se transmite el paquete. Un cero en cualquier posición de bit de este byte implica que el bit no se debe cambiar.

Valor por omisión: 00 (no se cambia ningún bit)

transmitted ds-byte modify value Marca del byte DS (TOS) de IP para el reenvío acelerado que debe aplicarse a los paquetes que reenviará este dispositivo. Los ceros de la máscara implican que el bit correspondiente no se cambiará. Un uno implica que el bit se marcará con el valor de bit del byte de marca. La operación es: newTOSByte = (Mask & receivedTOSByte) | (Mask&Mark) El ^ ∧ es un complemento basado en bits (Mask:Mark)

Ejemplo:

```
11111101:00000001
```

En este ejemplo, un valor recibido de 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 vigilancia del reenvío acelerado.

1
Configuración por omisión

Los parámetros tasa de reposición de fichas y tamaño del contenedor de fichas se calcularán a partir de la configuración del parámetro ancho de banda.

2
Configuración a medida

Token Rate: Tasa de reposición de fichas.

Token Bucket Size: Tamaño del contenedor de fichas.

Notas:

1. Especifique la tasa de reposición de fichas en bytes de paquetes IP por segundo. Se incluye la cabecera IP, pero no las cabeceras específicas del enlace.
2. Especifique el tamaño del contenedor de fichas en bytes. El valor debe ser mayor que cero y mayor o igual que el tamaño del paquete IP más grande posible de la corriente.

interface-pair
El par de interfaces asocia un perfil con una interfaz específica o un conjunto de interfaces. Por omisión, el objeto de perfil no restringe la aplicación de la política a ninguna interfaz. Si es 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 entra en cualquier interfaz y sale de la interfaz pública y a la inversa.

```
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 fase 2.

Name
El nombre de la acción IPSec.

Action type
La acción que se aplicará a los paquetes que coincidan con el perfil de una política que contenga esta acción.

1 Bloquear (bloquear conexión).

2 Permitir (permitir los paquetes que coincidan con esta acción). Si no existe ninguna propuesta de IPSec, pasar el paquete; si existe una propuesta de IPSec, aplicar el proceso de seguridad IPSec en el paquete.

Valor por omisión: 2

La siguiente opción sólo está disponible si especifica pasar como tipo de acción:

Traffic flow type
Tipo de flujo de tráfico (túnel protegido o tráfico desprotegido).

1
Tráfico desprotegido

2
Túnel protegido

Valor por omisión: 2

La siguiente opción sólo está disponible si especifica el flujo de tráfico en protegido:

Tunnel start point
Dirección IPv4 del extremo inicial del túnel.

Tunnel end point
Dirección IPv4 del extremo final del túnel. (0.0.0.0 para el acceso remoto)

Valor por omisión: 0.0.0.0

Tunnel-in-tunnel
Especifica si el tráfico protegido por este túnel debe protegerlo también otra política configurada en este dispositivo.

Opciones válidas: Yes o No

Valor por omisión: No

Percentage of SA lifesize/lifetime to accept
Duración mínima de la SA (como porcentaje) de la duración de la SA. No se aceptará una duración con un valor inferior a éste.

Valor por omisión: 75

SA refresh threshold
El porcentaje en la duración de la SA o el valor de duración en que se debe renovar automáticamente la SA.

Valor por omisión: 85

DF-Bit-Setting
Especifica si se debe copiar el bit No fragmentar (DF) del paquete original y si se debe establecer o borrar en la cabecera exterior del paquete de IPSec si se ejecuta en modalidad de túnel.

1
Copiar

2
Establecer

3
Borrar

Valor por omisión: 1

Replay-Prevention
Especifica si el IPSec debe aplicar la prevención de repetición para los paquetes de IPSec recibidos. En esta modalidad, el IPSec asegura que los números de secuencia son válidos y no se reciben más de una vez.

1
Habilitar

2
Inhabilitar

Valor por omisión: 2

Negotiate SA Automatically
Especifica si el SA de la fase 2 se negocia automáticamente en la inicialización del sistema.

Yes o No

Valor por omisión: No

IPSec proposal
El nombre de la propuesta de IPSec (puede especificar hasta cinco propuestas) que se enviará o comprobará durante la fase 2. El orden en que se especifiquen determinará su prioridad: la primera será la superior.

IPSec-manual-tunn
Le solicita información para configurar manualmente el túnel de fase 2.

Tunnel name
El nombre del túnel manual de IPSec.

Tunnel lifetime
La duración del túnel (en minutos).

Valor por omisión: 46080

Encapsulation mode
La modalidad de encapsulación que se utilizará.

tunn
Modalidad del túnel

trans
Modalidad de transporte

Valor por omisión: tunn

Policy
El tipo de política de túnel que se utilizará.

AH
Cabecera de autenticación

ESP
Protocolo ESP (Encapsulating Security Payload)

AH-ESP
Para los paquetes de salida, especifica que el cifrado se ejecuta antes que la autenticación.

ESP-AH
Para los paquetes de salida, especifica que la autenticación se ejecuta antes que el cifrado.

Valor por omisión: AH-ESP

Local IP address
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
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 se va a utilizar la autenticación de ESP local.

Yes o No

Valor por omisión: Yes

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
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 se verificará el relleno de cifrado remota.

Yes o No

Valor por omisión: No

Remote ESP authentication
Especifica si se va a utilizar la autenticación de ESP remota.

Yes o No

Valor por omisión: Yes

DF bit
Especifica cómo se debe procesar el bit No fragmentar (DF).

Copy
Copia el bit DF.

Set
Activa el bit DF.

Clear
Desactiva el bit DF.

Valor por omisión: COPY

Enable tunnel
Especifica si se debe habilitar el túnel cuando se cree.

Yes o No

Valor por omisión: Yes

IPSec-proposal
Le solicita información para la creación de una propuesta de IPSec.

IPSec proposal name
El nombre de la propuesta de IPSec.

Perfect forward secrecy
Especifica si se va a utilizar el IKE, para evitar que cualquiera determine una clave actual desde una clave concedida anteriormente.

Yes o No

Valor por omisión: No

Diffie Hellman Group ID
El tipo de grupo Diffie Hellman.

1
Diffie Hellman Grupo 1

2
Diffie Hellman Grupo 2

Valor por omisión: 1

AH transform
El nombre de la transformación de AH (puede especificar hasta cinco transformaciones) para esta propuesta. El orden en que se especifiquen determinará su prioridad: la primera será la superior.

ESP transform
El nombre de la transformación de ESP (puede especificar hasta cinco propuestas) para esta propuesta. El orden en que se especifiquen determinará su prioridad: la primera será la superior.

IPSec-transform
Le solicita información acerca de las transformaciones de IPSec.

IPSec transform name
El nombre de la transformación de IPSec.

Protocol ID
El protocolo de seguridad que se utilizará.

1
IPSec-AH

2
IPSec-ESP

Valor por omisión: 1

AH Authentication Algorithm
El algoritmo de autenticación de AH que se utilizará.

1
HMAC-MD5

2
HMAC-SHA

Valor por omisión: 1

Encapsulation mode
La modalidad de encapsulación que se utilizará.

1
Túnel

2
Transporte

Valor por omisión: 1

ESP Authentication Algorithm
El algoritmo de autenticación de ESP que se utilizará.

0
Ninguno

1
HMAC-MD5

2
HMAC-SHA

Valor por omisión: 2

ESP cipher algorithm
El algoritmo de cifras de ESP que se utilizará.

1
ESP DES

2
ESP 3DES

3
ESP CDMF

4
ESP Null (sin cifrado)

Valor por omisión: 1

SA lifesize
La 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 acerca de la acción ISAKMP que se aplicará.

Name
El nombre de la acción ISAKMP.

Exchange mode
El tipo de modalidad de intercambio para las negociaciones de fase 1.

1
Principal

2
Agresiva

Valor por omisión: 1

Percentage of Minimum SA lifesize/lifetime
Duración mínima de la SA (como porcentaje) de la duración de la SA. No se aceptará una duración con un valor inferior a éste.

Valor por omisión: 75

ISAKMP connection lifesize
La duración (en kb) de la conexión de fase 1. Cuando caduca la conexión de fase 1, la siguiente vez que se debe renovar la SA de la fase 2, la fase 1 vuelve a negociar completamente antes de que se inicie la fase 2.

Valor por omisión: 5000

ISAKMP connection lifetime
La duración (en segundos) de la conexión de fase 1. Cuando caduca la conexión de fase 1, la siguiente vez que se debe renovar la fase 2, la fase 1 se inicia completamente.

Valor por omisión: 5000

Negotiate SA automatically
Especifica si el SA se negocia automáticamente en la inicialización del sistema.

Yes o No

Valor por omisión: No

ISAKMP proposal
El nombre de la propuesta de ISAKMP (puede especificar hasta cinco propuestas) que se enviará o comprobará durante la modalidad rápida de fase 2. El orden en que se especifiquen determinará su prioridad: la primera será la superior.

ISAKMP-Proposal
Le solicita la información de propuesta de ISAKMP utilizada en las negociaciones de ISAKMP.

ISAKMP proposal name
El nombre de la propuesta de ISAKMP.

Authentication method
El tipo de autenticación que se utilizará durante las negociaciones de fase 1 de ISAKMP.

1
Clave previamente compartida

2
RSA SIG (modalidad certificada)

Valor por omisión: 1

Hash algorithm
El tipo de algoritmo hash que se utilizará durante las negociaciones de fase 1.

1
MD5

2
SHA

Valor por omisión: 1

Cipher algorithm
El tipo de algoritmo de cifras que se utilizará durante las negociaciones de fase 1.

1
DES

2
3DES

Valor por omisión: 1

Diffie Hellman Group ID
El tipo de grupo Diffie Hellman que se utilizará durante las negociaciones de fase 1.

1
Diffie Hellman Grupo 1

2
Diffie Hellman Grupo 2

Valor por omisión: 1

SA lifesize
La 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 acerca de la configuración de la política: nombre de perfil (obligatorio), 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: Válido siempre

Name El nombre de configuración de la política

Priority Prioridad relativa de esta política respecto a otras políticas (cuanto más alto es el número, más alta es la prioridad). Se utiliza para resolver conflictos si se aplican múltiples políticas a un paquete.

Valor por omisión: 5

Profile El nombre de un perfil de tráfico de datos configurado anteriormente que se utilizará para esta política.

Validity period El nombre de un período de validez configurado anteriormente que se utilizará para esta política.

IPSec action Si esta política aplicará una acción IPSec, el nombre de una acción IPSec configurada anteriormente que se utilizará para esta política. Si especifica una acción IPSec segura, también debe especificar una acción ISAKMP.

ISAKMP action El nombre de una acción ISAKMP configurada anteriormente que se utilizará para esta política. Si especifica una acción ISAKMP segura, también debe especificar una acción IPSec.

Diffserv action Si desea correlacionar una acción DiffServ con esta política, el nombre de una acción DiffServ configurada anteriormente.

RSVP action El nombre de una acción RSVP que aplicará esta política.

Profile
Le solicita información para definir un conjunto de selectores (condicionales) para un perfil de política en la que se llevarán a cabo acciones.

name
El nombre del perfil de política

ipv4-src-address-format
El formato de la dirección IPv4 de origen (rango, máscara de red, dirección única).

ipv4-src-address
La dirección IPv4 de origen (dirección baja si el formato de dirección es *rango*).

Valor por omisión: 0.0.0.0

ipv4-src-mask
La máscara IPv4 de origen (dirección alta si el formato de dirección es *rango*).

Valor por omisión: 255.0.0.0

ipv4-dest-address-format
El formato de la dirección IPv4 de destino (rango, máscara de red, dirección única).

ipv4-dest-address
La dirección IPv4 de destino (dirección baja si el formato de dirección es *rango*).

Valor por omisión: 0.0.0.0

ipv4-dest-mask
La máscara IPv4 de destino (dirección alta si el formato de dirección es *rango*).

Valor por omisión: 255.0.0.0

protocol-id
El ID de protocolo para el que se aplicarán filtros.

1
TCP

2
UDP

3
Todos los protocolos

4
Especificar rango

Valor por omisión: 3

src-port-start
El primer número de puerto del rango de números de puerto de origen.

Valor por omisión: 0

src-port-end
El último número de puerto del rango de números de puerto de origen.

Valor por omisión: 65535

dest-port-start
El primer número de puerto del rango de números de puerto de destino.

Valor por omisión: 0

dest-port-end
El último número de puerto del rango de números de puerto de destino.

Valor por omisión: 65535

src-id-type
El tipo de ID de origen, que se envía a la ubicación remota. Este valor se utiliza para determinar la política que contiene la información de ISAKMP necesaria durante las negociaciones de fase 1 de ISAKMP. Se compara con la información de la carga de útil de identificación del paquete ISAKMP. Esta información es necesaria si el igual remoto debe identificar el dispositivo con un valor distinto a la dirección IP.

1
Extremo final de túnel local

2
Nombre de dominio totalmente calificado del sistema principal

3
Nombre de dominio totalmente calificado del usuario

4
ID de clave

any-user-access
Permite el acceso para cualquier usuario que se encuentre en la definición de perfil. Si ha especificado que No, se le solicitará el nombre del grupo de usuarios remotos de ese perfil. Este atributo sólo es necesario si quiere limitar el acceso de iguales remotos a una política específica.

Yes o No

Valor por omisión: Yes

Received DS byte mask
La máscara de 8 bits que se aplicará al byte DS (TOS) de un paquete de entrada.

Valor por omisión: 0

Received DS byte match
El patrón de 8 bits que se utilizará para comparar el resultado de aplicar una operación AND en el byte DS (TOS) de entrada con el valor de máscara de byte DS recibido.

Valor por omisión: 0

Interface pairs
Si esta política debe restringir los flujos de tráfico a interfaces específicas, es el nombre del grupo de pares de interfaces.

RSVP-Action
Le solicita información acerca de las acciones RSVP que se aplicarán.

Name
El nombre de la acción 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
La cantidad máxima de ancho de banda (en kbps) que RSVP asignará para un flujo individual.

Valor por omisión: 100

Max duration
La cantidad máxima de tiempo (en segundos) que puede durar un flujo (0 significa siempre).

Valor por omisión: 600

RSVP-to-DS
Especifica si se deben correlacionar los flujos de RSVP que coinciden con esta acción con una acción DiffServ configurada. RSVP utiliza la información de la acción DiffServ para marcar el byte TOS para el siguiente dispositivo ascendente habilitado con DiffServ. Esto es para utilizarlo en una red en la que los paquetes dejan una red habilitada con RSVP en una red habilitada con DiffServ.

Yes o No

Valor por omisión: No

User
Le solicita información sobre la definición del perfil de usuario para el igual IKE remoto. Entre esta información se incluye: cómo debe identificarse el igual durante las negociaciones de la fase 1, qué método de autenticación utilizar para este igual y, si el mecanismo de identificación es mediante el uso de una clave previamente compartida, qué clave utilizar. Si se utiliza una clave previamente compartida, se **deberá** definir un usuario para poder asociar la clave previamente compartida con un tipo de ID y un nombre. Este mandato establece para un usuario concreto la clave que se utilizará en la negociación de la fase 1. La clave la utilizan los iniciadores en los mensajes 1 y 5 y los que los responden, en los mensajes 2 y 6.

Identification
Identificación del usuario. Para la autenticación de la modalidad principal, el tipo de identificación del usuario **debe** ser la dirección IP. Para la autenticación de la modalidad agresiva, el tipo de identificación debe ser uno de los otros tipos. La razón es que en la modalidad principal los ID no se intercambian hasta los mensajes 5 y 6, lo que es demasiado tarde para la clave previamente compartida, de modo que el único mecanismo de búsqueda es mediante la dirección IP del igual IKE. En la modalidad agresiva, los ID se intercambian en los mensajes 1 y 2, por lo que la búsqueda de la clave previamente compartida puede realizarse mediante el tipo de ID y el valor correspondiente.

1 Dirección IP.

2 Nombre de dominio totalmente calificado.

3 Nombre de dominio totalmente calificado del usuario.

4 ID de clave (cualquier serie de caracteres).

Valor por omisión: 1

Group
Nombre del grupo en el que colocar este usuario.

Valor por omisión: ninguno

Authentication
Método de autenticación que utilizar con el igual.

1 Clave previamente compartida.

1 Clave en formato ASCII.

Valores válidos: Un número par de entre 2 y 128 caracteres

2 Clave en formato hexadecimal.

Valores válidos: Un número para de entre 2 y 256 dígitos hexadecimales

2 Certificado público.

Valor por omisión: 1

VALIDITY-PERIOD
Le solicita información acerca del período de validez de la política y crea un perfil de política.

Name
El nombre del perfil de período de validez.

yyyymmddhhmmss:yyyymmddhhmmss
El período durante el cual son válidas las políticas que contiene este perfil de período de validez.

Ejemplo:

```
19980101000000:19981231000000
```

Months
Los meses durante los cuales son válidas las políticas que contienen este perfil de período de validez. Puede especificar cualquier secuencia de meses, utilizando las tres primeras letras de cada mes en inglés (por ejemplo jan o dec), con los meses separados por espacios o puede especificar `all` para indicar todos los meses del año.

Days
Las fechas en las que son válidas las políticas que contienen este perfil de período de validez. Puede especificar cualquier secuencia de días, utilizando las tres primeras letras de cada día en inglés (por ejemplo mon o fri), con los días separados por espacios o puede entrar `all` para especificar todos los días de la semana.

Starting time
La hora en que son válidas las políticas que contienen este perfil de período de validez. Especifique esta opción en el formato hh:mm:ss o * si quiere que la política sea válida todo el día.

Valor por omisión: *

Ending time
La hora en que caduca la validez de las políticas que contienen este perfil de período de validez. Especifique esta opción en el formato hh:mm:ss.

Valor por omisión: Ninguno

Change

Utilice el mandato **change** para cambiar la información en un objeto de política. Consulte la descripción del mandato **add** para 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 los objetos disponibles. (El par de interfaces, el túnel manual y las opciones de usuario, 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 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 se inhabilitará.

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 se habilitará.

List

Utilice el mandato **list** para visualizar la información que desee de la configuración de política.

Sintaxis: list all
default-policy
ldap
refresh

All Muestra toda la información de la configuración de política.

Default-policy
Muestra el nombre de la política por omisión.

LDAP
Muestra los nombres de las configuraciones de LDAP definidas.

Refresh
Lista el estado de renovación de la política (habilitado o inhabilitado) y el tiempo del intervalo de renovación.

Qconfig

Utilice el mandato **qconfig** para crear rápidamente políticas de seguridad para un dispositivo de red. Después de seleccionar uno de los casos de configuración que se ofrecen en una corta lista, el mandato mostrará una breve serie de preguntas sencillas basadas en la selección. A continuación, se creará una política completa (conjuntos cerrados de opciones de políticas compatibles) utilizando plantillas predefinidas relacionadas con el caso. Esto elimina la necesidad de que el usuario tenga que especificar todos los detalles de la política, reduciendo el tiempo necesario para configurar una política y la posibilidad de cometer un error.

Este mandato solicita al usuario que especifique un nivel de seguridad para todos los casos, excepto el caso "Custom" (a medida).

Sintaxis: qconfig *nombre-política*
caso

nombre-política
Especifica un nombre de como máximo 29 caracteres que asignar a la política.

Valor por omisión: Un nombre exclusivo generado por el sistema.

caso
Especifica el caso para el que se creará una política.

Valor por omisión: ninguno

1 Caso de una sucursal.

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:

Subred IP local

Extremo final del túnel IP local

Subred IP remota

Extremo final del túnel IP remoto

Puertos y protocolos

Nivel de seguridad

1: Strong Security. Seleccione esta opción si lo que se quiere es seguridad, rendimiento y flexibilidad. Negociará un conjunto de propuestas (sin PFS) que incluye combinaciones de los algoritmos de autenticación SHA y MD5 y de los algoritmos de cifrado DES y 3DES. Las propuestas fuertes se negocian primero, seguidas de las propuestas más fuertes, por lo que no se compromete el rendimiento.

2: Very Strong Security. Elija esta opción si se quiere es nivel más alto de seguridad. Negociará un conjunto reducido de propuestas (con PFS, Grp 1) que incluye combinaciones de los algoritmos de autenticación SHA y MD5 y de los algoritmos de cifrado 3DES.

Método de autenticación

1: Clave previamente compartida - clave ASCII

2: Certificado (firmas RSA) - ID local

Acciones DiffServ

0:Optimizada (sin DiffServ)

1:EF

2:AF11

3:AF21

4:AF31

5:AF41

También aparecerán en la lista las otras acciones DiffServ que se hayan configurado localmente.

Períodos de validez

1. 1: allTheTime
2. 2: allTheTimeMonThruFri
3. 3: 9to5MonThruFri
4. 4: 5to9MonThruFri

También aparecerán en la lista los otros períodos de tiempo que se hayan configurado localmente.

Prioridad de la política

2 Caso de usuario que accede de forma remota (IPSec y L2TP).

Esta selección le permite especificar las opciones de política para una conexión protegida entre una pasarela de seguridad y un usuario que accede de forma remota. En este caso se supone que el cliente que accede de forma remota puede ejecutar L2TP sobre IPSec en la modalidad de transporte.

L2TP configura una conexión punto a punto entre la dirección IP pública del cliente que accede de forma remota y la dirección IP pública de la pasarela de seguridad. UDP proporciona la conexión de la capa de transporte y el puerto de origen y de destino es el 1701. Es importante que L2TP se configure en el direccionador que realice funciones de pasarela de seguridad con la opción fixed-udp-source-port. IPSec proporciona la protección para la conexión L2TP en esos puertos y protocolos.

Cuando se ha terminado la configuración del caso, se deben añadir usuarios a la función de política para aquellas personas que se autenticarán utilizando una clave previamente compartida. Para realizar la autenticación mediante certificados, se deben configurar en el direccionador los parámetros PKI y asegurarse de que se cargan los certificados adecuados.

Las opciones son:

Dirección IP de interfaz segura.

Generalmente tiene el mismo valor que el del extremo final del túnel IP local. Representa la dirección IP de la interfaz desde la que se envían y se reciben paquetes protegidos.

Nivel de seguridad

1: Strong Security

2: Very Strong Security

Acciones DiffServ

0:Optimizada (sin DiffServ)

1:EF

2:AF11

3:AF21

4:AF31

5:AF41

También aparecerán en la lista las otras acciones DiffServ que se hayan configurado localmente.

Períodos de validez

1. 1: allTheTime
2. 2: allTheTimeMonThruFri
3. 3: 9to5MonThruFri
4. 4: 5to9MonThruFri

También aparecerán en la lista los otros períodos de tiempo que se hayan configurado localmente.

Prioridad de la política

3 Descartar el tráfico que no coincide en una interfaz que no es de confianza. Este caso es necesario para las configuraciones en las que el dispositivo actúa de cortafuegos. En muchas configuraciones de red, delante de la pasarela de seguridad hay un cortafuegos, por lo que no se necesitan reglas de descarte. Si se necesitan reglas de descarte, selecciones este caso.

Las opciones son:

Dirección IP de interfaz que no es de confianza.

Esta es la dirección IP de la interfaz para la que se descartan los paquetes no deseados. Generalmente, suele ser la dirección IP de la conexión con la red pública o que no es de confianza.

4 **Caso a medida.**

Esta selección proporciona la mayor flexibilidad al utilizar el mandato **qconfig** para definir una política. Se le solicitará que seleccione una modalidad de encapsulación (o de túnel o de transporte). Si se elige la modalidad de túnel, se le formularán las mismas preguntas que en el caso de una sucursal. Si se elige la modalidad de transporte, se le formularán las mismas preguntas que en el caso de una sucursal, excepto las relacionadas con las subredes local y remota, puesto que no son aplicables.

Mandatos de configuración del servidor de políticas de LDAP

Los mandatos de configuración del servidor de políticas de LDAP le permiten especificar las opciones del servidor LDAP para recuperar la información de políticas. La Tabla 39 resume los mandatos de configuración de LDAP y el resto de este apartado los describe detalladamente. Escríbalos en el indicador `Policy config>`. Puede entrar el mandato y las opciones en una línea o entrar sólo el mandato y responder a las indicaciones. Para ver una lista de opciones de mandato válidas, entre el mandato con un interrogante en vez de las opciones.

Tabla 39. 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 xxxii.
Disable ldap	Inhabilita las opciones de configuración de LDAP.
Enable ldap	Habilita las opciones de configuración de LDAP.
Set ldap	Especifica las 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 xxxiii.

Disable LDAP

Utilice el mandato **disable ldap** para inhabilitar las funciones de búsqueda de políticas de LDAP en el directorio o para inhabilitar la lectura de las políticas almacenadas en antememoria desde el servidor LDAP a un almacenamiento persistente.

Sintaxis: disable ldap cached-search
policy-search

cached-search
Impide que LDAP lea las políticas almacenadas en antememoria desde el servidor a un almacenamiento persistente.

policy-search
Impide que LDAP realice funciones de búsqueda en el directorio.

Enable LDAP

Utilice el mandato **enable ldap** para habilitar las funciones de búsqueda de políticas de LDAP en el directorio o para habilitar la lectura de las políticas almacenadas en antememoria desde el servidor LDAP a un almacenamiento persistente.

Sintaxis: enable ldap cached-search
policy-search

cached-search
Permite que LDAP realice funciones de búsqueda en el directorio o que lea las políticas almacenadas en antememoria desde el servidor LDAP a un almacenamiento persistente.

Si se habilita esta opción si la opción policy-search está inhabilitada, el motor de búsqueda de políticas sólo leerá políticas de la antememoria local. Si se habilitan las opciones cached-search y policy-search, el motor de búsqueda de políticas primero intentará leer del servidor LDAP y, si no lo consigue, lo intentará de los objetos de políticas de LDAP almacenados en antememoria. Consulte el mandato **cache-ldap-polcys** en el apartado "Mandatos de supervisión

de políticas” en la página 379 para obtener una explicación de cómo guardar en antememoria políticas de LDAP.

policy-search
Habilita LDAP para el uso de funciones de búsqueda en el directorio.

Set Default-Policy

Utilice el mandato **set default-policy** para especificar las opciones de política que se utilizarán mientras se renueva la base de datos de políticas. 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 se utilizarán mientras se renueva la base de datos de políticas.

Nota: El valor por omisión determina el comportamiento del dispositivo si se produce un error al reconstruir la base de datos de políticas. Si se produce un error, estas opciones determinarán el comportamiento del dispositivo. Son:

1. Restablecer la base de datos de políticas a la seguridad por omisión.
2. Desechar las reglas leídas de LDAP, cargar las reglas locales más la seguridad por omisión.

Estos valores sólo son válidos si se ha producido un error al crear la base de datos de políticas. Todas las opciones heredan la seguridad por omisión de desconexión o pase cuando se produce un error. Si selecciona la opción 2, todo el tráfico se desconecta o pasa a menos que coincida con una política definida localmente. Si la base de datos de políticas se crea satisfactoriamente, esta opción no se utiliza.

default-security
Especifica las opciones de seguridad que se utilizarán mientras se renueva la base de datos de políticas.

Nota: Una vez creada satisfactoriamente la base de datos de políticas, se define el comportamiento por omisión como en el pase. Esto significa que si el paquete no coincide con ninguna regla de política, se pasará libremente. Si quiere que los paquetes que no coincidan con una regla se desconecten globalmente o sólo para algunas interfaces, defina una política.

1 Aceptar y reenviar todo el tráfico de IP.

2 Permitir el tráfico de LDAP, descartar el resto de tráfico de IP.

Si selecciona esta opción, se le solicitarán las direcciones IP locales del dispositivo en el que se enviará y recibirá el tráfico de LDAP.

3 Permitir y proteger el tráfico de LDAP, descartar el resto de tráfico de IP.

Si selecciona esta opción, se le solicitará la siguiente información:

DHGroupId
El Id de grupo Diffie-Hellman que se utilizará durante las negociaciones de fase 1 de ISAKMP.

1 DH Grupo 1.

2 DH Grupo 2.

Phase1-Hash-Algorithm
El algoritmo hash que se utilizará durante las negociaciones de fase 1. El algoritmo hash proporciona la autenticación de los mensajes de la fase 1.

1 MD5.

2 SHA.

Phase1-Cipher-Algorithm
El algoritmo de cifras que se utilizará durante las negociaciones de fase 1. El algoritmo de cifras proporciona protección de cifrado para las negociaciones de fase 1.

1 DES

2 3DES

Phase1-Authentication-Method
El método de autenticación que se utilizará con el igual remoto. Especifica cómo ISAKMP determina si el igual remoto es actualmente el dispositivo correcto con el que negociar.

1 Clave previamente compartida

2 Certificado (RSA SIG)

Pre-Shared-Key-Value
Si ha especificado el método de autenticación de fase 1 de clave previamente compartida, se le solicitará que entre el valor de clave en ASCII.

Phase2-ESP-Authentication-Algorithm
ESP es el único protocolo IPSec permitido para la seguridad por omisión. Se le solicitará el algoritmo de autenticación que se utilizará durante las negociaciones de ISAKMP de fase 2.

0 Ninguno

1 HMAC-MD5

2 HMAC-SHA

Phase2-ESP-Cipher-Algorithm
ESP es el único protocolo IPSec permitido para la seguridad por omisión. Se le solicitará el algoritmo de cifrado que se utilizará durante las negociaciones de ISAKMP de fase 2.

1 ESP DES

2 ESP 3DES

3 ESP CDMF

4 ESP NULL

Primary-Tunnel-Start
La dirección IP del dispositivo que se utilizará para el tráfico de IKE e IPSec entre el dispositivo y la pasarela de seguridad que protege el servidor LDAP principal.

Primary-Tunnel-End
La dirección IP de la pasarela de seguridad remota que protege el servidor LDAP principal que se utilizará para el tráfico de IKE e IPSec.

Secondary-Tunnel-Start
La dirección IP del dispositivo que se utilizará para el tráfico de IKE e IPSec entre el dispositivo y la pasarela de seguridad que protege el servidor LDAP secundario.

Secondary-Tunnel-End
La dirección IP de la pasarela de seguridad remota que protege el servidor LDAP secundario que se utilizará para el tráfico de IKE e IPSec.

Set LDAP

Utilice el mandato **set ldap** para configurar los parámetros de funcionamiento de LDAP.

Sintaxis: set ldap anonymous-bind

yes

no

bind-name <*nombre*>
bind-pw <*contraseña*>
policy-base <*serie de caracteres*>
primary <*dirección ip*>
secondary <*dirección ip*>
version <*valor*>

anonymous-bind [Yes o No]
Especifica si se desea vincular con el directorio LDAP de forma anónima o con el nombre o contraseña de enlace que ha especificado.

Valor por omisión: Yes

bind-name <*nombre*>
Le solicita la información necesaria para vincularse al servidor LDAP antes de poder realizar una búsqueda en su directorio. El parámetro *nombre* especifica el nombre distintivo que utiliza el direccionador para identificarse. Si no entra este parámetro, se emite el mandato como una solicitud anónima.

bind-pw <*contraseña*>
Le solicita la información necesaria para vincularse al servidor LDAP antes de poder realizar una búsqueda en su directorio. El parámetro *contraseña* es la contraseña relacionada con el nombre distintivo. Si no entra este parámetro, se emite el mandato como una solicitud anónima.

policy-base <*serie de caracteres*>
Le solicita que entre una serie de caracteres que se utilizará para definir el ámbito de la búsqueda para las políticas del servidor LDAP y SRAM del direccionador. Por ejemplo, puede utilizar esta opción para devolver políticas que sólo se aplican al direccionador A o para NHD o para IBM-US. La base de política es el nombre distintivo del objeto DeviceProfile en el servidor LDAP.

primary <*dirección ip*>
Le solicita la dirección IPv4 del servidor LDAP desde el cual se recuperan las políticas.

secondary <*dirección ip*>
Le solicita las direcciones IPv4 de un servidor LDAP de reserva que se utiliza si no se puede alcanzar el servidor por omisión.

version <*valor*>
Le solicita el número de versión de LDAP soportado por el servidor 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 al día. Si se habilita, la base de datos de políticas se renueva una vez al día a la hora especificada. De esta forma se activan todos los direccionadores habilitados para políticas de la red para que incorporen automáticamente los cambios de política que se han producido en el directorio LDAP. Para restablecer este parámetro, utilice el mandato **reset refresh** de Talk 5 de la función de política.

Sintaxis: set refresh

enabled
yes
no
<*hora*>

enabled [yes o no]
Especifica si se realizará la renovación automática.

<*hora*>
Si ha habilitado el mandato, designa la hora del día (en formato de 24 horas) en la que se producirá la renovación.

Acceso al indicador de supervisión de políticas

El fragmento de consola de la función de política le permite ver las políticas que se encuentran en la base de datos y habilitar o inhabilitar políticas individuales. Para acceder al entorno de supervisión de políticas, escriba **talk 5** en el indicador OPCON (*):

```
* t 5
```

A continuación, entre el siguiente mandato en el indicador **+**:

```
+ feature policy
Policy>
```

Mandatos de supervisión de políticas

Estos mandatos le permiten ver los perfiles definidos en la base de datos de políticas y habilitar o inhabilitar políticas individuales. La Tabla 40 resume los mandatos de supervisión de políticas y el resto del apartado los describe. Escriba los mandatos en el indicador `Policy console>`. Puede entrar el mandato y las opciones en una línea o entrar sólo el mandato y responder a las indicaciones. Para ver una lista de opciones de mandato válidas, entre el mandato con un interrogante en vez de las opciones.

Tabla 40. Mandatos de supervisión de políticas

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 xxxii.
Cache-ldap-plcys	Almacena una copia de la información de políticas más reciente, leída desde el servidor LDAP al almacenamiento de configuración persistente del direccionador.
Check-consistency	Comprueba la coherencia de las políticas individuales y entre todas las políticas configuradas.
Disable	Inhabilita una política que está cargada en la base de datos de políticas.
Enable	Habilita una política que está cargada en la base de datos de políticas.
Flush-cache	Borra la información de políticas del almacenamiento de configuración persistente del direccionador.
Reset	Renueva o restablece los criterios relacionados con la política.
Search	Comprueba o depura la actividad entre el servidor y el cliente LDAP.
Status	Muestra información acerca de la base de datos de políticas.
List	Muestra información acerca de la configuración de LDAP y las políticas definidas.
Test	Consulta el motor de políticas y recupera las reglas que se han seleccionado
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiii.

Cache-LDAP-Plcys

Utilice el mandato **cache-ldap-plcys** para almacenar una copia de la información de políticas más reciente desde el servidor LDAP al almacenamiento de configuración persistente del direccionador. Esto elimina toda la información de políticas almacenada en antememoria que existiera en el almacenamiento persistente.

Sintaxis: cache-policy

Nota: En las plataformas 2212 y 2216, al ejecutar este mandato también se escribe toda la configuración del direccionador, como ocurre al ejecutar el mandato **write** de Talk 6.

Check-Consistency

Utilice el mandato **check-consistency** para comprobar las posibles incoherencias entre las opciones configuradas en una política individual (interna) y entre las políticas que tienen definiciones que se solapan (externas). En caso de que existieran, habría que tomar medidas para resolver los conflictos.

Una incoherencia *interna* es la que existe entre los objetos de acción de una sola política, por ejemplo, una política que tenga un tipo de acción Deny de DiffServ y que también tenga una acción Permit de IPSec. Una incoherencia *externa* es la que existe entre políticas diferentes con perfiles que se solapan, por ejemplo, una política que tenga un tipo de acción Block de DiffServ y otra política que tenga un tipo de acción Permit de IPSec. Otro ejemplo sería si las políticas que se solapan tuvieran distintos tipos de acción IPSec.

Sintaxis: check-consistency

Ejemplo:

Supongamos que las políticas se han configurado de la forma siguiente:

Nombre de la política: dsDown
Cargada de: local
Estado: habilitada y válida
Prioridad: 5
Aciertos: 0
Perfil: DSUP
Validez: always
DiffServ: dsDown
RSVP: rsvpActUp
Nombre de la política: ManualTunnel
Cargada de: local
Estado: habilitada y válida
Prioridad: 5
Aciertos: 0
Perfil: DSUP
Validez: always
ID del túnel: 1
Nombre de la política: ike
Cargada de: local
Estado: habilitada y válida
Prioridad: 30
Aciertos: 0
Perfil: DSUP
Validez: always

IPSec: ipsecUP

ISAKMP: generalPhase1Action

La salida del mandato **consistency-check** será parecida a esta:

```
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 que está cargada en la base de datos de políticas. Se aplicarán las decisiones predeterminadas a todos los paquetes de datos que inhabilite y que coincidan con los criterios de una política.

Sintaxis: disable *nombre de política*

Enable

Utilice el mandato **enable** para habilitar una política que está cargada en la base de datos de políticas. Se configurarán decisiones para las políticas aplicadas a todos los paquetes de datos que habilite y que coincidan con los criterios de una política.

Sintaxis: enable *nombre de política*

Flush-Cache

Utilice el mandato **flush-cache** para borrar la copia almacenada en antememoria más reciente de la información de políticas leída desde el servidor LDAP al almacenamiento de configuración permanente del direccionador.

Sintaxis: flush-cache

Reset

Utilice el mandato **reset** para renovar o restablecer los criterios relacionados con la 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 serán activos para la siguiente operación de búsqueda. Este mandato también obliga a restablecer la base de datos de políticas e inactiva el tiempo de renovación de ésta.

policy-database
Renueva la base de datos de políticas. Detiene todos los túneles, SA de fase 1 y fase 2, restablece las estructuras de datos de RSVP y DiffServ y vacía la base de datos de políticas. Luego se cargan las políticas del servidor LDAP y se lleva a cabo un inicio automático. Mientras se reconstruye la base de datos, no se permitirá la entrada ni la salida de paquetes del direccionador a excepción de los paquetes que se dirijan o provengan del servidor LDAP.

refresh-time
Establecer la hora en que se renovará automáticamente cada día la base de datos de políticas. Si ha inhabilitado el tiempo de renovación, la base de datos no se renovará hasta que se rearranque o reinicie el direccionador.

Search

Utilice el mandato **search** para comprobar o depurar la actividad entre el servidor y el cliente LDAP. Puede realizar búsquedas en el directorio y que los resultados aparezcan 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 la información acerca de la base de datos de políticas.

Sintaxis: status

status
Muestra el resultado de la renovación más reciente de la base de datos de políticas, el tiempo que ha transcurrido desde la última renovación y la hora en que está programada la siguiente.

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 la información acerca de las políticas y configuraciones 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 SRAM.

policy

basic Lista los componentes de la política por nombre de política lógica. Puede seleccionar una política o listarlas todas. El listado muestra los nombres de los componentes de políticas tal como se han entrado durante la configuración en Talk 6.

complete Lleva a cabo la misma acción que list policy basic, sólo que el listado muestra la lista completa de todos los valores de parámetro de cada política lógica.

generated Lleva a cabo la misma acción que list policy basic, sólo que el listado muestra los nombres de todas las reglas generadas para cada política lógica.

refresh
Lista el estado de renovación de la política (habilitado o inhabilitado) y el tiempo del intervalo de renovación.

rule
Lista la información acerca de las reglas generadas según las siguientes opciones:

basic Lista todas las reglas generadas. Puede seleccionar una regla de la lista o listarlas todas. El listado muestra los nombres de los componentes de las reglas. Los componentes son:
policy name
loaded from (LDAP o local)
state

priority
number of hits
profile
validity (seguido de una lista de acciones que son las siguientes)
IPSec (y, o)
ISAKMP (y, o)
DiffServ (y, o)
RSVP

complete Lleva a cabo la misma acción que rule basic, sólo que el listado muestra los nombres de todos los parámetros para cada componente.

stats
Lista las reglas que se han cumplido y el número de veces. Una regla puede tener diversas acciones y es posible que no se hayan cumplido todas las acciones, por lo que esta opción indica también la acción de la regla que se ha cumplido y el número de veces.

Test

Utilice el mandato **test** para verificar el comportamiento de la base de datos de políticas. Le permite entrar un conjunto de selectores que consulta el motor de políticas y recupera las reglas que deben coincidir. Se le solicitan las direcciones de origen y destino, los puertos de origen y destino, el ID de protocolo y el valor de TOS. Si coincide una regla, el mandato devuelve su nombre. Si no, indica *No match found*.

Sintaxis: test forwarder
ISAKMP
IPSec
RSVP

forwarder
Simula una consulta de base de datos del motor de reenvío de IP y devuelve las decisiones de política que produciría esta consulta. El tipo de política devuelta podría incluir la información de DiffServ, información de fase 1 y 2 de IKE y los ID de túnel manual de IPSec.

ISAKMP
Simula una consulta de base de datos de IKE para la información de políticas de fase 1 y devuelve las decisiones de política que produciría esta consulta. Si utiliza esta opción, deberá establecer las direcciones de origen y destino en las direcciones IP del extremo final del túnel, el protocolo en 17 y los puertos de origen y destino en 500.

IPSec
Simula una consulta de base de datos de IKE para la información de políticas de fase 2 y devuelve las decisiones de política que produciría esta consulta. Si utiliza esta opción, deberá establecer las direcciones de origen y destino en las direcciones IP del extremo final del túnel, el protocolo en 17 y los puertos de origen y destino en 500.

RSVP
Simula una consulta de base de datos de RSVP y devuelve las decisiones de política de RSVP que produciría esta consulta.

Soporte de reconfiguración dinámica de la función de política

En este apartado se describe la reconfiguración dinámica (DR) y cómo afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

La función de política no da soporte al mandato **delete interface** de CONFIG (Talk 6).

Mandato activate interface de GWCON (Talk 5)

El mandato **activate interface** de GWCON (Talk 5) no es aplicable a la función de política. La configuración de la función de política determina el conjunto de reglas y las acciones ulteriores que se aplicarán al tráfico IP, que es independiente de una interfaz en concreto.

Mandato reset interface de GWCON (Talk 5)

El mandato **reset interface** de GWCON (Talk 5) no es aplicable a la función de política. La configuración de la función de política determina el conjunto de reglas y las acciones ulteriores que se aplicarán al tráfico IP, que es independiente de una interfaz en concreto.

Mandatos de restablecimiento de componente de GWCON (Talk 5)

La función de política da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos de la función de política:

Mandato GWCON, feature policy, reset, database

Descripción: Todas las políticas configuradas en la función de política se leerán de la configuración local. Si está habilitada la función de búsqueda de LDAP, las políticas de este dispositivo se leerán del servidor LDAP. Los cambios en los objetos de políticas subyacentes, como las acciones DiffServ, o los objetos de políticas IPSec e IKE utilizados por las políticas, también se volverán a cargar de la configuración.

Después de leer todas las políticas, la base de datos de políticas se creará a partir de la colección de reglas generadas por dichas políticas. Durante el período en el que se están leyendo las políticas, se creará una base de datos por omisión con la regla por omisión configurada en Talk 6, utilizando el mandato **feature policy, set default-policy**.

Efecto en la red: Durante el período en el que se está creando la base de datos de políticas, el tráfico IPv4 de difusión individual se reenviará según la política por omisión configurada en Talk 6. La política por omisión o bien pasará todo el tráfico, o bien descartará todo el tráfico excepto el tráfico de LDAP proveniente y dirigido al 2212, o bien descartará todo el tráfico excepto el tráfico de LDAP protegido mediante IPSec proveniente y dirigido al 2212.

Limitaciones: Ninguna.

En la tabla siguiente se resumen los cambios en la configuración de la función de política que se activan cuando se ejecuta el mandato **GWCON, feature policy, reset, database**:

Mandatos cuyos cambios se activan al ejecutar 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 de LDAP para la función de política.

Efecto en la red: La próxima vez que se renueve la base de datos de políticas, se utilizarán los nuevos parámetros de configuración de LDAP para determinar si buscar el servidor y, en tal caso, qué parámetros utilizar.

Limitaciones: Ninguna.

En la tabla siguiente se resumen los cambios en la configuración de la función de política que se activan cuando se ejecuta el mandato **GWCON, feature policy, reset, ldap**:

Mandatos cuyos cambios se activan al ejecutar 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

Mandato GWCON, feature policy, reset, refresh

Descripción: Se cargarán 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, en tal caso, a que hora.

Efecto en la red: Si la función de renovación de políticas está habilitada, cuando sea la hora del suceso especificada en la configuración de renovación, la base de datos de políticas se renovará. Esto tiene el mismo efecto que ejecutar manualmente el mandato **reset database**.

Limitaciones: Ninguna.

En la tabla siguiente se resumen los cambios en la configuración de la función de política que se activan cuando se ejecuta el mandato **GWCON, feature policy, reset, refresh**:

Mandatos cuyos cambios se activan al ejecutar el mandato GWCON, feature policy, reset, refresh
CONFIG, feature policy, set, refresh

Mandatos de cambio inmediato de CONFIG (Talk 6)

La función de política da soporte a los siguientes mandatos de CONFIG que permiten modificar inmediatamente el estado operativo del dispositivo. Estos cambios se guardan y se mantienen si el dispositivo se reinicia, si se vuelve a cargar o si se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
CONFIG, feature policy, set, default-policy **Nota:** La próxima vez que se renueve la base de datos de políticas, se utilizarán los valores de la política por omisión durante el período de renovación y también servirán para manejar las condiciones de error que se puedan producir durante ese período.
CONFIG, feature policy, add, user
CONFIG, feature policy, change, user **Nota:** La clave previamente compartida definida para el usuario puede utilizarse inmediatamente sin tener que reiniciar o volver a cargar el dispositivo. Si este usuario forma parte de un grupo asociado con el grupo de usuarios remotos de un perfil, la base de datos de políticas deberá restablecerse antes de que se pueda realizar la asociación.

Utilización de la seguridad IP

Este capítulo explica cómo utilizar la función de Seguridad IP e incluye los siguientes apartados:

Visión general de la seguridad IP

Este apartado proporciona una visión general de las posibilidades de seguridad IP tanto para IPv4 como para IPv6.

Utilización de los túneles protegidos

Para proteger los paquetes IP enviados a otro sistema principal, direccionador o cortafuegos, puede configurar un túnel protegido para cada ruta IP que deba estar protegida. Un túnel IPSec es una conexión lógica de dos vías hacia el sistema principal remoto, direccionador o cortafuegos a través del cual el direccionador envía paquetes IP protegidos. Los túneles protegidos se identifican por parámetros como las direcciones del sistema principal de origen y destino, números de puerto e ID de túnel.

Con IPv4 puede definir un túnel negociado configurando una política de túnel en la base de datos de políticas o crear un túnel manual mediante el mandato **add tunnel** de Talk 6 como se muestra en el apartado "Configuración del túnel para el direccionador A" en la página 424. Con IPv6, utilice el mandato **add tunnel** de Talk 6.

Para establecer un túnel IPSec protegido, una política puede especificar la función AH (Authentication Header) de IP (consulte el apartado "Cabecera de autenticación de IP" en la página 392), que conecta las cabeceras de autenticación especiales, y la función ESP (Encapsulation Security Payload) (consulte el apartado "Protocolo ESP (Encapsulating Security Payload) de IP" en la página 393), que cifra los datos. La política establece que se implementen las siguientes medidas de seguridad para los paquetes:

- Claves de autenticación de AH y algoritmo AH (consulte el apartado "Configuración de los algoritmos" en la página 414 o el "Configuración de los algoritmos" en la página 427 según sea apropiado).
- Claves de cifrado y descifrado de ESP y algoritmo de cifrado de ESP (consulte el apartado "Configuración de los algoritmos" en la página 414 o el "Configuración de los algoritmos" en la página 427 según sea apropiado).
- Índices de parámetros de seguridad (SPI) (consulte el apartado "Asociaciones de seguridad" en la página 394).

Nota: Para cada túnel de seguridad, el remitente y el destinatario deben seleccionar opciones idénticas.

Conceptos de seguridad IP

Los paquetes enviados mediante el protocolo de Internet (IP) pueden protegerse mediante la función de seguridad IP del 2212.

La seguridad, tal como se define en la RFC 2401 (sección acerca de la arquitectura de la seguridad para el protocolo de Internet), consta de las siguientes funciones:

Autenticación
Confirmación de que los datos recibidos son los mismos que los datos enviados y que el remitente especificado es realmente el remitente.

Integridad
Confirmación de que los datos se han transmitido del origen al destino sin alteración no detectada.

Confidencialidad
Comunicación en la que los destinatarios reales saben lo que se ha enviado, pero que no permite a terceros determinarlo.

No repudio
Comunicación en la que el destinatario puede verificar que el remitente ha enviado ciertos datos aunque el remitente niegue más tarde haberlos enviado.

Nota: En algunos países, no se proporciona el soporte de cifrado debido a las regulaciones de exportación de EE.UU. y no se visualizan los parámetros de cifrado. Sin embargo, el algoritmo ESP-NULL siempre está disponible. Para ver la definición del algoritmo ESP-NULL, consulte el apartado “Algoritmos de cifrado de ESP” en la página 393.

Terminología de seguridad IP

Se utilizan los siguientes términos para describir los temas de IPSec relacionados con IPv4:

Cabecera de autenticación (AH)
Área de datos que contiene información de cabecera del paquete y que proporciona la autenticación de origen de datos, integridad de los datos y protección de repetición.

Certificado
Elemento de datos de codificación ASN.1 (según las normas 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 de ISAKMP.) La entidad final debe registrar el ID y clave pública con una autoridad certificadora (CA) sometiendo una solicitud de certificado. La CA verifica la solicitud, la firma y la emite a la entidad. ISAKMP utiliza el certificado de clave pública durante el procesamiento de fase 1 para autenticar los intercambios de mensajes iniciales que configuran la clave secreta original (clave criptográfica) entre direccionadores.

Autoridad certificadora (CA)
Una autoridad fiable que emite certificados digitales X.509 “firmados” que deben utilizar los usuarios para intercambiar datos de usuario seguros mediante ISAKMP. Para participar en intercambios de datos seguros con otras partes habilitadas para ISAKMP, el direccionador se debe registrar en una CA y obtener un certificado digital X.509 para utilizarlo en la autenticación.

Nota: Para garantizar que la lista de partes habilitadas para ISAKMP que se está utilizando está actualizada, deben realizarse comprobaciones regulares con la CA. Para obtener más detalles, consulte la información sobre el mandato **load** de PKI Talk 6 en el apartado “Mandatos de configuración de la infraestructura de claves públicas” en la página 411.

Firma digital
Elemento de datos que contiene un ID codificado de usuario que forma parte de un certificado digital X.509. Los usuarios intercambian certificados durante las negociaciones de fase 1 para autenticarse mutuamente. La firma se genera mediante una operación con la clave pública en un área de datos de entrada que se firmará.

ESP (Encapsulating Security Payload)
Función de IPSec que puede encapsular y cifrar un datagrama de forma que sólo el destinatario y nadie más puede determinar el contenido. Comprende la integridad de los datos y la protección de repetición. La función ESP también proporciona autenticación de origen de los datos. Funciona en las siguientes modalidades: modalidad de transporte, que cifra sólo la carga útil del datagrama original y deja la información de dirección visible a las partes no autorizadas y la modalidad de túnel, en la que se cifra todo el datagrama original, incluida la cabecera. Oculta la información de dirección sensible.

IKE (Internet Key Exchange)
Protocolo derivado de los protocolos ISAKMP y Oakley, que utiliza la comunidad Internet para intercambiar claves criptográficas y autenticar las partes de una comunicación.

ISAKMP (Internet Security Association and Key Management Protocol)
Protocolo para la gestión de claves y la asociación de seguridad de Internet. Esta función configura automáticamente las asociaciones de seguridad y gestiona claves criptográficas de paquetes durante un intercambio de datos.

MIB (Management Information Base)
Bloque de datos enviados por un direccionador como respuesta a una consulta de una autoridad fiable central que ha solicitado información estadística acerca de las operaciones del direccionador. La autoridad puede detectar problemas en la red y ponerse en contacto con un interlocutor responsable para tomar medidas con el fin de resolverlos.

Oakley
Protocolo de gestión de claves criptográficas utilizado por ISAKMP.

PFS (Perfect Forward Secrecy)
Nivel de seguridad de datos obtenido si las negociaciones de fase 2 proporcionan información de claves criptográficas nueva para cada negociación. ISAKMP lo consigue habilitando el intercambio de valores de Diffie Hellman públicos entre las partes. Esta función de seguridad evita que cualquiera determine una clave criptográfica actual de una clave concedida anteriormente.

Negociaciones de fase 1
Comunicación entre un remitente y un destinatario que establece una asociación de seguridad y claves criptográficas de ISAKMP que protegen los mensajes ISAKMP que se intercambiarán durante las negociaciones de fase 2. La fase 1 es intensiva para el procesador y no se suele realizar con frecuencia, tal vez sólo diaria o semanalmente.

Negociaciones de fase 2
Intercambio de mensajes ISAKMP entre un remitente y un destinatario durante el cual se negocian las asociaciones de seguridad y las claves criptográficas que protegerán los intercambios de datos del usuario. Estas negociaciones se suelen producir frecuentemente, cada dos o tres minutos, y se utilizan para renovar las claves criptográficas regularmente sin la intervención del usuario.

Proxy
Direccionador que se asigna para funcionar en nombre de otro dispositivo de la red.

Infraestructura de claves públicas (PKI)
Marco que utiliza una CA para enlazar los ID de usuario con su clave pública y distribuye la clave pública del enlace de forma que asegure su protección.

Modalidad rápida
Término utilizado para describir las negociaciones de fase 2 para asociaciones de seguridad que no son de ISAKMP.

Repetición
Acto de captura de un datagrama y el intento de determinar su contenido o montar un ataque de negación de servicio reenviándolo repetidamente.

Asociación de seguridad (SA)
Área de datos que reúne información acerca de un paquete de datos, por ejemplo su algoritmo criptográfico e información de claves, las identidades de las partes participantes, etc.

Transformación
Colección nombrada de información acerca de una configuración de selecciones de autenticación y cifrado.

Cabecera de autenticación de IP

La cabecera de autenticación (AH) se describe en la sección acerca de la cabecera de autenticación de IP de la RFC 2402. Esta cabecera contiene datos de autenticación para el datagrama de IP.

Para IPv4 con IPSec negociado, la política asignada a un datagrama implementa una función de autenticación criptográfica que confía en el protocolo IKE (Internet Key Exchange) y del par de claves pública/privada. Para los túneles manuales IPv4 y para IPv6, el remitente utiliza una función criptográfica que confía en una clave de autenticación secreta. En cualquier caso, la función de autenticación criptográfica se aplica al contenido del datagrama. Puede especificar AH solo o con ESP. Consulte el apartado “Utilización de AH y ESP” en la página 394 para obtener detalles.

Algoritmos de autenticación de AH

Los túneles protegidos que utilizan la política de túnel de AH deben utilizar uno de los siguientes algoritmos de autenticación:

- Autenticación de IP HMAC-MD5 con prevención de repetición
- Autenticación de IP HMAC-SHA-1 con prevención de repetición

Estos algoritmos AH combinan una función de autenticación de mensajes con clave utilizando el código hash criptográfico (hashed message authentication code, abreviado como HMAC) con una función de prevención de repetición opcional. La prevención de repetición utiliza un número de secuencia incluido en la AH para

verificar que no se ha recibido anteriormente un paquete. La prevención de repetición protege al destinatario de los ataques de negación de servicio, en los que se envía repetidamente el mismo paquete y el direccionador está tan ocupado procesando paquetes duplicados que no puede procesar el tráfico legítimo. Se aplica un código de autenticación a una clave criptográfica secreta y los datos, luego a la salida de la clave secreta y la salida de la primera operación. Consulte la Figura 33 para ver una muestra de cómo se realiza para HMAC-MD5.

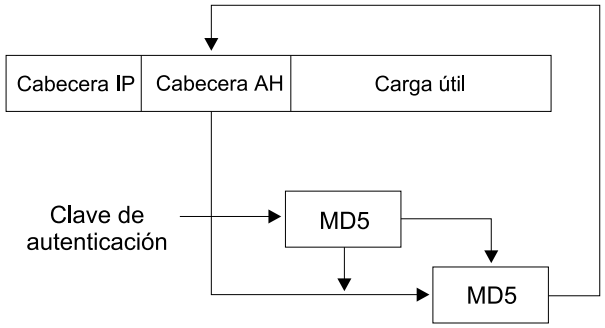


Figura 33. Creación de un mensaje autenticado por MD5 de HMAC

Protocolo ESP (Encapsulating Security Payload) de IP

La función ESP (Encapsulating Security Payload) de IP se describe en la sección acerca de la función Encapsulating Security Payload de IP de la RFC 2406. ESP cifra una parte o todo el paquete IP para proporcionar confidencialidad además de autenticación (opcional) e integridad. Sin embargo, si selecciona el algoritmo ESP-NULL, ESP realiza sólo la autenticación y comprobación de la integridad. Puede especificar ESP solo o con AH. Consulte el apartado “Utilización de AH y ESP” en la página 394 para obtener detalles.

Algoritmos de autenticación de ESP

Los algoritmos disponibles para la autenticación de ESP son los mismos que los de AH, mostrados anteriormente en el apartado “Algoritmos de autenticación de AH” en la página 392.

Algoritmos de cifrado de ESP

Los túneles protegidos que utilizan la política de cifrado de ESP deben utilizar uno de los siguientes algoritmos de autenticación o el algoritmo ESP_NULL:

- DES-CBC (Data Encryption Standard in Cipher Block Chaining Mode)
- CDMF (Commercial Data Masking Facility)
- 3DES (Triple DES)

Nota: A excepción de ESP-NULL, los algoritmos de cifrado de ESP están sujetos a las leyes de exportación de EE.UU. Si el 2212 no le permite utilizar algunos de estos algoritmos, es posible que la venta de éstos esté prohibida en su país. Consúltelo con el representante de IBM para obtener más información.

El algoritmo ESP-NULL no cifra los datos de texto plano y está disponible en todos los países. Habilita sólo la autenticación de ESP y la comprobación de la integridad, no el cifrado. Si utiliza ESP-NULL, ***debe*** utilizar uno de los algoritmos de autenticación de ESP.

Utilización de AH y ESP

Un túnel protegido puede utilizar una de las siguientes selecciones de autenticación/cifrado: AH, ESP, AH-ESP o ESP-AH. Si desea una combinación de AH y ESP, las siguientes sentencias son aplicables:

- La política AH-ESP especifica que para los paquetes de salida, el cifrado se ejecuta antes de la autenticación. En este caso, en el direccionador de destino se ejecuta primero la función de autenticación de AH, comprobación de paquetes de entrada y sólo los paquetes que pasan la autenticación se reenvían al ESP para la descifrado.
- La política ESP-AH especifica que para los paquetes de salida, la autenticación se ejecuta antes del cifrado. En este caso, en el direccionador de destino la función ESP descifra primero los paquetes de entrada y sólo los paquetes que se descifran satisfactoriamente se reenvían para la autenticación de AH.

Asociaciones de seguridad

Una Asociación de seguridad (SA) es una “conexión” simple que proporciona servicios de seguridad al tráfico que gestiona. Los servicios de seguridad se proporcionan a una SA mediante el uso de AH o ESP, pero no ambos. Si se aplica tanto la protección de AH como de ESP a una corriente de tráfico, se crean dos (o más) SA para proporcionar protección a la corriente. Para proteger la comunicación bidireccional típica entre dos sistemas principales o dos pasarelas de seguridad, son necesarias dos SA (una en cada dirección).

Modalidad de túnel y modalidad de transporte

La modalidad operacional (túnel o transporte) determina la manera como IPSec maneja los paquetes de IP. La modalidad de túnel es el valor por omisión y es obligatorio si el direccionador actúa como pasarela de seguridad. Protege los datos en un solo segmento de una vía de acceso a través de una red. La modalidad de transporte está permitida sólo cuando el direccionador actúa como sistema principal y protege los datos de extremo a extremo, a lo largo de una vía de acceso completa.

Modalidades AH y operacional

En la modalidad de túnel, la AH se coloca en la parte frontal del paquete de IP y se crea una cabecera de IP nueva que se coloca frente a la AH. La cabecera de IP del paquete que se coloca en el túnel (cabecera interior) incluye las direcciones definitivas de origen y destino del paquete. La cabecera de IP nueva (cabecera exterior) pude contener las direcciones de las pasarelas de seguridad, que son extremos del túnel. La AH protege todo el paquete nuevo, tanto la cabecera de IP nueva como el paquete de IP que se coloca en el túnel, excepto los cambios mudables de la cabecera de IP nueva.

En la modalidad de transporte, la AH se inserta después de la cabecera de IP y antes de la cabecera de un protocolo de la capa superior, por ejemplo TCP o UDP. En esta modalidad, la AH autentica la cabecera de protocolo de la capa superior y el contenido del paquete de IP, excepto los campos mudables de la cabecera de IP (como el tiempo de vida [TTL], suma de comprobación, distintivo de fragmentos, desplazamiento de fragmentos y tipo de servicio [TOS]).

La Figura 34 en la página 395 muestra el formato de los datagramas de AH protegida.

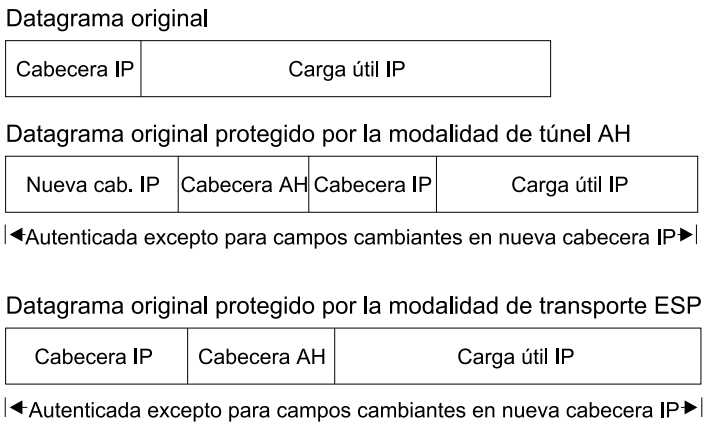


Figura 34. Formato de datagramas de AH protegida

Modalidades ESP y operacional

En la modalidad de túnel, los datos de carga útil contienen todo el paquete de IP y se crea una cabecera de IP nueva que se coloca frente a la cabecera de ESP. La cabecera de IP del paquete que se coloca en el túnel (cabecera interior) contiene las direcciones definitivas de origen y destino del paquete, mientras que la cabecera de IP nueva (cabecera exterior) contiene las direcciones de las pasarelas de seguridad. ESP cifra el paquete de IP que se coloca en el túnel. Si utiliza la autenticación de ESP, se autentican la cabecera de ESP, el paquete de IP que se coloca en el túnel y la cola de ESP.

En la modalidad de transporte, los datos de carga útil contienen los datos de protocolo de la capa superior cifrados, por ejemplo los datos de TCP o UDP. Si utiliza la autenticación, se autentican la cabecera de ESP, los datos de protocolo de la capa superior y la cola de ESP.

La Figura 35 muestra el formato de los datagramas de ESP protegida.

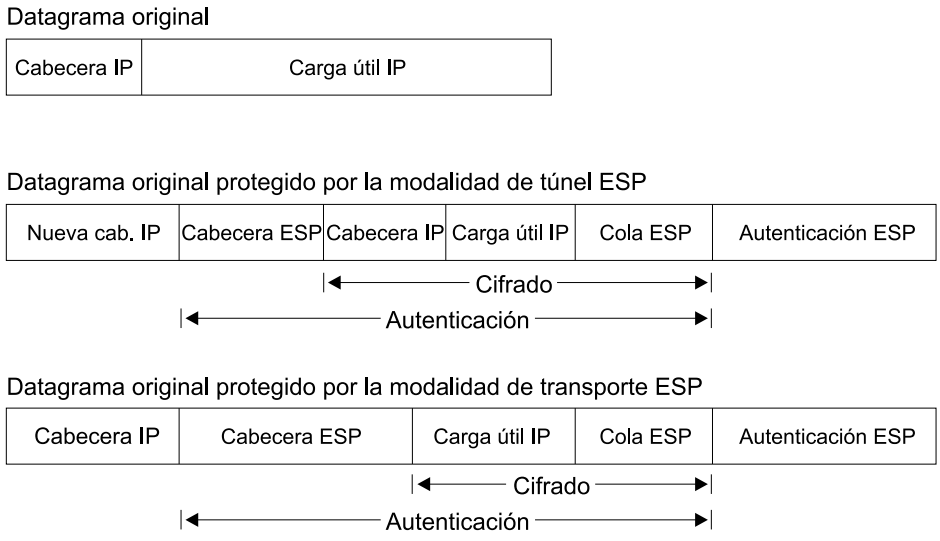


Figura 35. Formato de datagramas de ESP protegida

Anidación de AH y ESP

Puede anidar un protocolo dentro de otra instancia de sí mismo o de otro protocolo. La Figura 36 muestra los efectos de la anidación de un datagrama de ESP protegida dentro de un túnel de AH.

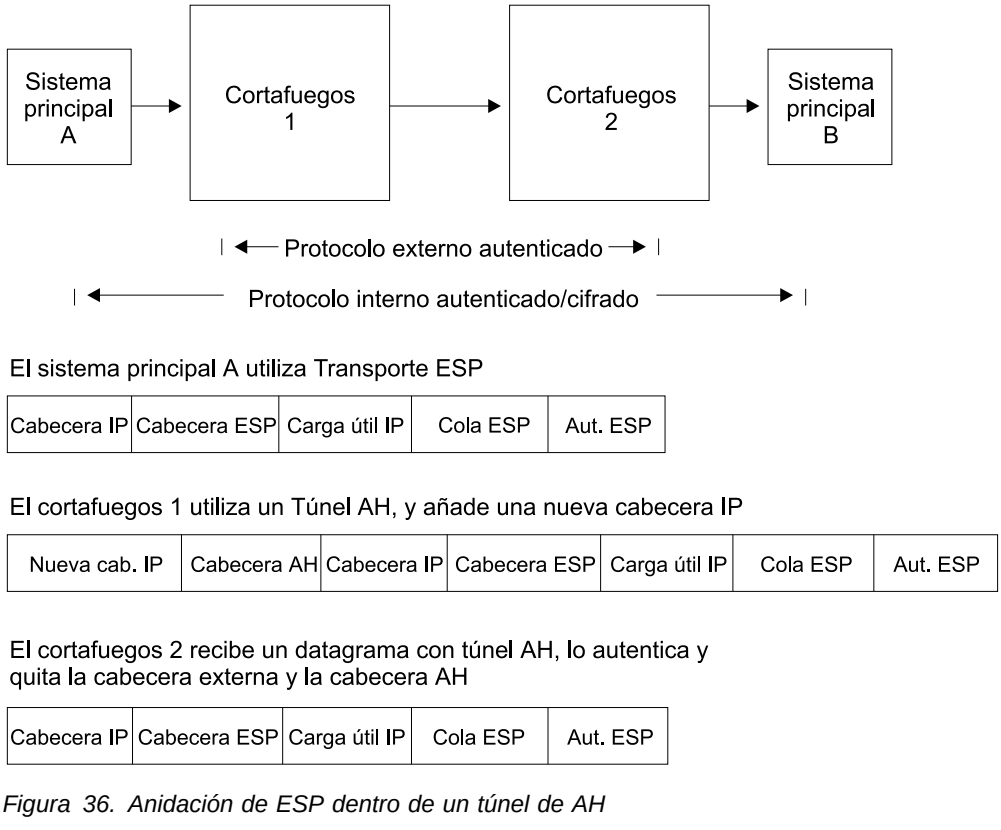


Figura 36. Anidación de ESP dentro de un túnel de AH

Utilización de la seguridad IP con paquetes L2TP

Con IPv4, también puede utilizar IPSec para proteger paquetes L2TP. Después de crear un túnel L2TP encapsulando un marco L2TP dentro de un paquete UDP, puede encapsular el paquete UDP dentro de un paquete de IP cuyas direcciones de origen y destino definan los extremos del túnel. Luego puede aplicar los protocolos AH, ESP y ISAKMP al paquete de IP. La Figura 37 muestra un paquete L2TP de IP encapsulado que incluye PPP y su protocolo de carga útil para la transmisión a través de Internet.

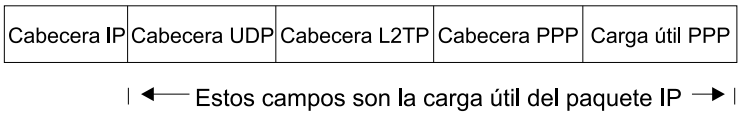


Figura 37. Paquete de L2TP de IPSec protegido

Modalidad de túnel en túnel

Para una mayor seguridad, además de las funciones de seguridad tratadas anteriormente, puede encapsular los paquetes de una corriente de tráfico dos veces y transmitirlos primero a través de un túnel IPSec y luego a través de otro túnel (túnel en túnel).

Nota: El uso del cifrado múltiple (utilizando la modalidad de túnel en túnel cuando se realiza el cifrado para ambos túneles) dentro del direccionador está restringido por las regulaciones de exportación del gobierno de EE.UU. Sólo se da soporte a esta opción en las cargas de software que se encuentran bajo un control estricto de exportación (cargas de software que dan soporte a RC4 con claves de 128 bits y triple DES).

Con IPv4, una regla de la base de datos de políticas designa un paquete para el encapsulado (interior) para el primer túnel, y antes de que se envíe el paquete, la regla hace que se envíe el paquete a un segundo túnel para un segundo encapsulado (exterior). Con IPv6, una regla de control de acceso de filtro de paquetes identifica un paquete para el encapsulado (interior) para el primer túnel, y antes de que se envíe el paquete, una segunda regla hace que se envíe el paquete a un segundo túnel para un segundo encapsulado (exterior).

Los dos túneles IPSec se originan en el mismo direccionador y los extremos remotos de los túneles se encuentran en la misma ubicación física, pero en distintas máquinas. El extremo remoto del primer túnel puede ser una pasarela o un sistema principal protegidos; el extremo remoto del segundo túnel *debe* ser un direccionador de pasarela protegido. Puesto que los túneles tienen diferentes destinos, deben tener direcciones IP remotas distintas. Los dos túneles utilizados para el túnel en túnel deben estar configurados para la modalidad de túnel y no se permite el 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 ese túnel, se elimina el encapsulado externa y el paquete se reenvía al primer túnel (interno), según la información de la cabecera creada por el encapsulado del primer túnel. Al final de este túnel, se elimina el encapsulado interno y el paquete se reenvía al destino final.

Descubrimiento de la unidad de transmisión máxima de la vía de acceso

Para IPv4 y IPv6, IPSec da soporte al Descubrimiento de PMTU (Unidad de transmisión máxima de la vía de acceso) si el 2212 actúa como pasarela de seguridad. El soporte del Descubrimiento de PMTU es interesante si no se puede fragmentar un paquete. Con IPv4, los paquetes no se pueden fragmentar si tienen establecido el bit No fragmentar (DF). Con IPv6, los direccionadores intermedios no pueden fragmentar los paquetes. En estas situaciones, si el paquete no cabe en un enlace de la vía de acceso de un extremo del túnel protegido al otro, se envía un mensaje de error de ICMP de “paquete demasiado grande” al autor del paquete.

Puesto que el direccionador actúa como una pasarela de seguridad, el paquete con el error se devuelve al direccionador de origen en vez de al autor verdadero del paquete. El direccionador de recepción debe pasar la MTU al autor verdadero, quien reducirá el tamaño del paquete para que pueda llegar al destino final. El soporte para el descubrimiento de PMTU se trata en la sección acerca de la arquitectura de seguridad para el protocolo de Internet de la RFC 2401.

IPv4 proporciona las siguientes opciones para el valor de bit DF en la cabecera exterior del paquete que se ha colocado en el túnel:

1. Copiar de la cabecera interior
2. Siempre establecido
3. Siempre libre

Estas opciones están disponibles al configurar la modalidad de túnel en túnel, por ejemplo utilizando la función de política **add ipsec-manual-tunn** (IPv4) o el mandato **add tunnel** (IPv6) de Talk 6. El bit DF se maneja según la opción seleccionada excepto bajo estas condiciones:

- 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 es mayor que la MTU mínima.

En estas circunstancias, para IPv4, el bit DF no está establecido, independientemente de la configuración, y el paquete protegido se puede fragmentar según sea necesario en la vía de acceso al receptor. Para IPv6, el paquete se fragmenta según sea necesario cuando sale de la pasarela de seguridad para que quepa en la PMTU del túnel. Esta acción especial es necesaria porque el paquete de entrada ya es menor o igual que la MTU mínima, por lo que el sistema principal de origen no disminuirá el tamaño. Si la fragmentación no estuviera permitida, esta paquete no llegaría nunca a su destino final

Puesto que los cambios en la configuración o la topología de la red pueden cambiar la PMTU, el valor de PMTU debe caducar periódicamente y restablecerse al máximo. El valor por omisión de temporizador de caducidad es de 10 minutos y se puede configurar con el mandato **set path** de Talk 6. Si se establece el parámetro de caducidad en 0 se inhabilita la caducidad de la PMTU.

Diagrama de una red con un túnel de seguridad IP

La Figura 38 en la página 399 muestra un ejemplo de una red con dos túneles IPSec que conectan el direccionador A (con IPSec) al direccionador B (con IPSec y Conversión de direcciones de red para IPv4).

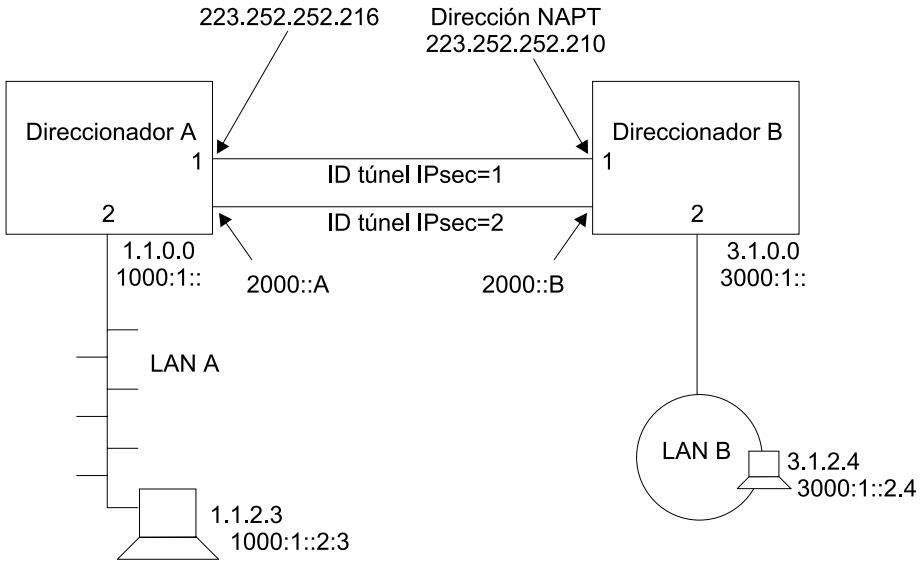


Figura 38. Red con IPSec y NAT

En esta red, se ha configurado un túnel IPSec con ID de túnel IPSec 1 de la dirección IPv4 223.252.252.216 del direccionador A a la dirección IPv4 223.252.252.210 del direccionador B. Se ha configurado el direccionador A para IPSec. Se ha configurado el direccionador B para IPSec y NAT.

También en esta red, se ha configurado un túnel IPSec con ID de túnel IPSec 2 de la dirección de IPv6 2000::A del direccionador A a la dirección de IPv6 2000::B del direccionador B.

Con IPv4, si desea configurar esta red para IKE, siga los pasos que empiezan en el apartado “Configuración del intercambio de claves en Internet (IPv4)” en la página 409. Para IPv4 con IPSec manual, siga los pasos que empiezan en el apartado “Configuración de un túnel manual (IPv4)” en la página 424. Para IPv6, siga los pasos que empiezan en el apartado “Configuración de un túnel manual (IPv6)” en la página 428.

Nota: Aunque no tenga previsto utilizar NAT en la red, la descripción de configuración del direccionador B puede ayudarle a comprender mejor la relación entre los parámetros de cada extremo del túnel IPSec.

Utilización del intercambio de claves de Internet

Este apartado explica la manera de utilizar el intercambio de claves de Internet (IKE) para automatizar la definición y creación de asociaciones de seguridad de IPSec (SA). IKE es un estándar soportado por el IETF (RFC 2409) que proporciona a los productos habilitados para IPSec del mismo proveedor o de proveedores distintos una forma estándar para comunicarse acerca de los requisitos de seguridad.

IKE proporciona un marco en el cual se cumplen los siguientes requisitos de seguridad:

Autenticación de la entidad de negociación remota (igual de IKE) A través del uso de una clave previamente compartida o un certificado digital, IKE autentica la identidad de la entidad con la que se está comunicando al hacer que la entidad demuestre que es quien dice ser.

Creación de material de claves idéntico en ambos iguales Si se utiliza el mecanismo de clave pública y privada de Diffie-Hellman, IKE proporciona el intercambio del componente clave pública y la generación independiente de claves idénticas para todos los iguales.

Proporciona protección para la negociación de asociaciones de seguridad de IPSec A través de un proceso de dos fases, descrito en el siguiente tema, IKE proporciona la creación de asociaciones de seguridad que se utilizan sólo para proteger la negociación de los *túneles* de IPSec, y la negociación y creación de *asociaciones de seguridad* que IPSec utiliza para proteger los datos del usuario.

Fases del intercambio de claves de Internet

IKE define dos intercambios de negociación distintos: la fase 1 y la fase 2. La fase 1 configura un túnel seguro entre los dos iguales de IKE, que proporcionará protección para las negociaciones de túnel IPSec siguientes. Las siguientes acciones se producen durante la fase 1 en el orden que se muestra:

1. Los iguales de IKE negocian y acuerdan las características de la asociación de seguridad de la fase 1. Estas características incluyen el algoritmo de cifrado que se utilizará para cifrar *las comunicaciones de IKE*, al algoritmo hash que se utilizará, el método de autenticación y el grupo Diffie-Hellman que se utilizará al generar claves.
2. Las claves Diffie-Hellman se generan y las partes públicas se intercambian con el igual de IKE. Estas claves se utilizan para generar claves de cifrado que cifrarán las negociaciones de fase 1 y permitirán también la generación de claves que utilizarán los túneles IPSec.
3. El igual de IKE se autentica utilizando uno de estos dos métodos soportados—modalidad de clave previamente compartida y modalidad de firma.

   En la modalidad de clave previamente compartida, los dos iguales de IKE, mediante un proceso de fuera de línea previo, han intercambiado una clave y ésta se utiliza durante la fase 1 para autenticar el igual. La clave previamente compartida se configura mediante el mandato **add user** de la función de política.

   En la modalidad de firma, se utiliza un certificado digital X.509 para proporcionar las claves que se utilizan para cifrar y descifrar las cargas útiles de los mensajes de fase 1. La firma y verificación satisfactoria comprende la autenticación del igual. Para ver una descripción detallada de la modalidad de firma y el uso de certificados digitales X.509, consulte el apartado. “Utilización de la infraestructura de claves públicas (PKI)” en la página 402.

Las negociaciones de fase 1 pueden producirse a través de una de estas dos modalidades de intercambio:

- La modalidad principal utiliza seis mensajes para llevar a cabo las negociaciones de fase 1 y cifra las identidades de los iguales de la negociación.
- La modalidad agresiva utiliza tres mensajes para llevar a cabo las negociaciones de la fase 1. Los iguales intercambian las identidades no protegidas en los dos primeros mensajes.

Negociación de un túnel de seguridad IP

El proceso descrito en este tema se produce cuando un direccionador se prepara para enviar un paquete cuyos atributos coinciden con los definidos en una regla de una base de datos de políticas. La negociación de un túnel se produce en dos fases. Durante la fase 1, el direccionador de envío inicia la comunicación transmitiendo el primer mensaje de un intercambio de seis mensajes, lo que establece las opciones de seguridad que se utilizarán durante la fase 2. El receptor responde y las dos partes negocian las características de la asociación de seguridad (SA) de ISAKMP y los algoritmos de autenticación y cifrado que se utilizarán, y autentican mutuamente su identidad. Durante la fase 2, las partes intercambian un total de tres mensajes para negociar las SA y las claves que se utilizarán para proteger los datagramas de IP que se envían entre sí. La fase 1 sigue de esta manera:

1. Mensaje 1: El remitente propone cómo se realizará la actividad de comunicación—el método de autenticación (por ejemplo, firmas digitales), el algoritmo de autenticación (por ejemplo, HMAC-MD5) y el algoritmo de cifrado (por ejemplo, DES-CBC) que se utilizarán.
2. Mensaje 2: El receptor indica al remitente a qué opciones de seguridad da soporte.
3. Mensaje 3: El remitente transmite el valor público de Diffie Hellman y un valor aleatorio desde el que se crearán las claves de cifrado.
4. Mensaje 4: El receptor transmite su propio valor público de Diffie Hellman y un valor aleatorio desde el que se crean las claves de cifrado. En este momento, las dos partes crean claves públicas y privadas e información relacionada con las claves que se utilizará en los intercambios de mensajes de ISAKMP.
5. Mensaje 5: El remitente transmite una autorización digital y puede incluir un certificado digital X.509 firmado por una autoridad certificadora (CA) fiable. Si el remitente no incluye un certificado válido, el receptor debe utilizar el protocolo LDAP para obtener un certificado de una CA fiable, un servidor de DNS seguro, una antememoria local que correlaciona los certificados utilizados anteriormente con sus valores de ID respectivos o puede solicitar un certificado de un remitente, quien debe enviarlo inmediatamente.
6. Mensaje 6: Después de verificar la firma digital del remitente, el receptor transmite el mismo tipo de información de identificación sobre sí mismo al remitente.

En este momento, las dos partes se han autenticado mutuamente, han acordado las características de la SA y han producido claves e información relacionada con las claves para manejar SA de ISAKMP. Ahora las partes entran en la fase 2 para negociar las claves y SA que no son de ISAKMP, que se utilizarán para proteger los datagramas de IP intercambiados. La fase 2 sigue de esta manera:

1. Mensaje 1: El remitente propone una SA que no es de ISAKMP transmitiendo una selección de algoritmos ESP o AH e incluye también otra información relacionada con la seguridad.
2. Mensaje 2: El receptor indica al remitente la propuesta que ha seleccionado e incluye información relacionada con la seguridad.
3. Mensaje 3: El remitente transmite un registro hash de varios elementos para indicar al receptor que está listo para continuar utilizando los protocolos de seguridad negociados. Cuando el receptor verifica la información, el enlace está completo y las partes pueden empezar a intercambiar corrientes de datos protegidas.

Utilización de la infraestructura de claves públicas (PKI)

Este apartado explica cómo utilizar la infraestructura de claves públicas (PKI). A través de PKI, IKE soporta la modalidad de claves públicas para la autenticación de entidades de IKE. Aunque esta versión da soporte a la modalidad de clave previamente compartida, que no requiere el soporte a PKI, esta modalidad contiene una desventaja inherente. Para la autenticación, requiere la configuración de cada una de las entidades de IKE con la clave previamente compartida de cada uno de los iguales. Esto limita enormemente la escalabilidad de las operaciones de IKE. La firma basada en claves públicas o la modalidad de cifrado proporcionan una escalabilidad mucho mejor. En esta versión, el certificado digital X.509 se utiliza en las negociaciones de fase 1 de IKE de la modalidad de firma para autenticar las entidades de IKE.

Asigne una identidad a cada entidad IKE que quiera que participe en las negociaciones de IKE especificando un valor exclusivo en el campo de ID de ISAKMP cuando configure el perfil de políticas del usuario. Cada entidad de IKE autentica su identidad con sus iguales.

PKI se está definiendo y desarrollando para dar soporte a la operación de claves públicas. En PKI, un certificado digital X.509 enlaza la clave pública de una entidad con su identidad establecida. Una entidad de IKE puede extraer la clave pública incluida en un certificado. Puede llevar a cabo una operación de claves públicas para autenticar la identidad de un igual 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 a las entidades de IKE una forma escalable de autenticar la identidad de otra entidad de IKE.

Configuración de PKI

Esta versión asume que las dos entidades de IKE de una negociación utilizan la misma CA. Antes de empezar las negociaciones de IKE con su firma, deberá configurar PKI para el direccionador. También debe generar la clave privada y el certificado del direccionador, y debe haber bajado el certificado de la CA raíz. Los siguientes pasos explican cómo configurar la PKI:

1. Genere el par de claves y solicite el certificado.

   Puesto que la operación de claves públicas 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 solicitud de certificado, debe enviar la clave pública generada a la CA para ponerla en un certificado digital X.509. Luego, cada igual de IKE potencial podrá extraer su clave pública del certificado emitido por la CA. La clave privada reside en el direccionador y se mantiene en secreto, sólo la sabe el direccionador.

   En esta versión, puede emitir un mandato **certificate request** que hace lo siguiente:

   a. Genera un par de claves, cuya longitud puede especificar en 512, 768 ó 1024 bits. La clave privada generada se mantiene en la antememoria.

   b. Solicita que entre información para incluir en la solicitud de certificado (por ejemplo, el ID del direccionador en forma de dirección IP, nombre de dominio o nombre de correo electrónico.

c. Crea una solicitud de certificados (en formato PKCS#10) que contiene la clave pública generada y la información que ha entrado.

d. Lleva a cabo un TFTP en la solicitud del certificado para una máquina de sistema principal.

2. Emita el certificado (fuera del direccionador)

   La CA recibe la solicitud de certificado de PKCS#10. La CA puede verificar manualmente la solicitud 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, que se convierte en información digital fiable siempre que se confíe en la CA que firma. El certificado ya está preparado para utilizarse en las negociaciones de IKE. (Este proceso está fuera del ámbito del funcionamiento del direccionador y no se explica más detalladamente en esta publicación).

3. Baje el certificado del direccionador

   Cuando la CA haya emitido el certificado, la PKI puede bajarlo al direccionador. Según cómo la CA publique el certificado, la PKI puede utilizar TFTP o LDAP para bajarlo.

   Tenga en cuenta que la clave privada y la clave pública del certificado del direccionador deben coincidir para llevar a cabo el funcionamiento de clave pública como la firma digital. Cuando la PKI baja el certificado al direccionador, la clave privada que se ha generado con la clave pública debe estar en la antememoria clave del direccionador. El certificado bajado es inútil si pierde la clave privada que coincide. Esto significa que desde el momento en que se emite la solicitud de certificado al momento en que se baja el certificado **no debe** reiniciar o recargar el direccionador, borrar la antememoria o emitir una nueva solicitud de certificado. Cualquiera de estas operaciones destruirían la clave privada de la antememoria en ejecución del direccionador.

4. Baje el certificado de la CA

   Para verificar el certificado del igual de IKE, PKI debe obtener el certificado de la CA raíz. Esta versión da soporte a la operación de la CA de un solo nivel, lo que significa que se deben asignar las entidades de IKE a la misma CA. Cada entidad de IKE (en este caso, cada direccionador) debe bajar el certificado de la CA (mediante TFPT o LDAP) para verificar que el certificado recibido del igual es válido.

5. Guarde y vuelva a cargar el certificado

   Cuando el direccionador ha obtenido el certificado, la clave privada coincidente y el certificado de la CA, puede empezar la negociación de IKE. Puesto que los certificados suelen ser válidos durante meses o años, es posible que quiera guardar el certificado y la clave privada en SRAM para que no tenga que emitir una solicitud de certificado y bajarlo cada vez que vuelva a cargar o reiniciar el direccionador. Esta versión proporciona los mandatos **cert save** y **cert load** para guardar o recuperar el certificado y la clave privada en SRAM.

   Tenga en cuenta que el certificado y la clave privada del direccionador se deben procesar como una pareja (por ejemplo, siempre se guardan o se recuperan juntos de la memoria SRAM).

Utilice los mandatos de Talk 6 para configurar y listar la información de servidor de TFTP y LDAP tal como se muestra en los siguientes ejemplos:

Ejemplo: añadir servidor (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: listar configuración de servidor (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: listar certificados raíz (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: solicitud de certificados (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: listar certificados de direccionadores (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: guardar certificado (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: carga de certificados (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 la seguridad IP manual (IPv4)

La función de seguridad de IP que se incluye en IPv4 para el 2212, junto con la función de política y otros procesos relacionados con IPSec, proporciona integridad de la autenticación, confidencialidad y no repudio. Para implementar IPSec manualmente, preconfigure una política que contenga un subconjunto de opciones de IPSec en una base de datos de políticas para definir el período de validez y el perfil del túnel manual. También puede preconfigurar todo el conjunto de opciones de IPSec (política) de la base de datos para que cuando un direccionador habilitado para políticas se prepara para enviar un paquete de IPSec, negocie y establezca dinámicamente las opciones de IPSec con el direccionador de destino, según el contenido de la política. Para definir un túnel manual, consulte el apartado “Configuración de la seguridad IP manual (IPv4)” en la página 414. Para obtener una explicación de las opciones de política, consulte el “Utilización de la función de política” en la página 309.

Utilización de la seguridad de IP manual (IPv6)

La función de seguridad IP incluida en IPv6 para el 2212 proporciona autenticación, integridad y confidencialidad. Para definir un túnel manual, consulte el apartado “Configuración de la seguridad IP manual (IPv6)” en la página 426.

Configuración y supervisión de la seguridad IP

Este capítulo describe el modo de configurar y supervisar la seguridad IP y el modo de utilizar los mandatos de supervisión de la seguridad IP. Por lo que se refiere a IPv4, el “Utilización de la función de política” en la página 309 y el “Configuración y supervisión de la función de política” en la página 353 proporcionan información adicional sobre la configuración y supervisión de las políticas de seguridad IP. Este capítulo consta de los apartados siguientes:

Nota: Si se crea un túnel IPSec para transportar el tráfico TN3270, APPN®-ISR o APPN-HPR y se pretende dar prioridad a dicho tráfico mediante BRS, tendrá que utilizar la función de BRS de establecimiento del bit de prioridad de IPv4. Consulte “Proceso de bits de prioridad de IP versión 4 para tráfico SNA en túneles seguros IP y fragmentos secundarios” en la página 10 si desea obtener más información.

Configuración del intercambio de claves en Internet (IPv4)

Este tema describe la manera de configurar el intercambio de claves en Internet (IKE).

Antes de establecer un túnel IPSec, deberá:

1. Configurar los atributos de paquetes que el túnel utilizará y las acciones resultantes que se deberán llevar a cabo (la política).
2. Configurar las opciones de cifrado y autenticación que desee.

Si desea obtener información detallada sobre cómo llevar a cabo dichas tareas, consulte el “Utilización de la función de política” en la página 309, “Configuración y supervisión de la función de política” en la página 353 y el “Configuración de la infraestructura de claves públicas (IPv4)” en la página 410.

Configuración de la infraestructura de claves públicas (IPv4)

Este tema describe la manera de configurar la infraestructura de claves públicas (PKI) con IPv4.

Antes de establecer un túnel IPSec, deberá:

1. Crear un par de claves de cifrado públicas/privadas y obtener un certificado digital de una Autoridad certificadora (CA) de confianza. Consulte “Obtención de un certificado” si desea obtener información detallada al respecto.
2. Decidir qué algoritmos IPSec, SA y demás opciones desea utilizar para los direccionadores cuyas políticas está configurando. Consulte “Negociación de un túnel de seguridad IP” en la página 401 y los temas posteriores para obtener información detallada.
3. Configurar el IKE y la base de datos de política. Consulte “Configuración del intercambio de claves en Internet (IPv4)” en la página 409, el “Utilización de la función de política” en la página 309 y el “Configuración y supervisión de la función de política” en la página 353 si desea obtener información detallada al respecto.

Obtención de un certificado

Antes de establecer un túnel IPSec, lo debe seleccionar y registrar con una Autoridad certificadora (CA) de confianza, tal y como se describe en “Utilización de la infraestructura de claves públicas (PKI)” en la página 402. La CA devuelve un certificado digital X.509 firmado que le permite identificarse y autenticarse ante terceros en la red. El certificado consiste en un ID digital codificado (firma) y un par de claves de cifrado públicas/privadas. Lleve a cabo lo siguiente:

1. Identifique una CA y obtenga su dirección de servidor.
2. Configure las opciones de recuperación del depósito de certificados mediante los mandatos **add ldapserver** o **add tftpserver** de PKI Talk 6, tal y como se describe en “Mandatos de configuración de la infraestructura de claves públicas” en la página 411.
3. Cree un par de claves públicas/privadas mediante el mandato **certificate request** de PKI Talk 5, tal y como se describe en “Mandatos de supervisión de la infraestructura de claves públicas” en la página 435. Esto lo puede realizar tanto en el direccionador como remotamente, en calidad de administrador de la red privada virtual (VPN), en cuyo caso deberá cifrar y transferir de manera segura el par de claves al direccionador.
4. Envíe una petición de certificado inicial a la CA mediante el mandato **certificate request** de PKI Talk 5, tal y como se describe en “Mandatos de supervisión de la infraestructura de claves públicas” en la página 435. La petición se envía en un mensaje PKCS#10 vía correo electrónico o FTP. La CA vincula el par de claves al certificado, lo firma con su clave privada y lo almacena en un depósito central (LDAP o FTP) o se lo devuelve en un mensaje PKCS#7. Habitualmente, un certificado es válido durante varios meses o más, al cabo de los cuales se renueva. Con ello se identifican las partes de una red que aún son de confianza.
5. Guarde el certificado en una SRAM del direccionador mediante el mandato **certificate save** de PKI Talk 5, tal y como se describe en “Mandatos de supervisión de la infraestructura de claves públicas” en la página 435.

Notas:

1. Para visualizar una lista de los registros de certificados de memoria SRAM utilice el mandato **list certificate** de PKI Talk 6, tal y como se describe en “Mandatos de configuración de la infraestructura de claves públicas” en la página 411.
2. Para suprimir registros de certificados de la memoria SRAM , utilice el mandato **delete certificate** de PKI Talk 6, tal y como se describe en “Mandatos de configuración de la infraestructura de claves públicas” en la página 411.
3. Para eliminar la necesidad de volver a enviar una petición de certificado durante futuras negociaciones de IPSec, utilice el mandato **certificate load** de PKI Talk 5, tal y como se describe en “Mandatos de supervisión de la infraestructura de claves públicas” en la página 435 para cargar el certificado recibido en la antememoria.

Mandatos de configuración de la infraestructura de claves públicas

Add

Utilice el mandato **add** de PKI Talk 6 para configurar el servidor de depósitos de certificados y su ubicación.

Sintaxis:

a**dd** server

server Especifica que la operación de adición se aplica a un servidor.

Ejemplo 1: Adición de 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 **change** de PKI Talk 6 para cambiar el servidor de depósitos de certificados y su ubicación.

Sintaxis:

c**hange**
server

server Especifica que la operación de adición se aplica a un servidor.

Ejemplo 1: Cambio de 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 **delete** de PKI Talk 6 para suprimir un registro de certificados o de claves privadas de la memoria SRAM del direccionador o para suprimir un servidor.

Sintaxis:

delete
- certificate
- private-key
- server

certificate

Especifica que la operación de supresión se aplica a uno o más registros de certificados.

- **all** Especifica que se deben suprimir todos los registros de certificados.
- **id** Especifica el ID del registro del certificado a suprimir.

Ejemplo 1: Supresión de 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: Supresión de claves privadas

```
PKI config>delete private-keys
Private Key Name []? test
Private Key [TEST] deleted successfully
Corresponding box certificate [TEST] deleted successfully
```

Ejemplo 3: Supresión de registros de servidor

```
PKI config>delete server
Name []? myldap
Server MYLDAP deleted successfully
```

private-key

Especifica que la operación de supresión se aplica a uno o más registros de claves privadas.

server Especifica que la operación de supresión se aplica a un servidor.

List

Utilice el mandato **list** de PKI Talk 6 para listar los registros de certificados o de claves de la memoria SRAM de un direccionador o para ver la lista de certificados revocados (CRL; lista de partes habilitadas para ISAKMP, cuyos certificados han sido revocados). Para obtener la CRL actual, utilice el mandato **load** de PKI Talk 6.

Sintaxis:

list certificates
crl
private-keys
servers

certificates
Especifica que la operación de listado se aplica a los registros de certificados.

crl Especifica que la operación de listado se aplica a la lista de certificados revocados.

private-keys
Especifica que la operación de listado se aplica a los registros de claves privadas.

servers Especifica que la operación de listado se aplica a los registros de servidor.

Ejemplo: Listado de 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: Listado de la lista crl

```
PKI config>list crl
```

Ejemplo: Listado de claves privadas

```
PKI config>list private-keys
Private Keys In SRAM:

1) Name W
```

Ejemplo: Listado de 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 **load** de PKI Talk 6 para recuperar la lista de certificados revocados (CRL) más reciente de la CA. Si se quiere garantizar la validez de la copia de la lista, esta operación debe realizarse frecuentemente. Durante el proceso de autenticación, la función IPSec valida el certificado según el contenido de la CRL.

Sintaxis:

load crl

Configuración de la seguridad IP manual (IPv4)

En este apartado se describen las opciones de configuración disponibles para la IPSec manual con IPv4. Todas las funciones IPSec se aplican a IPv4.

Lleve a cabo los siguientes pasos para configurar un túnel manual IPSec:

1. Cree el túnel IPSec.
2. Restablezca IPSec.
3. Configure la política del túnel manual (perfil, validez, política).
4. Restablezca la política.

Configuración de los algoritmos

Puede configurar políticas de túnel con los algoritmos que aparecen en la Tabla 41 en la página 415.

Tabla 41. Algoritmos configurados con varias políticas de túneles	
Política de túnel	**Algoritmos**
AH, AH-ESP o ESP-AH	• Algoritmo de autenticación AH local—Obligatorio • Algoritmo de autenticación AH remota—Opcional
ESP, AH-ESP o ESP-AH	• Algoritmo de cifrado local—Obligatorio • Algoritmo de cifrado remoto—Opcional • Algoritmo de autenticación ESP local—Opcional • Algoritmo de autenticación ESP remota—Opcional **Nota:** Si su carga de software no incorpora cifrado, no verá los parámetros relacionados con el cifrado.

Una política de túnel utiliza un algoritmo local para los paquetes de salida y un algoritmo remoto para los paquetes de entrada. El algoritmo local del direccionador que se encuentra en el extremo más cercano de un túnel debe coincidir con el algoritmo remoto del direccionador que se encuentra en el extremo más alejado del túnel. Los valores de los algoritmos remotos son opcionales y toman por omisión el valor de los algoritmos locales correspondientes. El algoritmo de autenticación ESP local es opcional porque la autenticación ESP es opcional.

Configuración de las claves de cifrado

Para cada algoritmo local que configure debe configurar también una clave que sea idéntica a la clave del algoritmo correspondiente en el sistema principal remoto. Consulte la descripción de las claves del mandato **add tunnel** en “Mandatos de configuración de seguridad IP manual”.

Acceso al entorno de configuración de la seguridad IP

Para acceder al entorno de configuración de la seguridad IP, entre **t 6** en el indicador OPCON (*) y, a continuación, entre la siguiente secuencia de mandatos en el indicador `Config>`:

```
   Config> feature ipsec
IP Security feature user configuration
   IPsec config>ipv4
   IPV4-IPsec config>
```

Mandatos de configuración de seguridad IP manual

En este apartado se describen los mandatos de configuración de la seguridad IP. Entre estos mandatos en el indicador `IPV4-IPsec config>`.

Tabla 42. Resumen de mandatos de configuración de seguridad 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 xxxii.
Add tunnel	Añade un túnel seguro.
Change tunnel	Cambia los valores de los parámetros de configuración de un túnel seguro.
Delete tunnel	Suprime un túnel seguro.
Disable	Inhabilita todo el proceso de seguridad IP de manera segura (se eliminan los paquetes que coinciden con los filtros de paquete), inhabilita todo el proceso de seguridad IP de manera no segura (se aceptan los paquetes que coinciden con los filtros de paquete) o inhabilita un túnel seguro.
Enable	Habilita todo el proceso de seguridad IP o inhabilita un túnel seguro.
List	Lista información global sobre la seguridad IP 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 xxxiii.

Add Tunnel

Utilice el mandato **add tunnel** para añadir los parámetros necesarios para definir un túnel IPSec.

Sintaxis:

add tunnel...

tunnel-name

Parámetro opcional para etiquetar el túnel. Debe ser exclusivo dentro del 2212.

Valores válidos: hasta 15 caracteres; el primer carácter tiene que ser una letra; no se pueden dejar espacios en blanco.

Valor por omisión: ninguno

lifetime

El tiempo en minutos durante el que el túnel puede estar activo. El valor 0 indica que el túnel no caduca nunca.

Valores válidos: 0 - 525600 (0 = no caduca; 525600 = 365 días)

Valor por omisión: 46080 (32 días)

encapsulation-mode

La manera como está encapsulado el paquete IP. En modalidad de túnel, todo el paquete IP se encapsula y se crea una nueva cabecera IP; en modalidad de transporte, la cabecera IP no se encapsula. Si uno de los extremos del túnel seguro es un direccionador, se ***debe*** utilizar, pues, la modalidad de túnel, de acuerdo con el borrador de arquitectura de seguridad del equipo negociador de ingeniería de internet (IETF).

Valores válidos: tunnel (*TUNN*) o translate (*TRANS*)

Valor por omisión: tunnel (*TUNN*)

tunnel-policy
Una de las cuatro opciones que definen la política de túnel: la cabecera de autenticación (AH) de IP, el protocolo Encapsulating Security Payload (ESP) de IP o las combinaciones de dichos 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 autenticación AH se ejecuta en primer lugar en los paquetes de salida. Algunos parámetros son exclusivos de ESP o AH. Los parámetros de cifrado se configuran sólo si ESP, AH-ESP o ESP-AH está seleccionado; los parámetros de autenticación se configuran sólo si AH, AH-ESP o ESP con autenticación está seleccionado.

Valores válidos: AH, ESP, AH-ESP, ESP-AH

Valor por omisión: AH-ESP

local-IP-address
Dirección IP para este extremo del túnel.

Valores válidos: una dirección IP válida que se ha configurado para una interfaz o como dirección interna del 2212.

Valor por omisión: una de las direcciones IP configuradas para el direccionador

local-spi
Una asociación de seguridad es una conexión de seguridad unidireccional 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 seguro. Este parámetro, que es obligatorio, identifica el SPI esperado en este túnel para paquetes de entrada recibidos en el extremo local del túnel. Este valor no puede coincidir con el SPI local de otro túnel que disponga de la misma dirección local de IP. Independientemente de la política de túnel (ESP, AH, AH-ESP o ESP-AH), sólo se configura un SPI local para el tráfico de entrada de un túnel seguro de IP.

Valores válidos: cualquier valor de 32 bits mayor de 255

Valor por omisión: 256

local-encryption-algorithm
El algoritmo de cifrado utilizado para ESP en paquetes de salida enviados desde el direccionador local, que es obligatorio para la configuración de ESP. En algunos países, es probable que algunos o todos estos algoritmos 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 evita que ESP lleve a cabo un cifrado. Este algoritmo está disponible en todos los países. Si se selecciona ESP-NULL, ESP debe activarse para autenticación seleccionando uno de los algoritmos de autenticación HMAC-MD5 o HMAC-SHA-1.

Valores válidos: DES-CBC, CDMF, 3DES o ESP-NULL

Valor por omisión: DES-CBC

local-encryption-key
La clave o claves utilizadas con el algoritmo de cifrado ESP local. Deben coincidir con las claves correspondientes que están configuradas en el extremo opuesto del túnel seguro. Esta clave no está configurada cuando el algoritmo de cifrado ESP-NULL está seleccionado.

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 independientes, sin que se repita ninguna, teniendo cada una 16 caracteres hex (0 - 9, a - f, A - F)

Valor por omisión: ninguno

padding-for-local-encryption
Tamaño en bytes de relleno adicional que se añade a los paquetes ESP de salida. El relleno adicional se puede utilizar para disfrazar el tamaño de los paquetes IP que se están cifrando cuando el algoritmo de cifrado da como resultado un paquete cifrado que es del mismo tamaño que el paquete original. Los valores de relleno ESP deben ser múltiplos de 8. Si se configura un valor que no es divisible por 8, dicho valor se redondea a la alza hasta el siguiente valor que sí que es divisible por 8.

Cuando el algoritmo de cifrado es ESP-NULL, el relleno no es necesario porque el algoritmo ESP-NULL añade un byte al tamaño del paquete original. Si se configura relleno para cifrado local, el valor es ignorado.

Valores válidos: 0 - 120

Valor por omisión: 0

local-ESP-authentication
Selecciona autenticación ESP local, si se desea. La autenticación es obligatoria si el algoritmo de cifrado es ESP-NULL.

Valores válidos: Yes o No

Valor por omisión: Yes

local-authentication-algorithm
Algoritmo de autenticación que se utiliza en los paquetes de salida. Es un parámetro opcional para ESP y no será obligatorio a no ser que se seleccione la autenticación ESP. Para AH , AH-ESP o ESP-AH, este parámetro es obligatorio. El algoritmo de autenticación utilizado debe coincidir con el algoritmo de autenticación remoto utilizado en el extremo más alejado del túnel IPSec.

Valores válidos: HMAC-MD5 o HMAC-SHA

Valor por omisión: HMAC-MD5

local-authentication-key
Clave utilizada con el algoritmo de autenticación local. Debe coincidir con la clave equivalente que está configurada en el extremo opuesto del túnel IPSec. Es obligatorio si la política es AH, AH-ESP o ESP-AH o si la política es ESP y se ha configurado el algoritmo de autenticación 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

remote-IP-address
Dirección IP para el extremo remoto del túnel. Es un parámetro obligatorio.

Valores válidos: una dirección IP válida

Valor por omisión: ninguno

remote-spi
Una asociación de seguridad es una conexión de seguridad unidireccional 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 seguro. Este parámetro, que es obligatorio, identifica el SPI esperado en ESP o AH para paquetes de salida destinados para el sistema principal remoto. Este valor no puede coincidir con el SPI remoto de otro túnel que disponga de la misma dirección remota de IP. Independientemente de la política de túnel (ESP, AH, AH-ESP, or ESP-AH), sólo se configura un SPI local para tráfico de salida para un túnel IPSec.

Valores válidos: cualquier valor de 32 bits mayor de 255

Valor por omisión: 256

remote-encryption-algorithm
Algoritmo de descifrado utilizado en paquetes de entrada recibidos desde el sistema principal remoto. Debe coincidir con el algoritmo de cifrado local.

El algoritmo ESP-NULL evita que ESP lleve a cabo un cifrado. Si se selecciona ESP-NULL, ESP debe activarse para autenticación seleccionando uno de los algoritmos de autenticación HMAC-MD5 o HMAC-SHA-1.

Valores válidos: DES-CBC, CDMF, 3DES o ESP-NULL

Valor por omisión: valor del algoritmo de cifrado local

remote-encryption-key
Clave o claves utilizadas con el algoritmo de cifrado ESP remoto. Deben coincidir con las claves equivalentes que están configuradas en el extremo opuesto del túnel seguro. Esta clave no está configurada cuando el algoritmo de cifrado ESP-NULL está seleccionado.

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 independientes, sin que coincida ninguna, teniendo 16 caracteres en hex (0 - 9, a - f, A - F)

Valor por omisión: ninguno

verification-of-remote-encryption-padding
Determina si el tamaño del relleno del cifrado de los paquetes recibidos debe ser verificado.

Valores válidos: Yes o No

Valor por omisión: No

padding-for-remote-encryption
Tamaño en bytes de relleno adicional que se espera en los paquetes ESP recibidos. Este parámetro es obligatorio y válido si el valor *verification-of-*

remote-encryption-padding es Yes. Los valores de relleno deben ser múltiplos de 8. Si se configura un valor que no es divisible por 8, dicho valor se redondeará al alza hasta el siguiente valor que sí que sea divisible por 8.

Valores válidos: 0 - 120

Valor por omisión: 0

remote-ESP-authentication
Selecciona la autenticación ESP remota para paquetes de entrada, si se desea.

Valores válidos: Yes o No

Valor por omisión: Yes

remote-authentication-algorithm
Algoritmo de autenticación utilizado para paquetes de entrada. Es un parámetro opcional para ESP y no será obligatorio a no ser que se seleccione la autenticación ESP. Este parámetro es obligatorio para AH o combinaciones de AH y ESP (AH-ESP o ESP-AH). El algoritmo de autenticación utilizado debe coincidir con el algoritmo de autenticación local utilizado en el extremo más alejado del túnel IPSec.

Valores válidos: HMAC-MD5 o HMAC-SHA

Valor por omisión: HMAC-MD5

remote-authentication-key
Clave utilizada con el algoritmo de autenticación remota. Debe coincidir con la clave equivalente que está configurada en el extremo opuesto del túnel seguro. Es obligatorio en AH, AH-ESP y ESP-AH y en ESP si el algoritmo de autenticación ESP remota se ha configurado.

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

enable-replay-prevention
Especifica si la prevención de reproducción está habilitada o no. Si la prevención de reproducción está habilitada, los números de secuencia de las cabeceras de seguridad IP se supervisan para evitar que el túnel receptor procese paquetes duplicados. No se recomienda utilizar la prevención de reproducción porque la asociación de seguridad de túnel debe estar desactivada cuando el contador de números de secuencia del emisor alcanza el límite. Cuando ello sucede, es necesaria una intervención manual para reiniciar la asociación de seguridad existente o crear una nueva.

Así mismo, si la prevención de reproducción está habilitada y se reinicia IPSec mediante el mandato **reset ipsec**, debe asegurarse de que IPSec también se reinicia en el direccionador que se encuentra en el otro extremo del túnel IPSec. Ello es necesario para reinicializar el número de secuencias en los dos extremos del túnel. Si IPSec se reinicia en un extremo del túnel y en el otro no, es posible que los direccionadores que se encuentran en cada uno de los extremos del túnel eliminen paquetes a causa de la discrepancia de números de secuencia.

Valores válidos: Yes o No

Valor por omisión: No

DF-bit
Especifica el manejo del bit No fragmentar (DF) en la cabecera externa para túneles seguros de modalidad de túnel. Se puede establecer este bit en cabeceras IPv4 para especificar que el paquete no se puede fragmentar. El parámetro bit DF indica al 2212 cómo debe manejar el bit en paquetes entrantes: ya sea copiando en la cabecera externa el valor del bit DF hallado en la cabecera interna, o estableciendo o borrando el bit en la cabecera externa.

Si se establece el bit DF y el paquete no se puede fragmentar, IPSec utiliza la función Path MTU (PMTU) Discovery. Consulte “Descubrimiento de la unidad de transmisión máxima de la vía de acceso” en la página 397 si desea obtener más información.

Valores válidos: Copy, Set, Clear

Valor por omisión: Copy

enable-tunnel
Especifica si el túnel está habilitado. El túnel habilitado no filtrará paquetes hasta que se haya configurado un filtro de paquete para definir la interfaz sobre la que este túnel IPSec operará y hasta que IP se haya restablecido o reiniciado en el 2212. Puede utilizar el mandato **reset ip** para restablecer IP.

Valores válidos: Yes o No

Valor por omisión: Yes

Change Tunnel

Utilice el mandato **change tunnel** para cambiar un parámetro de túnel IPSec que se haya configurado anteriormente mediante el mandato **add tunnel**.

Sintaxis:

change tunnel ...
Consulte el mandato **add tunnel** para obtener una lista de los parámetros que se pueden cambiar.

Delete Tunnel

Utilice el mandato **delete tunnel** de Talk 6 para suprimir un túnel IPSec.

Sintaxis:

delete tunnel
id-túnel
nombre-túnel
all

id-túnel Especifica el identificador del túnel IPSec que se debe suprimir.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre-túnel
Especifica el nombre del túnel IPSec que se debe suprimir.

Valores válidos: cualquier nombre de túnel configurado

Valor por omisión: ninguno

all Especifica que todos los túneles IPSec de esta interfaz deben ser suprimidos.

Disable

Utilice el mandato **disable** para inhabilitar el túnel IPSec o para inhabilitar todos los túneles IPSec ya sea de manera segura (los paquetes que coinciden con los filtros IPSec se eliminan), ya sea de manera insegura (se aceptan los paquetes que coinciden con los filtros IPSec).

Sintaxis:

d**isable**
ipsec drop
ipsec pass
tunnel ...

ipsec drop
Inhabilita la seguridad IP en el direccionador de manera segura. Todos los túneles IPSec se inhabilitarán pero la información de túnel seguro de las reglas de filtro de paquetes se utiliza para identificar los paquetes que coinciden con los filtros de paquetes de túnel IPSec. Los paquetes coincidentes se eliminan.

ipsec pass
Inhabilita la seguridad IP en el direccionador de manera no segura. Se inhabilitarán todos los túneles IPSec. Los paquetes que coinciden con los filtros de paquetes de túnel se reenvían como tráfico ordinario.

tunnel *id-túnel nombre-túnel* **all**
Inhabilita la seguridad IP en un túnel especificado o en todos los túneles.

id-túnel
Especifica el identificador del túnel seguro que se debe inhabilitar.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre de túnel
Especifica el nombre del túnel seguro que se debe inhabilitar.

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 IP en todas las interfaces o en un único túnel. Debe habilitar IPSec de manera global en el direccionador antes de que los túneles IPSec habilitados de manera individual se activen.

Sintaxis:

e**nable**
ipsec
tunnel ...

ipsec
Habilita la seguridad IP a través del direccionador.

tunnel *id-túnel nombre-túnel* **all**
Habilita la seguridad IP en un túnel especificado o en todos los túneles.

id-túnel
Especifica el identificador del túnel seguro que se debe habilitar.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre de túnel
Especifica el nombre del túnel seguro que se debe habilitar.

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 IP actual. Los túneles globales incluyen todos los túneles del direccionador, tanto activos como definidos. Todos los túneles incluyen todos los túneles configurados en esta interfaz, tanto activos como definidos. Los túneles activos son los que están activos en este momento; los túneles definidos son los que están definidos pero no están activos. Para IPv4, también se listan los certificados seleccionados en la memoria 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 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 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 PMTU del túnel.

Sintaxis:

set path-mtu-age-timer

path-mtu-age-timer
Especifica el tiempo (en minutos) que transcurrirá antes de que el 2212 restaure el valor PMTU del túnel al valor máximo.

Valor por omisión: 10 (0 significa inhabilitado)

Configuración de un túnel manual (IPv4)

Este tema proporciona información sobre la configuración de un túnel manual IPv4 para la red que aparece en la Figura 38 en la página 399.

Configuración del túnel para el direccionador A

El siguiente ejemplo muestra la manera de configurar un túnel manual IPSec para el direccionador A en la red que aparece en la Figura 38 en la página 399 mediante 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 comprobar en este ejemplo, se le solicitan los parámetros que es necesario especificar. La configuración de un túnel ESP, AH-ESP o ESP-AH solicita parámetros similares.

Nota: Los valores de las claves no se visualizan al entrarlos. Por lo tanto, no son visibles en el ejemplo. Si las claves de la autenticación HMAC-MD5 fueran visibles, se verían 32 caracteres hexadecimales. Por ejemplo, una clave puede tener el valor: X' 1234567890ABCDEF1234567890ABCDEF'.

Configuración del túnel para el direccionador B

Debe configurar dentro del direccionador B el mismo túnel manual IPSec que se haya configurado para el direccionador A, túnel 1 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 demás parámetros de túnel IPSec deben coincidir con los parámetros que se han configurado para el direccionador A.

Ejemplo: configuración manual de un túnel de seguridad IP con ESP

Observe que se le solicita que establezca el bit DF cuando el túnel está en modalidad de túnel y la política de túnel es ESP. Este ejemplo muestra sólo la configuración del túnel IPSec, no de los filtros de paquetes.

```
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: configuración manual de un túnel de seguridad IP con ESP y ESP-NULL

Observe que la autenticación es obligatoria.

```
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 IP manual (IPv6)

En este apartado se describen las opciones de configuración disponibles para IPSec manual con IPv6. Todas las funciones IPSec se aplican a IPv6. Observe los siguientes cambios en las preguntas de configuración IPSec al configurar IPSec para IPv6:

- Entre las direcciones en el formato de direcciones IPv6 (por ejemplo, 8:0:9:8::1).
- No se le solicita que establezca el bit DF.

Lleve a cabo los siguientes pasos para configurar un túnel manual IPSec:

1. Cree el túnel IPSec.
2. Restablezca IPSec.
3. Configure las reglas de filtro.
4. Restablezca IPV6.

Configuración de los algoritmos

Puede configurar políticas de túnel con los algoritmos que aparecen en la Tabla 43.

Tabla 43. Algoritmos configurados con varias políticas de túneles

Política de túnel	Algoritmos
AH, AH-ESP o ESP-AH	• Algoritmo de autenticación AH local—Obligatorio • Algoritmo de autenticación AH remota—Opcional
ESP, AH-ESP o ESP-AH	• Algoritmo de cifrado local—Obligatorio • Algoritmo de cifrado remoto—Opcional • Algoritmo de autenticación ESP local—Opcional • Algoritmo de autenticación ESP remota—Opcional **Nota:** Si su carga de software no incorpora cifrado, no verá los parámetros relacionados con el cifrado.

Una política de túnel utiliza un algoritmo local para los paquetes de salida y un algoritmo remoto para los paquetes de entrada. El algoritmo local del direccionador que se encuentra en el extremo más cercano de un túnel debe coincidir con el algoritmo remoto del direccionador que se encuentra en el extremo más alejado del túnel. Los valores de los algoritmos remotos son opcionales y toman por omisión el valor de los algoritmos locales correspondientes. El algoritmo de autenticación ESP local es opcional porque la autenticación ESP es opcional.

Configuración de las claves de cifrado

Para cada algoritmo que configure debe configurar también una clave que sea idéntica a la clave del algoritmo correspondiente en el sistema principal remoto. Consulte la descripción de las claves del mandato **add tunnel** en “Mandatos de configuración de seguridad IP manual” en la página 415.

Acceso al entorno de configuración de la seguridad IP

Para acceder al entorno de configuración de la seguridad IP, entre **t 6** en el indicador OPCON (*) y, a continuación, entre la siguiente secuencia de mandatos en el indicador `Config>`:

```
   Config> feature ipsec
IP Security feature user configuration
IPsec config> ipv6
IPV6-IPsec config>
```

Mandatos de configuración de seguridad IP manual

Consulte “Mandatos de configuración de seguridad IP manual” en la página 415 si desea obtener una descripción de los mandatos de configuración de seguridad IP disponibles para IPv6. Los mandatos para IPv6 son los mismos que los utilizados para IPv4 a menos que se indique lo contrario. Entre los mandatos en el indicador `IPV6-IPsec config>`.

Configuración de un túnel manual (IPv6)

Consulte la red de ejemplo en la Figura 38 en la página 399 mientras lee este tema. El túnel 1 IPSec tiene un extremo en la interfaz 1 del direccionador A. El direccionador A se configurará para IPSec. Lleve a cabo los siguientes pasos para configurar un direccionador A manualmente:

1. Cree el túnel IPSec.
2. Cree un filtro de paquetes de salida en la interfaz del direccionador que es el extremo final del túnel IPSec.
3. Cree reglas de control de acceso para los filtros de paquetes.
4. Restablezca IPSec.
5. Restablezca IPv6.

Creación del túnel de seguridad IP para el direccionador A

El siguiente ejemplo muestra la manera de crear el túnel 1 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 comprobar en este ejemplo, se le solicitan los parámetros que es necesario especificar. La configuración de un túnel ESP, AH-ESP o ESP-AH solicita parámetros similares.

Nota: Los valores de las claves no se visualizan al entrarlos. Por lo tanto, no son visibles en el ejemplo. Si las claves de la autenticación HMAC-MD5 fueran visibles, vería 32 caracteres hex. Por ejemplo, una clave puede tener un valor X'1234567890ABCDEF1234567890ABCDEF'.

Configuración de filtros de paquetes para el direccionador A

Después de haber creado el túnel IPSec para el direccionador A, debe definir un filtro de paquetes IP. La creación del filtro de paquetes *out-router-A* aparece en el siguiente ejemplo. Consulte los apartados Filtros IPv6 y Control de acceso del capítulo Utilización de IPv6 de la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 1* si desea obtener más información sobre la configuración de filtros de paquetes IPv6 y reglas de control de acceso.

```
*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 las reglas del control de acceso de filtros de paquetes para el direccionador A

El siguiente paso es la configuración de las reglas de control de acceso de filtros de paquetes. Cree dos reglas de control de acceso en el filtro de paquetes de salida *out-router-A*.

Las reglas de control de acceso del filtro de paquetes de salida llevan a cabo las siguientes funciones:

- Una de las reglas de control de acceso define el rango de las direcciones fuente y destino de los paquetes que deben pasar al túnel IPSec.
- La otra regla de control de acceso permite que el tráfico IPSec pase a través del filtro de paquetes.

Configure la primera regla de control de acceso para el filtro de paquetes *out-router-A*. Esta regla 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 regla de control de acceso para *out-router-A* permite que los paquetes seguros pasen entre los dos extremos del túnel 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>
```

Como ocurre con los demás filtros de paquetes, es probable que desee configurar una regla de control de acceso comodín para que *out-router-A* pase tráfico que no coincida con ninguna de las reglas de control de acceso.

Restablecimiento de la seguridad IP y de IP en el direccionador A

Cuando acabe de configurar la política, utilice el mandato **reset ipsec** de Talk 5 para volver a cargar la memoria SRAM con la nueva configuración IPSec. El mandato **reset ipsec** no afecta a ninguna configuración IP. A continuación, utilice el mandato **reset ipv6** de Talk 5 para restablecer de manera dinámica IPv6 dentro del direccionador. Como alternativa, también puede reiniciar el direccionador para restablecer cada componente. Puede restablecer IPSec y IPv6 o reiniciar el direccionador para garantizar que las reglas de filtro se vuelven a cargar. De lo contrario, es probable que la configuración no reciba el soporte adecuado en la interfaz. Consulte el “Configuración y supervisión de la seguridad IP” en la página 409 y el mandato **reset ipv6** de la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 2* si desea obtener más información.

Tal y como aparece en la Figura 38 en la página 399, el túnel 2 IPSec tiene un extremo en la interfaz 1 del direccionador B. Lleve a cabo los siguientes pasos para configurar el direccionador B manualmente.

1. Cree el túnel IPSec.
2. Cree un filtro de salida en la interfaz del direccionador que es el extremo final del túnel IPSec.
3. Cree reglas de control de acceso para los filtros de paquetes.
4. Restablezca IPSec.
5. Restablezca IPv6.

Creación del túnel de seguridad IP para el direccionador B

Dentro del direccionador B, se debe crear el mismo túnel IPSec, túnel 2 de IPSec, que se ha creado para el direccionador A. 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 IPSec deben coincidir con los parámetros que se han especificado para el direccionador A.

Configuración de filtros de paquetes para el direccionador B

Tal y como hizo para el direccionador A, configure un filtro de paquetes de salida (*out-router-B*) en la interfaz 1, que es la interfaz del direccionador B que es el extremo final del túnel 1 de IPSec.

Configuración de las reglas de control de acceso del filtro de paquetes para el direccionador B

Configure una regla de control de acceso en *out-router-B* para pasar paquetes de salida desde la red 3000:1:: a IPSec para proceso y transmisión a través del túnel 2 de IPSec. Esta regla de control de acceso es del 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 cree para *out-router-B*, una regla de control de acceso inclusiva que permita que los paquetes que IPSec ha procesado pasen a través del túnel 2 IPSec.

```
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 *out-router-B*, cree una regla de control de acceso comodín inclusiva si desea aceptar, en lugar de eliminar, los paquetes que no coinciden con una de las dos reglas de control de acceso, por ejemplo, tráfico no destinado al túnel 2 de IPSec.

Restablecimiento de la seguridad IP y de IPv6 en el direccionador B

Antes de que la función IPSec funcione y de que se activen los filtros, debe restablecer IPSec e IPv6. Utilice el mandato **reset IPSec** de Talk 5 para restablecer IPSec e IPv6. Consulte “Restablecimiento de la seguridad IP y de IP en el direccionador A” en la página 430 si desea obtener más información sobre el restablecimiento de IPSec. Después de restablecer IPSec, utilice el mandato **reset IPv6** de Talk 5 para reiniciar IPv6. Como alternativa, también puede reiniciar el direccionador para restablecer cada componente.

Ejemplo: configuración de un túnel de seguridad IP con ESP

Observe que este ejemplo muestra sólo la configuración del túnel IPSec, no la de los filtros de paquetes.

```
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 IP con ESP y ESP-NULL

Observe que la autenticación es obligatoria.

```
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 IP manual (IPv4)

En este apartado se explica la manera de supervisar IPSec manual con IPv4. Describe la manera de acceder al entorno intercambio de claves en Internet y los mandatos disponibles.

Acceso al entorno intercambio de claves en Internet

En este apartado se explica la manera de utilizar el protocolo intercambio de claves en Internet (IKE) con IPv4.

Para acceder al entorno de supervisión de IKE de la seguridad IP, entre la secuencia de mandatos siguiente en el indicador +:

```
+ feature ipsec
IPSP>ike
IKE>
```

Mandatos de supervisión de intercambio de claves en Internet

En este apartado se describen los mandatos de supervisión de IKE.

Tabla 44. 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 xxxii.
Delete	Suprime de manera dinámica un SA de Fase 1 ISAKMP de un túnel específico o todos los SA de Fase 1.
List	Lista información sobre un SA de Fase 1 de un túnel específico o de todos los SA de Fase 1.
Stats	Visualiza las estadísticas de un túnel.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiii.

Delete

Utilice el mandato **delete** de IKE para suprimir de manera dinámica un SA de Fase 1 de un túnel o todos los SA de Fase 1.

Sintaxis:

de**lete**
- tunnel
- all

tunnel Especifica que se debe suprimir un SA de Fase 1 para un túnel específico.

all Especifica que se deben suprimir todos los SA de 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 un SA de Fase 1 de un túnel específico o sobre todos los SA.

Sintaxis:

list
- tunnel
- all

tunnel Especifica que se debe visualizar información de SA de un túnel específico.

all Especifica que se debe visualizar información de todos los SA.

Ejemplo: Listado de información de todos los 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 de túnel o id de túnel.

Ejemplo: Visualización de las 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 la infraestructura de claves públicas (IPv4)

En este apartado se explica la manera de utilizar la infraestructura de claves públicas (PKI) con IPv4.

Para acceder al entorno de supervisión de PKI de la seguridad IP, entre la siguiente secuencia de mandatos en el indicador +:

```
+ feature ipsec
IPSP>pki
PKI>
```

Mandatos de supervisión de la infraestructura de claves públicas

En este apartado se describen los mandatos de supervisión de la infraestructura de claves públicas (PKI).

Tabla 45. 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 xxxii.
Cert-load	Carga un certificado en la memoria SRAM de un direccionador.
Cert-req	Envía una petición de certificado a una CA.
Cert-save	Guarda un certificado en la antememoria para su posible uso futuro.
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 SRAM en la antememoria en 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 xxxiii.

Cert-load

Utilice el mandato de PKI **cert-load** para cargar un registro que contenga el certificado y la clave privada de SRAM en la antememoria de certificados en tiempo de ejecución.

Sintaxis:

cert-load

Ejemplo: Carga de un registro de certificado de SRAM a 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: Petición 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** 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 SRAM a la antememoria en tiempo de ejecución.

Sintaxis:

load certificate

Ejemplo: Carga de un certificado en la 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 la seguridad IP (IPv4)

Para acceder al entorno de supervisión de la seguridad IP de IPv4, escriba **t 5** en el indicador OPCON (*):

```
* t 5
```

A continuación, entre la siguiente secuencia de mandatos en el indicador +:

```
+ feature ipsec
IPSP>ipv4
IPV4-IPsec>
```

Mandatos de supervisión de la seguridad IP (IPv4)

En este apartado se describen los mandatos de supervisión de la seguridad IP.

Tabla 46. Resumen de mandatos de supervisión de la seguridad 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 xxxii.
Change tunnel	Cambia de manera dinámica los valores de los parámetros de configuración de un túnel seguro.
Delete tunnel	Suprime de manera dinámica un túnel seguro.
Disable	Inhabilita de manera dinámica todo el proceso de seguridad IP de manera segura (los paquetes coincidentes se eliminan), inhabilita todo el proceso de seguridad IP de manera no segura (se reenvían los paquetes coincidentes) o inhabilita un túnel seguro concreto.
Enable	Habilita de manera dinámica todo el proceso de seguridad IP o habilita un túnel seguro.
Itp	Hace ping en el túnel de seguridad IP. Determina si es posible ponerse en contacto con la parte del extremo más alejado de un túnel IPSec.
List	Lista información global sobre la seguridad IP y sobre túneles activos y definidos.
Reset	Restablece la seguridad IP o restablece un túnel seguro. Este mandato vuelve a cargar la configuración que se ha creado en Talk 6. Al restablecer se alterarán temporalmente los valores de los parámetros configurados mediante Talk 5 por los que se hayan configurado mediante Talk 6.
Set	Establece de manera dinámica el temporizador de antigüedad Path MTU (PMTU).
Stats	Visualiza estadísticas de todos los túneles o de 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 xxxiii.

Change Tunnel

Cambia de manera dinámica un túnel seguro.

Sintaxis:

c**hange** t**unnel ...**

Consulte la descripción del mandato **add tunnel** en “Mandatos de configuración de seguridad IP manual” en la página 415 si desea obtener una descripción de los parámetros.

Delete Tunnel

Utilice el mandato **delete** para suprimir de manera dinámica un túnel seguro o todos los túneles seguros.

Sintaxis:

delete t**unnel**

id-túnel
nombre-túnel
all

id-túnel Especifica el identificador del túnel IPSec que se debe suprimir.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre-túnel
Especifica el nombre del túnel IPSec que se debe suprimir.

Valores válidos: cualquier nombre de túnel configurado

Valor por omisión: ninguno

all Especifica que todos los túneles IPSec de esta interfaz deben ser suprimidos.

Disable

Utilice el mandato **disable** para inhabilitar de manera dinámica el protocolo de seguridad IP en todas las interfaces o en un solo túnel.

Sintaxis:

di**sable**
ipsec drop
ipsec pass
tunnel ...

ipsec drop
Inhabilita la seguridad IP en el direccionador de manera segura. Todos los túneles IPSec se inhabilitarán pero la información de túnel seguro de las reglas de filtro de paquetes se utiliza para identificar los paquetes que coinciden con los filtros de paquetes de túnel IPSec. Los paquetes coincidentes se eliminan.

ipsec pass
Inhabilita la seguridad IP en el direccionador de manera no segura. Se inhabilitarán todos los túneles IPSec. Los paquetes que coinciden con los filtros de paquetes de túnel se reenvían como tráfico ordinario.

tunnel *id-túnel* **all**
Inhabilita la seguridad IP en un túnel especificado o en todos los túneles.

id-túnel
Especifica el identificador del túnel seguro que se debe inhabilitar.

Valores válidos: 1 - 65535

Valor por omisión: 1

all Todos los túneles.

Enable

Utilice el mandato **enable** para habilitar de manera dinámica el protocolo de seguridad IP en todas las interfaces o en un solo túnel. Debe habilitar IPSec de manera global en el direccionador antes de que los túneles IPSec habilitados de manera individual se activen.

Nota: No se puede habilitar dinámicamente a IPSec si el direccionador se ha reiniciado con IPSec inhabilitado.

Sintaxis:

e**nable**
    ipsec
    tunnel ...

ipsec
    Habilita la seguridad IP a través del direccionador.

tunnel *id-túnel* **| all**

id-túnel
    Especifica el identificador del túnel seguro que se debe habilitar.

    Valores válidos: 1 - 65535

    Valor por omisión: 1

all Todos los túneles.

Itp

Utilice el mandato **itp** (hace ping en un túnel IPSec) para crear y enviar un paquete IP especial a través de un túnel IPSec, lo que, en caso de que éste responda devolviendo el paquete, permite verificar que el direccionador del extremo más alejado del túnel puede responder. El paquete se envía repetidamente con la frecuencia especificada en el argumento rate (cadencia) hasta que se pulse la tecla **Intro**, lo cual interrumpe el mandato. Al pulsar la tecla **Intro**, itp imprime el estado de todos los paquetes enviados.

Nota: El mandato **itp** solamente funciona en túneles que funcionen en la modalidad de túnel. Además, el otro direccionador debe ser capaz de reenviar paquetes IP y debe tener habilitada esa función.

Sintaxis:

itp tunnel-id
    size
    rate

tunnel-id
    Obligatorio. Entero con signo de dos bytes asignado a un túnel concreto.

size Opcional. Tamaño de la carga útil de los datos del paquetes de ping. Este valor debe ser mayor que el tamaño mínimo creado por itp y menor que la MTU del túnel.

rate Opcional. Frecuencia (en segundos) a la que se transmitirá el paquete de datos de ping.

    Valor por omisión: 1

List

Utilice el mandato **list** para visualizar la configuración de seguridad IP actual. Los túneles globales incluyen todos los túneles del direccionador, tanto activos como definidos. Todos los túneles incluyen todos los túneles configurados en esta interfaz, tanto activos como definidos. Los túneles activos son los que están activos en este momento; los túneles definidos son los que 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 uno de los túneles definidos

```
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 uno de los túneles activos

```
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 IP es IPv4, se visualiza un mensaje que define el manejo del bit DF: COPY, SET o CLEAR.

Reset

Utilice el mandato **reset** para restablecer de manera dinámica la seguridad IP en el direccionador o en un solo túnel. Después de reiniciar IPSec o los túneles, asegúrese de que utiliza el mandato **reset IP** para restablecer la configuración IP. Esto es necesario para volver a cargar información del control de acceso como los filtros de paquetes y sus reglas de control de acceso. Si no restablece IP, es probable que los filtros de paquetes y las reglas de control de acceso no ofrezcan soporte a la nueva configuración IPSec.

Como alternativa a la utilización de los mandatos **reset**, se puede rearrancar el direccionador. De todos modos, si rearranca el direccionador, lo aísla de la red durante unos instantes, mientras que los mandatos **reset** sólo interrumpen las funciones de IP.

Sintaxis:

reset
ipsec
tunnel *id-túnel nombre-túnel* all

ipsec
Restablece la seguridad IP en el 2212. La seguridad IP se inhabilita de manera temporal y, a continuación, se reinicia. Mientras la seguridad IP está inhabilitada, los paquetes que normalmente manejan los túneles IPSec se eliminan hasta que el reinicio ha finalizado. Reiniciar la seguridad IP no afecta a otras funciones del 2212. Este mandato activa la configuración de seguridad que se ha creado mediante Talk 6. La configuración de seguridad IP de Talk 6 sobreescribe la configuración Talk 5.

tunnel
Restablece la seguridad IP en un túnel especificado. Si el túnel está inhabilitado en el momento del reinicio, la configuración del túnel se reconstruye a partir de la configuración de SRAM, pero el túnel permanece inhabilitado después del reinicio.

id-túnel
Especifica el identificador del túnel seguro a iniciar.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre de túnel
Especifica el nombre del túnel seguro a iniciar.

Valores válidos: cualquier nombre de túnel configurado

Valor por omisión: ninguno

all Todos los túneles.

Set

Establece de manera dinámica el temporizador de antigüedad Path MTU (PMTU).

Sintaxis:

set path

path
Este parámetro define el tiempo en minutos que transcurrirá antes de que el 2212 establezca de nuevo MTU en su valor máximo.

Valor por omisión: 10 (0 significa inhabilitado)

Stats

Utilice el mandato **stats** para visualizar estadísticas sobre un túnel específico o sobre 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 seguro.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre-túnel
Especifica el nombre de un túnel seguro 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 2212.

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 la seguridad IP manual (IPv6)

En este apartado se explica la manera de supervisar IPSec manual con IPv6. Describe la manera de acceder al entorno de seguridad IP y los mandatos disponibles.

Acceso al entorno de supervisión de la seguridad IP

Para acceder al entorno de supervisión de la seguridad IP, escriba **t 5** en el indicador OPCON (*):

```
* t 5
```

A continuación, entre la siguiente secuencia de mandatos en el indicador +:

```
+ feature ipsec
IPSP>ipv6
IPV6-IPsec>
```

Mandatos de supervisión de la seguridad IP (IPv6)

Los mandatos de supervisión de la seguridad IP para IPv6 son los mismos que los utilizados para IPv4, a menos que se indique lo contrario. Consulte “Mandatos de supervisión de la seguridad IP (IPv4)” en la página 438 si desea obtener una descripción de los mandatos. Entre los mandatos en el indicador `IPV6-IPsec>`.

Soporte de reconfiguración dinámica de la seguridad IP

En este apartado se describe la reconfiguración dinámica (DR) y cómo afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

La seguridad IP (IPSec) no da soporte al mandato **delete interface** de CONFIG (Talk 6).

Mandato activate interface de GWCON (Talk 5)

El mandato **activate interface** de GWCON (Talk 5) no es aplicable a IPSec. IPSec no depende de ninguna interfaz en concreto.

Mandato reset interface de GWCON (Talk 5)

El mandato **reset interface** de GWCON (Talk 5) no es aplicable a IPSec. IPSec no depende de ninguna interfaz en concreto.

Mandatos de restablecimiento de componente de GWCON (Talk 5)

IPSec da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos de IPSec:

Mandato GWCON, feature IPSec, Ipv4, reset IPSec

Descripción: IPSec se reinicializará.

Efecto en la red: Cuando IPSec se restablece, se cierran todos los túneles. Los túneles manuales se volverán a crear a partir de la memoria SRAM. Los túneles negociados desaparecerán. Esto provocará que el tráfico que utiliza esos túneles se detenga momentáneamente.

Limitaciones: Ninguna.

En la tabla siguiente se resumen los cambios en la configuración de la función de seguridad IP que se activan cuando se ejecuta el mandato **GWCON, feature IPSec, ipv4, reset IPSec**:

Mandatos cuyos cambios se activan al ejecutar 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: Un túnel o todos los túneles se reinicializarán.

Efecto en la red: Se puede restablecer un túnel o todos lo túneles. Los túneles manuales se volverán a crear a partir de la memoria SRAM. Los túneles negociados desaparecerán. Esto provocará que el tráfico que utiliza esos túneles se detenga momentáneamente.

Limitaciones: Ninguna.

En la tabla siguiente se resumen los cambios en la configuración de la función de seguridad IP que se activan al ejecutar el mandato **GWCON, feature IPSec, ipv4, reset tunnel**:

Mandatos cuyos cambios se activan al ejecutar 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 da soporte a los siguientes mandatos de GWCON que cambian temporalmente el estado operativo del dispositivo. Estos cambios se perderán si el dispositivo se reinicia, si se vuelve a cargar, o si se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
GWCON, feature ipsec, ipv4, change tunnel **Nota:** Los parámetros de un túnel pueden cambiarse en memoria.
GWCON, feature ipsec, ipv4, disable tunnel **Nota:** Se puede inhabilitar un túnel o todos los túneles. El tráfico de esos túneles se detendrá.
GWCON, feature ipsec, ipv4, disable IPSec pass **Nota:** Se inhabilita IPSec y el tráfico se reenviará sin seguridad.
GWCON, feature ipsec, ipv4, disable IPSec stop **Nota:** Se inhabilita IPSec y el tráfico se descartará.
GWCON, feature ipsec, ipv4, delete tunnel **Nota:** Suprime uno o todos los túneles. El tráfico de esos túneles se descartará.
GWCON, feature ipsec, ipv4, enable tunnel **Nota:** Habilita uno o todos los túneles. Se permitirá el tráfico a través de esos túneles.
GWCON, feature ipsec, ipv4, enable IPSec **Nota:** Habilita IPSec. IPSec puede procesar tráfico.
GWCON, feature ipsec, ipv4, set path-MTU-age-timer **Nota:** Cambia el temporizador de antigüedad Path MTU.

Mandatos no reconfigurables dinámicamente

En la tabla siguiente se describen los mandatos de configuración de la función de seguridad IP que no pueden modificarse dinámicamente. Para activarlos es necesario reiniciar o volver a cargar el dispositivo.

Mandatos
CONFIG, enable ipsec **Nota:** La primera vez que se habilita IPSec después de haber inicializado el dispositivo, éste tiene que reiniciarse o volver a cargarse.

Utilización de la función de servicios diferenciados

En este capítulo se describe la manera de utilizar la función de servicios diferenciados (DiffServ) para que un direccionador pueda proporcionar servicio preferente a los paquetes de datos IP adecuados. Según la información de la cabecera IP, el direccionador clasifica paquetes comparándolos con las configuraciones predefinidas en la base de datos de política (creada con la función de política). Consulte el “Utilización de la función de política” en la página 309 si desea obtener información detallada al respecto. Como resultado, algunos paquetes pueden recibir servicio preferente. Este capítulo consta de los apartados siguientes:

- “Visión general de los servicios diferenciados”
- “Terminología de los servicios diferenciados” en la página 455
- “Configuración de los servicios diferenciados” en la página 456

Visión general de los servicios diferenciados

La mayoría de dispositivos de reenvío instalados en una red IP proporcionan un servicio estándar optimizado para los paquetes de datos basado en el modelo "el primero que llega es el primero en ser servido". Este método de entrega es el adecuado para la mayoría de tráfico pero emergen nuevas aplicaciones que requieren una transmisión más rápida y fácil de algunos paquetes.

La función de servicios diferenciados (DiffServ) proporciona diferentes niveles de servicio a paquetes IP cuando un direccionador los procesa para transmitirlos. DiffServ proporciona a algunos paquetes servicio preferente al reservarles recursos del sistema (almacenamientos intermedios) y recursos de enlace (ancho de banda). Una función clasificadora DiffServ determina el tipo de servicio que se ofrece a los paquetes IP examinando varios campos en la cabecera IP, por ejemplo, rangos de direcciones IP de origen y destino y números de puerto, el tipo de protocolo y el byte DS entrante (TOS). Para poder llevar a cabo su tarea de una manera adaptable, los flujos individuales se unen en corrientes. Las corrientes son las entidades mediante las que DiffServ gestiona el acceso a almacenamientos intermedios y ancho de banda. La Figura 39 muestra cómo DiffServ procesa los paquetes de una corriente.

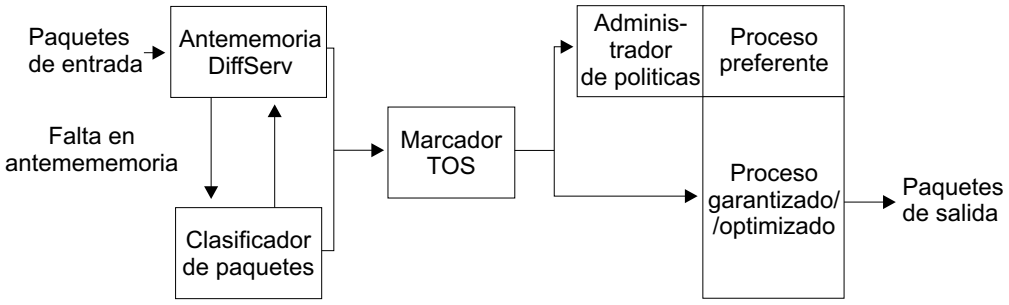


Figura 39. Ruta que sigue un paquete de datos de DiffServ

Además del servicio tradicional optimizado, DiffServ proporciona los siguientes tipos de servicio:

Reenvío acelerado (EF) El servicio de reenvío acelerado es la implementación de DiffServ de un servicio preferente y ambos términos se utilizan indistintamente en el texto siguiente. Este servicio garantiza una tasa de transmisión específica y un retraso menor que los de los servicios de reenvío garantizado u optimizado. Si se genera demasiado tráfico, DiffServ descarta el tráfico sobrante. La cola preferente proporciona servicio EF y aparece en la Figura 40 en la página 451 como cola EF.

Reenvío garantizado (AF) El servicio de reenvío garantizado es la implementación de DiffServ de un servicio garantizado y ambos términos (reenvío garantizado y servicio garantizado) se utilizan indistintamente en este texto. El servicio AF garantiza una tasa de transmisión específica, pero no ofrece garantías sobre los retrasos. Si existen recursos desocupados, DiffServ puede enviar el tráfico sobrante a una tasa mayor.

Opcionalmente, el tráfico de AF se puede medir y vigilar mediante la configuración de la política. Los tipos de vigilancia que se soportan son los del marcador de tres colores (TCM) de una tasa y de dos tasas. TCM permite clasificar los paquetes o volverlos a marcar dependiendo de las características del tráfico entrante. Los colores con que se clasifican los paquetes son: verde, amarillo y rojo. La política contempla la posibilidad de especificar umbrales para la clasificación de colores. La cola AF/BE ofrece el servicio AF y se muestra en Figura 40 en la página 451.

Optimizado (BE) Se trata del servicio optimizado estándar que no ofrece garantías sobre el servicio ni sobre los retrasos. Se debe encontrar un equilibrio entre reservar recursos para los servicios EF y AF y dejar suficientes recursos libres para que el tráfico optimizado reciba un servicio adecuado. La cola AF/BE proporciona servicio BE y aparece en Figura 40 en la página 451.

Los direccionadores locales crean y envían paquetes de control, por lo que también debe dejar suficientes recursos libres para que reciban un servicio adecuado.

La medición, el marcado y la vigilancia de DiffServ en un direccionador periférico, permiten que el direccionador central de redes en que está habilitada la función DiffServ clasifique los paquetes basándose en el elemento de código DS (TOS) y controlar la congestión descartando el tráfico que no satisface determinados criterios o reduciendo su nivel de servicio. Por ejemplo, el direccionador central puede descartar todos los paquetes rojos, reenviar los amarillos como optimizados y los verdes con una probabilidad baja de descartarlos. Esto ayuda a que en las redes en que está habilitada la función DiffServ la velocidad de transmisión del tráfico preferente sea mayor y el retardo menor.

La función DiffServ está implementada actualmente en enlaces PPP, PPP de multienlace y Frame Relay, y puede utilizarla el subsistema RSVP. La Figura 39 en la página 449 muestra cómo se procesan los paquetes de una corriente. Cuando un direccionador recibe el primer paquete de un flujo (suponiendo que se le ha asignado un servicio preferente), no existe ninguna indicación de su categoría de servicio en la antememoria de DiffServ, de manera que el paquete es procesado por la vía lenta. DiffServ ejecuta una búsqueda en la base de datos de políticas para obtener los criterios de manejo de paquetes (política). La acción definida por la política se guarda en la antememoria de DiffServ. Cuando el direccionador recibe un paquete posterior de este flujo, ya existe una entrada en la antememoria

de DiffServ para dicho flujo con lo que se aplica la acción definida por la política y el paquete toma la vía rápida. Por lo tanto, los paquetes posteriores procedentes de este flujo reciben un servicio preferente.

La Figura 40 muestra la relación entre el vigilante, la gestión del almacenamiento intermedio, las colas y el planificador—algunos de los componentes básicos que proporcionan diferentes niveles de calidad de servicio (Qos).

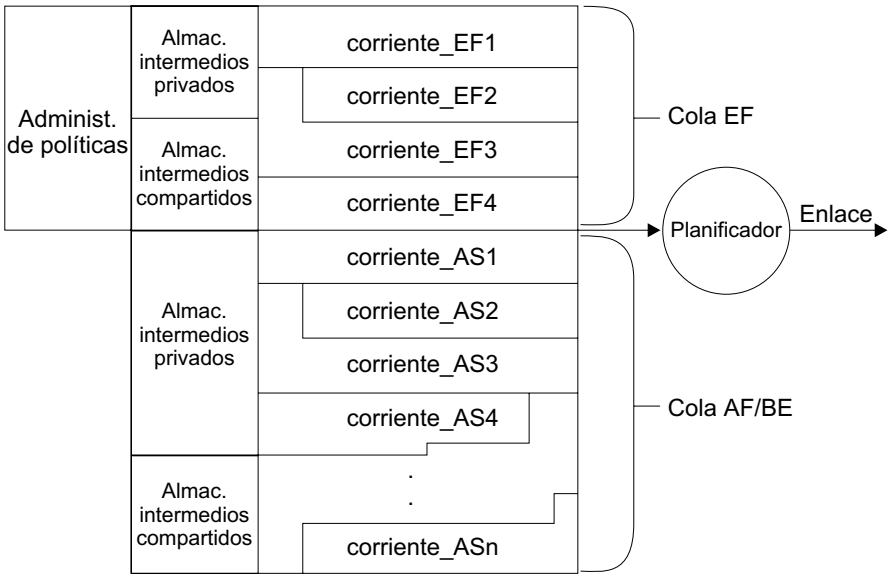


Figura 40. Relación entre el vigilante, los almacenamientos intermedios, las colas y el planificador

Los servicios de reenvío acelerado (EF) y reenvío garantizado (AF) tienen distintas características soportadas por tres funciones del direccionador: (1) el contador y el vigilante, (2) la gestión de almacenamientos intermedios y de colas, y (3) el planificador. Dichas funciones proporcionan un control más sofisticado del tráfico que el disponible en un dispositivo direccionador BE tradicional.

Después de haber utilizado la función de política para configurar las políticas adecuadas, el primer paso para implementar DiffServ es utilizar los mandatos de DiffServ **enable ds** para habilitar la función DiffServ y **set interface** para habilitar la interfaz de salida.

Se pueden configurar opciones de DiffServ de tal manera que los recursos de la red se comprometan o se reserven en exceso, es decir, los controles del condicionador de tráfico están configurados como si hubiera más ancho de banda o almacenamiento intermedio que los que hay realmente disponibles. DiffServ no da soporte a los excesos de reservas.

Si una corriente DiffServ queda desocupada (no se han enviado paquetes en la corriente durante algún tiempo), el sistema reclama los recursos para que otras corrientes puedan utilizarlos. Si la corriente se reactiva, los recursos vuelven a él. Si los recursos ya no están disponibles a causa de un exceso de reserva, DiffServ intenta de manera periódica volver a asignar los recursos.

En qué consiste el elemento de código de DiffServ

DiffServ proporciona una cabecera que sustituye el octeto de TOS de IPv4 (descrito en el documento RFC 791), que consta de un byte llamado campo Diffserv (DS) (que se muestra en la Figura 41). Los seis bits más significativos del campo DS se utilizan como elemento de código de DiffServ (DSCP) para determinar el comportamiento en cada salto (PHB). Los dos bits restantes se reservan para su uso futuro. El ejemplo siguiente muestra el formato del campo DS:

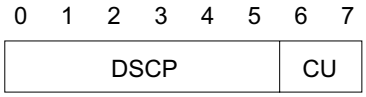


Figura 41. Formato del elemento de código de DiffServ para la cabecera del octeto de TOS de IPv4

donde:

DSCP = elemento de código de los servicios diferenciados
CU = en la actualidad no se utiliza

El elemento de código recomendado para el PHB de EF es 101110xx.

La Figura 42 muestra el formato del campo DS para el PHB de AF:

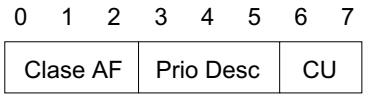


Figura 42. Formato del elemento de código de DiffServ para la cabecera del PHB de AF

donde:

Tres bits para el tipo de clase de AF
001 - clase AF11
010 - clase AF21
011 - clase AF31
100 - clase AF41
Tres bits para la prioridad de descarte
010 - Prioridad de descarte baja, equivalente al color verde en TCM
100 - Prioridad de descarte media, equivalente al color amarillo en TCM
110 - Prioridad de descarte alta, equivalente al color rojo en TCM
CU = en la actualidad no se utiliza

En la lista siguiente se muestran los valores recomendados de los elementos de código de AF con clases de AF y los valores de prioridad de descarte:

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

En qué consisten los contadores y el vigilante

Es posible medir y vigilar tráfico de EF y de AF, si se especifica en la política. El algoritmo EF mide el tráfico y descarta los paquetes que sobrepasan determinado umbral. El algoritmo AF mide el tráfico y posiblemente vuelve a marcar los paquetes, pero no los descarta.

Reenvío acelerado (EF)

El tráfico de EF tiene un vigilante por omisión basado en contenedores de fichas, que descarta paquetes si superan el valor especificado en la configuración del parámetro del ancho de banda de la política. Se pueden especificar los parámetros tasa de reposición de fichas (TR) y tamaño del contenedor de fichas (TBS) para modificar el funcionamiento por omisión del vigilante. El contador determina si el contenedor contiene el número suficiente de fichas para enviar un paquete. Si hay fichas disponibles, el paquete se envía. Si no, el vigilante descarta el paquete. El contenedor repone fichas a la tasa especificada por el parámetro tasa de reposición de fichas. La tasa de reposición de fichas se mide en bytes por segundo, es decir, incluye la cabecera IP, pero no las cabeceras específicas del enlace. La tasa de reposición de fichas se mide antes de comprimir la cabecera IP y de realizar las operaciones de cifrado y de compresión de datos del protocolo de capa 2. El parámetro tamaño del contenedor de fichas se utiliza para manejar ráfagas que temporalmente sobrepasan el límite de la tasa, sin penalizar el tráfico.

Reenvío garantizado (AF)

El tráfico de AF tiene tres opciones de vigilancia: (1) marcador de tres colores de una tasa (srTCM), (2) marcador de tres colores de dos tasas (trTCM) y (3) ninguna (sin vigilancia). Estas opciones de vigilancia están disponibles para las clases AF1, AF2, AF3 y AF4 y se especifican durante la configuración de la política.

La opción srTCM mide una corriente de tráfico según un algoritmo de contenedores de fichas de dos contenedores y una única tasa de reposición de fichas. Marca sus paquetes como verdes, amarillos o rojos, de acuerdo con tres parámetros de tráfico: (1) la tasa de información comprometida (CIR; Committed Information Rate), (2) el tamaño de ráfagas comprometido (CBS, Committed Burst Size) y (3) el tamaño de ráfagas en exceso (EBS, Excess Burst Size). Un paquete se marca de color verde si no sobrepasa el CBS, amarillo si sobrepasa el CBS pero no el EBS y, en rojo si sobrepasa el EBS. La CIR se mide en bytes de paquetes IP por segundo, es decir, incluye la cabecera IP, pero no las cabeceras específicas del enlace. La CIR se mide antes de comprimir la cabecera IP y de realizar las operaciones de cifrado y de compresión de datos del protocolo de capa 2. El CBS y el EBS se miden en bytes.

El contador funciona en dos modalidades: sensible a los colores y no sensible a los colores. En la modalidad no sensible a los colores, se supone que los paquetes entrantes están marcados de color verde, sea cual sea el valor de los bits de prioridad de descarte de su elemento de código DS. CBS representa el tamaño del contenedor verde, y EBS representa el tamaño del contenedor amarillo. En primer lugar, se comprueba si hay fichas disponibles en el contenedor verde. Si hay bastantes fichas verdes, el paquete se marca de color verde y se envía. Si no hay bastantes fichas verdes, se comprueba el contenedor amarillo. Si hay bastantes fichas amarillas, el paquete se marca de color amarillo y se envía. Si no hay bastantes fichas amarillas, el paquete se marca de color rojo. En la modalidad sensible al color, se comprueba el color del paquete entrante y a continuación se comprueba el contenedor del color respectivo. Si hay fichas disponibles, se enviará tal

como se ha recibido. Si no, se reducirá su valor de prioridad de descarte según corresponda. La modalidad sensible a los colores es útil si los paquetes de entrada ya están clasificados y se han marcado previamente con colores.

La opción trTCM también es un algoritmo de contenedores de fichas, parecido al de la opción srTCM, excepto que proporciona tasas de reposición independientes para los contenedores verde y amarillo. Los parámetros de configuración son: (1) la tasa de información comprometida (CIR), (2) el tamaño de ráfagas comprometido (CBS), (3) la tasa de información pico (PIR, Peak Information Rate) y (4) el tamaño de ráfagas pico (PBS, Peak Burst Size). CBS representa el tamaño del contenedor verde y PBS representa el tamaño del contenedor amarillo. El algoritmo es igual que el de srTCM, excepto que el valor CIR determina la tasa de reposición del contenedor verde y el valor PIR determina la tasa de reposición del contenedor amarillo. La opción trTCM es útil si es necesario aplicar una tasa pico aparte de la tasa de información comprometida. Los paquetes que sobrepasen la PIR se marcarán de color rojo (probabilidad de descarte más alta).

En qué consiste la gestión de almacenamientos intermedios y de colas

Si el tráfico es para EF, o se trata de tráfico de AF o BE permitido por el vigilante, la función de *gestión del almacenamiento intermedio* basada en la tasa lo procesará. Esta función asigna almacenamientos intermedios para la interfaz de salida en que está habilitada la función DiffServ o bien desde una agrupación privada o bien desde una agrupación compartida común. Los almacenamientos intermedios para el tráfico de EF se asignan solamente desde la agrupación privada.

Utilice el mandato de configuración **set receive-buffers** de Talk 6 (consulte la publicación *Access Integration Services Guía del usuario de software* para obtener una descripción y la sintaxis del mandato) para especificar la cantidad total de almacenamiento intermedio físico disponible para una interfaz. Utilice el mandato **set interface** de Talk 6 para establecer el tamaño del almacenamiento intermedio de salida de las colas de servicio preferente y garantizado. Este es el espacio de almacenamiento intermedio que DiffServ gestiona.

DiffServ gestiona dos agrupaciones independientes—una para la cola preferente (EF) y la otra para la cola de reenvío garantizado (AF). Asegúrese de que el espacio de almacenamiento intermedio que especifica refleje la cantidad real de espacio de almacenamiento intermedio disponible en el sistema.

La gestión de almacenamiento intermedio determina si los almacenamientos intermedios de la agrupación privada de su interfaz están disponibles para el paquete. Si lo están, acepta el paquete y lo pone en cola. Si no lo están, intenta asignar espacio de almacenamiento intermedio de la agrupación compartida y, si lo consigue, pone en cola el paquete. Si no hay espacio de almacenamiento intermedio compartido, la gestión del almacenamiento intermedio descarta el paquete.

En qué consiste el planificador

La función *planificador* examina las colas regularmente, retira de la cola los paquetes que están en cola y los envía al adaptador de la interfaz para su transmisión. Se trata de un planificador de colocación en cola equilibrada autosincronizado, que es una variante del algoritmo de colocación en cola equilibrada ponderada. Puede configurar los factores de ponderación del planificador y especificar la frecuencia con la que el planificador examina las colas.

Terminología de los servicios diferenciados

Los siguientes términos se utilizan para describir DiffServ:

Tasa de información comprometida (CIR, Committed Information Rate)
Este parámetro especifica la tasa máxima a la que se permite operar a una corriente de tráfico de AF de un usuario antes de considerarse que está enviando información en exceso. Se mide en bytes de paquetes IP por segundo (incluyendo la cabecera IP pero no las cabeceras específicas del enlace). La utilizan tanto la función TCM de una tasa como la de dos tasas para las corrientes de tráfico de AF.

Tamaño de ráfagas comprometido (CBS, Committed Burst Size)
Este parámetro especifica (en bytes de paquetes IP) el número máximo de bytes que pueden enviarse en una ráfaga, a una tasa que supere la CIR. El CBS limita el tamaño del contenedor de fichas comprometidas en las funciones TCM de una tasa y de dos tasas.

Antememoria de DiffServ
Esta antememoria contiene el tráfico y el perfil de servicio de los flujos IP activos más recientes servidos por el direccionador.

Tamaño de ráfagas en exceso (EBS, Excess Burst Size)
Este parámetro especifica (en bytes de paquetes IP) el número máximo de bytes que pueden enviarse en una ráfaga que exceda el CBS, a una tasa que supere la CIR. Este parámetro lo utilizan las funciones TCM de una tasa y limita el tamaño del contenedor de fichas en exceso.

Flujo
Secuencia de paquetes con el mismo puerto y dirección de origen, protocolo IP y puerto y dirección de destino.

Tasa de reposición de fichas
Este parámetro especifica la tasa máxima a la que se permite operar a la corriente de tráfico de EF de un usuario antes de considerarse que está enviando un exceso de datos. Se mide en bytes de paquetes IP por segundo (incluyendo la cabecera IP pero no las cabeceras específicas del enlace).

Tamaño del contenedor de fichas
Este parámetro mide el número máximo de bytes de paquetes IP de una corriente de tráfico de EF que pueden enviarse en una ráfaga a una tasa superior a la de reposición de fichas.

Tamaño de ráfagas pico (PBS, Peak Bucket Size)
Este parámetro lo utilizan únicamente las funciones TCM de dos tasas. Especifica (en bytes de paquetes IP) el máximo número de bytes que pueden enviarse en una ráfaga a una velocidad que supere la PIR. Este parámetro limita el tamaño máximo del contenedor de fichas de pico.

Tasa de información pico (PIR, Peak Information Rate)
Este parámetro lo utilizan únicamente las funciones TCM de dos tasas. Representa la tasa pico (en bytes de paquetes IP por segundo, incluyendo la cabecera IP pero no las cabeceras específicas del enlace) a la que el usuario puede enviar paquetes en una corriente de AF, más allá de la cual, la prioridad de descarte del paquete se establecerá al valor más alto.

Corriente
Agregación de flujos.

Interfaz virtual (VIF)
En el caso de los enlaces Frame Relay, cada conexión DLCI se considera una interfaz virtual.

Configuración de los servicios diferenciados

El siguiente procedimiento proporciona una descripción paso a paso sobre el modo de configurar DiffServ a fin de proporcionar un servicio preferente a los paquetes seleccionados. En primer lugar, debe acceder a la función DiffServ:

1. En el indicador *, entre **talk 6**.
2. En el indicador Config>, entre **feature ds**. A continuación aparece el indicador DS config> y se abre el diálogo de configuración.

```
* talk 6
Config>feature ds
DS config>
```

3. Habilite la función DiffServ en un direccionador:

```
DS config>enable ds
DiffServ enabled
```

4. Habilite y establezca los parámetros de la 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 la solicitud "Configure Advanced setting", se utilizarán los parámetros por omisión de cola preferente y cola garantizada/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 de la carga del planificador se conceden a la cola EF. El tamaño del almacenamiento intermedio de salida de la cola EF es de 5500 bytes, del que un 95 por ciento se puede asignar a corrientes QoS. El tamaño del almacenamiento intermedio de salida de la cola AF/BE es de 27 500 bytes (que son 50 paquetes con un tamaño medio de paquete de 550 bytes), del que un 80 por ciento se puede asignar a corrientes QoS.

5. Cuando haya acabado de habilitar DiffServ en los direccionadores y de establecer los parámetros, entre **Ctrl-P** para volver al indicador *.

Después de habilitar DiffServ y establecer los parámetros de interfaz, debe reiniciar o volver a cargar el dispositivo para activar DiffServ. Si desea obtener información más detallada sobre cómo especificar los mandatos de DiffServ, consulte el “Configuración y supervisión de la función de servicios diferenciados” en la página 457.

Configuración y supervisión de la función de servicios diferenciados

Esta capítulo describe los mandatos que la función de servicios diferenciados (DiffServ) proporciona para la configuración de direccionadores e interfaces a fin de facilitar un servicio preferente para paquetes de datos seleccionados. Consta de los apartados siguientes:

Acceso al indicador de configuración de los servicios diferenciados

Para entrar los mandatos de configuración de DiffServ:

1. Entre **talk 6** en el indicador OPCON (*).
2. Entre **feature ds** en el indicador Config>.

Aparece el indicador DS Config>. Ahora ya puede entrar los mandatos de configuración de DiffServ.

Mandatos de configuración de los servicios diferenciados

Estos mandatos le permiten configurar las opciones de DiffServ, las cuales determinan un servicio preferente para los paquetes de datos seleccionados. La Tabla 47 resume los mandatos de configuración y el resto de este apartado los describe de manera detallada. Entre los mandatos en el indicador DS Config>. Entre el mandato y las opciones en una línea o entre sólo el mandato y, a continuación, responda a las solicitudes. Para ver una lista de las opciones de mandato, entre el mandato con un interrogante en lugar de las opciones.

Tabla 47. 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 xxxii.
Delete	Suprime un registro de configuración de DiffServ de 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 el sistema DiffServ de un direccionador y los valores relacionados con la interfaz.
Set	Especifica los valores de un direccionador relacionados con DiffServ.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxiii.

Delete

Utilice el mandato **delete** para suprimir un registro de configuración del sistema de DiffServ o un registro de interfaz de la SRAM de un direccionador.

Sintaxis: delete ds
interface

ds Suprime el registro de configuración del sistema de DiffServ del direccionador.

Ejemplo:

```
DS Config> delete ds
Diffserv system config record deleted
```

interface
Le solicita el número de interfaz a suprimir.

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 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 a inhabilitar.

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 a habilitar.

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 el sistema DiffServ y los valores relacionados con la interfaz de un direccionador.

Sintaxis: list all
ds
interface

all Visualiza información sobre las configuraciones de DiffServ y de interfaz de un direccionador.

ds Visualiza la configuración 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 de habilitación/inhabilitación de DiffServ y los parámetros de cada interfaz y de cada 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 el sistema DiffServ de un direccionador y los parámetros relacionados con la interfaz.

Sintaxis: set
- be-alloc-min
- ctl-alloc-min
- interface
- pkt-size

be-alloc-min

Especifica el porcentaje mínimo del espacio total de almacenamiento intermedio de salida a asignar al servicio optimizado.

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 almacenamiento intermedio de salida a 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 se debe habilitar para DiffServ y le solicita los parámetros específicos de la interfaz.

Queue bandwidth Especifica el porcentaje del enlace de salida que se debe utilizar para la cola preferente. El porcentaje restante se utiliza para el valor de cola garantizada.

Valor por omisión: 20

Queue weight Especifica el porcentaje de tiempo durante el cual el planificador supervisa la cola preferente. El porcentaje restante se utiliza para el valor de cola garantizada. El valor por omisión del peso de cola es 90 por ciento a fin de que el planificador reaccione con rapidez ante el tráfico EF.

Valor por omisión: 90

Egress buffer size Especifica la cantidad de datos (en bytes) que se pueden poner en la cola preferente y en la cola garantizada.

En el caso de la cola preferente, este parámetro controla la cantidad de datos (en bytes) que se pueden colocar en la cola preferente. Si se establece un valor demasiado alto para este parámetro, se puede generar un gran retraso en la colocación en cola del tráfico preferente. Por ejemplo, si se establece en 25 kilobytes y la velocidad del enlace de salida es de 1,5 Mbps (velocidad de T1), en ese caso existe un posible retraso de colocación en cola de 133 milisegundos (25 000 bytes * 8 bits/byte)/1 500 000 bps o 0,133

segundos (133 milisegundos). Si se establece un valor demasiado bajo para este parámetro, será imposible colocar ráfagas pequeñas en almacenamiento intermedio. Por ejemplo, si se establece en 2 kb, ello implica que no habrá suficiente almacenamiento intermedio para una ráfaga de 2 paquetes de 1.500 bytes (ya que requieren 3.000 bytes de espacio de almacenamiento intermedio).

Como valor de compromiso entre ambos extremos, el valor por omisión es 5.500 bytes, que es diez veces el tamaño por omisión del paquete, 550.

Valor por omisión: 5.500 (cola preferente)

En el caso de la cola garantizada, este parámetro controla la cantidad de datos (en bytes) que se pueden colocar en la cola garantizada. Las consideraciones sobre este valor de parámetro son las mismas que para la cola preferente, excepto por el hecho de que el tráfico de la cola garantizada no dispone de requisitos de retraso muy estrictos. Más bien, es más probable que el tráfico de cola garantizada consista en flujos TCP, que por naturaleza suele ser a ráfagas. Es por ello que se debe definir el suficiente espacio de almacenamiento intermedio a fin de dar cabida a ráfagas procedentes de varios flujos.

El tamaño por omisión es 27 500 bytes, que es cincuenta veces el tamaño por omisión del paquete, 550.

Valor por omisión: 27500 (cola garantizada)

Egress QoS allocation Especifica la cantidad de tamaño del almacenamiento intermedio de salida (expresada en porcentaje) que todas las corrientes DiffServ pueden reservar. El porcentaje restante se utiliza para el tamaño mínimo de la agrupación compartida.

Valor por omisión: 95 (cola preferente)

Valor por omisión: 80 (cola garantizada)

Notas:

1. Para PPP de multienlace, habilite DiffServ en la interfaz virtual del paquete. No se permite habilitar DiffServ en un enlace individual de la interfaz del paquete.
2. Para las subinterfaces Frame Relay, habilite DiffServ en la red Frame Relay básica. No se permite habilitar 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). Ello permite que DiffServ determine el espacio de almacenamiento intermedio disponible en las interfaces de entrada y de salida. Si este valor se modifica, se debe reiniciar el direccionador y los valores del mandato **set interface** deben ser revisados y cambiados, si fuera necesario.

Valor por omisión: 550

Ejemplo:

```
DS Config> set pkt-size
Average packet size (64 - 64000) [550]?
```

Acceso al entorno de supervisión de los servicios diferenciados

La parte de la consola de la función DiffServ le permite ver y gestionar los valores relacionados con DiffServ. Para acceder al entorno de supervisión, entre **talk 5** en el indicador OPCON (*):

```
* t 5
```

A continuación, entre el mandato siguiente en el indicador **+**:

```
+ feature ds
DS Console>
```

Mandatos de supervisión de los servicios diferenciados

Estos mandatos le permiten ver los valores relacionados con DiffServ. La Tabla 48 resume los mandatos de supervisión de DiffServ y el resto del apartado los describe. Entre los mandatos en el indicador `DS Console>`. Entre el mandato y las opciones en una línea o entre sólo el mandato y, a continuación, responda a las solicitudes. Para ver una lista de las opciones de mandato, entre el mandato con un interrogante en lugar de las opciones.

Tabla 48. 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 xxxii.
Clear	Borra estadísticas de una corriente entre un par de interfaces de entrada y de salida específicas.
DScache	Borra o visualiza información sobre la antememoria de DiffServ de un direccionador.
List	Visualiza información sobre el sistema DiffServ de un direccionador y los valores relacionados con la interfaz.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiii.

Clear

Utilice el mandato **clear** para borrar las estadísticas de una corriente entre un par de interfaces de entrada y salida específicas.

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 se deben llevar a cabo para los paquetes enviados desde el origen IP especificado al destino IP especificado, y el ID de corriente de DiffServ, si lo hay.

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 salto siguiente.

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 en 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 las estadísticas de los paquetes enviados desde el origen IP al destino IP especificados.

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 el sistema DiffServ y los valores relacionados con la interfaz de un direccionador.

Sintaxis: list interface
queue
stream
vifs

interface

Lista las interfaces de un direccionador, su estado de habilitación/inhabilitación de DiffServ y sus asignaciones de almacenamiento intermedio, además de otra información.

Net Visualiza el número de la interfaz.

Status Visualiza el estado de DiffServ.

KB/s Visualiza la velocidad del enlace en kb por segundo.

VirtTime Visualiza la hora virtual utilizada por el planificador (indica n/a, si el enlace no es DiffServ, o bien 0, si no hay paquetes en proceso).

InMax Visualiza el tamaño de almacenamiento intermedio máximo configurado para el reenvío garantizado.

InCurr Visualiza la cantidad de espacio de almacenamiento intermedio que se está utilizando en este momento para la corriente de entrada. Los almacenamientos intermedios contienen paquetes en proceso.

InShar Visualiza la cantidad de espacio de almacenamiento intermedio compartido disponible para esta interfaz de salida.

InMaxA Visualiza la cantidad máxima de espacio de almacenamiento intermedio que se puede asignar a todas las corrientes QoS en agregado.

InCurA Visualiza la cantidad de espacio de almacenamiento intermedio asignado disponible que la corriente de entrada puede utilizar.

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 colocados en cola actualmente (0 indica que no hay paquetes en cola en este momento).

Svc Tag Visualiza la siguiente hora virtual en que esta cola debe recibir servicio.

Weight Visualiza el peso del 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 de esta cola.

out_curr_buff Visualiza la cantidad de espacio de almacenamiento intermedio asignado actualmente que se está utilizado para paquetes.

out_share_buff Visualiza la cantidad de espacio de almacenamiento intermedio que se halla en este momento 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

Muestra información sobre la medición y marcado de corrientes de AF.

Id Número de identificación de la corriente

t Tipo de corriente

- **D** Corriente de DiffServ
- **B** Corriente optimizada
- **C** Corriente de control de red
- **R** Corriente RSVP

I/o q Tipo de cola de la interfaz de salida

- **q1** Cola preferente
- **q2** Cola garantizada/BE

pkt snt Número total de paquetes enviados por esta corriente.

buf drp Número de paquetes eliminados de esta corriente porque no había espacio de almacenamiento intermedio disponible.

snt g Número de paquetes marcados de color verde enviados

snt y Número de paquetes de color amarillo enviados

snt r Número de paquetes de color rojo enviados

g->y En la modalidad sensible al color, número de paquete marcados de color verde marcados de color amarillo antes de enviarlos

g->r En la modalidad sensible al color, número de paquete marcados de color verde marcados de color rojo antes de enviarlos

y->r En la modalidad sensible al color, número de paquete marcados de color amarillo marcados de color rojo antes de enviarlos

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

Muestra información sobre los paquetes de las corrientes.

Id Número de identificación de la corriente

t Tipo de corriente

- **D** Corriente de DiffServ
- **B** Corriente optimizada
- **C** Corriente de control de red
- **R** Corriente RSVP

I/o q Tipo de cola de la interfaz de salida

- **q1** Cola preferente
- **q2** Cola garantizada/BE

allo/cur(K) Espacio total de almacenamiento intermedio (en kilobytes) asignado y actualmente utilizado por esta corriente.

tot pkt Número total de paquetes recibidos por esta corriente para su transmisión.

tot Kby Cantidad total de kilobytes recibidos por esta corriente para su transmisión.

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 mediante almacenamientos intermedios compartidos.

buf drp Número de paquetes eliminados de esta corriente porque no había espacio de almacenamiento intermedio disponible.

pol drop Número de paquetes eliminados por el administrador de políticas en la cola preferente.

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

Muestra información sobre el parámetro de vigilancia configurado para las corrientes de EF y AF.

Id Número de identificación de la corriente

t Tipo de corriente

- **D** Corriente de DiffServ
- **B** Corriente optimizada
- **C** Corriente de control de red
- **R** Corriente RSVP

I/o q Tipo de cola de la interfaz de salida

- **q1** Cola preferente
- **q2** Cola garantizada/BE

TR/CIR in B/s Tasa de reposición de fichas o tasa de información comprometida configuradas, en bytes por segundo.

TBS/CBS in bytes Tamaño del contenedor de fichas o tamaño de ráfagas comprometido configurados, en bytes

PIR in B/s Tasa de información pico en bytes por segundo.

EBS/PBS in bytes Tamaño de ráfagas en exceso o tamaño de ráfagas pico configurados, en bytes.

pol typ Tipo de acción de vigilancia.

- **None** Sin vigilancia.
- **SRCB** TCM de una tasa, no sensible a los colores.
- **SRCA** TCM de una tasa, sensible a los colores.
- **TRCB** TCM de dos tasas, no sensible a los colores.
- **TRCA** TCM de dos tasas, sensible a los colores.
- **EF-DRP** Vigilante de EF con acción de descarte 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 las 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 los servicios diferenciados

En este apartado se describe la reconfiguración dinámica (DR) y cómo afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

Los servicios diferenciados (o DiffServ o DS) dan soporte al mandato **delete interface** de CONFIG (Talk 6) teniendo en cuenta que:

Suprime el registro SRAM de la interfaz DiffServ correspondiente. Hay que volver a arrancar el dispositivo para activar este cambio.

Mandato activate interface de GWCON (Talk 5)

DiffServ da soporte al mandato **activate interface** de GWCON (Talk 5), teniendo en cuenta que:

Si se activa una interfaz configurada para los servicios diferenciados, DS seguirá la secuencia activar red y desactivar red normal.

Mandato reset interface de GWCON (Talk 5)

DiffServ da soporte al mandato **reset interface** de GWCON (Talk 5) teniendo en cuenta que:

- Si DiffServ se habilita para esta interfaz, sucederá lo siguiente: **reset interface** borrará todas las corrientes creadas hacia o desde esta interfaz. También borrará la antememoria de diffserv. Si la función BRS está habilitada, BRS

tendrá prioridad sobre DiffServ en esta interfaz. Para realizar cualquier operación de adición, supresión o cambio en el registro SRAM de la interfaz DiffServ, habrá que volver a arrancar el dispositivo para activar el cambio.

Mandatos no reconfigurables dinámicamente

En la tabla siguientes se describen los mandatos de configuración de DiffServ que no pueden cambiarse dinámicamente. Para activarlos es necesario reiniciar o volver a cargar 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 función de detección anticipada aleatoria

En este capítulo se describe cómo utilizar la función de detección anticipada aleatoria (RED) para que un dispositivo de red, basándose en esta probabilidad de descarte configurada, marque aleatoriamente paquetes de entrada para descarte en caso de que se produzca una congestión, evitando un desbordamiento. Esta función favorece al tráfico con buen comportamiento, como es el caso del tráfico TCP, que responde a la indicación de congestión reduciendo el tamaño de la ventana de transmisión. RED da soporte a los enlaces PPP, PPP de multienlace y Frame Relay. Este capítulo consta de este apartado:

- "Utilización de la detección anticipada aleatoria"

Utilización de la detección anticipada aleatoria

RED le permite evitar el desbordamiento si se produce una congestión. RED calcula la longitud promedio de una cola y si está dentro de los límites especificados, basados en una probabilidad de descarte configurable, se marcará un paquete entrante para descarte. Utilizar la longitud *promedio* de la cola en lugar de la longitud real de la cola impide que una cola que reciba tráfico a ráfagas afecte a la tasa de descarte.

Supongamos que se han especificado los valores siguientes para los parámetros de la función 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 qué influencia tiene una cola actual en el cálculo de la longitud promedio de la cola.

El valor mínimo de este parámetro (1) indica menos peso y es un valor conservador. Con este valor, la longitud promedio de la cola en un momento dado es parecida a la anterior longitud promedio de la cola, con lo que el tráfico a ráfagas con una longitud de cola grande apenas afecta al cálculo de la nueva longitud promedio de la cola.

El valor máximo de este parámetro (8) indica un mayor peso y es una configuración agresiva. Con este valor, la longitud promedio de la cola es igual a la longitud actual de la cola, con lo que el tráfico a ráfagas con una longitud de cola grande afecta en gran medida al cálculo de la nueva longitud promedio de la cola.

2 Este valor es la probabilidad de descarte de un paquete en picos de la longitud promedio de la cola.

Si la longitud promedio de la cola es constantemente igual al valor umbral máximo, se marcará uno de cada 2^9 (512) para descarte. La probabilidad de un descarte aumenta linealmente a medida que aumenta la longitud promedio de la cola desde el umbral mínimo hasta el umbral máximo.

3 Este valor indica los requisitos mínimos de la cola para calcular una probabilidad de descarte de un paquete y marcarlo convenientemente.

Se expresa como un porcentaje del valor máximo de la cola del dispositivo, que es un valor no configurable determinado por el protocolo de capa 2. Por ejemplo, si se especifica un valor del 40 por cien y el valor máximo de la cola del dispositivo es 16, el valor umbral mínimo se establece en 6 (0,4*16).

4 Este valor indica los requisitos máximos de la cola para calcular una probabilidad de descarte de un paquete y marcarlo convenientemente.

Se expresa como un porcentaje del valor máximo de la cola del dispositivo, que es un valor no configurable determinado por el protocolo de capa 2. Por ejemplo, si se especifica un valor del 100 por cien y el valor máximo de la cola del dispositivo es 16, el valor umbral mínimo se establece en 16 (1,0*16).

5 Este valor indica el valor inicial utilizado para calcular la probabilidad de descarte de un paquete.

Se expresa como un porcentaje del valor máximo de la cola del dispositivo, que es un valor no configurable determinado por el protocolo de capa 2. Impide que el tráfico a ráfagas aumente el peso en el cálculo de la longitud promedio de la cola antes de que se establezca un valor de cola promedio para el propio tráfico. (Al inicializar un dispositivo, la longitud de la cola es cero y no existe ninguna indicación de una longitud promedio de la cola anterior). Se debe especificar un valor relativamente bajo, como se muestra en el ejemplo precedente.

Después de habilitar RED y de establecer los parámetros de la interfaz, para activar RED se debe reiniciar o volver a cargar el dispositivo. Para obtener más detalles cobre como se especifican los mandatos de la función RED, consulte el capítulo siguiente, “Configuración y supervisión de la función de detección anticipada aleatoria” en la página 473.

Configuración y supervisión de la función de detección anticipada aleatoria

En este capítulo se describen los mandatos de la función de detección anticipada aleatoria (RED, Random Early Detection) para configurar las interfaces para que descarten aleatoriamente paquetes en condiciones de congestión. Consta de los apartados siguientes:

- "Acceso al indicador de configuración de la detección anticipada aleatoria"
- "Mandatos de configuración de la detección anticipada aleatoria"
- "Acceso al entorno de supervisión de la detección anticipada aleatoria" en la página 476
- "Mandatos de supervisión de la detección anticipada aleatoria" en la página 476

Acceso al indicador de configuración de la detección anticipada aleatoria

Para entrar mandatos de configuración de RED:

1. Entre **talk 6** en el indicador OPCON (*).
2. Escriba **feature red** en el indicador Config>.

Aparecerá el indicador RED Config>. Ahora ya puede entrar los mandatos de configuración de RED.

Mandatos de configuración de la detección anticipada aleatoria

Estos mandatos le permiten configurar las opciones de RED, que determinarán cómo se descartarán los paquetes durante los períodos en que el tráfico esté congestionado. Esto puede evitar un desbordamiento y tener que volver a sincronizar el tráfico de forma global. En la Tabla 49 en la página 474 se resumen los mandatos de configuración de RED y en el resto del apartado se describen con más detalle. Entre los mandatos en el indicador RED Config>. Entre el mandato y las opciones en una línea o entre sólo el mandato y, a continuación, responda a las solicitudes. Para ver una lista de las opciones del mandato, en lugar de escribir el mandato con las opciones, escríbalo con un interrogante.

Tabla 49. Mandatos de configuración de la detección anticipada aleatoria

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 xxxii.
Delete	Suprime un registro de configuración de RED o un registro de la interfaz de una SRAM del 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	Muestra información sobre el estado de la función RED del dispositivo de red y otros valores relacionados con la interfaz.
Set	Especifica los 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 xxxiii.

Delete

Utilice el mandato **delete** para suprimir un registro de configuración de RED para una interfaz de una SRAM del dispositivo de red.

Sintaxis: delete interface

interface

Le solicita el número de interfaz a suprimir.

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 la función RED para un dispositivo de red o para una interfaz de salida específica.

Sintaxis: disable red
interface

red

Inhabilita la función RED para un dispositivo de red.

Ejemplo:

```
RED Config> disable red
RED disabled
```

interface

Inhabilita la función 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 la función RED para un dispositivo de red o para una interfaz de salida específica.

Sintaxis: enable red
interface

red

Habilita la función RED para un dispositivo de red.

Ejemplo:

```
RED Config> enable red
RED enabled
```

interface

Habilita la función RED en una interfaz de salida específica.

Ejemplo:

```
RED Config> enable interface
Enter RED Interface number [0]? 2
RED interface enabled
```

Nota: RED puede habilitarse solamente en enlaces PPP, PPP de multienlace y Frame Relay.

List

Utilice el mandato **list** para visualizar información sobre el estado de la función RED del dispositivo de red y otros valores relacionados con la interfaz.

Sintaxis: list all

all Muestra el estado de la función RED del 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 la función RED para una interfaz específica de un dispositivo de red.

Sintaxis: set interface

interface *número*

Especifica el número de la interfaz para la que establecer las opciones de la función RED.

Valor por omisión: none

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 la detección anticipada aleatoria

La parte de la consola de la función de detección anticipada aleatoria permite ver y gestionar los valores relacionados con la función RED. Para acceder al entorno de supervisión de la función RED, escriba **talk 5** en el indicador OPCON (*):

```
* t 5
```

A continuación, entre el mandato siguiente en el indicador **+**:

```
+ feature red
RED Console>
```

Mandatos de supervisión de la detección anticipada aleatoria

Estos mandatos le permiten ver los valores relacionados con la función RED. En la Tabla 50 en la página 477 se resumen los mandatos de supervisión de la función RED y el resto del apartado se dedica a describirlos. Entre los mandatos en el indicador `RED Console>`. Entre el mandato y las opciones en una línea o entre sólo el mandato y, a continuación, responda a las solicitudes. Para ver una lista de las opciones del mandato, en lugar de escribir el mandato con las opciones, escríbalo con un interrogante.

Tabla 50. 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 xxxii.
Clear	Restablece los valores de los parámetros de la función RED de una interfaz.
List	Muestra los valores de la interfaz del dispositivo de red para el que está habilitada la función RED.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiii.

Clear

Utilice el mandato **clear** para restablecer los valores de los parámetros de la función RED de una interfaz. El ejemplo de la descripción del mandato **list** ilustra el resultado del mandato **clear**.

Sintaxis: clear *número-interfaz*

List

Utilice el mandato **list** para mostrar información sobre los valores de la interfaz del dispositivo de red para el que está habilitada la función RED.

Sintaxis: list *número-interfaz*

número-interfaz
Lista los valores de la función RED para la interfaz concreta 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 túneles de capa 2 (L2TP, PPTP, L2F)

En este capítulo se estudian los túneles de capa 2. Consta de los apartados siguientes:

Los túneles de capa 2 (L2T) constan de los protocolos de túnel L2TP, L2F y PPTP.

El protocolo de túnel de capa 2 (L2TP) es un protocolo de pistas de estándares IETF para túneles PPP en una red de paquetes, tal como UDP/IP. L2TP está orientado a la conexión.

El reenvío de capa 2 (L2F) y el protocolo de túnel punto a punto (PPTP) son protocolos informativos IETF para túneles PPP en una red IP.

Visión general de L2TP

L2TP permite que muchos dominios de protocolo independientes y autónomos compartan una infraestructura de acceso común que incluye módems, servidores de acceso y direccionadores RDSI. L2TP permite los túneles de la capa de enlace PPP, por ejemplo, HDLC y HDLC asíncrono. Mediante dichos 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 se proporciona sólo para direcciones IP registradas. L2TP define una nueva clase de aplicación de marcación virtual que permite varios protocolos y direcciones IP no registradas en Internet. Esta clase de aplicación de red es útil para dar soporte a conexiones de marcación IP, IPX y AppleTalk direccionadas a través de PPP en una infraestructura de Internet existente de forma privada.

El soporte de estas aplicaciones de marcación virtual de varios protocolos es beneficioso para usuarios finales, empresas y proveedores de servicios de Internet porque permite compartir inversiones significativas en infraestructuras de acceso y básicas y permite que los usuarios efectúen llamadas locales para acceder a los servicios.

L2TP permite también el uso seguro de las inversiones existentes en aplicaciones de protocolo no IP dentro de la infraestructura de Internet existente.

En la Figura 43 en la página 480 se muestra un ejemplo de una red L2TP que utiliza RDSI. La red puede utilizar cualquier tipo de medio entre el L2TP Network Access Concentrator (LAC) y el L2TP Network Server (LNS). El ejemplo utiliza el modelo obligatorio de túneles. En este capítulo también se describe la configuración del modelo voluntario de túneles.

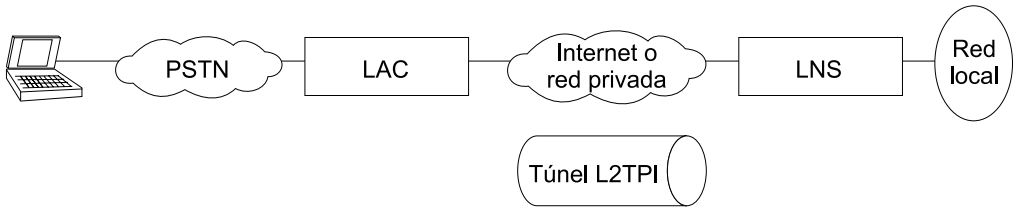


Figura 43. Ejemplo de red L2TP

Términos de L2TP

Los siguientes términos se utilizan para describir L2TP:

AVP (Attribute Value Pair)
Método uniforme de codificar tipos y cuerpos de mensajes. Este método maximiza la capacidad de extensión a la vez que permite la interoperabilidad de L2TP.

LAC (L2TP Access Concentrator)
Dispositivo conectado a una o más redes telefónicas de servicio público (PSTN) o líneas RDSI capaces de manejar tanto el funcionamiento de PPP como el protocolo L2TP. LAC implementa el medio sobre el que trabaja L2TP. L2TP pasa el tráfico a uno o más L2TP Network Servers (LNS). L2TP puede crear un túnel para cualquier protocolo transportado por la red PPP.

LNS (L2TP Network Server)
Un LNS trabaja en cualquier plataforma que pueda ser una estación final PPP. LNS maneja el lado servidor del protocolo L2TP. Como L2TP sólo confía en el único medio por el que llegan los túneles L2TP, LNS sólo puede disponer de una interfaz LAN o WAN, aunque aún pueda interrumpir llamadas procedentes de cualquier interfaz PPP soportada por un LAC.

NAS (Network Access Server)
Dispositivo que proporciona a los usuarios acceso temporal a la red, a petición. Dicho acceso se efectúa punto a punto mediante líneas PSTN o RDSI.

Sesión (llamada)
L2TP crea una sesión cuando se intenta una conexión PPP de extremo a extremo entre un usuario de marcación y LNS. Los datagramas de la sesión se envían sobre el túnel entre LAC y LNS. LNS y LAC mantienen la información de estado para cada usuario conectado a un LAC.

Túnel
Un túnel viene definido por un par de LNS-LAC. El túnel transporta los datagramas PPP entre LAC y LNS. Un único túnel puede multiplexar muchas sesiones. Una conexión de control que opera sobre el mismo túnel controla el establecimiento, la liberación y el mantenimiento de todas las sesiones y del propio túnel.

Funciones soportadas

L2TP se ejecuta en UDP/IP y da soporte a las siguientes funciones:

- Túneles de clientes de marcación de un único usuario.
- Túneles de direccionadores pequeños, por ejemplo un direccionador con una única ruta estática a definir según un perfil de usuario autenticado.

- Las llamadas se pueden iniciar desde LAC al LNS (entrada), desde LNS al LAC (salida) o por cualquiera de los dos nodos. Las llamadas de salida pueden ser una sesión de túnel L2 *fija* (siempre activa) o una sesión de túnel L2 basada en la demanda.
- Varias llamadas por túnel.
- Autenticación mediante proxy para PAP, CHAP y MS-CHAP.
- Proxy LCP.
- Reinicio de LCP en el caso de que no se utilice un proxy LCP en LAC.
- Autenticación del extremo del túnel.
- AVP oculto para transmisión de una contraseña PAP de proxy.
- Túneles mediante una tabla de búsqueda de reinos (es decir usuario@reino).
- Túneles mediante la búsqueda de nombres de usuario PPP en el subsistema AAA.
- Gestión de túneles L2TP mediante SNMP. Consulte “Gestión SNMP” en la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 1*.

Nota: Los túneles de reino requieren nombres de usuario en el formato *nombre@reino*. Este tipo de túneles requieren software para consultar dos tablas a fin de resolver el destino al que el usuario de marcación accede mediante un túnel. La ventaja de utilizar este método de creación de túneles es que sólo es necesario definir el reino y los nombres de usuario que coincidan con el reino accederán al mismo destino mediante el túnel.

La creación de túneles basada en usuarios se resuelve en una única tabla. Le permite la granularidad de dirigir cada usuario a un destino exclusivo mediante túneles.

- BRS para un LNS (como un extremo de PPP).
- Capacidad de utilizar el mandato **delete interface** para suprimir dispositivos L2TP.
- Capacidad de volver a configurar de manera dinámica dispositivos L2TP.
- Establecimiento de un canal de control de secuencia, colas, retransmisión y flujo. L2TP también lleva a cabo el control de secuencia en el canal de datos.
- Capacidad de corregir el puerto L2TP UDP (1701) para que se puedan establecer filtros de seguridad IP basados en el puerto UDP.
- Un cliente de direccionador L2TP. Un cliente de direccionador L2TP es un modelo “iniciado por cliente” (también conocido como creación de túneles voluntaria). Esta función proporciona servicios Virtual Private Network (VPN) multiprotocolo, por túnel y seguros, independientemente de la topología del proveedor de servicios. Esta función junta al cliente y al LAC en una unidad física de hardware.
- Conexión de una llamada de entrada a la interfaz adecuada según una coincidencia de nombre de sistema principal remoto. Si el nombre del sistema principal remoto no coincide con ninguna de las interfaces configuradas para la coincidencia de nombres de sistema principal, la llamada se realiza en una interfaz de entrada que no utiliza la coincidencia de nombres de sistema principal remoto.

Nota: Si ha configurado varias correlaciones de red entre el mismo par de LAC - LNS, asegúrese de que sólo existe un túnel para cada correlación.

- Configuración automática de IP, IPX y de puentes de redes de entrada que no utilizan la coincidencia de nombres de sistema principal remoto. Debe configurar manualmente las redes de salida y las redes de entrada que utilizan la coincidencia de nombres de sistema principal remoto.

Otros protocolos de túnel de capa 2 con soporte son:

- Se da soporte tanto a las funciones NAS y de pasarela de L2F.
- Se da soporte al cliente de direccionador de PPTP, al PAC (concentrador de acceso de PPTP) y al PNS (servidor de red de PPTP).

L2F proporciona túneles de capa 2 con capacidad de interoperación al conectar con dispositivos de red que no soportan L2TP.

PPTP proporciona túneles de capa 2 con capacidad de interoperación al conectar con dispositivos de red que no dan soporte a L2TP. PPTP se puede utilizar de manera específica para servicios VPN desde Microsoft Windows 95 (DUN 1.2 y posteriores), Windows 98 y Windows NT a direccionadores IBM.

Nota: Tanto L2F como PPTP se configuran en la función de túnel de capa 2.

Consideraciones de tiempo

La creación de túneles para paquetes PPP en redes direccionadas genera algunas circunstancias relacionadas con el tiempo que se deben tener en cuenta. L2TP presupone que la conexión entre LAC y LNS no sufre un retraso lo suficientemente largo para exceder el tiempo de espera de los iguales conectados mediante túnel. Si la latencia entre iguales alcanza o supera repetidamente la del tiempo de espera de la máquina de estado PPP (normalmente 3 segundos), la conectividad puede verse entorpecida. Observe que si la latencia entre LAC y LNS es tan pobre, la conectividad en general es tan pobre que la conexión no será razonable aunque las máquinas de estado PPP se mantengan vivas artificialmente. Si ambas partes poseen dicha capacidad, se puede ampliar el tiempo de espera PPP para alcanzar la conectividad en una conexión muy pobre.

Además de la latencia, una discrepancia de ancho de banda entre el par LAC/LNS y el par LAC/cliente puede ocasionar problemas. Por ejemplo, si el ancho de banda real entre LAC y LNS es significativamente menor que el ancho de banda del cliente PPP, LAC puede dedicar un tiempo considerable a intentar enviar paquetes al LNS. Por otra parte, si la conexión entre LNS y un sistema principal en una red local LNS es excepcionalmente rápida comparada con el cliente de marcación, es probable que se sobrecargue LNS al intentar enviar datos al LAC.

Consideraciones sobre LCP

Al utilizar un proxy LCP, LAC negocia el LCP y PPP continúa procesando en LNS. LAC envía opciones LCP al LNS para que LNS esté al corriente de lo que se ha negociado. LNS debe continuar siendo flexible a los parámetros negociados por el cliente y LAC. Si existen parámetros que no son aceptables para LNS, L2TP

intenta volver a negociar el LCP enviando una *Petición de configuración de LCP* al cliente a través del túnel.

El requisito de que LNS continúe siendo flexible es de especial importancia por lo que se refiere al MRU. En el IBM LNS, el MRU configurado es el máximo permitido para el proxy LCP. Si el valor del mensaje del proxy LCP procedente de un LAC es mayor que el MRU configurado en LNS, L2TP intentará renegociar el LCP con un MRU igual al MRU configurado sin cambiar otras opciones LCP dLAC.

Configuración de túneles de capa 2

Para configurar L2T:

1. Acceda a la función de túnel de capa 2 mediante el mandato **feature**.

```
Config> feature layer-2-tunneling
Layer-2-Tunneling config>
```

2. Habilite L2TP, L2F y PPTP, según convenga.

```
Layer-2-Tunneling config> enable L2TP

Layer-2-Tunneling config> enable L2F

Layer-2-Tunneling config> enable pptp
```

3. Añada las redes L2T necesarias. Si tiene que 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 con 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 túneles L2TP, L2F o PPTP.

      Para configurar un túnel L2TP mediante 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 la autorización de túnel en LAC, así como la creación de túneles de “reino” en la forma “user@lns.org.”

Puede establecer que la autenticación y la autorización de túneles se realice en un servidor RADIUS concreto. Consulte “Utilización de la seguridad de autenticación, autorización y contabilidad (AAA)” en la publicación *Utilización y configuración de las funciones*.

Si está configurando un LNS y la autenticación de túneles está inhabilitada tanto en LAC como en LNS, no es necesario configurar perfiles de túneles.

Para crear un túnel por nombre de usuario PPP en un LAC mediante una 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 coincidencia de nombres de sistema principal remoto para los túneles de entrada, si es necesario.

   Observe que en casos de conexiones de marcación de cliente, habitualmente este paso no es necesario. Utilice esta opción cuando una conexión deba utilizar una red específica.

   Presuponiendo que la configuración anterior fuera para la red 10:

   ```
   Config> net 10
   L2TP 10> set remote-hostname
   Remote Tunnel Hostname: [] ibm.com
   ```

   Nota: Para desactivar la coincidencia de nombres de sistema principal remoto, utilice los siguientes mandatos:

   ```
   Config> net 10
   L2TP 10> set any-remote-hostname
   ```

4. Configure las llamadas salientes L2TP. El siguiente ejemplo muestra un LAC con la dirección IP 1.1.1.1 y un LNS con la dirección IP 1.1.1.2. LNS está configurado para hacer una llamada RDSI a petición de línea conmutada a 5552160 desde 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)? [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 autenticación en el caso de que el dispositivo LNS se autentique. Hay otros indicadores de mandatos que no aparecen en este ejemplo. Si desea obtener más detalles al respecto, consulte “Configuración de la autenticación PPP” en el capítulo “Utilización de las interfaces del protocolo punto a punto” de la publicación *Access Integration Services Guía del usuario de software*.

b. Añada usuarios a autenticar en LNS. Hay otros indicadores de mandatos que no aparecen en este ejemplo. Consulte Add en el capítulo “El proceso y los mandatos CONFIG (CONFIG - talk 6)” de la publicación *Access Integration Services Guía del usuario de software* si desea obtener una descripción de la sintaxis de mandatos y de las opciones.

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: Utilizado para efectuar la llamada física.

5. Configure los clientes de direccionador L2T. El siguiente ejemplo muestra una conexión directa L2TP mediante la función de cliente de direccionador L2TP. Esta conexión se establece en una sola dirección y está basada en peticiones.

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 autenticación en el caso de que el dispositivo cliente se autentique. Hay otros indicadores de mandatos que no aparecen en este ejemplo. Para obtener más detalles, consulte el capítulo “Configuración de la autenticación PPP” en la publicación *Access Integration Services 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 a autenticar en LNS. Hay otros indicadores de mandatos que no aparecen en este ejemplo. Si desea obtener más

detalles al respecto, consulte “el mandato Config **add**” en la publicación *Access Integration Services Guía del usuario de software*.

6. Configure los diversos parámetros de la función L2T mediante los mandatos **set** y **enable**, si lo desea.

```
Layer-2-Tunneling Config>set ?
Layer-2-Tunneling Config>enable ?
```

7. Configure los parámetros PPP para todas las redes L2 que se hayan definido para entrada y especifique *any* como nombre de sistema principal de túnel de entrada mediante el mandato encapsulator, si lo desea.

```
Layer-2-Tunneling Config>encapsulator
PPP-L2TP Config>
```

   Cuando haya finalizado de configurar PPP, entre **exit** para volver al entorno de configuración de la función L2T.

Configuración y supervisión de los protocolos de túneles de capa 2

Este capítulo describe la configuración de túneles de capa 2 (L2T) y sus mandatos operativos. L2T consta del protocolo de túneles de capa 2 (L2TP), del protocolo de reenvío de capa 2 (L2F) y del protocolo de túneles punto a punto (PPTP). Este capítulo consta de estos apartados:

Acceso al indicador de configuración de la interfaz de L2T

Para acceder al indicador de configuración de la interfaz de L2T:

1. Entre **talk 6** en el indicador OPCON (*).
2. Entre **add dev layer-2-tunneling** en el indicador `Config>` (o utilice el mandato **add l2–nets**. Consulte "Add" en la página 492).
3. Entre **n** *núm_interfaz* en el indicador `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 la interfaz de túneles L2

La Tabla 51 resume los mandatos de configuración de la interfaz de L2T. Entre estos mandatos en el indicador `L2T Config n>` (donde *n* es el número de red).

Tabla 51. Mandatos de configuración de la interfaz de túneles 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 xxxii.
Disable	Inhabilita las llamadas salientes.
Enable	Habilita las llamadas salientes.
Encapsulator	Le permite configurar los parámetros PPP de la interfaz L2T. **Nota:** La opción encapsulator sólo está disponible si una interfaz tiene un nombre de sistema principal remoto configurado.
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 xxxiii.

Disable

Utilice el mandato **disable** para inhabilitar llamadas salientes del concentrador de acceso de L2TP (LAC).

Sintaxis:

disable outbound-calls-from-lac

outbound-calls-from-lac
Evita que LNS inicie una señal de marcación desde LAC a través de un túnel L2TP.

Enable

Utilice el mandato **enable** para habilitar llamadas de salida desde el concentrador de acceso de L2TP (LAC). Este mandato sólo se puede utilizar con L2TP.

Sintaxis:

enable outbound-calls-from-lac

outbound-calls-from-lac
Permite que LNS inicie una señal de marcación desde LAC a través de un túnel L2TP.

Ejemplo:

```
L2T 10> enable outbound-call-from-lac
        Outbound Call Type (ISDN)? [ISDN]
        Outbound calling address: 1234
        Outbound calling subaddress:
L2T 10>
```

Encapsulator

Utilice el mandato **encapsulator** para configurar los parámetros PPP de la interfaz L2T.

Sintaxis:

encapsulator

Este mandato está disponible sólo cuando se ha configurado un nombre de sistema principal remoto. Si desea obtener una lista de los mandatos disponibles en el indicador `ppp-L2tp config>`, consulte “Encapsulator” en la página 494.

List

Utilice el mandato **list** para visualizar el estado de los diversos parámetros de configuración de la 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 la interfaz L2T.

Sintaxis:

set
- any-remote-hostname
- connection-direction
- idle
- remote-hostname

any-remote-hostname
Borra el nombre del sistema principal remoto de salida e inhabilita la comparación de nombres de sistema principal remoto de entrada de esta red.

connection-direction [inbound] o [outbound] o [both]
Especifica si se puede puede iniciar la conexión mediante el igual (inbound), el dispositivo local (outbound) o mediante ambos el igual y el dispositivo local (both) de esta red. Si especifica both, no podrá especificar cero como tiempo de inactividad.

Valor por omisión: inbound

idle-time *segundos*
Especifica los segundos de inactividad al cabo de los cuales los túneles L2 desconectarán la sesión de túnel en esta red. Cero indica que el túnel es fijo y que no debe desconectarse.

Valores válidos: de 0 a 1024

Valor por omisión: 0

remote-hostname *nombre_de_sistema_principal*
Especifica el nombre de sistema principal del túnel del igual.

En el caso de un túnel de salida, el nombre de sistema principal especifica un perfil de túnel configurado en el subsistema AAA. Debe ser el nombre del sistema principal de túnel que el igual utiliza para identificarse a sí mismo.

En el caso de un túnel de entrada, sólo los iguales de túnel que se identifican a sí mismos con este nombre de sistema principal se pueden conectar a esta interfaz.

Valores válidos: Cualquier nombre de 1 a 64 caracteres ASCII

Valor por omisión: *Nombre*

Acceso al indicador de configuración de la función de túneles L2

Para acceder al indicador de configuración de la función de túnel L2:

1. Entre **talk 6** en el indicador OPCON (*).
2. Entre **feature layer-2-tunneling** en el indicador `Config>`.

Mandatos de configuración de la función de túnel L2

La Tabla 52 resume los mandatos de configuración de la función de túnel L2 y el resto de este apartado describe dichos mandatos. Entre estos mandatos en el indicador `Layer-2-Tunneling Config>`.

Tabla 52. Mandatos de configuración de la función de túnel 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 xxxii.
Add	Añade redes e iguales de túneles L2.
Disable	Inhabilita las funciones de túnel L2.
Enable	Habilita las funciones de túnel L2.
Encapsulator	Le permite configurar los parámetros PPP de todas las redes L2 que no están configuradas con un nombre de sistema principal remoto (ANY).
List	Visualiza información sobre la configuración de túneles L2.
Set	Le permite establecer almacenamientos intermedios, la ventana de recepción de llamadas y otros parámetros de túneles L2.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxiii.

Add

Utilice el mandato **add** para añadir redes L2. Es obligatoria una red L2 para cada sesión PPP simultánea que acabe en este direccionador. El extremo de una sesión PPP por túneles es el extremo LNS del túnel.

Sintaxis:

`add` L2-nets

L2-nets

Nota: Todo el mandato se puede entrar en minúsculas. El carácter inicial aparece en mayúsculas para mayor claridad.

Añade redes L2 a la configuración de túneles L2. Es obligatoria una red L2 para cada sesión PPP simultánea que deba finalizar en este direccionador. Si este direccionador se utiliza estrictamente como un LAC, no se necesitan redes L2 virtuales. Cuando se entra este mandato, se le solicita el número de redes adicionales y si desea añadir direcciones IP no numeradas para cada red L2.

El número de redes adicionales hace referencia al número de redes que se añaden de manera automática en este momento. Estas redes se suman a las redes L2 que ya existen.

Al añadir direcciones IP no numeradas para cada red L2, se añaden de manera automática entradas IP no numeradas a la tabla de direccionamiento de cada una de las redes L2. Las direcciones IP no numeradas son el modo de operación preferente. Si necesita direcciones numeradas para las redes L2, las puede alterar en el entorno de configuración del protocolo IP (consulte el capítulo titulado "Configuring IP" de la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 1*).

Disable

Utilice el mandato **disable** para inhabilitar las funciones de túnel 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
Autoriza mediante un puerto UDP fijo. Si inhabilita este parámetro deberá configurar filtros de seguridad IP entre LAC y LNS por dirección IP.

force-chap-challenge
Inhabilita el reintento de LNS CHAP de un cliente. Es necesario que inhabilite el reintento de CHAP si el cliente PPP tiene problemas con los reintentos CHAP.

hiding-for-pap-attributes
Inhabilita el cifrado de información de un proxy PAP entre LAC y 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 autenticación por proxy PPP de LAC a LNS.

proxy-lcp
Inhabilita el envío de información LCP de LAC a LNS.

sequencing
Inhabilita el control de secuencia en el canal de datos.

tunnel-auth
Inhabilita la autenticación de iguales de túneles basada en un secreto compartido de este direccionador.

Enable

Utilice el mandato **enable** para habilitar las funciones de túnel 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 a la dirección de destino de entrada.

fixed-udp-source-port
La habilitación de este parámetro le permite configurar filtros de seguridad IP por puerto UDP para túneles L2 de manera que puede cifrar o autenticar fácilmente tráfico de túneles L2. Establece el puerto UDP en 1701 para L2TP.

force-chap-challenge
Habilita el reintento de CHAP de LNS de un cliente aunque LNS reciba un proxy CHAP. Esto es preferible desde el punto de vista de la seguridad, en el caso de que se sepa que el cliente puede manejar dicho reintento sin problemas.

hiding-for-pap-attributes
Habilita el cifrado de información de un proxy PAP entre LAC y 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 autenticación por proxy PPP de LAC a LNS.

proxy-lcp
Habilita el envío de información LCP de LAC a LNS.

sequencing
Habilita el control de secuencia en el canal de datos.

tunnel-auth
Habilita la autenticación de iguales de túneles basada en un secreto compartido de este direccionador.

Encapsulator

Utilice el mandato **encapsulator** para acceder al indicador `ppp-L2tp config>` a fin de configurar los parámetros PPP de todas las interfaces de túneles de capa 2 que estén configuradas como de entrada y especificar *any* como nombre de sistema principal remoto.

Sintaxis:

encapsulator

List

Utilice el mandato **list** para visualizar el estado de los diversos parámetros de configuración de túneles 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 túneles L2.

Sintaxis:

set
- buffers
- error-check-direction
- host-lookup-password
- local-hostname
- max-calls
- max-tunnels
- transmit-retries
- tunnel-rcv-window

buffers

Especifica el número de almacenamientos intermedios de túneles L2 internos solicitados. Si no hay suficiente memoria para satisfacer la petición, sólo estará disponible una parte de los almacenamientos intermedios en el momento del rearranque. Para confirmar la cantidad de memoria mientras L2T está activo, utilice el mandato **memory** (consulte “Memory” en la página 501).

Valores válidos: de 1 a 4000

Valor por omisión: depende del release:

Release	Valor
R1	600
R2	900

error-check-period [segundos]
Especifica el periodo de sondeo de errores de hardware de LAC. Cada periodo de sondeo generará un mensaje de notificación de errores de WAN transmitido de LAC a LNS. Los valores están comprendidos entre 60 y 65 000 segundos.

Valor por omisión: 120 segundos.

host-lookup-password
Especifica el secreto compartido para la autorización de túneles 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 el direccionador local y que se envía en mensajes de configuración de túneles.

Valor por omisión: IBM

max-calls
Especifica el número máximo de llamadas en todos los túneles que pueden estar activas en un momento determinado como LAC o LNS.

Valores válidos: depende del release:

Release	Rango
R1	de 1 a 500
R2	de 1 a 2000

Valor por omisión:depende del release:

Release	Valor por omisión
R1	200
R2	300

max-tunnels
Especifica el número máximo de túneles que pueden estar activos en un momento determinado como LAC o LNS.

Valores válidos: depende del release:

Release	Rango
R1	de 1 a 500
R2	de 1 a 2000

Valor por omisión:depende del release:

Release	Valor por omisión
R1	200
R2	300

transmit-retries
Especifica el número de veces que se vuelve a transmitir un paquete L2TP en el canal de control antes de que la sesión o el túnel se declaren inactivos y concluyan.

Valores válidos: de 2 a 100

Valor por omisión: 6

tunnel-rcv-window
Especifica el tamaño de ventana de recepción L2TP para el transporte de conexiones de control de confianza. Dicho transporte transmite y recibe los mensajes necesarios para la configuración, el desmantelamiento y el mantenimiento de túneles o sesiones.

Valores válidos: de 1 a 100

Valor por omisión: 4

Acceso al indicador de supervisión de túneles L2

Para acceder al indicador de supervisión de túneles L2:

1. Entre **talk 5** en el indicador OPCON (*).
2. Entre **feature layer-2-tunneling** en el indicador GWCON (+).

Mandatos de supervisión de túneles L2

En este apartado se resumen y, a continuación, se describen los mandatos de supervisión de túneles L2. Entre los mandatos en el indicador `Layer-2-Tunneling Console>`.

La Tabla 53 resume los mandatos de supervisión de túneles L2.

Tabla 53. Mandatos de supervisión de túneles 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 xxxii.
Call	Visualiza estadísticas e información sobre cada llamada en proceso.
Kill	Finaliza un túnel de manera inmediata.
Memory	Visualiza la asignación y el uso del almacenamiento intermedio de túneles L2.
Start	Inicia un túnel con otro igual.
Stop	Detiene un túnel y permite que cada igual lleve a cabo cualquier tarea de administración necesaria.
Tunnel	Visualiza estadísticas e información de 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 xxxiii.

Call

Utilice el mandato **call** para visualizar estadísticas e información de 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 a esta llamada.

Serial #

El número utilizado para el registro cronológico de esta llamada.

ACK-timeout

El número de veces que se ha recibido del igual una notificación de tiempo de espera excedido.

Dropped pkts

El número de paquetes que se han declarado perdidos para esta llamada. Son los paquetes que se deberían haber recibido, pero que el igual ha señalado como perdidos.

physical-errors

Visualiza errores de 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 a esta llamada.

Serial #

El número utilizado para el registro cronológico de esta llamada.

CRC Errors

El número de paquetes en los que no ha coincidido el CRC.

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 que ha transcurrido desde el último sondeo de errores.

queue

Visualiza información sobre la cola de 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 a esta llamada.

Serial #

El número utilizado para el registro cronológico de esta llamada.

Tx Win

La ventana de recepción máxima para datos del igual.

Rx Win

La ventana de transmisión máxima local.

Ns El siguiente número de secuencia de paquetes a enviar para esta llamada.

Nr El siguiente número de secuencia de paquete 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 que esperan a ser transmitidos por L2TP.

out Q

El número de paquetes PPP regulares que esperan a 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 a esta llamada.

Serial #

El número utilizado para el registro cronológico de esta llamada.

Net #

El número de dispositivo asociado a esta llamada. En el caso de una llamada LNS, es la red L2. En el caso de una llamada LAC, es el dispositivo PPP que ha recibido la llamada inicial.

State

El estado de llamada actual. Los estados de llamada válidos son:

Established

Preparado para tráfico de red enviado por túneles.

Idle
La llamada está desocupada.

Wait Cs Answer
Esperando que el enlace de comunicación se abra.

Wait Reply
Esperando respuesta del igual.

Wait Tunnel
Esperando establecimiento del túnel.

Time since chg
El tiempo que ha transcurrido desde el último cambio de estado.

PeerID
El ID de llamada del igual.

TunnelID
El túnel local asociado a esta llamada.

statistics
Visualiza estadísticas sobre la transmisión de datos de 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 a esta llamada.

Serial #
El número utilizado para el registro cronológico de 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 calculado actualmente para esta llamada.

ATO
El tiempo de espera de adaptación calculado actualmente para esta llamada.

Kill

Utilice el mandato **kill** para finalizar de manera inmediata un túnel. Este mandato libera todos los recursos locales de un túnel, con lo que se fuerza la finalización de la conexión. No se envía ninguna notificación de la finalización del túnel al igual.

Nota: Utilice este mandato sólo si el mandato **stop** no puede finalizar un túnel.

Sintaxis:

kill tunnel *id_túnel*

tunnel *id_túnel*
Especifica el túnel a finalizar.

Memory

Utilice el mandato **memory** para visualizar el nivel de utilización de memoria actual del 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. En este momento, 200 están en uso y 1000 están libres.

Start

Utilice el mandato **start** para iniciar un túnel con otro igual.

Sintaxis:

start **tunnel** *nombre_de_sistema_principal*

(no se le solicitarán parámetros para el nombre de sistema principal)

tunnel*nombre_de_sistema_principal*
El nombre del sistema principal con el que L2T establece el túnel.

Stop

Utilice el mandato **stop** para detener un túnel. Se llevan a cabo las operaciones de limpieza necesarias antes de que finalice el túnel.

Sintaxis:

stop tunnel *id_túnel*

tunnel *id_túnel*
Especifica el túnel a finalizar.

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 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 a un túnel.

Type
El tipo de protocolo de túnel que se está utilizando.

ACK-timeouts
El número de veces que se ha recibido del igual una notificación de tiempo de espera excedido.

peer
Visualiza los túneles y los iguales asociados a los túneles.

Ejemplo:

```
Layer-2-Tunneling Console> tunnel peer
Tunnel ID | Type | Peer ID | Peer Hostname
 96785    | L2TP |   89777 | igual1
 11264    | L2F  |   46538 | igual2
 34653    | L2F  |   11209 | igual3
 87511    | PPTP |   55377 | igual4
```

Tunnel ID
El identificador local asociado a un túnel.

Type
El tipo de protocolo de túnel que se está utilizando.

Peer ID
El identificador de túnel del igual asignado a este túnel.

Peer Hostname
El nombre del sistema principal igual tal y como aparece en la base de datos local.

queue
Visualiza información sobre la cola de 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 a un túnel.

Type
El tipo de protocolo de túnel que se está utilizando.

Rx Win
El número local máximo de paquetes que constituyen la ventana de recepción.

Tx Win
El número máximo de paquetes del igual que constituyen la ventana de recepción.

Ns El número de secuencia del siguiente paquete a enviar.

Nr El número de secuencia del siguiente paquete a recibir.

Rx Q
El número de paquetes que se hallan actualmente en la cola de recepción.

Tx Q
El número de paquetes que se hallan 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 a un túnel.

Type
El tipo de protocolo de túnel que se está utilizando.

Peer ID
El identificador de túnel del igual asignado a este túnel.

State
El estado de túnel actual. Los estados de túnel válidos son:

Established
El túnel se ha establecido.

Idle
El túnel está desocupado.

Wait Ctrl Reply
El sistema principal está esperando una respuesta del igual.

Wait Ctrl Conn
El sistema principal está esperando una indicación de conexión.

Time since chg
El tiempo que ha transcurrido desde el último cambio de estado.

 # Calls
El número de llamadas activas en este túnel.

Flags
Los indicadores utilizados para controlar los mensajes de conexión de este túnel.

statistics
Visualiza las estadísticas asociadas a 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 a un túnel.

Type
El tipo de protocolo de túnel que se está utilizando.

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 calculado actualmente para mensajes de conexión de control de túneles.

ATO
El tiempo de espera de adaptación calculado actualmente para mensajes de conexión de control de túneles.

transport
Visualiza información referente a 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 a un túnel.

Type
El tipo de protocolo de túnel que se está utilizando.

Peer IP address
La dirección IP del igual para este túnel.

UDP Src
El puerto UDP de origen para este túnel.

UDP Dest
El puerto UDP de destino para este túnel.

Soporte de reconfiguración dinámica de túneles L2

En este apartado se describe la reconfiguración dinámica (DR) y cómo afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

Los túneles de capa 2 dan soporte al mandato **delete interface** de CONFIG (Talk 6) sin restricciones.

Mandato activate interface de GWCON (Talk 5)

Los túneles de capa 2 dan soporte al mandato **activate interface** de GWCON (Talk 5) teniendo en cuenta que:

No existen limitaciones adicionales sobre otras interfaces PPP.

Todos los cambios en la configuración de los túneles de capa 2 se activan automáticamente, excepto estos:

Mandatos cuyos cambios no se activan al ejecutar el mandato activate interface de GWCON (Talk 5)
CONFIG, net, enable ccp **Nota:** No se habilitará la compresión si ésta es la primera red PPP con la función CCP habilitada.
CONFIG, net, set lcp options (opción mru) **Nota:** El valor MRU no se establecerá a un valor mayor que el tamaño del almacenamiento intermedio asignado para el direccionamiento durante el rearranque.

Mandato reset interface de GWCON (Talk 5)

Los túneles de capa 2 dan soporte al mandato **reset interface** de GWCON (Talk 5), tendiendo en cuenta que:

No existen limitaciones adicionales sobre otras interfaces PPP.

Todos los cambios en la configuración de los túneles de capa 2 se activan automáticamente, excepto estos:

Mandatos cuyos cambios no se activan al ejecutar el mandato reset interface de GWCON (Talk 5)
CONFIG, net, enable ccp **Nota:** No se habilitará la compresión si ésta es la primera red PPP con la función CCP habilitada.
CONFIG, net, set lcp options (opción mru) **Nota:** El valor MRU no se establecerá a un valor mayor que el tamaño del almacenamiento intermedio asignado para la interfaz PPP durante el rearranque.

Mandatos de cambio inmediato de CONFIG (Talk 6)

Los túneles de capa 2 dan soporte a los siguientes mandatos de CONFIG que permiten modificar inmediatamente el estado operativo del dispositivo. Estos cambios se guardan y se mantienen si el dispositivo se reinicia, si se vuelve a cargar 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

En la tabla siguiente se describen los mandatos de configuración de los túneles de capa 2 que no pueden cambiarse dinámicamente. Para activarlos es necesario reiniciar o volver a cargar 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, el 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 la red pública conozcan algunas de las direcciones de la red privada. NAT funciona utilizando direcciones públicas IP para que representen direcciones privadas IP.

Las direcciones públicas IP son las direcciones válidas de sistemas principales en la red pública 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 exclusivas suministradas por el Network Information Center (NIC).

El direccionador conoce las direcciones privadas, pero la red pública no las conoce. Las direcciones de cada red privada deben ser exclusivas; de todos modos, la misma dirección se puede duplicar en dos redes privadas diferentes. Las direcciones privadas se asignan a sistemas principales dentro de redes apéndice. Las redes apéndice son redes que tienen acceso a la red pública a través de un solo direccionador.

NAT amplía el número de direcciones IP disponibles de diversas maneras:

- Permite que cada dirección pública represente varias direcciones privadas mediante la rotación del uso de las direcciones públicas.
- Permite la duplicación de direcciones en la medida en que cada dirección duplicada se utilice en una red privada diferente.
- Permite que el administrador de la red utilice las direcciones IP de las redes privadas, en lugar de las direcciones NIC que se están convirtiendo en recursos limitados.

La utilización de direcciones privadas oculta también éstas frente al mundo exterior. Esta función de NAT lo hace útil como cortafuegos para evitar que se conozcan las direcciones privadas.

Importante: Tal y como se señala en la sección 5.4 del documento borrador de Internet que define NAT, “cualquier aplicación que transporte (y utilice) la dirección IP (y el puerto TCP/UDP, en el caso de la NAPT) dentro de la aplicación no operará a través de NAT...”. Se debe tener en cuenta que DLSw y XTP toman decisiones basadas en las direcciones IP de los extremos— concretamente deciden cuál es el asociado que dispone de la dirección más alta. Como la aplicación (DLSw o XTP) que está funcionando a través de NAT cree que su dirección es la dirección privada y la aplicación asociada del otro direccionador cree que la dirección de la aplicación es la dirección pública, se pueden tomar decisiones incorrectas.

La Figura 44 en la página 508 muestra el plano de una estación de trabajo en una red apéndice. En dicho ejemplo, la red apéndice consta de una subred IP que tiene la dirección IP 10.33.96.0 con la máscara de subred 255.255.255.0.

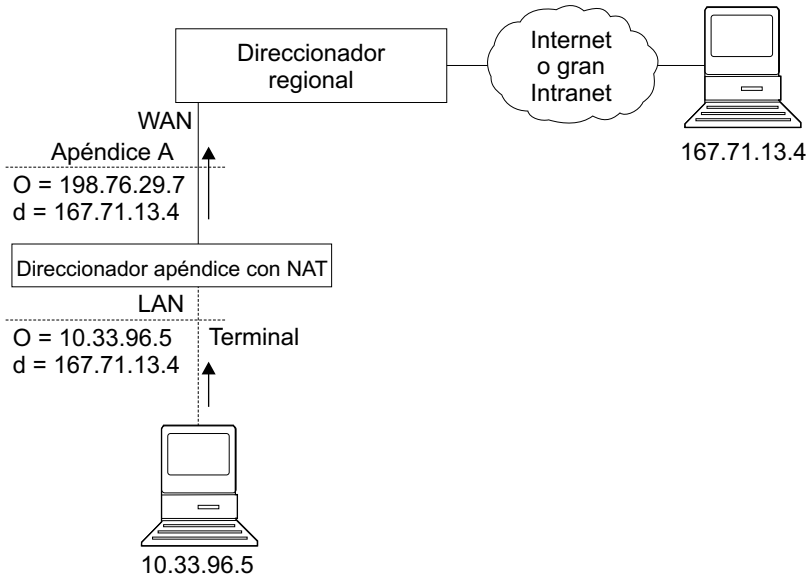


Figura 44. Red en la que se ejecuta NAT

Para utilizar NAT, el administrador de la red asigna una o más direcciones IP públicas a una agrupación de direcciones públicas en el 2212 y asigna una dirección IP privada a cada estación de trabajo de la red 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 enlaza en primer lugar la dirección privada de una estación de la red privada a una de las direcciones públicas. Enlazar significa que todos los paquetes que posean dicha dirección privada se convertirán a dicha dirección IP pública cuando el paquete salga. Los paquetes de entrada tiene la dirección IP pública como destino. NAT reconoce la dirección pública, la convierte en la dirección IP privada y reenvía el paquete. Después de que se detenga el tráfico, el enlace se mantiene hasta que un temporizador que el usuario puede establecer excede el tiempo de espera. En este momento, NAT finaliza el enlace y pone a disposición la dirección pública para que se pueda volver a utilizar.

En este ejemplo, se transmite un paquete desde la dirección de origen privada de envío 10.33.96.5 a una dirección de destino de Internet, 167.71.13.4. La función NAT del 2212 convierte la dirección privada 10.33.96.5 en la dirección pública 198.76.29.7. Esta conversión oculta a la red pública la dirección privada 10.33.96.5, de manera que ningún paquete entrante se dirige directamente a la dirección privada 10.33.96.5. Los paquetes entrantes de 167.71.13.4 se dirigen, en cambio, a la dirección pública 198.76.29.7. Cuando el direccionador de NAT recibe paquetes dirigidos a 198.76.29.7, 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

NAPT se puede utilizar sólo para tráfico TCP y UDP. En NAPT, varias direcciones privadas pueden utilizar una única dirección pública simultáneamente. Mientras que NAT correlaciona una dirección pública con una dirección privada, NAPT correlaciona la dirección pública NAPT ***y*** el número del puerto público con una dirección

privada y un número de puerto privado. Sólo se puede configurar una dirección NAPT para cada agrupación de direcciones públicas.

NAPT se configura fácilmente especificando una dirección pública o una interfaz de direcciones dinámicas (que esté utilizando PPP/IPCP para recuperar una dirección pública) que se utilizará para tráfico NAPT. La ventaja de NAPT es que puede habilitar una dirección de la agrupación de direcciones IP públicas para que ofrezcan soporte a muchas direcciones IP privadas de manera simultánea.

Correlaciones de direcciones estáticas

Es probable que en ocasiones desee configurar una estación o servidor en la red privada al que se puede acceder directamente desde la red pública. En ese caso, deberá llevar a cabo una correlación estática de la dirección privada de la estación con una dirección pública concreta. Todos los mensajes que salen de la dirección privada se convierten a la dirección pública designada y todos los mensajes que entran para la dirección pública designada se reenvían de manera automática a la dirección privada asociada. Existen dos tipos de correlaciones de direcciones estáticas: NAT y NAPT.

Correlación de direcciones estáticas NAT

En una correlación NAT, todos los protocolos IP pueden acceder al sistema principal. El siguiente es un ejemplo de la configuración de una correlación NAT:

Dirección privada	10.1.1.2
Puerto privado	0
Dirección NAT pública	9.67.1.1
Puerto público	0

Correlación de direcciones estáticas NAPT

Para especificar una aplicación TCP o UDP, tiene la opción de especificar una correlación NAPT que incorpore un puerto privado conocido públicamente. En el caso de correlación de direcciones estáticas, se debe configurar una dirección pública NAPT. Por ejemplo, para configurar un sistema principal Telnet en la dirección privada 10.1.1.1 para utilizar la dirección pública NAPT 9.67.1.2, la correlación estática se configuraría del siguiente modo:

Dirección privada	10.1.1.1
Puerto privado	23
Dirección NAPT pública	9.67.1.2
Puerto público	23

Los puertos públicos y privados se correlacionan con el puerto 23, que es el puerto conocido públicamente para Telnet. Ahora, si el administrador también dispone de un servidor FTP (dirección conocida públicamente 21) en la misma dirección privada 10.1.1.1 a correlacionar con la dirección pública NAPT 9.67.1.2, dicha correlación tendrá un aspecto similar a éste:

Dirección privada	10.1.1.1
Puerto privado	21
Dirección NAPT pública	9.67.1.2
Puerto público	21

El servidor de la dirección 10.1.1.1 tiene la misma dirección pública NAPT (9.67.1.2) para ambas aplicaciones pero NAPT las puede diferenciar utilizando números de puerto diferentes (23 y 21). De todos modos, NAPT no puede diferenciar dos servidores que utilizan la misma dirección pública NAPT y que tienen el mismo número de puerto y de aplicación. Por ejemplo, si la dirección pública NAPT y el puerto conocido públicamente son los mismos para 10.1.1.3 puerto 21 que para 10.1.1.1 puerto 21, NAPT no puede indicar si debe enviar tráfico FTP entrante al servidor 10.1.1.3 o al servidor 10.1.1.1. Para configurar más de un servidor con las mismas dirección NAPT y aplicación, deberá utilizar un puerto que no sea el puerto conocido públicamente en el servidor (por ejemplo, iniciar el daemon FTP en el puerto 200).

Establecimiento de filtros de paquetes y de reglas de control de acceso para NAT

Además de identificar el rango de direcciones privadas que NAT o NAPT deben convertir, el administrador debe configurar filtros de paquetes y reglas de control de acceso para IP en el 2212. La configuración de NAT requiere que se configuren un filtro de paquetes de entrada y uno de salida en la interfaz que esté conectada a la red pública. Es necesario que configure una o más reglas de control de acceso en el filtro de paquetes de entrada y una o más reglas de control de acceso en el filtro de paquetes de salida. Las reglas de control de acceso del filtro de entrada dejan pasar a NAT los paquetes de entrada que tengan definidas las direcciones públicas adecuadas. Las reglas de control de acceso del filtro de salida dejan pasar a NAT los paquetes de salida que tengan definidas las direcciones privadas adecuadas.

Las reglas de control de acceso que se aplican para NAT disponen de los tipos de reglas de control de acceso ***I*** (inclusivo) y ***N*** (NAT). Consulte la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 1* para obtener más información acerca de la configuración de controles de acceso IP.

Nota: NAT también se puede configurar junto con un túnel IPsec. Encontrará un ejemplo de dicha configuración en “Configuración de las reglas del control de acceso de filtros de paquetes para el direccionador A” en la página 429.

Ejemplo: Configuración de NAT con filtros IP y reglas de control de acceso

Este ejemplo le muestra cómo configurar NAT para el direccionador apéndice en la red que aparece en la Figura 45 en la página 511. Consulte “Configuración y supervisión del conversor de direcciones de red” en la página 515 si desea obtener una descripción de los mandatos.

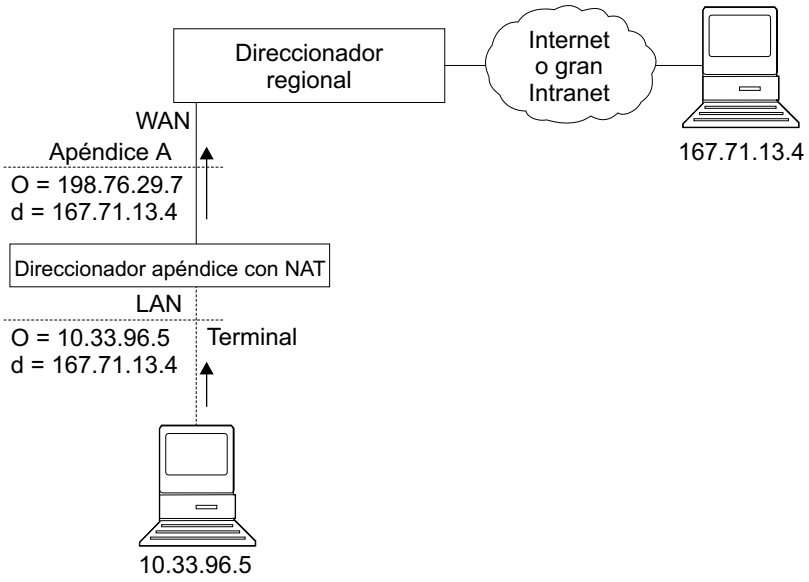


Figura 45. Red en la que se ejecuta NAT

Siga los pasos siguientes:

1. Configure agrupaciones de direcciones públicas para que NAT y NAPT las utilicen. Para hacerlo, 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 denominada *pool1*. La dirección NAPT de la agrupación es 198.76.29.7. Las direcciones 198.76.29.13 y 198.76.29.14 no están disponibles, con lo que la agrupación está configurada para excluirlas. Los parámetros que se entran son: *dirección-pública, máscara, número-en-grupo, nombre y dirección-napt*. El valor 0.0.0.0 como dirección NAPT significa que ninguna de las direcciones de este grupo es la dirección NAPT. Utilice 0.0.0.0 como dirección NAPT de todos los grupos si no configura NAPT para la agrupación.

2. Utilice el mandato **translate** para establecer los rangos de direcciones privadas que las direcciones públicas deben convertir en pool1. Los parámetros que se entran son: *dirección-privada, máscara y nombre*.

   ```
   NAT config> translate 10.33.96.0 255.255.255.0 pool1
   ```

3. Configure las correlaciones estáticas para estaciones dentro de la red privada que deban estar correlacionadas permanentemente con una de las direcciones públicas. Los siguientes mandatos identifican una máquina (10.33.96.5) que recibirá cualquier tipo de tráfico desde la red pública. Una segunda máquina (10.33.96.4) es tanto un servidor Telnet como un servidor HTTP. Los parámetros son *dirección-privada, número-puerto-privado, dirección-pública y número-puerto-público*. Observe que la dirección NAPT para pool1 se utiliza como la dirección pública para el sistema principal que está configurado 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 NAT.

   ```
   NAT config> enable NAT
   ```

5. Cree dos filtros de paquete IP para que IP deje pasar paquetes a NAT. Se trata de filtros de paquetes de entrada y 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 que aparezca el indicador `packet-filter 'filter-name' Config>`. Añada una regla de control de acceso para NAT al filtro de entrada. Los paquetes recibidos en la interfaz pública (red 0) que están destinados para una dirección de la agrupación de direcciones públicas reservadas de NAT se deben dejar pasar a NAT. NAT sustituirá la dirección pública (y el puerto público si el paquete está destinado a la dirección NAPT) con la dirección privada correcta (y el puerto privado si el paquete está destinado a la dirección NAPT). La dirección 0.0.0.0 y la máscara del origen de Internet indican que todas las direcciones de origen de la red pública pasará a 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 regla de control de acceso es mayor que el rango de direcciones definido en pool1. Si la dirección del paquete que se ha dejado pasar a NAT se encuentra en el rango definido en la regla de control de acceso pero no es uno de los que forman parte de la agrupación de direcciones, NAT devuelve el paquete a IP sin modificarlo.

7. Si desea que el direccionador pase paquetes que no cumplen con la regla de control de acceso, en lugar de eliminarlos, puede crear una regla comodín de control de acceso. El siguiente ejemplo muestra este tipo de regla de control de acceso:

```
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 regla de control de acceso para NAT al filtro de paquetes de salida. Los paquetes que se reenvíen desde la interfaz 0 de red y que disponen de una dirección de origen en la red privada son identificados a fin de que IP los pueda pasar a NAT. NAT sustituye la dirección privada por una de la 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 *in-0*, puede añadir una regla comodín de control de acceso inclusivo como última regla de control de acceso si prevé reenviar paquetes que no cumplen con la regla de control de acceso.

9. Puede utilizar el mandato **list packet-filter** *nombre-filtro* desde el indicador `IP Config>` para comprobar la precisión y la secuencia de las reglas de control de acceso en cada filtro de paquete.
10. Habilite los controles de acceso para IP.

    ```
    IP Config> set access-control on
    ```

11. Restablezca IP y NAT mediante talk 5. Hasta ahora, se han efectuado modificaciones en la configuración del direccionador pero dichos cambios no han afectado al direccionador. Los mandatos de restablecimiento (reset) de IP y NAT hacen que el direccionador lea en la nueva configuración y que ejecute con las reglas definidas en la configuración.

    ```
    NAT> reset NAT
    IP> reset IP
    ```

Configuración y supervisión del conversor de direcciones de red

En este capítulo se describen los mandatos de configuración y de supervisión del conversor de direcciones de red (NAT) y consta de los apartados siguientes:

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 `Config>`:

```
Config> feature nat
Network Address Protocol user configuration
NAT config>
```

Mandatos de configuración del conversor de direcciones de red

En este apartado se describen los mandatos de configuración del conversor de direcciones de red (NAT). Para configurar NAT, entre estos mandatos en el indicador `NAT config>`.

Tabla 54. 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 xxxii.
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 NAT.
Enable	Habilita NAT.
List	Lista información sobre la configuración de NAT.
Map	Crea un enlace 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 en la configuración NAT y ejecute según las reglas NAT que se han configurado.
Set	Establece tiempos de espera.
Translate	identifica las direcciones IP privadas que se la agrupación de direcciones públicas NAT debe convertir.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxiii.

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 que le permiten modificar las características de cualquiera de las agrupaciones de reserva de direcciones IP públicas (como, por ejemplo, direcciones IP y máscaras).

Valores válidos: Un número de índice para identificar la agrupación configurada. Dicho número se visualiza cuando se entra el mandato **list reserve pools**.

Valor por omisión: ninguno

translate *rangos*
Proporciona indicadores que le permiten modificar las características de cualquiera de los rangos de conversión de direcciones IP privadas (como, por ejemplo, direcciones IP y máscaras).

Valores válidos: Un número de índice para identificar el rango de conversión configurado. Dicho número se visualiza cuando se entra el mandato **list translate**.

Valor por omisión: ninguno

mappings
Proporciona indicadores que le permiten modificar las características de cualquiera de las correlaciones de direcciones estáticas (como, por ejemplo, direcciones IP y puertos).

Valores válidos: Un número de índice para identificar la correlación configurada. Dicho número se visualiza cuando se 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 direcciones IP privadas y correlaciones.

Sintaxis:

delete reserve
translate
mappings

reserve *agrupaciones*
Proporciona indicadores que le permiten suprimir cualquiera de las agrupaciones de reserva de direcciones IP públicas.

Valores válidos: Un número de índice para identificar la agrupación configurada. Dicho número se visualiza cuando se entra el mandato **list reserve pools**.

Valor por omisión: ninguno

translate *rangos*
Proporciona indicadores que le permiten suprimir cualquiera de los rangos de conversión de direcciones IP privadas.

Valores válidos: Un número de índice para identificar el rango de conversión configurado. Dicho número se visualiza cuando se entra el mandato **list translate**.

Valor por omisión: ninguno

mappings
Proporciona indicadores que le permiten suprimir cualquiera de las correlaciones de direcciones estáticas.

Valores válidos: Un número de índice para identificar la correlación configurada. Dicho número se visualiza cuando se entra el mandato **list mappings**.

Valor por omisión: ninguno

Disable

Utilice el mandato **disable** para inhabilitar NAT. Puede inhabilitar NAT para que elimine paquetes que requieren conversión o puede inhabilitar NAT para que deje pasar paquetes que requieren conversión.

Sintaxis:

disable nat

drop

pass

drop
Inhabilita NAT para que elimine paquetes que requieren conversión.

pass
Inhabilita NAT para que deje pasar paquetes que requieren conversión.

Enable

Utilice el mandato **enable** para habilitar NAT. Al habilitar NAT ya está preparada para ejecutarse pero no lo hará 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, los rangos de conversión de direcciones IP privadas, las correlaciones, los valores globales o toda la información de NAT.

Sintaxis:

list	reserve
	addresses
	pools
	translate
	mappings
	global
	all

En el ejemplo siguiente, el tiempo se visualiza en horas, minutos y segundos. La antigüedad de la entrada es el tiempo que ha transcurrido desde que la estrada se utilizó por última vez. Enlace significa que el tráfico está fluyendo entre estas dos direcciones. Los tiempos de espera determinan el tiempo que transcurrirá después de la última comunicación hasta que se elimine un enlace. Consulte el mandato **set** si desea obtener más información sobre los tiempos de espera.

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 de manera estática un sistema principal o servidor de la red privada a un dirección pública. Este mandato, que se puede utilizar para configurar servidores de la red privada, establece una asociación cuando se arranca NAT que no cambia nunca.

Las correlaciones estáticas con el número de puerto privado o público 0 son correlaciones NAT; las que poseen otros valores de número de puerto son correlaciones 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 de sistema principal de Internet en un formato IP válido. Debe ser la dirección asignada a una estación en la red apéndice que requiere acceso permanente desde la red pública, como, por ejemplo, un servidor.

Valor por omisión: ninguno

número de puerto privado
El número de puerto TCP/UDP de la aplicación que se ejecuta en el dispositivo con la dirección privada. Si entra **0** se crea un enlace NAT y si entra otro valor se crea un enlace NAPT. Valores de puerto comunes para NAPT son 23 para Telnet, 21 para FTP y 80 para HTTP.

Valores válidos: 0 - 65535

Valor por omisión: 0

dirección pública
La dirección IP pública con la que se debe correlacionar esta dirección privada. Debe ser una dirección NAPT en el caso de una correlación NAPT y una dirección NAT en el caso de una correlación NAT.

Valores válidos: una dirección IP válida exclusiva de la red pública. La red pública puede ser Internet o una intranet, en función del diseño de la red.

Valor por omisión: ninguno

número de puerto público
El número de puerto de los paquetes que se deben convertir 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 dirección IP privada 10.11.12.200 acepta todo el tráfico de Internet; el servidor con 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. Se puede utilizar así mismo para añadir una interfaz IP dinámica a la agrupación de direcciones públicas.

Sintaxis:

reserve *dynamic [interface][dirección-pública][máscara][número-en-grupo] nombre [dirección-napt]*

Nota: Los valores que aparecen entre corchetes se visualizan ahora de manera opcional.

- Dynamic - Especifica si esta entrada es para un grupo de direcciones públicas o para una interfaz de direcciones dinámicas que recuperarán su dirección IP de una conexión PPP que está utilizando IPCP. Los valores válidos son *yes* (sí) o *no*. El valor por omisión es *no*. Si Dynamic=*yes* (sí), sólo deberá especificar la interfaz y el

nombre. Si Dynamic=*no*, no deberá especificar la interfaz pero sí el resto de valores.

- Interface - Especifica la interfaz de direcciones dinámicas tal y como está configurada dentro de IP. Se puede especificar cualquier número de interfaz válido. El valor por omisión es cero.

dirección pública
La primera dirección IP pública en la secuencia de direcciones que componen este rango o grupo de la agrupación. Por ejemplo, si este grupo de la agrupación consta de 12 direcciones comprendidas en la secuencia que va desde 9.8.7.6 a 9.8.7.17, dicho valor es 9.8.7.6.

Nota: Para añadir otro rango de direcciones a la agrupación de direcciones públicas, utilice el mandato **reserve** independientemente para cada grupo, relacionando un grupo con otro mediante la utilización del mismo nombre de agrupación. Por ejemplo, las direcciones que van de 9.8.7.6 a 9.8.7.17 se pueden configurar en un grupo dentro de la pool1 y las direcciones que van de 9.8.7.1 a 9.8.7.3 se pueden configurar en otro grupo dentro de la misma agrupación. Por lo tanto, esta agrupación no configura ni utiliza las direcciones 9.8.7.4 y 9.8.7.5.

Valores válidos: una dirección IP válida que sea exclusiva de la red pública

Valor por omisión: ninguno

máscara
Una máscara para seleccionar bits de la dirección IP. La máscara, al igual que una dirección IP, tiene una longitud de 32 bits. Los unos (1) de la máscara seleccionan la parte de red o subred de la dirección. Los ceros (0) seleccionan la parte de sistema principal. Por ejemplo, la dirección 9.8.7.6 y la máscara 255.255.0.0 incluyen el rango de todas las direcciones cuyos primeros dos bytes son 9.8 (es decir, de 9.8.0.0 a 9.8.255.255).

Valores válidos: cualquier máscara IP válida

Valor por omisión: ninguno

número en el grupo
Especifica el número de direcciones secuenciales, empezando por la *dirección-pública*, que se incluyen en el grupo. En el caso de las direcciones de 9.8.7.6 a 9.8.7.17, este valor es 12.

Valores válidos: 1 - el valor que la máscara IP pueda definir

Valor por omisión: ninguno

nombre
El nombre de la agrupación de reserva de direcciones públicas. Esta serie de caracteres debe coincidir con el nombre de la agrupación del mandato **translate** correspondiente.

Valores válidos: cualquier nombre, con un máximo de 16 caracteres imprimibles; los espacios en blanco iniciales y finales se ignoran.

Valor por omisión: ninguno

dirección napt
La dirección IP de la agrupación de direcciones públicas que la conversión de puertos y direcciones de red (NAPT) utilizará. Esta dirección se utiliza para tráfico TCP y UDP a fin de correlacionar varias direcciones privadas con la

dirección NAPT según el número de puerto de protocolo. La utilización de NAPT es opcional. Si se utiliza, sólo puede haber una dirección NAPT por cada agrupación de direcciones públicas. Si no existe ninguna dirección NAPT para una agrupación o grupo, entre el valor **0.0.0.0**. Sólo tiene que entrar una vez la dirección NAPT para la agrupación.

Valores válidos: una de las direcciones IP públicas. No debe estar incluida necesariamente en el rango de valores definidos en la agrupación de direcciones públicas pero sí que debe hallarse en la misma subred.

Valor por omisión: 0.0.0.0 (que significa 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 NAT. Este mandato suprime todos los enlaces, libera toda la memoria utilizada por NAT y reinicia NAT según la configuración actual de Talk 6. Cuando se reinicia NAT no se interrumpe ningún otro componente del 2212.

Sintaxis:

reset n**at**

Tenga en cuenta que si NAT encuentra una configuración no válida, aparecerá un mensaje en ese sentido. Repase los mensajes NAT ELS para saber por qué ha fallado la inicialización.

Set

Utilice el mandato **set** para establecer tiempos de espera TCP y no TCP.

Sintaxis:

s**et** t**cp**

n**ontcp**

tcp *timeout*

El tiempo que NAT mantiene un enlace TCP después de que el último mensaje pase 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 45 días, aproximadamente)

Valor por omisión: 1440 minutos (24 horas)

nontcp *tiempo de espera*

El tiempo que NAT mantiene un enlace que no es TCP después de que el último mensaje haya pasado entre las dos estaciones 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 45 días, aproximadamente)

Valor por omisión: 1 minuto

Translate

Utilice el mandato **translate** para añadir una subred a la lista de direcciones que NAT convertirá. Cada subred es un rango de conversión. Este mandato se debe entrar para cada rango de conversión que NAT deba conocer. Cualquier número de rangos de conversión puede utilizar una única agrupación de reserva de direcciones públicas.

Sintaxis:

translate *Dirección-privada máscara nombre*

dirección privada
Cualquier sistema principal IP o dirección de subred que se deba convertir.

Valores válidos: una dirección en formato IP decimal con puntos válida. Cuando se realiza una operación AND con su máscara de subred, esta dirección identifica todas las direcciones de una subred apéndice. Una subred apéndice es una red que accede a la red pública sólo a través del direccionador.

Valor por omisión: ninguno

máscara
Valores válidos: La máscara de red o subred asociada con la red apéndice que debe ser convertida.

Valor por omisión: la máscara de clase de la dirección privada

nombre
El nombre de la agrupación de direcciones públicas que NAT debe utilizar para este rango de direcciones privadas.

Valores válidos: cualquier nombre, con 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 de red

Para acceder al entorno de supervisión de NAT, escriba

```
* t 5
```

A continuación, entre el siguiente mandato en el indicador **+**:

```
+ feature NAT
NAT>
```

Aparece el indicador NAT>.

Mandatos de supervisión del conversor de direcciones de red

En este apartado se describen los mandatos de supervisión de la Seguridad IP. Entre estos mandatos en el indicador NAT>.

Tabla 55. 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 xxxii.
List	Lista información sobre NAT.
Reset	Hace que el direccionador lea en la configuración NAT y ejecute según las reglas de acceso NAT que se han configurado. NAT no afecta al funcionamiento del direccionador hasta que se 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 xxxiii.

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, el tiempo se visualiza en horas, minutos y segundos. La antigüedad de la entrada es el tiempo que ha transcurrido desde que la estrada se utilizó por última vez. Un enlace significa que se ha establecido una sesión entre estas dos direcciones. Los tiempos de espera determinan el tiempo que transcurrirá después de la última comunicación hasta que se elimine un enlace. Consulte el mandato **set** de Talk 6 si desea obtener más información sobre los tiempos de espera.

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 NAT. Este mandato suprime todos los enlaces, libera toda la memoria utilizada por NAT y reinicia NAT según la configuración actual de Talk 6. Cuando se reinicia NAT no se interrumpe ningún otro componente del 2212.

Sintaxis:

reset n**at**

Soporte de reconfiguración dinámica de NAT

En este apartado se describe la reconfiguración dinámica (DR) y cómo afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

NAT no da soporte al mandato **delete interface** de CONFIG (Talk 6).

Mandato activate interface de GWCON (Talk 5)

El mandato **activate interface** de GWCON (Talk 5) no es aplicable a NAT. NAT no tiene registros SRAM asociados con una interfaz.

Mandato reset interface de GWCON (Talk 5)

El mandato **reset interface** de GWCON (Talk 5) no es aplicable a NAT. NAT no tiene registros SRAM asociados con una interfaz.

Mandatos de restablecimiento de componente de GWCON (Talk 5)

NAT da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos de NAT:

Mandato GWCON, feature NAT, reset NAT

Descripción: El mandato **reset** hace que se detengan todos los temporizadores de NAT, inhabilita la función y libera toda la memoria que utilizaba. Se borran todas las correlaciones de conversión, fragmentos de paquetes e información sobre la sesión TCP. La rutina de inicialización de NAT leerá el estado de NAT de los registros de configuración. Si NAT está habilitado, a partir de los registros de configuración se inicializarán las agrupaciones de direcciones públicas, los rangos de direcciones privadas, las tablas de correlaciones, las tablas de reensamblado de fragmentos, los tiempos de espera y los temporizadores. En este momento, NAT vuelve a estar preparado para recibir paquetes de filtros de paquetes IP.

Efecto en la red: Si NAT estaba habilitado anteriormente, todas las sesiones TCP caducarán, lo que se notificará a las aplicaciones. Se perderán las correlaciones UDP y de datagramas y se descartarán los paquetes que pertenezcan a dichas corrientes de datos. En cuanto se vuelva a inicializar NAT, pueden restablecerse las sesiones TCP, así como las corrientes de paquetes de datagramas de UDP y de otros tipos.

Limitación: Loa filtros de paquetes IP deben configurarse correctamente para que IP pueda pasarle paquetes a NAT.

El mandato **GWCON, feature nat, reset nat** da soporte a todos los mandatos de NAT.

Mandatos de cambio inmediato de CONFIG (Talk 6)

NAT da soporte a los siguientes mandatos de CONFIG que cambian inmediatamente el estado operativo del dispositivo. Estos cambios se guardan y se mantienen si el dispositivo se reinicia, si se vuelve a cargar 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 (DIALs)

Un servidor DIALs permite a los usuarios remotos establecer una conexión de entrada con una LAN y acceder a los recursos de la LAN del mismo modo que si estuvieran conectados localmente con un adaptador de LAN. De manera similar, el servidor DIALs también permite a los usuarios conectados a la LAN establecer una conexión de salida con los recursos de la WAN (como, por ejemplo, boletines de anuncios, máquinas de FAX, proveedores de servicios de Internet (ISP) y otros servicios en línea), con lo cual desaparece la necesidad de una línea telefónica analógica y de un módem en su estación de trabajo.

el servidor DIALs se puede configurar simultáneamente tanto para usuarios de conexión de entrada como para usuarios de conexión de salida. El cliente de marcación de entrada IBM DIALs se ejecuta en la estación de trabajo remota y proporciona la función de marcación de entrada. La Figura 46 en la página 528 muestra un ejemplo de un dispositivo utilizado como un servidor DIALs que da soporte a la función de marcación de entrada.

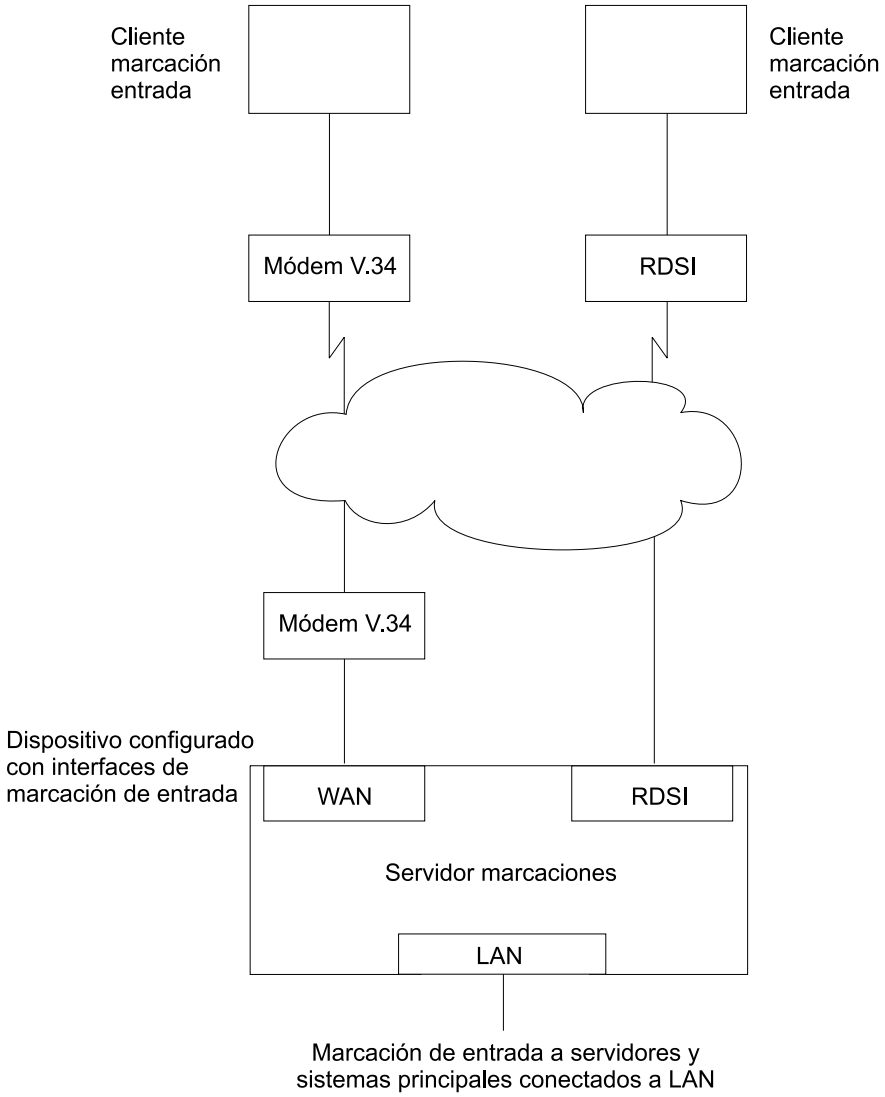


Figura 46. Ejemplo de servidor DIALs que da soporte a la función de marcación de entrada

El cliente de marcación de salida IBM DIALs se ejecuta en la estación de trabajo conectada a la red y proporciona la función de marcación de salida. Figura 47 en la página 529 muestra un ejemplo de un 2212 utilizado como un servidor DIALs que da soporte a la función de marcación de salida.

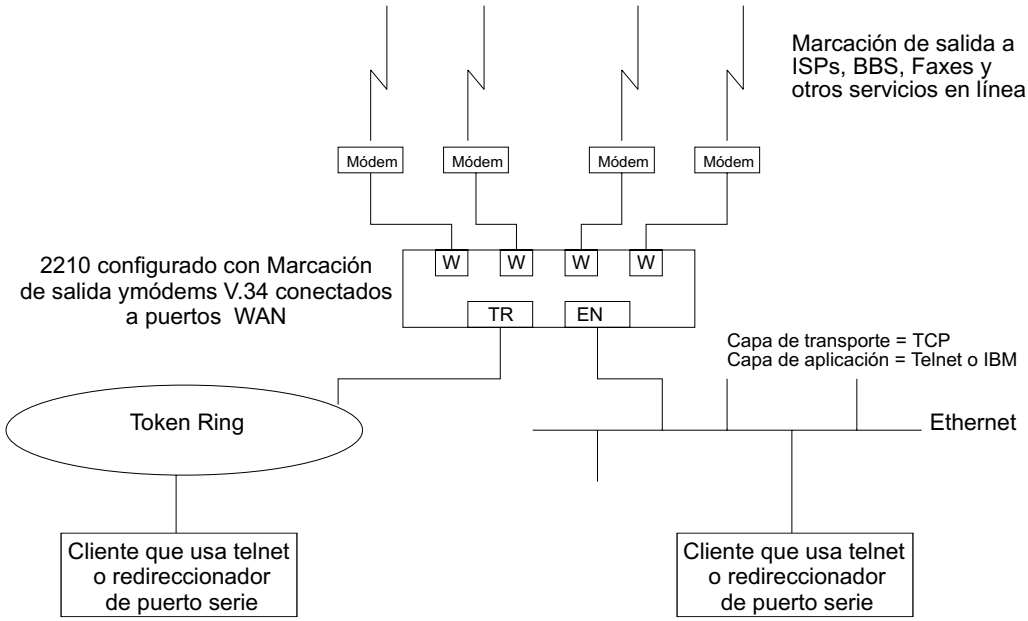


Figura 47. Ejemplo de servidor DIALs que da soporte a la función de marcación de salida,

Antes de utilizar el acceso de marcación de entrada

Antes de utilizar el acceso de marcación de entrada, es necesario que:

- Una estación de trabajo ejecute el cliente de marcación de entrada IBM DIALs u otro cliente de marcación de entrada PPP (a los que se hará referencia con los nombres ***cliente de marcación de entrada*** o ***cliente de marcación de entrada PPP*** a lo largo de los apartados siguientes).
- Existan configuraciones de protocolo completadas en la máquina cliente.
- Existan las interfaces RDSIy RDSI/Módem digital, las interfaces de módem integrado, una interfaz de módem nulo o módems V.34 externos conectados a puertos WAN del 2212 que quiera utilizar para la función de marcación de entrada de un único usuario.
- Que haya un servidor DIALs totalmente configurado en la LAN.

Configuración del acceso de marcación de entrada

En este apartado se describe cómo configurar las funciones de marcación de entrada y de marcación de salida en el servidor DIALs. La configuración de un cliente para utilizar el 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 del 2212 son un tipo especial de circuitos de marcación. Como la mayoría de los valores de un circuito de marcación habitual no son importantes para las aplicaciones de marcación de entrada de un único usuario, se puede añadir un nuevo tipo de dispositivo denominado ***de marcación de entrada*** que establezca los valores por omisión adecuados para el circuito de marcación. Al añadir un dispositivo de marcación de entrada también se configuran

los valores por omisión de configuración del encapsulador PPP que trabajan con la mayoría de clientes de marcación de entrada PPP, incluido el cliente de marcación de entrada IBM DIALs. Estos valores por omisión se describen en “Valores por omisión de parámetros de circuitos de marcación para interfaces de marcación de entrada” en la página 530 y “Parámetros de encapsulador PPP de circuito de marcación para circuitos de marcación de entrada” en la página 531.

Nota: La función DIALs sólo se puede habilitar en circuitos de marcación de entrada. A los circuitos de marcación de entrada les dan soporte las redes V.34, RDSI y RDSI con módem digital.

Valores por omisión de parámetros de circuitos de marcación para interfaces de marcación de entrada

Notas:

1. No modifique los parámetros descritos en este apartado. Si lo hace la función de marcación de entrada no funcionará correctamente.
2. Es probable que algunos parámetros no se visualicen o no se puedan configurar. Si desea obtener una descripción completa de los parámetros, consulte “Configuración y supervisión de circuito de marcación” en la publicación *Access Integration Services Guía del usuario de software*.

Se establecen los siguientes valores por omisión cuando se añade una interfaz de marcación de entrada:

- El ***Tiempo de inactividad*** se establece en 0. Observe que se define un circuito estándar como circuito en los casos en que el temporizador de inactividad no tiene sentido. No será un circuito fijo con el que establecer una conexión de salida. La única vez que el circuito establecerá una conexión de salida será si se ha negociado una devolución de llamada PPP o si se ha habilitado el protocolo PPP de multienlace para este circuito. Consulte “Shiva Password Authentication Protocol (SPAP)” y “Utilización del protocolo PPP de multienlace” en la publicación *Access Integration Services Guía del usuario de software* .
- Se permiten ***llamadas de entrada***. Se configuran todas las entradas porque los clientes de marcación de entrada no utilizan el intercambio LID implementado por los circuitos de marcación Nways.
- Se permiten ***llamadas de salida***.

  Nota: La “salida” para un circuito de marcación de entrada no es la misma que para un circuito de marcación de salida. Consulte “Antes de la configuración de interfaces de marcación de salida” en la página 532.
- Se configura una dirección de destino para “dirección_por_omisión”. Esta dirección se añade a la lista de direcciones V.34. Como estas llamadas son de entrada y una devolución de llamada o un intercambio de PPP de multienlace sólo dará como resultado llamadas de salida, la dirección de destino no tiene sentido. De todos modos, la dirección es necesaria para los parámetros de circuito. No suprima esta dirección o sus circuitos se inhabilitarán.

Parámetros de encapsulador PPP de circuito de marcación para circuitos de marcación de entrada

Nota: Si desea obtener una descripción completa de los siguientes parámetros, consulte “Using Point-to-Point Protocol Interfaces” en la publicación *Access Integration Services Guía del usuario de software*.

Se establecen los siguientes valores por omisión cuando se añade una interfaz de marcación de entrada:

- Se habilita la autenticación para SPAP, CHAP y PAP.
- El MRU de PPP se establece en 1522. Este tamaño de MRU es necesario para las versiones de Windows 3.1, OS/2 y DOS de los clientes de marcación de entrada IBM DIALs. No cambie este valor a menos que sepa que no está utilizando estos clientes.
- Habilita de manera automática DIALs en el encapsulador PPP. Ello activa algunas de las funciones importantes para los usuarios del acceso de marcación de entrada a las LAN, como pueden ser el protocolo NetBIOS Control, el protocolo NetBIOS Frame Control, el tiempo restante, la autenticación SPAP, las devoluciones de llamada, la autenticación LCP y la adición y supresión automáticas de las rutas estáticas IP que van al cliente. Consulte “Utilización de interfaces con el protocolo punto a punto” en la publicación *Access Integration Services Guía del usuario de software* si desea obtener más información sobre las funciones de DIALs.

Añadir una interfaz de marcación de entrada

Para añadir una interfaz de marcación de entrada:

1. Configure una interfaz V.34, RDSI o RDSI/Módem digital en el 2212. Consulte “Using the V.34 Network Interface” en la publicación *Access Integration Services Guía del usuario de software* si desea obtener detalles sobre la configuración. Consulte “ Using the ISDN Interface” en la publicación *Access Integration Services Guía del usuario de software* para obtener información sobre interfaces RDSI y de módem digital.
2. Entre **talk 6** para acceder al indicador `Config >`.
3. Entre **add device dial-in** en el indicador `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 sobre sus números de red, solicitará el número de red base y solicitará la habilitación del protocolo PPP de multienlace.

   Ejemplo: suponga que la red máxima actual es 3 y que desea agregar 1 red de marcación de entrada a la red base 2.

La Figura 48 es un ejemplo de definición de una interfaz de marcación conexión de entrada.

Figura 48. Añadir 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 la configuración de interfaces de marcación de salida

Antes de configurar y utilizar las interfaces de marcación de salida en el 2212, es necesario que:

- El software IBM con soporte para DIALs esté cargado en un 2212.
- Se disponga de un módem V.34 externo, un módem integrado o un módem nulo, si se conecta con un puerto de WAN disponible en el 2212. Consulte “Using the V.34 Network Interface” en la publicación *Access Integration Services Guía del usuario de software* si desea obtener información de configuración.
- Se disponga de una estación de trabajo conectada a la LAN que tenga acceso al servidor DIALs del 2212.
- Se disponga de software en el cliente como, por ejemplo, Telnet, un direccionador de Telnet o los clientes de marcación de salida IBM DIALs. IP debe estar configurado correctamente en el cliente para que el cliente de marcación de salida funcione.

Utilización del módem nulo

Cuando utilice un módem nulo, utilice el reconocimiento completo 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 siguientes pasos describen la manera de configurar una interfaz de marcación de salida en el dispositivo.

1. Conecte un módem V.34 al puerto de WAN que utilizará como interfaz de marcación de salida.
2. Conecte con la consola del servidor DIALs del 2212.

3. Entre **talk 6** en el indicador *.
4. Configure una interfaz V.34. Consulte " Using the V.34 Network Interface" en la publicación *Access Integration Services Guía del usuario de software* si desea obtener más detalles.
5. Añada una interfaz de marcación de salida mediante el mandato **add device dial-out**. Cuando se le solicite la interfaz, utilice un número de interfaz V.34.

   Notas:

   a. Se pueden configurar varios circuitos en el principio de una red base V.34. De todos modos, sólo puede haber activo un circuito en un momento determinado.

   b. El software define una dirección V.34 denominada ***dirección_por_omisión***. Si no suprime esta dirección tal y como requiere la función de marcación de salida, ésta no funcionará sin ella.
6. Configure el servidor de autenticación PPP, si está configurando el cliente de marcación de salida IBM DIALs y añada usuarios PPP, tal y como se describe en el capítulo "Protocolos de autenticación de PPP" en la publicación *Access Integration Services Guía del usuario de software*. Los usuarios PPP añadidos deben tener la función de marcación de salida habilitada. La función de marcación de salida mediante Telnet no requiere autenticación, por lo tanto no configure la autenticación para sesiones Telnet.
7. Configure los parámetros de marcación de salida global mediante el mandato **feature dials**. Consulte el mandato **feature** en la publicación *Access Integration Services Guía del usuario de software*.

   En este entorno puede configurar el temporizador de inactividad de marcación de salida, el nombre del servidor de marcación de salida, las agrupaciones de módems y otros parámetros.
8. Para que el cliente de marcación de salida IBM DIALs funcione correctamente, SNMP debe estar habilitado en el 2212 y debe definirse una comunidad SNMP llamada *public* en el 2212 con acceso de lectura. Esto es obligatorio para que la aplicación de seleccionador de marcación de salida pueda descubrir los servidores de marcación de salida en la red. Consulte el capítulo "Gestión de SNMP" en la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 1* para obtener más información sobre cómo habilitar SNMP y 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 solo módem. Cuando el usuario necesita establecer una conexión de salida, se utiliza el primer módem disponible de esta agrupación. Las agrupaciones de módems se crean en el servidor DIALs del 2212 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. El asignar un nombre de manera individual a las interfaces de marcación de salida le permite a un usuario seleccionar un módem concreto para establecer una conexión de salida.

Para configurar una agrupación de módems:

1. Entre **talk 6** en el indicador *.

2. Entre **net *n***, donde ***n*** es el número de la interfaz de marcación de salida, tal y como se define en “Utilización de la interfaz de red V.34” en la publicación *Access Integration Services Guía del usuario de software*. Esta acción le sitúa en el entorno de configuración de la interfaz.
3. Entre **encapsulator** (consulte “ Configuración y supervisión de circuitos de marcación” en la publicación *Access Integration Services Guía del usuario de software*) en el indicador `Circuit Config>`. Esta acción le sitúa en el entorno de configuración de la función de marcación de salida.
4. Entre **set portname** en el indicador `Dial-out Config>`. Esta acción le solicitará el nombre del puerto (hasta 30 caracteres). Si especifica un número de puerto existente, el módem se añade a la agrupación con ese nombre.
5. Reinicie el 2212.

Antes de la configuración de los parámetros de DIALs globales

En este apartado se describen los parámetros de servidor DIALs globales.

Direcciones IP proporcionadas por el servidor

El direccionador puede estar configurado para proporcionar una dirección IP para que un cliente de marcación de entrada la utilice mientras dure su conexión. La dirección que el direccionador asigne al cliente se puede recuperar de cuatro maneras diferentes, que 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 pide una dirección IP, el direccionador recupera la dirección configurada en ese perfil de usuario PPP del usuario. Ello le permite al usuario obtener siempre la misma dirección IP pero obliga a que haya una dirección IP exclusiva 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 interfaces de marcación de entrada. Cuando un cliente conecta y pide una dirección IP, el direccionador recupera la dirección de la interfaz a través de la cual se ha efectuado la conexión. Este método obliga a que haya 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 de la interfaz.
   - Utilice el mandato `PPP Config>` **set ipcp** para establecer la dirección IP de interfaces.

3. Agrupación

   Se pueden almacenar bloques de direcciones IP en una agrupación de direcciones IP. Cuando un cliente se conecta y pide una dirección, el direccionador

recupera una dirección de la agrupación. Cuando el cliente se desconecta, la dirección vuelve a la agrupación. Este método proporciona una única ubicación para configurar direcciones IP del cliente de marcación de entrada sin la necesidad de un servidor de direcciones.

Utilice el mandato `DIALs config>` **add ip-pool** para añadir una agrupación de direcciones IP.

4. Proxy DHCP

   Se puede ceder una dirección IP de un servidor servidor DHCP. Cuando un cliente se conecta y pide una dirección, el direccionador solicita una dirección del servidor DHCP en nombre del cliente. Este método obliga a que un servidor DHCP esté presente en la LAN o configurado en el direccionador. Un servidor DHCP puede proporcionar direcciones para clientes en varios direccionadores. Consulte “Protocolo de configuración dinámica de sistemas principales (DHCP)” si desea obtener más información.

   Utilice el mandato `DIALs config>` **add dhcp-server** para agregar un servidor DHCP.

Métodos de asignación de direcciones IP

La dirección IP que un cliente de marcación de entrada utiliza durante la conexión puede proceder de cinco fuentes diferentes, que se listan en orden de preferencia:

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 va pasando por estas fuentes hasta que encuentra una dirección o agota todas las fuentes. Si no se puede encontrar ninguna dirección, la negociación 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: Por omisión, no hay direcciones configuradas en el perfil de usuario PPP, en la interfaz o en la agrupación de direcciones.

Protocolo de configuración dinámica de sistemas principales (DHCP)

El protocolo de configuración dinámica de sistemas principales (DHCP) se ha desarrollado para proporcionar parámetros de configuración a sistemas principales de una red. Entre otros parámetros de configuración, DHCP dispone de un mecanismo para la asignación de direcciones de red a sistemas principales.

La función proxy DHCP actúa como un cliente *en nombre* de un usuario PPP de marcación de entrada. Ello permite al dispositivo obtener una cesión de dirección IP durante la sesión de marcación de entrada o hasta que la cesión finalice. La

dirección IP que se ha asignado desde el servidor DHCP se comunica con el cliente de marcación de entrada mediante el IPCP de PPP (consulte “Protocolo de control de IP” en la publicación *Access Integration Services Guía del usuario de software* si desea obtener una descripción de IPCP). El software del cliente de marcación de entrada no sabe que DHCP se ha utilizado para asignar una dirección IP y, por lo tanto, no requiere activación de DHCP alguna.

El proxy DHCP obliga a que por lo menos un servidor DHCP esté configurado y sea accesible desde el direccionador.

El proxy DHCP obliga a que las direcciones que se están asignando a usuarios de marcación de entrada estén dentro de la misma subred de una LAN conectada directamente. En una configuración habitual, ello obliga a que se habilite el direccionamiento de subred del proxy ARP a fin de que el direccionador pueda responder las peticiones ARP de sistemas principales de la red local en nombre de los clientes de marcación de entrada.

Configuración DHCP básica

La configuración más básica llama a un único servidor DHCP de la misma red que el direccionador, con las direcciones de marcación de entrada a ceder dentro de la misma subred que esta LAN.

Cuando el cliente establece una conexión de entrada, se obtiene la cesión de una dirección IP del servidor DHCP que se utiliza en la negociación IPCP con el cliente.

1. Conecte el 2212 y DHCP a la misma LAN.
2. Configure e inicie el servidor DHCP (consulte la documentación del servidor DHCP para saber cómo configurar el servidor para ceder direcciones IP. Recuerde que las direcciones IP a ceder DEBEN estar dentro de una subred de una LAN conectada de manera directa y que el proxy ARP debe estar habilitado en el 2212).
3. La configuración habitual del proxy DHCP inhabilita las opciones "Client-Specified", "Userid" e "Interface and Pool IP Address Negotiation":

   ```
   Dials Config>list ip
   DIALs client IP address specification:
   Client : disabled
   UserID : disabled
   Interface : disabled
   DHCP Proxy : enabled
   ```

4. Añada un servidor DHCP (`Dials Config>` **add dhcp 10.0.0.111**)
5. Establezca el software de cliente de marcación de entrada como *Server assigned*.

   Notas:

   a. La configuración de *Server assigned* varía entre las diferentes implementaciones de clientes de marcación de entrada.

   b. El software de cliente no debe estar configurado para obtener su dirección de DHCP. El cliente debe obtener su dirección enviando una dirección de 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.

Varios saltos para acceder al servidor DHCP

Los servidores configurados DHCP deben ser direcciones IP a las que se pueda acceder desde el direccionador conectado. Es necesario que se pueda aplicar siempre ping al servidor desde el recuadro de acceso remoto.

Cuando el servidor DHCP se encuentra a una distancia de varios saltos, es necesario que el servidor conozca una dirección a la cual responder y que indique la agrupación desde la que se debe asignar una dirección IP. La agrupación desde la que se debe asignar una IP es importante porque el servidor DHCP se puede utilizar para servir direcciones a un número determinado de subredes y debe haber, así mismo, alguna indicación en cuanto a la agrupación de direcciones desde donde se debe hacer la selección. La dirección de pasarela DHCP (*giaddr*) se utiliza para esto (esta terminología se basa en la definición que establece la RFC 2131). La *giaddr* debe ser una dirección local al 2212, como la red en anillo o el puerto LAN de Ethernet. Además, como *giaddr* es la dirección que el servidor DHCP utilizará para responder, asegúrese de que puede aplicar ping a esta dirección desde el mismo servidor DHCP.

Red de varios servidores DHCP

Puede configurar varios servidores DHCP para obtener redundancia. Cuando se configuran varios servidores, el cliente del proxy DHCP solicita a todos los servidores una dirección y acepta la primera respuesta que recibe. Si alguno de los servidores DHCP están a más de un salto de distancia o están conectados a una subred que no está asociada con las direcciones de esta agrupación, se debe configurar la *giaddr*. Consulte “Varios saltos para acceder al servidor DHCP”.

Aunque puede haber más de un servidor DHCP que ofrezca direcciones, es importante no dejar que la agrupación de direcciones configurada de cada servidor se solape. Así mismo, como sólo hay una *giaddr* a la que el servidor DHCP deba responder y con la que éste deba llevar a cabo una búsqueda, cada agrupación de direcciones debe hallarse en la misma subred que la otra.

Servidor de nombres de dominio dinámico (DDNS)

Un servidor de nombres de dominio (DNS) correlaciona direcciones IP con nombres de sistema principal y habitualmente es estático por naturaleza. El DNS dinámico es una función que, cuando se utiliza con el servidor DDNS DHCP y un servidor DNS, permite que DHCP actualice de manera dinámica el servidor DNS con una dirección IP y una correlación de nombres de sistema principal. Dicha función sólo se puede utilizar junto con el proxy DHCP.

Cuando se habilita un DNS dinámico en el 2212 y se configura un nombre de sistema principal en el perfil de usuario (consulte “PPP Authentication Protocols” en la publicación *Access Integration Services Guía del usuario de software*), ese nombre de sistema principal pasa como opción 81 (DDNS) al servidor DHCP. Si ha configurado el servidor DHCP correctamente para DDNS, el servidor DHCP actualiza el servidor DDNS con la dirección IP que se ha cedido al direccionador y el nombre del sistema principal que el direccionador le ha enviado. Ello permite a los demás usuarios acceder al cliente de marcación de entrada a través del nombre del sistema principal evitando la necesidad de que el cliente conozca la dirección IP seleccionada de manera dinámica.

Configuración de DIALs

Este capítulo describe la configuración de DIALs y sus mandatos operativos. Consta de los apartados siguientes:

Acceso al entorno de configuración global de DIALs

Utilice el procedimiento siguiente para acceder al proceso de configuración global.

1. En el indicador OPCON, entre **talk 6**. (Si desea obtener más información sobre este mandato, consulte *El proceso y los mandatos de OPCON* en la publicación Access Integration Services Guía del usuario de software). Por ejemplo:

   ```
   * talk 6
   Config>
   ```

   Después de entrar el mandato **talk 6**, el mandato CONFIG (`Config>`) aparece en el terminal. Si el indicador no aparece cuando se entra por primera vez la configuración, pulse **Intro** de nuevo.

2. Entre el mandato **feature dials** en el indicador CONFIG para acceder al indicador `DIALs Config>` y al entorno de configuración de parámetros globales de DIALs.

Mandatos de configuración global de DIALs

Tabla 56. Mandatos de configuración global de DIALs

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 xxxii.
Add	Añade un servidor DHCP (protocolo de configuración dinámica de sistemas principales) 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 establecimiento de conexión de salida, MP multichasis, SPAP Banner y DNS dinámico.
Enable	Habilita varios métodos de asignaciones de direcciones IP, protocolos de establecimiento de conexión de salida MP multichasis, SPAP Banner y DNS dinámico.
List	Lista los parámetros globales de DIALs y sus valores.
Set	Establece el tiempo permitido, la dirección de la pasarela dhcp, las direcciones del servidor de nombres de NetBIOS, las direcciones MAC asignadas localmente, las conexiones virtuales (VC) las direcciones del servidor de nombre dinámico, el temporizador de inactividad de la interfaz de marcación de salida y el nombre del servidor de la interfaz 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 xxxiii.

Add

Utilice el mandato **add** para añadir un nuevo servidor proxy DHCP a un lista de servidores o para añadir una agrupación IP de direcciones.

La lista del servidor proxy DHCP contiene las direcciones IP de los servidores DHCP que ceden, por su parte, las direcciones a clientes de marcación de entrada. Se pueden añadir varios servidores para obtener redundancia. El número máximo de servidores es 20.

La 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 dicha dirección durante toda la conexión con el direccionador. Una agrupación consta de uno o más bloques de direcciones IP. El número máximo de bloques es 20. Cada uno de dichos bloques se define mediante una dirección IP base y el número de direcciones del bloque. Las direcciones de cada bloque son ascendentes y contiguas, empezando por la dirección base.

Sintaxis:

add dhcp-server *dirección_ip*

ip-pool *dirección_base núm_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 núm_direcciones*

Añade un bloque de direcciones a la agrupación 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 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 núm_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 núm_direcciones*

Elimina un bloque de direcciones de la agrupación 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 establecimiento de conexión de salida, SPAP Banner 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 Telnet o de marcación de salida IBM DIALs. Puede especificar:

dials Inhabilita todos los clientes de marcación de salida IBM DIALs

telnet Inhabilita todos los clientes Telnet.

Para inhabilitar ambos tipos de clientes, debe entrar el mandato disable dial-out para cada uno de los tipos. Si se inhabilitan ambos tipos de clientes, se inhabilita el establecimiento de conexión de salida en el 2212.

dynamic-dns
Inhabilita el envío de DHCP opción 81 para el nombre de sistema principal del usuario. Consulte “Servidor de nombres de dominio dinámico (DDNS)” en la página 537 si desea obtener más información.

IP-address-assignment *tipo*
Inhabilita varias técnicas de asignación de direcciones IPCP. Se puede especificar una de las siguientes:

- Cliente – Evita la asignación de direcciones IP asignadas por el cliente.
- ID de usuario – Evita la utilización del perfil de usuario autenticado para una dirección IP.
- Interfaz – Evita que el direccionador utilice los valores IPCP para la interfaz.
- Agrupación – Evita que el direccionador utilice la agrupación de direcciones IP para asignar direcciones a clientes.
- Proxy DHCP – Evita que el direccionador ceda una dirección del servidor DHCP.

Consulte “Direcciones IP proporcionadas por el servidor” en la página 534 si desea obtener información adicional sobre las técnicas de asignación.

spap-banner
Inhabilita el envío de un mensaje de cabecera de SPAP a un usuario remoto autenticado con SPAP.

Nota: Si se entra \n se forzará un carácter de nueva línea en el mensaje de cabecera que se visualiza en el cliente.

Enable

Utilice el mandato **enable** para habilitar la asignación de direcciones IP, protocolos de establecimiento de conexión de salida SPAP Banner y DNS dinámico.

Sintaxis:

enable dynamic-dns
ip-address-assignment . . .
spap-banner

dial-out *tipo*
Habilita la utilización de la interfaz de marcación de salida con Telnet o con clientes de marcación de salida IBM DIALs. Ambos tipos de clientes están habilitados por omisión. Puede especificar:

dials Habilita todos los clientes de marcación de salida IBM DIALs

telnet Habilita todos los clientes Telnet.

dynamic-dns

Inhabilita el envío de DHCP opción 81 para el nombre de sistema principal del usuario. Consulte “Servidor de nombres de dominio dinámico (DDNS)” en la página 537 si desea obtener más información.

IP-address-assignment *tipo*

Habilita varias técnicas de asignación de direcciones IPCP. El direccionador probará todos los métodos habilitados en el orden que se lista. Se puede especificar una de las siguientes:

- Cliente – Permite que el cliente especifique la dirección que desea utilizar.
- Id de usuario – El direccionador buscará una dirección IP en el perfil de usuario PPP autenticado. Si la dirección no es cero, será ofrecida al cliente.
- Interfaz – El direccionador buscará en la dirección IP configurada en la interfaz. Si la dirección no es cero, será ofrecida al cliente.
- Agrupación – El direccionador solicitará una dirección de la agrupación de direcciones IP. Si hay una dirección disponible, será ofrecida al cliente.
- Proxy DHCP – El direccionador intentará ceder una dirección del DHCP. Si lo consigue, la dirección se le ofrecerá al cliente.

Consulte “Direcciones IP proporcionadas por el servidor” en la página 534 si desea obtener información adicional sobre las técnicas de asignación.

spap-banner

Habilita el envío de un mensaje de cabecera de SPAP a un usuario remoto autenticado con SPAP. Utilice el mandato **set spap-banner** que se describe en el mandato “Set” en la página 545 para entrar el texto del mensaje de cabecera de SPAP. Consulte “Shiva Password Authentication Protocol (SPAP)” en la publicación *Access Integration Services Guía del usuario de software* si desea obtener más información.

List

Utilice el mandato **list** para visualizar la configuración actual. Los tiempos del estado DHCP y de cesión de cada red se pueden supervisar desde la consola punto a punto. Consulte el mandato **listipcp** en la publicación *Access Integration Services Guía del usuario de software* si desea 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
Welcome to the network...

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 o no habilitadas. Recibiría esta sección de la pantalla y la sección que contiene los valores de establecimiento de conexión de salida de nivel de recuadro como respuesta al mandato **list ip-address-assignment**.

IP address pools

Visualiza las agrupaciones de direcciones IP configuradas. Recibiría esta sección de la pantalla como respuesta al mandato **list ip-pool**.

Configured DHCP servers

Visualiza la lista de direcciones IP configuradas actualmente como servidores DHCP. Esta sección lista también la interfaz que se utiliza para

la pasarela DHCP. Recibiría esta sección de la pantalla como respuesta al mandato **list dhcp-servers**.

Dynamic Name Servers
Visualiza si el DNS dinámico está habilitado. Recibiría una sección de esta pantalla como respuesta al mandato **list dynamic-dns**.

primary domain server (dns)
Esta línea y las siguientes visualizan los servidores de nombres primario y secundario configurados. Recibiría esta sección de la pantalla como respuesta al mandato **list name-servers**.

time allowed
Visualiza el el tiempo máximo (en minutos) para los usuarios de dials. Recibiría esta sección de la pantalla como respuesta al mandato **list time-allowed**.

spap banner
Visualiza el contenido del mensaje de cabecera de spap. Recibiría esta sección de la pantalla como respuesta al mandato **list spap-banner**.

vc connections
Visualiza información sobre las conexiones virtuales configuradas.

multi-chassis mp
Visualiza el discriminador de extremo configurado.

Set

Utilice el mandato **set** para establecer el tiempo permitido, la dirección de pasarela, las direcciones del servidor de nombres de NetBIOS, las direcciones del servidor de nombres dinámico, el temporizador de inactividad del establecimiento de conexión de salida y el nombre del servidor de establecimiento de conexión de salida..

Sintaxis:

set dhcp-gateway-address
dial-out . . .
dns . . .
laa
multi-chassis-mp
nbns . . .
spap-banner . . .
time-allowed
vc-parameters

dhcp-gateway-address ***núm_interfaz dirección_ip***
Establece la dirección IP asociada con la pasarela DHCP. DHCP utiliza la dirección como:

1. Una dirección a la que responde DHCP
2. Una indicación de la agrupación de direcciones desde la que DHCP asigna una dirección IP

Si el servidor DHCP no se halla en una interfaz LAN conectada de manera directa, deberá configurar entonces esta dirección como la dirección de una las interfaces LAN que dispone de conectividad IP con el servidor DHCP. Consulte “Protocolo de configuración dinámica de sistemas principales (DHCP)” en la página 535 y la definición de “giaddr” en la RFC 1541 si desea obtener más información.

dial-out ***parámetro***

Establece el temporizador de inactividad o el nombre del servidor para redes de establecimiento de conexión de salida. El ***Parámetro*** puede ser:

inactivity-timer

Establece el temporizador de inactividad de establecimiento de conexión de salida para redes de establecimiento de conexión de salida. Se define como el tiempo, en minutos, durante el que un usuario puede estar conectado sin tráfico de datos en la conexión. Por ejemplo, si el temporizador de inactividad se establece en 5 minutos y durante un intervalo cualquiera de 5 minutos no se reciben ni transmiten datos, la conexión quedará desactivada y el módem estará disponible. El valor por omisión es 0, que significa que el temporizador de inactividad está inhabilitado y que se mantendrá la conexión de manera indefinida.

servername

Establece el nombre del servidor de establecimiento de conexión de salida. Puede ser cualquier serie de hasta 30 caracteres. Por omisión es “2210_DIALS_SERVER”. Se trata del nombre que los clientes de marcación de salida IBM DIALs ven cuando utilizan la aplicación “Chooser” para descubrir servidores de marcación de salida. Este parámetro no tiene sentido para los clientes de marcación de salida de Telnet.

dns ***tipo dirección_ip***

Configura los servidores de nombres de dominio primario y secundario (DNS). El ***Tipo*** puede ser:

primary

Establece la dirección IP del servidor DNS primario para que el cliente de marcación de entrada lo utilice. Este valor se negocia durante el IPCP para algunos clientes de acceso telefónico (en concreto Windows® 95).

secondary

Establece la dirección IP del servidor DNS secundario para que el cliente de marcación de entrada lo utilice. Este valor se negocia durante el IPCP para algunos clientes de acceso telefónico (en concreto Windows 95).

laa *núm_direcciones_MAC dirección_base_MAC*

Establece el número de direcciones MAC y la dirección base para la tabla de direcciones administradas localmente (LAA). Sólo utilizarán LAA las redes de túnel de capa 2.

núm_direcciones_MAC

Especifica el número de direcciones Mac a añadir a la tabla LAA, empezando por la *Dirección_Base_MAC*.

Valores válidos: de 0 a 256

Valor por omisión: 0

base_direcciones_MAC
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 extremo a utilizar. Todos los enlaces que deben unir el mismo paquete deben disponer del mismo discriminador de extremo.

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 NetBIOS de nombres primario y secundario. El ***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 han completado de manera satisfactoria la autenticación SPAP.

Ejemplo:

```
DIALs config>set spap-banner
SPAP banner  :Disabled

Enter Banner: Welcome to the network...
```

time-allowed
Establece el tiempo permitido para los usuarios de establecimiento de conexión de entrada PPP y los usuarios de establecimiento de conexión de salida.. Este parámetro define el tiempo máximo (en minutos) que un usuario puede estar conectado. El valor por omisión es 0, lo que significa que el usuario se puede conectar durante tiempo ilimitado.

vc-parameters
Utilice este parámetro para establecer los atributos de conexión virtual por omisión. El sistema le solicita el número máximo de conexiones, el tiempo máximo de suspensión y el valor del 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 un número más que el número de conexiones físicas.

Valores válidos: de 0 a 255

Valor por omisión: 50

Maximum suspended time El tiempo máximo, en horas, que una conexión virtual puede estar suspendida antes de que el sistema finalice la conexión. Si se especifica 0 para este parámetro, se permite que una conexión virtual esté suspendida de manera indefinida.

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 que se suspenda.

Valores válidos: de 10 a 1024

Valor por omisión: 30

Acceso al entorno de supervisión global de DIALs

Utilice el siguiente procedimiento para acceder a los mandatos de supervisión de DIALs.

1. Entre **talk 5** en el indicador OPCON. (Si desea obtener detalles sobre este mandato, consulte el capítulo “The OPCON Process and Commands” en la publicación *Access Integration Services Guía del usuario de software*.) Por ejemplo:

   ```
   * talk 5
   +
   ```

   Después de entrar el mandato **talk 5**, el indicador GWCON (+) aparece en el terminal. Si el indicador no aparece cuando se entra por primera vez la configuración, pulse **Intro** de nuevo.

2. Entre el mandato **feature dials** en el indicador + para acceder al indicador `DIALS Console>` y al entorno de supervisión global.

   Ejemplo:

   ```
   + feature dials
   DIALS Console>
   ```

Mandatos de supervisión global de DIALs

Tabla 57. Mandatos de supervisión global DIALs

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 de manera dinámica 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 xxxiii.

Clear

Utilice el mandato **clear** para borrar 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 el mandato **list suspended-vcs**.

List

Utilice el mandato **list** para visualizar todas las conexiones virtuales, las conexiones virtuales activas, las conexiones virtuales suspendidas o los valores de los parámetros 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. Consulte la descripción del parámetro **all-vcs** si desea obtener una descripción de los atributos.

all-vcs Visualiza los atributos de todas las conexiones virtuales activas y suspendidas. Esta pantalla es una combinación de las pantallas de 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 de 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 AAA. El usuario RADIUS o de la lista local que establece la conexión virtual.

Para VC activas:

Interface La interfaz de red que gestiona la conexión virtual.

> **Nota:** No asigne direcciones IP a clientes de acceso telefónico mediante la asignación de interfaces para evitar problemas generados por otros usuarios que utilizan la interfaz que la VC ha suspendido.

Idle Timeout El tiempo de inactividad, en segundos, al cabo del cual el sistema suspenderá la VC. Corresponde al valor del temporizador de inactividad del mandato **set**.

Connected HHH:MM:SS El tiempo total en horas, minutos y segundos que la VC ha estado conectada a una interfaz.

Para VC suspendidas:

Hrs. Max Suspended El número máximo de horas que una VC puede estar en estado de suspensión antes de que el sistema finalice la conexión. Corresponde al valor del tiempo de suspensión máximo del mandato **set**.

Suspended HH:MM:SS El tiempo total en horas, minutos y segundos que la VC ha estado suspendida.

dhcp-servers Visualiza información configurada sobre servidores DHCP y sus direcciones IP.

ip-address-assignment Visualiza los métodos mediante los cuales las direcciones IP se pueden asignar 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. Consulte la descripción del parámetro **all-vcs** si desea obtener una descripción de los atributos.

vc-parameters Visualiza los valores de los parámetros vc que se han establecido mediante el mandato **set vc-parameters**.

Reset

Utilice el mandato **reset** para activar de manera dinámica los cambios de configuración efectuados a la interfaz de DIALs en `talk 6`.

Sintaxis:

reset all

dhcp-parameters

ip-address-assignment

ip-pool

vc-parameters

all Activa de manera dinámica el DHCP, la asignación de direcciones IP y los cambios de configuración de agrupaciones IP.

dhcp-parameters
Activa de manera dinámica la configuración DHCP.

ip-address-assignment
Activa de manera dinámica la configuración de métodos de asignación de direcciones IP.

ip-pool Activa de manera dinámica la configuración de agrupaciones de direcciones IP.

vc-parameters
Actualiza de manera dinámica los cambios de configuración de VC.

Mandatos de configuración de interfaces de marcación de salida

Para acceder al entorno de los parámetros de la interfaz de marcación de salida:

1. Entre **talk 6** en el indicador `*`.
2. Entre **net *n*** en el indicador `Config >`.
3. Entre **encapsulator** en el indicador `Circuit config: n>`.

La Tabla 58 lista los mandatos disponibles desde el indicador `dial-out config>`.

Tabla 58. Mandatos de configuración 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 xxxii.
Set	Define el nombre de puerto asociado con un módem.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiii.

Set

Utilice el mandato **set** para definir el nombre de puerto de un módem.

Sintaxis:

s**et** portname *nombre*

portname

Define el nombre del puerto asociado con un módem. Utilice este nombre para definir ***agrupaciones de módem.*** El nombre puede tener hasta 30 caracteres.

Valor por omisión: ALL_PORTS

Ejemplo: `dial-out config>`**set portname localcalls**

Supervisión de interfaces de marcación de entrada

La supervisión de interfaces de marcación de entrada es la misma que para la supervisión de otros circuitos de marcación PPP. Si desea obtener más detalles, consulte el capítulo “Configuración y supervisión de interfaces del protocolo punto a punto” de la publicación *Access Integration Services Guía del usuario de software*.

Supervisión de interfaces de marcación de salida

La Tabla 59 en la página 553 lista los mandatos disponibles para la supervisión de interfaces de marcación de salida.

Tabla 59. 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 xxxii.
Clear	Restablece las estadísticas de 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 xxxiii.

Clear

Utilice el mandato **clear** para restablecer las estadísticas del 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** visualiza siempre el estado actual de la red de establecimiento de conexión de salida, el tiempo transcurrido desde el cambio de estado y el número de bytes recibidos y transmitidos.

Sintaxis:

l**ist**

Ejemplo de 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 mediante Telnet, no hay presente ningún nombre de usuario porque el servidor no ha llevado a cabo ninguna autenticación.

Ejemplo de 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 de cliente de marcación de salida IBM DIALs 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 servidores DIALs

En este apartado se describe la reconfiguración dinámica (DR) y cómo afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

El servidor de acceso de marcación de entrada a las LAN (DIALs) no da soporte al mandato **delete interface** de CONFIG (Talk 6).

Mandato activate interface de GWCON (Talk 5)

El servidor de acceso de marcación de entrada a las LAN (DIALs) da soporte al mandato **activate interface** de GWCON (Talk 5) sin restricciones.

En la tabla siguientes se resumen los cambios en la configuración del servidor de acceso de marcación de entrada a las LAN (DIALs) que se activan al ejecutar el mandato **activate interface** de GWCON (Talk 5):

Mandatos cuyos cambios se activan al ejecutar el mandato activate interface de GWCON (Talk 5)
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

Mandato reset interface de GWCON (Talk 5)

El servidor de acceso de marcación de entrada a las LAN (DIALs) da soporte al mandato **reset interface** de GWCON (Talk 5) sin restricciones.

En la tabla siguientes se resumen los cambios en la configuración del servidor DIALs que se activan al ejecutar el mandato **reset interface** de GWCON (Talk 5):

Mandatos cuyos cambios se activan al ejecutar el mandato reset interface de GWCON (Talk 5)
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 de restablecimiento de componente de GWCON (Talk 5)

El servidor DIALs da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos del servidor DIALs:

Mandato GWCON, feature dials, reset DHCP-parameters

Descripción: Este mandato restablece los parámetros de DIALs asociados con la función proxy DHCP.

Efecto en la red: Ninguno.

Limitaciones: Ninguna.

En la tabla siguiente se resumen los cambios en la configuración del servidor DIALs que se activan cuando se ejecuta el mandato **GWCON, feature dials, reset dhcp-parameters**:

Mandatos cuyos cambios se activan al ejecutar 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 los cambios realizados a los métodos de asignación de direcciones IP. No cambiará las direcciones asignadas actualmente, sino que especifica cómo se asignarán las direcciones IP de las conexiones futuras. Con este mandato también se activan los cambios en la configuración de DNS dinámico.

Efecto en la red: Ninguno.

Limitaciones: Ninguna.

En la tabla siguiente se resumen los cambios en la configuración del servidor DIALs que se activan cuando se ejecuta el mandato **GWCON, feature dials, reset ip-address-assignment**:

Mandatos cuyos cambios se activan al ejecutar 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 mandado restablece la definición de la agrupación de direcciones IP (direcciones añadidas o eliminadas) sin interrumpir las conexiones a la red. Si una nueva definición de la agrupación de direcciones IP no incluye las direcciones que había antes en la agrupación y que se están utilizando actualmente, las direcciones se seguirán utilizando después del restablecimiento. Cuando la interfaz libere las direcciones, no volverán a la agrupación de direcciones IP y no se volverán a asignar.

Efecto en la red: Ninguno.

Limitaciones: Ninguna.

En la tabla siguiente se resumen los cambios en la configuración del servidor DIALs que se activan cuando se ejecuta el mandato **GWCON, feature dials, reset ip-pools**:

Mandatos cuyos cambios se activan al ejecutar 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 y el tamaño de la tabla de la conexión virtual (VC).

Efecto en la red: Si el tamaño de la tabla se reduce, algunos circuitos virtuales se desconectarán.

Limitaciones: Ninguna.

En la tabla siguiente se resumen los cambios en la configuración del servidor DIALs que se activan cuando se ejecuta el mandato **GWCON, feature dials, reset vc-parameters**:

Mandatos cuyos cambios se activan al ejecutar 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 pueden restablecerse mediante los mandatos de restablecimiento de DIALs.

Efecto en la red: Consulte todos los mandatos reset.

Limitaciones: Ninguna.

En la tabla siguiente se resumen los cambios en la configuración del servidor de acceso de marcación de entrada a las LAN (DIALs) que se activan cuando se ejecuta el mandato **GWCON, feature dials, reset all**:

Mandatos cuyos cambios se activan al ejecutar 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 DIALs da soporte a los siguientes mandatos de CONFIG que cambian inmediatamente el estado operativo del dispositivo. Estos cambios se guardan y se mantienen si el dispositivo se reinicia, si se vuelve a cargar 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

En la tabla siguiente se describen los mandatos de configuración del servidor DIALs que no pueden modificarse dinámicamente. Para activarlos es necesario reiniciar o volver a cargar 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 la interfaz de marcación de salida

En este apartado se describe la reconfiguración dinámica (DR) y cómo afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

La interfaz de marcación de salida da soporte al mandato **delete interface** de CONFIG (Talk 6) sin restricciones.

Mandato activate interface de GWCON (Talk 5)

La interfaz de marcación de salida da soporte al mandato **activate interface** de GWCON (Talk 5) teniendo en cuenta que:

- No se puede activar una interfaz de marcación de salida a menos que la red base ya esté activa.
- No se puede activar una interfaz de marcación de salida a menos que el tipo de la red base sea V.34.

El mandato GWCON (Talk 5) **activate interface** da soporte a todos los mandatos específicos de la interfaz de marcación de salida.

Mandato reset interface de GWCON (Talk 5)

La interfaz de marcación de salida da soporte al mandato **reset interface** de GWCON (Talk 5), tendiendo en cuenta que:

No se puede restablecer una red de marcación de salida si la red base ha cambiado.

El mandato **reset interface** de GWCON (Talk 5) da soporte a todos los mandatos específicos de las interfaces de marcación de salida.

Utilización del servidor DHCP

En este capítulo se describe el modo de utilización del servidor DHCP. Consta de los apartados siguientes:

Introducción a DHCP

El protocolo de configuración dinámica de sistemas principales (DHCP) es un protocolo cliente/servidor basado en el protocolo de arranque (BOOTP). El servidor DHCP proporciona direcciones IP reutilizables controladas centralmente y otro tipo de información TCP/IP para clientes DHCP. Su funcionalidad puede mitigar el límite que se plantea a los gestores de red en cuanto a la distribución de información de configuración a usuarios nuevos y existentes. Esta función cumple con la RFC 2131 pero da soporte a muchas funciones adicionales que no se incluyen en dicho documento. Existe también soporte para clientes BOOTP tal y como se define en la RFC 951.

Con el DHCP, los clientes con soporte pueden enviar mensajes de DESCUBRIMIENTO de difusión para encontrar servidores DHCP en su red y, en consecuencia, se les pueden OFRECER los datos de configuración de éstos de manera dinámica en la red. DHCP utiliza los puertos BOOTP UDP conocidos públicamente (68 para el servidor y 67 para el cliente) a fin de comunicar peticiones y respuestas. Los clientes y servidores DHCP pueden utilizar los agentes BOOTP Relay para ampliar el alcance de su servicio. DHCP ofrece muchas ventajas en redes configuradas de manera estática, incluida la capacidad para dar soporte a redes cambiantes. Sólo se cede a los clientes las direcciones IP, de manera que, cuando ya no la necesitan o se desplazan a otra subred, la dirección puede ser LIBERADA y quedar a disposición de otros clientes para que la utilicen.

Operación DHCP

DHCP permite a los clientes obtener información de configuración de red IP, incluida una dirección IP, de un servidor DHCP central. Los servidores DHCP controlan si las direcciones que proporcionan a clientes se asignan de manera permanente o se ceden durante un periodo específico de tiempo. Cuando un cliente recibe una dirección cedida, debe solicitar de manera periódica que el servidor revalide la dirección y renueve la cesión.

Todos los procesos de asignación de direcciones, cesión y renovación de la cesión son gestionados por el cliente DHCP y los programas del servidor y son transparentes para los usuarios finales. Los clientes utilizan mensajes estructurados a partir de documentos RFC, para aceptar y utilizar las opciones que les sirve el servidor DHCP. Por ejemplo:

1. El cliente difunde un mensaje (que contiene su ID de mensaje) en el que anuncia su presencia y solicita una dirección IP (mensaje DHCPDISCOVER) y

las opciones que le interesan, como por ejemplo la máscara de subred, el servidor de nombres de dominio, el nombre del dominio y la ruta estática.

2. De manera opcional, si los direccionadores de la red están configurados para reenviar mensajes DHCP y BOOTP (mediante BOOTP Relay), el mensaje de difusión se reenvía a los servidores DHCP de las redes conectadas.
3. Cada servidor DHCP que recibe el mensaje DHCPDISCOVER del cliente envía un mensaje de DHCPOFFER al cliente ofreciéndole una dirección IP. El servidor DHCP comprueba la existencia de direcciones IP en la red antes de emitir una oferta. Así mismo, comprueba el archivo de configuración para saber 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, eligiendo la que hace más tiempo que se ha utilizado. Una agrupación de direcciones es un rango de direcciones IP que deben cederse a 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. Una vez se ha efectuado la oferta, el servidor DHCP reserva la dirección ofrecida.
4. El cliente recibe los mensajes de oferta y selecciona el servidor que desea utilizar. Cuando un cliente DHCP recibe una oferta, toma nota de cuántas opciones de las solicitadas se han incluido en la oferta. El cliente DHCP continúa recibiendo ofertas de los servidores DHCP durante un intervalo de 4 segundos después de que se reciba la primera oferta, tomando nota de cuántas opciones de las solicitadas se han incluido en cada oferta. Cuando finaliza este intervalo, el cliente DHCP compara todas las ofertas y selecciona la que satisface sus criterios.
5. El cliente difunde un mensaje para indicar el servidor que ha seleccionado y el uso de las peticiones de la dirección IP ofrecida por dicho servidor (mensaje DHCPREQUEST).
6. Si un servidor recibe un mensaje DHCPREQUEST que indica que el cliente ha aceptado la oferta del servidor, el servidor marca dicha dirección como cedida. Si el servidor recibe un mensaje DHCPREQUEST que indica 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 un acuse de recibo que contiene información de configuraciones adicionales al cliente (mensaje DHCPACK).
7. El cliente determina si la información de configuración es válida. Una vez se ha recibido un mensaje DHCPACK, los clientes DHCP envían una petición de protocolo de resolución de direcciones (ARP) a la dirección IP suministrada para comprobar si ésta ya está en uso. Si recibe una respuesta a la petición ARP, el cliente declina (mensaje DHCPDECLINE) la oferta e inicia el proceso de nuevo. De lo contrario, el cliente acepta la información de configuración.
8. Al aceptar una cesión válida, el cliente entra en un estado de ENLACE con el servidor DHCP y procede a la utilización de la dirección y las opciones IP. Si el cliente DHCP es un cliente de direcciones dinámicas, el cliente DHCP notifica el servidor de nombres de dominio dinámico de su correlación de nombre de sistema principal con dirección IP.

Para los clientes DHCP que solicitan opciones, el servidor DHCP habitualmente proporciona opciones tales como la máscara de subred, el servidor de nombres de

dominio, el nombre de dominio, la ruta estática, el identificador de clase (que identifica a un proveedor concreto) y la clase de usuario.

De todos modos, un cliente DHCP puede solicitar su propio juego exclusivo de opciones. Por ejemplo, es obligatorio que los clientes DHCP de Windows NT 3.5.1 soliciten opciones. El juego de opciones DHCP solicitadas por omisión que IBM proporciona está formado por la máscara de subred, el servidor de nombres de dominio, el nombre de dominio y la ruta estática. Si desea obtener descripciones de las opciones, consulte “Opciones DHCP” en la página 567.

Renovaciones de cesiones

El cliente DHCP hace un seguimiento del tiempo de cesión restante. En un momento especificado anterior a la finalización de la cesión, normalmente cuando ha transcurrido la mitad del tiempo de cesión, el cliente envía al servidor de cesiones una petición de renovación que contiene su dirección IP actual e información de configuración. Si el servidor responde con una oferta de cesión, la cesión del cliente DHCP se renueva.

Si el servidor DHCP rechaza explícitamente la petición, el cliente DHCP puede continuar utilizando la dirección IP hasta que el tiempo de cesión finaliza e iniciar, a partir de entonces, el proceso de petición de direcciones, incluida la difusión de la petición de direcciones. Si no se puede acceder al servidor, el cliente puede continuar utilizando la dirección asignada hasta que la cesión finalice.

Movilidad del cliente

Uno de los beneficios de DHCP es la libertad que proporciona a un sistema principal cliente para moverse de una subred a otra sin tener que estar al corriente previamente de la información de configuración que necesita en la nueva subred. En la medida que las subredes a las que un sistema principal reubica disponen de acceso a un servidor DHCP, un cliente DHCP se configurará correctamente a sí mismo de manera automática para acceder a dichas subredes.

A fin de que los clientes DHCP se vuelvan a configurar para acceder a una nueva subred, se debe volver a arrancar el sistema principal cliente. Cuando un sistema principal se reinicia en una nueva subred, los clientes DHCP intentan renovar la antigua cesión con el servidor DHCP que originalmente asignó la dirección. El servidor rechaza la renovación de la petición ya que la dirección no es válida en la nueva subred. Al no recibir respuesta o instrucciones del servidor DHCP, el cliente inicia el proceso de petición de dirección IP para obtener una nueva dirección IP y acceder a la red.

Modificación de las opciones de servidor

Con el DHCP, se pueden efectuar cambios en el servidor, reinicializar el servidor y distribuir los cambios a todos los clientes adecuados. Un cliente DHCP retiene los valores de opciones DHCP asignados por el servidor DHCP mientras dure la cesión. Si se implementan modificaciones de configuración en el servidor mientras un cliente ya está activo y en funcionamiento, el cliente DHCP no procesa dichas modificaciones hasta que los clientes intentan renovar su cesión o hasta que se reinician.

Nota: Si el servidor no contiene un disco fijo o una tarjeta de almacenamiento flash y se reinicializa (mediante el mandato `t 5` **reset dhcp**), la información

de tiempo de cesión que muestra el direccionador se perderá hasta que los clientes DHCP renueven su cesión.

Número de servidores DHCP

El número de servidores necesario dependerá en gran medida del número de subredes de que disponga, del número de clientes DHCP a los que prevea dar soporte, de si utiliza BOOTP Relay, y del tiempo de cesión que elija. Recuerde que el protocolo DHCP no define actualmente comunicación de servidor a servidor. Por lo tanto, no pueden compartir información, ni uno de los servidores DHCP puede actuar como “servidor de reserva intercambiable en marcha” en el caso de que el otro falle. Los clientes DHCP envían mensajes de difusión. Por diseño, los mensajes de difusión no cruzan subredes. Para que los mensajes del cliente se puedan reenviar fuera de su subred, se deben configurar direccionadores adicionales para reenviar peticiones DHCP mediante el agente de BOOTP Relay. De lo contrario, será necesario configurar un servidor DHCP en cada subred.

Un único servidor DHCP

Si decide utilizar un único servidor DHCP para servir a sistemas principales en un subred, tenga en cuenta los efectos que puede tener el hecho de que dicho servidor falle. Por lo general, la anomalía de un servidor afectará sólo a los clientes DHCP que están intentando unirse a la red. En principio, los clientes DHCP que ya se hallan en la red continuarán funcionando sin verse afectados hasta que finalice la cesión. De todos modos, los clientes que dispongan de un tiempo de cesión bajo pueden perder su acceso de red antes de que el servidor se pueda reiniciar. Para minimizar el impacto del tiempo de inactividad del servidor si sólo dispone de un servidor DHCP para una subred, deberá elegir un tiempo de cesión lo suficientemente largo como para permitir que haya tiempo para reiniciar o responder al servidor DHCP que ha fallado.

Varios servidores DHCP

Para evitar un único punto de anomalía, puede configurar dos o más servidores DHCP para servir a la misma subred. Si un servidor falla, el otro puede continuar sirviendo a la subred. Se debe poder acceder a cada uno de los servidores DHCP mediante conexión directa a la subred o utilizando un agente BOOTP Relay.

Como dos servidores DHCP no pueden servir las mismas direcciones, las agrupaciones de direcciones definidas para una subred deben ser exclusivas entre los servidores. Por lo tanto, cuando se utilizan dos o mas servidores DHCP para servir a una subred en concreto, la lista completa de direcciones de dicha subred debe dividirse entre los servidores. Por ejemplo, puede configurar un servidor con una agrupación de direcciones que contenga un 70% de las direcciones disponibles para la subred y el otro servidor con una agrupación de direcciones que contenga el 30% restante de las direcciones disponibles.

Al utilizar varios servidores DHCP se reduce la probabilidad de sufrir una anomalía de acceso de red relacionada con DHCP pero su utilización no representa garantía alguna ante tal anomalía. Si un servidor DHCP de una subred en concreto falla, es probable que el otro servidor DHCP no pueda atender a todas las peticiones de los nuevos clientes que pueden, por ejemplo, agotar la agrupación limitada de direcciones disponibles del servidor.

De todos modos, puede desviar el servidor que agotará en primer lugar su agrupación de direcciones. Los clientes DHCP tienden a seleccionar el servidor DHCP que ofrece más opciones. Para desviar el servicio hacia el servidor DHCP con el 70% de direcciones disponibles, deberá ofrecer menos opciones DHCP del servidor que posee el 30% de direcciones disponibles para la subred.

Servidores BOOTP

Si ya dispone de clientes y servidores BOOTP en la red, es probable que desee considerar la posibilidad de sustituir los servidores BOOTP por servidores DHCP. Los servidores DHCP pueden servir de manera opcional 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 adoptar las siguientes medidas de precaución:

- Desactivar el soporte BOOTP en el servidor DHCP.
- Asegurarse de que los servidores BOOTP y los servidores DHCP no distribuyen las mismas direcciones.
- Configurar el soporte de BOOTP Relay en los direccionadores para reenviar difusiones BOOTP tanto a los servidores BOOTP como a los servidores DHCP adecuados.

Un servidor DHCP asigna una dirección IP permanente a un cliente BOOTP. En el caso de que las subredes se vuelvan a numerar de modo que un BOOTP asignado no se pueda volver a utilizar, el cliente BOOTP se deberá reiniciar y deberá obtener una nueva dirección IP.

Clientes DHCP especiales

Es probable que disponga de clientes DHCP o de servidores de red que tengan necesidades administrativas individuales o especiales como, por ejemplo:

- Una cesión permanente:

  Puede asignar cesiones permanentes para designar sistemas principales especificando un tiempo de cesión infinito. El servidor DHCP también asignará una cesión permanente a los clientes BOOTP que lo soliciten de manera explícita en la medida en que el soporte para clientes BOOTP esté habilitado. El servidor DHCP también asignará una cesión permanente a sistemas principales DHCP que lo soliciten de manera explícita.

- Una dirección IP específica:

  Puede reservar una dirección específica y parámetros de configuración para un sistema principal cliente DHCP o BOOTP de una subred concreta.

- Parámetros de configuración específicos:

  Puede asignar información de configuración específica a un cliente sin tener en cuenta su subred.

- Estaciones de trabajo definidas manualmente:

  Debe excluir de forma explícita de las subredes DHCP las direcciones de sistemas principales existentes que no utilizan DHCP o BOOTP para configurar su acceso de red IP. Aunque los servidores y clientes DHCP comprueban de manera automática si hay una dirección IP en uso antes de asignarla o utilizarla, éstos no podrán detectar direcciones de sistemas principales definidos manualmente que estén desactivados o que estén temporalmente fuera de red.

En tal caso, se pueden duplicar los problemas con las direcciones en el momento en que un sistema definido manualmente vuelva a acceder a la red, a menos que su dirección IP sea excluida de manera explícita.

Tiempos de cesión

El tiempo de cesión por omisión es de 24 horas. Recuerde que el tiempo de cesión DHCP puede afectar al funcionamiento y al rendimiento de la red:

- Los tiempos de cesión cortos aumentan la cantidad de tráfico de red debido a las peticiones de renovaciones de cesión DHCP. Por ejemplo, si establece un tiempo de cesión de 5 minutos, cada cliente envía una petición de renovación aproximadamente cada 2,5 minutos.
- Los tiempos de cesión que son demasiado largos pueden limitar la capacidad de reutilización de las direcciones IP. Los tiempos de cesión muy largos también retrasan los cambios en la configuración que se producen cuando un cliente reinicia o renueva una cesión.

El tiempo de cesión que elija dependerá en gran media de sus necesidades, entre las que se cuentan:

- El número de sistemas principales a los que se debe dar soporte comparado con el número de direcciones disponibles. Si tiene más sistemas principales que direcciones, es probable que desee seleccionar un tiempo de cesión corto de una o dos horas. Ello le ayudará a garantizar que las direcciones que no se utilicen se devuelvan a la agrupación lo antes posible.
- El tiempo disponible para realizar cambios de red. Los sistemas principales reciben cambios en la información de configuración cuando se reinician o renuevan su cesión. Asegúrese de que una ventana adecuada y oportuna pueda efectuar dichos cambios. Por ejemplo, si normalmente efectúa cambios durante la noche, puede asignar un tiempo de cesión de 12 horas.
- El número de servidores DHCP que están disponibles. Si dispone sólo de unos pocos servidores DHCP para una red grande, es probable que desee seleccionar un tiempo de cesión más largo para minimizar el impacto del tiempo de inactividad del servidor.

Se pueden definir clases DHCP para redes complejas que necesitan dar soporte a una combinación de requisitos de cesión de sistemas principales.

Conceptos y terminología

Los siguientes conceptos se utilizan para describir las funciones del servidor DHCP:

Ámbito El término ámbito, cuando se habla de configuración del servidor DHCP, se utilizará para identificar aquello a lo que pertenece un determinado valor de parámetro. La Figura 49 en la página 565 ilustra los siguientes ámbitos:

- Opción global 1
- Opción global 3
- Clase global ClassA

  ClassA ha redefinido la opción 1 pero heredará el valor de la opción 3 del ámbito global.

- Cliente global ClientA

  ClientA 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 la Opción 3 del ámbito global.
  - Define ClassB dentro del ámbito de SubA.

    Redefine el valor de la opción 1 pero heredará el valor de la opción 3 de SubA (que también heredará del ámbito global).
  - Define ClientB dentro del ámbito SubA.

    ClientB ha redefinido la opción 3 pero heredará el valor de la opción 1 de SubA.

- Opción de proveedor vendorA

  Las opciones de proveedor son una excepción. Las opciones de proveedor son independientes y no se heredan fuera del ámbito de opción de proveedor.

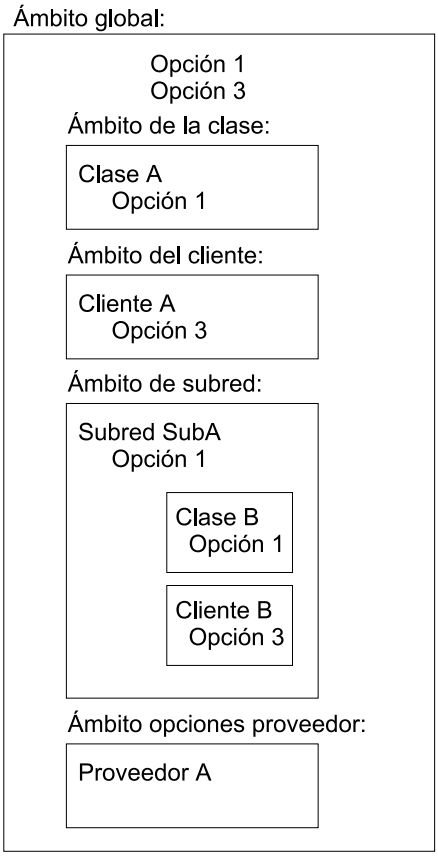


Figura 49. Conceptos de ámbito

Subred Una subred define los parámetros de una agrupación de direcciones administrada por un servidor DHCP. Una agrupación de direcciones es un rango de direcciones IP que deben cederse a clientes. Los parámetros que se pueden especificar son el tiempo de cesión y otras opciones

para clientes que utilicen la agrupación de direcciones. El tiempo de cesión y otras opciones se pueden heredar del ámbito global.

Grupos de subredes

Un grupo de subredes es una manera de identificar varias subredes que se deben agrupar en la misma interfaz. A todas las subredes de un grupo determinado se les concede el mismo nombre de grupo de subredes y una prioridad exclusiva. La prioridad se utiliza para determinar el orden en que se distribuyen las direcciones según la política de direcciones a la que está asociado el grupo. Una subred puede pertenecer a una o dos políticas de direcciones:

- Inorder

  Esta política es el valor por omisión. La política en servicio administra las direcciones empezando con la subred que tiene la prioridad más baja y acabando con la subred que tiene la prioridad más alta.

- Balance

  La política de equilibrio administra las direcciones del grupo de subredes definidas siguiendo un orden rotatorio. La primera dirección es administrada desde la subred con la prioridad más baja. La segunda dirección es administrada desde la subred con la siguiente prioridad más baja y así sucesivamente. Cuando se ha administrado una dirección de la subred de mayor prioridad, la política vuelve a la subred con menor prioridad hasta que todas las direcciones de todas las subredes del grupo se han agotado.

Clases Una clase define los parámetros de un grupo de clientes definido por el usuario y que es administrado por el servidor DHCP. Las clases se pueden definir bajo el ámbito global o de una subred. Cuando una clase se define dentro del ámbito de una subred, el servidor DHCP sólo servirá a clientes de la clase que estén ubicados en la subred especificada y a la vez soliciten la clase. Sólo las clases que se definen dentro de un ámbito de subred pueden especificar un rango de direcciones. El rango puede ser una subred del rango de subredes o puede ser equivalente al rango de subredes. A un cliente que 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. Al cliente se le ofrecen las opciones asociadas con la clase agotada.

Clientes Un cliente se puede utilizar para:

- Definir una dirección IP y opciones 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, un id de cliente y una dirección IP específicos. Los tipos de hardware se definen en la RFC 1340 y se muestran a continuación. Para todos los tipos de hardware excepto 0, el ID de cliente es la dirección de hardware de la estación final (o la dirección MAC). Para el tipo de hardware 0, el id de cliente es una serie de caracteres. Habitualmente se trata de un nombre de dominio.

Cuando se define un cliente, se le solicita una dirección IP *any* o *none*. Si define una dirección IP, dicha dirección IP se reserva para ese cliente. Si elige *any*, a ese cliente se le concederá cualquier dirección IP disponible dentro de esa subred. Si dispone de bastantes registros de subred definidos dentro de la misma subred, cada uno de los cuales con un rango exclusivo, un cliente que esté configurado con *any* obtendrá la primera dirección disponible dentro de la subred, no necesariamente del rango del registro de subred específico bajo el que está definido el cliente. Si elige *none*, a esa estación final no se le servirá dirección IP alguna. Para excluir la posibilidad de administrar una dirección IP, debería definir un registro de cliente con un tipo de hardware e id de cliente 0.

Los tipos de hardware definidos por la RFC 1340 y que pertenecen al IBM 2212 son:

```
Hardware Type                           Value
-------------                           -----
Reserved                                0
Ethernet                                1
IEEE 802 Networks (including Token Ring)    6
```

Si desea obtener una lista completa, consulte la RFC 1340.

Parámetros de servidor DHCP y de cesión

Los siguientes parámetros de servidor DHCP se pueden definir a nivel global:

- bootstrapserver
- canonical
- lease expire interval
- lease time default
- ping time
- support unlisted clients
- support bootp
- used ip address expire interval

Consulte “Set” en la página 615 si desea obtener una descripción de dichos parámetros.

Opciones DHCP

DHCP permite especificar opciones para proporcionar información de configuración adicional a un cliente. Las opciones se definen en la RFC 2132 y en otras RFC.

Formatos de opción

Todas las opciones esperan que los datos de configuración estén en uno de los siguientes formatos:

Formato	Definición
Dirección IP	Una única dirección IP en notación decimal de puntos.

Direcciones IP	Una o más direcciones IP en notación decimal de puntos, separadas por espacios en blanco.
Par de direcciones IP	Dos direcciones IP en notación decimal de puntos, separadas por espacios en blanco.
Pares de direcciones IP	Un o varios pares de direcciones IP, cada uno de ellos separado del otro por un espacio en blanco.
Booleano	0 ó 1 (verdadero o falso).
Byte	Un número decimal entre -128 y 127 (ambos incluidos).
Byte sin signo	Un número decimal entre 0 y 255 (ambos incluidos). No se puede especificar un valor negativo para un byte sin signo.
Lista de bytes sin signo	Uno o más números decimales entre 0 y 255 (ambos incluidos) separados por espacios en blanco. No se puede especificar un número negativo para un byte sin signo.
Entero corto	Un número decimal entre -32768 y 32767 (ambos incluidos).
Entero corto sin signo	Un número decimal entre 0 y 65535 (ambos incluidos). No se puede especificar un número negativo para un entero corto sin signo.
Lista de enteros cortos sin signo	Uno o más números decimales entre 0 y 65535 (ambos incluidos) separados por espacios en blanco. No se puede especificar un número negativo para un entero corto sin signo.
Entero largo	Un número decimal entre -2147483648 y 2147483647 (ambos incluidos).
Entero largo sin signo	Un número decimal entre 0 y 4294967295 (ambos incluidos). No se puede especificar un número negativo para un entero largo sin signo.
Serie de caracteres	Una serie de caracteres.
N/A	Indica que no es necesaria especificación alguna porque el cliente genera esta información.

Cada opción DHCP se identifica mediante un código numérico.

Las opciones estructuradas que van de la 0 a la 127 y la opción 255 están reservadas para definiciones en documentos RFC. El servidor DHCP, el cliente DHCP o ambos utilizan las opciones de ese conjunto. El administrador puede modificar algunas opciones estructuradas. Otras opciones son para uso exclusivo del cliente y del servidor.

Nota: No se permiten valores hexadecimales para las opciones estructuradas que tienen formatos conocidos.

Las opciones que el administrador no puede o no debe configurar en el servidor DHCP son:

52 Carga de opciones

53 Tipo de mensaje DHCP

54 Identificador de servidor

55 Lista de peticiones de parámetros

56 Mensaje

57 Tamaño máximo de mensaje DHCP

60 Identificador de clase

Las opciones de la 128 a la 254 son opciones definidas por el usuario que los administradores pueden definir para pasar información al cliente DHCP a fin de implementar parámetros de configuración específicos del sitio.

Además, IBM proporciona un conjunto de opciones específicas de IBM como la opción 192: TXT RR

El formato de una opción definida por el usuario es:

Sintaxis:

opción *código valor*

donde,

código Todos los códigos de opción que van del 1 al 254, excepto los códigos que ya están definidos en documentos RFC.

valor Debe ser siempre una serie de caracteres. En el servidor puede ser una serie de caracteres ASCII o una serie hexadecimal. En el cliente, sin embargo, aparece siempre como una serie hexadecimal cuando pasa al programa de proceso.

El servidor pasa el valor especificado al cliente. De todos modos, se debe crear un archivo de programa o 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 567 si desea obtener una descripción del formato de configuración.

1 **Máscara de subred** Esta opción se especifica sólo en el servidor DHCP. La máscara de subred del cliente se especifica en notación decimal de puntos de 32 bits. Aunque no es obligatorio, en la mayoría de configuraciones el servidor DHCP debe enviar la opción 1, la máscara de subred, a los clientes DHCP. El funcionamiento del cliente puede ser imprevisible si el cliente no recibe ninguna máscara de subred del servidor DHCP y presupone que existe una máscara de subred que no es la adecuada 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 **Diferencia horaria** Esta opción se especifica sólo en el servidor DHCP. La diferencia (en segundos) de la subred del cliente con la hora universal coordinada (CUT, Coordinated Universal Time). La diferencia es un entero de 32 bits con signo.

Formato de la opción: entero largo

3 **Direccionador** Esta opción sólo se especifica en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los direccionadores de la subred del cliente.

Formato de la opción: direcciones IP

4 **Servidor horario** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores horarios disponibles para el cliente.

Formato de la opción: direcciones IP

5 **Servidor de nombres** Esta opción se especifica sólo en el servidor DHCP. 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 se especifica sólo en el servidor DHCP. 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 dirección de interfaz IP no numerada (por ejemplo, 0.0.0.2)

Nota: Si se ha habilitado una dirección dinámica en la configuración de IP de una interfaz PPP, podrá recuperar una dirección DNS primaria y una secundaria mediante el IPCP de un proveedor de servicios de Internet (ISP). Para pasar estas direcciones DNS a los clientes DHCP, se debe configurar la opción 6 con una dirección de interfaz IP no numerada (como 0.0.0.n) que corresponda a la interfaz de dirección dinámica. El servidor DHCP la convertirá al valor recuperado del ISP cuando el cliente envíe una petición. Si se habilita la opción simple-internet-access en la configuración de IP, automáticamente se configurará la opción 6 con la interfaz IP no numerada. A los clientes que soliciten esta información de configuración del servidor antes de activar la interfaz PPP, se les ofrecerá un tiempo de cesión más corto (3 minutos) para dar tiempo a que la conexión PPP y el IPCP terminen. Después de obtener las direcciones DNS, se ofrecerán los tiempos de cesión configurados.

7 **Servidor de anotaciones** Esta opción se especifica sólo en el servidor DHCP. 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 de cookies** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de la Cookie o los servidores "cita del día" disponibles para el cliente.

Formato de la opción: direcciones IP

9 **Servidor LPR** Esta opción se puede especificar tanto en el cliente DHCP como en el servidor DHCP. No obstante, si se especifica sólo en el cliente DHCP, la configuración será incompleta. Las direcciones IP (en orden de preferencia) de los servidores de impresoras de línea 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 se especifica sólo en el servidor DHCP. 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 recursos** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores Resource Location (RLP) disponibles para el cliente. Los servidores RLP permiten que los clientes ubiquen los recursos que proporcionan un servicio determinado, como puede ser un servidor de nombres de dominio.

Formato de la opción: direcciones IP

12 **Nombre del sistema principal** Esta opción se puede especificar tanto en el cliente DHCP como en el servidor DHCP. Si el cliente DHCP no proporciona un nombre de sistema principal, el servidor DHCP ignora la opción 12. El nombre del sistema principal del cliente (que puede incluir el nombre de dominio local). La longitud mínima del nombre del sistema principal es 1 octeto y la máxima es 32 caracteres. Consulte la RFC 1035 si desea conocer las restricciones de juegos de caracteres.

Formato de la opción: serie de caracteres

13 **Tamaño del archivo de arranque** Esta opción se especifica sólo en el servidor DHCP. El tamaño (en bloques de 512 octetos) del archivo de configuración de arranque del cliente.

Formato de la opción: entero corto sin signo.

14 **Archivo de vuelco de mérito** Esta opción se especifica sólo en el servidor DHCP. El nombre de la vía de acceso del archivo de vuelco de mérito en el que la imagen de memoria del cliente se almacena si el cliente cae. La vía de acceso tiene el formato de una serie de caracteres del juego de caracteres de terminal virtual de redes (NVT) ASCII. La longitud mínima es 1 octeto.

Formato de la opción: serie de caracteres

15 **Nombre de dominio** Esta opción se especifica tanto en el cliente DHCP como en el servidor DHCP. Si no se especifica ningún valor en el servidor DHCP en la opción 15, se solicita al cliente que proporcione un valor para la opción 12, nombre del sistema principal, y para 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 de caracteres

16 **Servidor de intercambio** Esta opción se especifica sólo en el servidor DHCP. La dirección IP del servidor de intercambio del cliente.

Formato de la opción: dirección IP

17 **Vía de acceso raíz** Esta opción se especifica sólo en el servidor DHCP. La vía de acceso que contiene el disco raíz del cliente. La vía de acceso tiene el formato de una serie de caracteres del juego de caracteres NVT ASCII. La longitud mínima es 1 octeto.

Formato de la opción: serie de caracteres

18 **Vía de acceso de extensión** Esta opción se especifica sólo en el servidor DHCP. La opción de vía de acceso de extensión especifica una serie de caracteres que se puede utilizar para identificar un archivo que se puede recuperar mediante el protocolo de transferencia de archivos trivial (TFTP). La longitud mínima es 1 octeto.

Formato de la opción: serie de caracteres

Parámetros de capa IP por opciones de sistema principal

19 **Reenvío IP** Esta opción se especifica sólo en el servidor DHCP. Habilita (1) o inhabilita (0) el reenvío por parte del cliente de sus paquetes de capa IP.

Formato de la opción: booleano

20 **Direccionamiento de orígenes no locales** Esta opción se especifica sólo en el servidor DHCP. Habilite (1) o inhabilite (0) el reenvío por parte del cliente de sus datagramas de capa IP con rutas de orígenes no locales.

Formato de la opción: booleano

21 **Filtro de política** Esta opción se especifica sólo en el servidor DHCP. El par de máscaras de dirección IP-red que se utiliza para filtrar datagramas con rutas de orígenes no locales. Cualquier datagrama cuya siguiente dirección de salto no coincide con uno de los pares de filtros es descartado por el cliente. La longitud mínima de la opción de filtro de política es 8 octetos.

Formato de la opción: pares de direcciones IP

22 **Tamaño máximo de reensamblaje de datagramas** Esta opción se especifica sólo en el servidor DHCP. El datagrama de tamaño máximo que el cliente reensamblará. El valor mínimo es 576.

Formato de la opción: entero corto sin signo.

23 **Tiempo de vida IP por omisión** Esta opción se especifica sólo en el servidor DHCP. El tiempo de vida (TTL) por omisión que el cliente utiliza en los datagramas salientes. TTL es un octeto con un valor entre 1 y 255.

Formato de la opción: byte sin signo

24 **Tiempo de espera de antigüedad de Path MTU** Esta opción se especifica en el servidor DHCP. El tiempo de espera en segundos para establecer la antigüedad de los valores de la unidad de transmisión máxima (MTU) de vía de acceso descubiertos por el mecanismo que se describe en la RFC 1191.

Formato de la opción: entero largo sin signo

25 **Tabla plana de Path MTU** Esta opción se especifica sólo en el servidor DHCP. La tabla de tamaños de MTU a reclamar en el descubrimiento de Path MTU tal como se define en la RFC 1191. El valor mínimo de MTU es 68. La longitud mínima de la opción de tabla plana de Path MTU es 2 octetos. La longitud debe ser un múltiplo de 2.

Formato de la opción: entero corto sin signo.

Parámetros de capa IP por opciones de interfaz

26 **MTU de interfaz** Esta opción se especifica sólo en el servidor DHCP. La unidad de transmisión máxima (MTU) a presentar en esta interfaz. El valor mínimo de MTU es 68.

Formato de la opción: entero corto sin signo.

27 **Todas las subredes son locales** Esta opción se especifica sólo en el servidor DHCP. El cliente presupone (1) o no presupone (0) que todas las subredes utilizan la misma unidad de transmisión máxima (MTU). Un valor de 0 significa que el cliente presupone que algunas subredes tienen MTU más pequeñas.

Formato de la opción: booleano

28 **Dirección de difusión** Esta opción se especifica sólo en el servidor DHCP. La dirección de difusión que se utiliza en la subred del cliente.

Formato de la opción: dirección IP

29 **Realizar descubrimiento de máscara** Esta opción se especifica sólo en el servidor DHCP. El cliente realiza (1) o no realiza (0) el descubrimiento de la máscara de subred mediante el protocolo de mensajes de control de Internet (ICMP).

Formato de la opción: booleano

30 **Proveedor de máscaras** Esta opción se especifica sólo en el servidor DHCP. El cliente responde (1) o no responde (0) a las peticiones de máscara de subred mediante el protocolo de mensajes de control de Internet (ICMP).

Formato de la opción: booleano

31 **Realizar descubrimiento de direccionadores** Esta opción se especifica sólo en el servidor DHCP. El cliente solicita (1) o no solicita (0) direccionadores mediante el descubrimiento de éstos tal y como se define en la RFC 1256.

Formato de la opción: booleano

32 **Dirección de solicitación de direccionadores** Esta opción se especifica sólo en el servidor DHCP. La dirección a la que un cliente transmite las peticiones de solicitación de direccionadores.

Formato de la opción: dirección IP

33 **Ruta estática** Esta opción se especifica sólo en el servidor DHCP. Las rutas estáticas (los pares de direcciones-direccionadores de designación en 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 de destino. No especifique 0.0.0.0 como destino de ruta por omisión.

Formato de la opción: pares de direcciones IP

Parámetros de capa de enlace por opciones de interfaz

34 **Encapsulación de cola** Esta opción se especifica sólo en el servidor DHCP. El cliente negocia (1) o no negocia (0) el uso de cola al utilizar el protocolo de resolución de direcciones (ARP). Si desea obtener más información, consulte la RFC 893.

Formato de la opción: booleano

35 **Tiempo de espera de la antememoria ARP** Esta opción se especifica sólo en el servidor DHCP. El tiempo de espera en segundos para las entradas de antememoria del protocolo de resolución de direcciones (ARP).

Formato de la opción: entero largo sin signo

36 **Encapsulado de Ethernet** Esta opción se especifica sólo en el servidor DHCP. Para una interfaz Ethernet, el cliente utiliza la encapsulado de Ethernet IEEE 802.3 (1) descrita en RFC 1042 o la encapsulado de Ethernet V2 (0) descrita en la RFC 894.

Formato de la opción: booleano

Opciones de parámetros TCP

37 **TTL por omisión de TCP** Esta opción se especifica sólo en el servidor DHCP. El tiempo de vida (TTL) por omisión que el cliente utiliza para enviar segmentos de TCP.

Formato de la opción: byte sin signo

38 **Intervalo de mantenimiento de la actividad de TCP** Esta opción se especifica sólo en el servidor DHCP. Intervalo en segundos que el cliente espera antes de enviar un mensaje de mantenimiento de la actividad en una conexión de TCP. Un valor 0 indica que el cliente no envía mensajes de mantenimiento de la actividad a menos que la aplicación lo solicite.

Formato de la opción: entero largo sin signo

39 **Basura de mantenimiento de la actividad de TCP** Esta opción se especifica sólo en el servidor DHCP. El cliente envía (1) o no envía (0) mensajes de mantenimiento de la actividad de TCP que contienen un octeto desechable para alcanzar la compatibilidad con implementaciones anteriores.

Formato de la opción: booleano

Opciones de parámetros de aplicaciones y servicios

40 **Dominio del servicio de información de red** Esta opción se especifica sólo en el servidor DHCP. El dominio del servicio de información de red (NIS) del cliente. El dominio tiene el formato de una serie de caracteres del juego de caracteres NVT ASCII. La longitud mínima es 1 octeto.

Formato de la opción: serie de caracteres

41 **Dominio del servicio de información de red** Esta opción se especifica sólo en el servidor DHCP. 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 protocolo horario de red** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden of preferencia) de los servidores de protocolo horario de red (NTP) disponibles para el cliente.

Formato de la opción: direcciones IP

43 **Información específica del proveedor** La opción 43 se especifica sólo en el servidor DHCP, que la devuelve a un cliente que envía la opción 60, Identificador de clase. Esta opción de información es utilizada por clientes y servidores para intercambiar información específica de proveedores, que se especifica en la definición de opción de proveedores. Los siguientes aspectos se deben tener en cuenta al utilizar la opción 43 para encapsular información de proveedores:

- Para permitir la interoperabilidad entre clientes y servidores de diferentes proveedores, cada proveedor debe documentar de forma clara el contenido de su respectiva opción 43 utilizando el formato estándar descrito en la RFC 2132.
- Cada proveedor debe especificar las opciones concretas que se pueden encapsular dentro de la opción 43 de forma que los servidores DHCP de otro proveedor puedan implementarlas fácilmente. Por ejemplo, el proveedor deberá:
  - Representar dichas opciones en tipos de datos ya definidos para las opciones DHCP o en otros tipos de datos definidos públicamente.
  - Elegir opciones que se puedan codificar rápidamente en archivos de configuración para su intercambio con servidores suministrados por otros proveedores.
  - Poder recibir rápidamente el soporte de todos los servidores.

Los servidores que no pueden interpretar la información específica del proveedor enviada por un cliente deben ignorarla. Los clientes que no reciban las información específica del proveedor deseada deben intentar operar sin ella. Consulte las RFC 2131 y 2132 si desea obtener información adicional sobre esta opción.

Nota: Debido a las consideraciones anteriores, IBM utiliza, en cambio, las opciones 192 y 200 como sus opciones específicas.

Formato de la opción: serie de caracteres

44 **NetBIOS en el servidor de nombres TCP/IP** Esta opción se especifica sólo en el servidor DHCP. 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 en el servidor de distribución de datagramas TCP/IP** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores de nombres de distribución de datagramas del NetBIOS (NBDD) disponibles para el cliente.

Formato de la opción: direcciones IP

46 **NetBIOS en el tipo de nodo TCP/IP** Esta opción se especifica sólo en el servidor DHCP. El tipo de nodo utilizado para el NetBIOS en los clientes configurables TCP/IP tal y como se describe en las RFC 1001 y 1002. Los valores para especificar los tipos de clientes son:

- 0x1 nodo B
- 0x2 nodo P
- 0x4 nodo M
- 0x8 nodo H

Formato de la opción: byte sin signo

47 **NetBIOS en ámbito TCP/IP** Esta opción se especifica sólo en el servidor DHCP. El parámetro de NetBIOS en ámbito TCP/IP, tal y como se especifica en las RFC 1001 y 1002. La longitud mínima es 1 octeto.

Formato de la opción: byte sin signo

48 **Servidor de fonts del sistema X Windows** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden of preferencia) de los servidores de fonts del sistema X Windows disponibles para el cliente.

Formato de la opción: direcciones IP

49 **Gestor de visualización del sistema X Windows** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los sistemas que ejecutan el Gestor de visualización del sistema X Windows disponible para el cliente.

Formato de la opción: direcciones IP

Opciones de extensiones DHCP

50 **Dirección IP solicitada** Esta opción se especifica sólo en el cliente DHCP. El servidor DHCP puede rechazar la petición de una dirección IP específica por parte de un cliente DHCP. Esta opción permite al cliente solicitar una dirección IP concreta (DHCPDISCOVER).

Formato de la opción: D/N

51 **Tiempo de cesión de direcciones 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 el valor defaultLeaseInterval que el servicio DHCP ofrece. Permite al cliente solicitar (DHCPDISCOVER o DHCPREQUEST) un tiempo de cesión para una dirección IP. En una respuesta (DHCPOFFER), un servidor DHCP utiliza la opción para ofrecer un tiempo de cesión. Esta opción se puede especificar dentro del ámbito global, de subred, de clase o de cliente. Utilice X'ffffffff' para indicar una cesión infinita (permanente).

Formato de la opción: entero largo sin signo

58 **Valor de tiempo de renovación (T1)** Esta opción se especifica sólo en el servidor DHCP. El intervalo en segundos que transcurre entre el momento en que el servidor asigna una dirección y el momento en que el cliente pasa a estado de renovación.

Formato de la opción: entero largo sin signo

59 **Valor de tiempo de reenlace (T2)** Esta opción se especifica sólo en el servidor DHCP. El intervalo en segundos que transcurre entre el momento en que el servidor asigna una dirección y el momento en que el cliente entra en estado de reenlace.

Formato de la opción: entero largo sin signo

60 **Identificador de clase** Esta opción se especifica sólo en el cliente DHCP. El cliente genera esta información y no es necesario que se especifique. El tipo y la configuración del cliente, suministrados por éste al servidor. Por ejemplo, el identificador puede codificar la configuración de hardware específica de proveedor del cliente. Dicha información es una serie de *n* octetos, que los servidores interpretan. Por ejemplo: hex: X'01' X'02' X'03'. Los servidores no equipados para interpretar la información específica de clase enviada por un cliente deben ignorarla. La longitud mínima es 1 octeto.

Formato de la opción: D/N

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 exclusivo de cliente. El servidor DHCP puede utilizar la opción 61 para indexar la base de datos de enlaces de direcciones. Se espera que dicho valor sea exclusivo para todos los clientes de un dominio administrativo.

Formato de la opción: serie de caracteres

62 **Nombre de dominio NetWare/IP** Esta opción se especifica sólo en el servidor DHCP. El nombre del dominio Netware/IP. La longitud mínima es 1 octeto y la máxima 255

Formato de la opción: serie de caracteres

63 **NetWare/IP** Esta opción se especifica sólo en el servidor DHCP. Un código de opción con fines generales utilizado para transportar toda la información relacionada con NetWare/IP excepto el nombre del dominio NetWare/IP. Se transportará un cierto número de subopciones NetWare/IP mediante el código de opción. La longitud mínima es 1 y la máxima es 255.

Formato de la opción: serie de caracteres

64 **Nombre de dominio NIS** Esta opción se especifica sólo en el servidor DHCP. El nombre de dominio del cliente del servicio de información de red (NIS)+ V3. El dominio tiene el formato de una serie de caracteres del juego de caracteres NVT ASCII. La longitud mínima es 1.

Formato de la opción: serie de caracteres

65 **Servidores NIS** Esta opción se especifica sólo en el servidor DHCP. 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 del servidor** Esta opción se especifica sólo en el servidor DHCP. El nombre del servidor Trivial File Transfer Protocol (TFTP) utilizado cuando el campo “sname” de la cabecera DHCP se ha utilizado para opciones DHCP.

Formato de la opción: serie de caracteres

67 **Nombre del archivo de arranque** Esta opción se especifica sólo en el servidor DHCP. El nombre del archivo de arranque cuando el campo de archivo de la cabecera DHCP se ha utilizado para opciones DHCP. La longitud mínima es 1.

Nota: Utilice esta opción para pasar un nombre de archivo de arranque a un cliente DHCP. Es obligatorio que el nombre del archivo de arranque contenga el nombre de la vía de acceso totalmente calificada y que tenga menos de 128 caracteres. Por ejemplo: opción 67 c:\vía_acceso\nombre_archivo_arranque. Este archivo contiene información que se puede interpretar del mismo modo que el campo de extensión de proveedor de 64 octetos dentro de la respuesta BOOTP, con la excepción de que la longitud del archivo queda limitada por la cabecera BootP a 128 caracteres.

Formato de la opción: serie de caracteres

68 **Dirección de inicio** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los agentes de inicio IP móviles disponibles para el cliente. Esta opción habilita un sistema principal móvil para derivar las direcciones de inicio móviles y determina la máscara de subred de la red de inicio. La longitud habitual es cuatro octetos, incluyendo sólo una dirección de inicio del agente de inicio, pero puede ser cero octetos. Una longitud cero indica que no hay disponible ningún agente de inicio.

Formato de la opción: direcciones IP

69 **Servidores SMTP** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores de protocolo de transferencia de correo simple (SMTP) disponibles para el cliente.

Formato de la opción: direcciones IP

70 **Servidor POP3** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores de protocolo de oficina de correos (POP) disponibles para el cliente.

Formato de la opción: direcciones IP

71 **Servidor NNTP** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores de protocolo de transferencia de noticias de red (NNTP) disponibles para el cliente.

Formato de la opción: direcciones IP

72 **Servidor WWW** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores World Wide Web (WWW) disponibles para el cliente.

Formato de la opción: direcciones IP

73 **Servidor Finger** Esta opción se especifica sólo en el servidor DHCP. Las 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 se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores Internet Relay Chat (IRC) disponibles para el cliente.

Formato de la opción: direcciones IP

75 **Servidor StreetTalk** Esta opción se especifica sólo en el servidor DHCP. Las 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 se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores de asistencia de directorios StreetTalk (STDA) disponibles para el cliente.

Formato de la opción: direcciones IP

77 **Clase de usuario** Esta opción se especifica sólo en el cliente DHCP. Los clientes DHCP utilizan la opción 77 para indicar a los servidores DHCP la clase de la que es miembro el sistema principal. Se puede entrar manualmente la clase de usuario en el archivo \DHCPCD.CFG como valor para la opción 77 a fin de recibir los parámetros definidos para dicha clase en un servidor DHCP. EL archivo DHCPCD.CFG está ubicado en el directorio ONDEMAND\SERVER\ETC.

Formato de la opción: serie de caracteres

78 **Agente de directorios** Esta opción se especifica sólo en el servidor DHCP. El protocolo de configuración dinámica de sistemas principales proporciona una infraestructura para pasar información de configuración a sistemas principales en una red TCP/IP. Es necesario que las entidades que utilizan el protocolo de ubicación de servicios conozcan las direcciones de los agentes de directorios a fin de tramitar mensajes. En algunas otras instancias, es probable que sea necesario que descubran el ámbito correcto y la autoridad de nombres que se deben utilizar junto con los atributos de servicio y URL que se intercambian mediante el protocolo de ubicación de servicios. Los agentes de directorios disponen de un ámbito particular y es probable que estén al corriente de los esquemas definidos por una autoridad de nombres concreta.

Formato de la opción: dirección IP

79 **Ámbito del servicio** Esta opción se especifica sólo en el servidor DHCP. Esta extensión indica un ámbito que un agente de servicio debe utilizar al responder a mensajes de petición de servicio tal y como especifica el protocolo de ubicación de servicios.

Formato de la opción: serie de caracteres

80 **Autoridad de nombres** Esta opción se especifica sólo en el servidor DHCP. Esta extensión indica una autoridad de nombres que especifica la sintaxis de los esquemas que se pueden utilizar en URL para que las entidades los utilicen, a su vez, con el protocolo de ubicación de servicios.

Formato de la opción: serie de caracteres

Opciones específicas de IBM

IBM proporciona un conjunto de opciones propias definiendo las opciones del rango definido por el usuario (128-254). Tales opciones se utilizan sin que haya la necesidad de definir una opción de proveedor (opción 43) para IBM. Se recomienda que las vuelva a definir.

192 **TXT RR** Si se ha especificado esta opción en el servidor DHCP, es necesario que el usuario del cliente DHCP rellene los campos de información del administrador del sistema. Nota: esta opción sólo le dan soporte los clientes TCP/IP Versión 4.1 para OS/2. Proporciona, además, hasta cuatro etiquetas de texto o campos de entrada obligatorios que el administrador del sistema puede especificar, entre los que se encuentran, por ejemplo, el nombre de un usuario, su número de teléfono u otros campos que el programa de configuración del cliente DDNS solicita a éste. Dichos campos permiten que el administrador del sistema identifique la persona real que ha configurado el nombre del sistema principal u otros datos. El programa de configuración de DDNS no visualiza estos campos a menos que el administrador del sistema los especifique. Esta información se almacena en un registro de texto del DNS. Los pares de etiquetas de campos y datos son necesarios para ajustarse a un solo registro de recursos TXT. El espacio disponible se divide a partes iguales entre los pares. El valor se actualiza también en el archivo DDNSCLI.CFG del cliente de direcciones dinámicas.

Formato de la opción: serie de caracteres

Opciones de proveedor

El protocolo DHCP facilita un método para suministrar información específica del proveedor a un cliente DHCP mediante las opciones 43 y 60 estructuradas a partir de documentos RFC.

60 La **Opción 60** se configura en un cliente DHCP y se envía al servidor DHCP para identificar al primero como proveedor específico.

43 La **Opción 43** se configura en el servidor DHCP para definir la información específica de proveedor que debe volver al cliente en respuesta a la solicitud efectuada por el cliente mediante la opción 60. En lo que se refiere al servidor de código común DHCP, la opción se configura mediante el mandato add vendor-option. Las opciones de proveedor se definen únicamente dentro del ámbito global. La opción de proveedor consiste en el nombre del proveedor y los datos de opción. Los datos de opción tienen dos formatos:

Datos hexadecimales
Se entran con el nombre del proveedor cuando se ejecuta el mandato add vendor-option. Los datos hexadecimales se deben entrar como una serie hexadecimal con espacios en blanco entre los bytes: “01 AA 55”

Opciones
Se puede añadir cualquier opción DHCP a un ámbito de opción de proveedor mediante el mandato add option.

Nota: Los datos hexadecimales y las opciones se excluyen mutuamente en una definición de proveedor. Puede definir los unos o las otras pero no ambos.

Configuración de IP para DHCP

A fin de que el servidor DHCP asigne de manera satisfactoria direcciones IP e información de configuración para los clientes de una subred añadida, es necesario que el IP esté configurado de manera adecuada. Esto es necesario cuando el servidor DHCP está conectado directamente a una subred que se ha configurado a la que debe dar soporte.

Si se está utilizando un agente de BOOTP Relay para reenviar mensajes de peticiones DHCP a este servidor DHCP, es probable que no exista una configuración de IP necesaria para dar soporte a una subred que no está conectada directamente al servidor.

Adición de una dirección IP

Es necesario que una dirección IP que se sitúe dentro de la subred configurada DHCP se añada a la interfaz de conexión.

Ejemplo:

- DHCP ha añadido una subred de la forma 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 del acceso simple a Internet del IP

Si el acceso simple a Internet se ha habilitado en IP y no se ha configurado previamente DHCP, se generará de manera automática en el servidor DHCP la siguiente configuración. El acceso simple a Internet también configurará de manera automática la función NAT y otros filtros y controles de acceso IP. Si DHCP ya está configurado, no se producirán cambios/adiciones en la configuración DHCP. Consulte Utilización del acceso simple a Internet en el capítulo “Utilización de IP” de la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 1* si desea obtener más información general y sobre restricciones.

- Se ha configurado IP del siguiente modo:

```
IP config>enable simple-internet-access
Interface to Service Provider [0]? 3
SIMPLE-INTERNET-ACCESS enabled on interface 3

IP config>add address
Which net is this address for [0]? 0
New address []? 192.168.8.1
Address mask [255.255.255.0]?

IP config>list 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
```

- El servidor DHCP generará la siguiente configuración:

```
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 de ejemplo del servidor DHCP

Archivo de texto ASCII

En este apartado se muestra una configuración de servidor DHCP habitual en formato de texto ASCII. Este ejemplo tiene únicamente el fin de ilustrar una configuración en un formato que le puede ser familiar. El IBM 2212 no da soporte a las configuraciones ASCII.

Utilice los números de bloque (**1**) como referencia para las funciones que se describen en este ejemplo de ASCII con la configuración `talk 6` equivalente que se describe en “Configuración de OPCON (Talk 6)” en la página 584.

```
1  Configuration of Server parameters

leaseTimeDefault          120                  # 120 minutes
leaseExpireInterval       20 seconds
supportBOOTP              yes
supportUnlistedClients  yes


2  Global options.  Passed to every client unless overridden at a lower scope.

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  Vendor-options


vendor  XI-clients hex"01 02 03"

vendor XA-clients
{
   option 23 100   # IP TTL
}

4  A typical subnet

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  class manager defined at the subnet scope.  Option 9 here will override
the option 9 specified in the global manager class.
                 class manager

        {
                option 9   9.2.23.98
        }
```

```
6  Programmers have their own subnet range

        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  Example of a client that will accept any address but will have
its own set of options.

client 6        0x10005aa4b9ab  ANY
{
        option 51 999
        option 1 255.255.255.0
}

8  Exclude an address from service.

client 0       0               9.2.23.121
```

Configuración de OPCON (Talk 6)

El siguiente es un ejemplo de la misma configuración utilizando esta vez `talk 6`.

1 Configuration of Server parameters

```
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 Global options. Passed to every client unless overridden at a lower scope.

```
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 Vendor-options

```
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 A typical subnet

```
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 Programmers have their own subnet range

```
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 Example of a client that will accept any address but will have its own set of o

```
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 Exclude an address from service.

```
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 DHCP

En este capítulo se describe como utilizar los mandatos de configuración y de funcionamiento del servidor DHCP y consta de los apartados 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 OPCON, entre **talk 6**. Por ejemplo:

```
* talk 6
Config>
```

   Después de entrar el mandato **talk 6**, el indicador Config (`Config>`) aparece en el terminal. Si el indicador no aparece cuando se entra por primera vez la configuración, pulse **Intro** de nuevo.

2. Entre el mandato **feature dhcp-server** en el indicador Config para acceder al indicador `DHCP Server config>`.

Mandatos de configuración del servidor DHCP

Tabla 60. Resumen de 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 xxxii.
Add	Añade una clase, un cliente, una subred o una opción de proveedor.
Change	Cambia la definición de una clase, un cliente, una subred o una opción de proveedor.
Default	Devuelve algunas variables globales a sus valores por omisión.
Delete	Suprime una clase, un cliente, una subred o una opción de proveedor.
Disable	Inhabilita globalmente el servidor DHCP.
Enable	Habilita globalmente el servidor DHCP.
List	Lista las definiciones de una clase, un cliente, globales, una subred o una opción de proveedor.
Set	Establece definiciones de parámetros u opciones globales 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 xxxiii.

Add

Utilice el mandato **add** para añadir una clase, subred u opción de vendedor.

Sintaxis:

add **d**

class

client

option

subnet

vendor-option

class *ámbito [nombre_subred] nombre_clase [inicio_rango] [fin_rango]*

Define una clase.

ámbito Especifica el ámbito en el que se está añadiendo la clase.

Valores válidos: global o subnet

Valor por omisión: Ninguno

nombre_subred

Sólo es válido si el **ámbito** es *subnet*. Indica el nombre de la subred a la que se está añadiendo 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 de hasta 40 caracteres

Valor por omisión: Ninguno

inicio_rango

Sólo es válido si el **ámbito** es *subnet*. Especifica la dirección IP de inicio de la agrupación de direcciones IP a la que se asignará el cliente.

Valores válidos: Cualquier dirección IP válida dentro del rango de la subred a la que se está añadiendo la clase.

Valores por omisión: La primera dirección IP del rango de subred que pertenece a la subred especificada.

fin_rango

Sólo es válido si el **ámbito** es *subnet*. Especifica la dirección IP final de la agrupación de direcciones IP a la que se asignará el cliente.

Valores válidos: Cualquier dirección IP válida dentro del rango de la subred a la que se está añadiendo la clase. Dicho valor debe ser mayor que el valor especificado para **inicio-rango**.

Valor por omisión: La dirección IP de inicio más 5 de las del rango de subredes que pertenece a la subred especificada. Si la dirección IP resultante no es mayor dentro del rango de subredes, el valor por omisión será la dirección IP final del rango de subredes.

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 que se está añadiendo el cliente.

Valores válidos: global o subnet

Valor por omisión: Ninguno

nombre-subred

Sólo es válido si el **ámbito** es *subnet*. Indica el nombre de la subred a la que se está añadiendo 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. A continuación se muestran los tipos de hardware definidos en la RFC 1340 que son aplicables al IBM 2212.

Valores válidos:

0 No especificado. Indica un nombre simbólico para el cliente.

1 Ethernet

6 Redes IEEE 802 (incluida la 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** debe ser una serie de 64 caracteres. De lo contrario, el **valor-id** es una dirección MAC.

Nota: Un **tipo-id** *0* y un **valor-id** *0* indican que el servidor no debe distribuir la dirección IP especificada.

Valores válidos: 0 o cualquier dirección MAC válida (12 dígitos hexadecimales)

Valor por omisión: Ninguno

dirección Especifica la dirección IP a proporcionar al cliente o una serie de caracteres que indica que el cliente no recibirá servicio o que se puede suministrar al cliente cualquier dirección de la agrupación de direcciones IP.

Valores válidos:

Cualquier dirección IP válida En formato decimal de puntos. Si el cliente se define dentro de un ámbito de subred, la dirección IP debe formar parte de éste.

none Indica que el cliente coincidente no recibirá servicio

any Indica que se puede proporcionar al cliente cualquier dirección IP de la agrupación de subredes.

Valor por omisión: Ninguno

Nota: Un **tipo-id** *0* y un **valor-id** *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 ser globales o encontrarse dentro de un ámbito de subred, clase, cliente u opción de vendedor.

ámbito Especifica el ámbito al que se está añadiendo la opción.

Valores válidos:

- class-global
- class-subnet
- client-global
- client subnet
- global
- subnet
- vendor-option

Valor por omisión: Ninguno

nombre-subred

Sólo es válido si el **ámbito** es *subnet, class-subnet* o *client-subnet*. Indica el nombre de la subred a la que se está añadiendo el cliente.

Valores válidos: Cualquier nombre de subred existente

Valor por omisión: Ninguno

nombre-clase
Sólo es válido si el **ámbito** es *class-global* o *class-subnet*. Indica el nombre de la clase a la que se está añadiendo la opción.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

nombre-cliente
Sólo es válido si el **ámbito** es *client-global* o *client-subnet*. Indica el nombre del cliente al que se está añadiendo la opción.

Valores válidos: Cualquier nombre de cliente existente

Valor por omisión: Ninguno

nombre-proveedor
Sólo es válido si el **ámbito** es *vendor-option*. Indica el nombre del proveedor al que se está añadiendo la opción.

Valores válidos: Cualquier nombre de proveedor existente

Valor por omisión: Ninguno

código Especifica el código de la opción. Las opciones DHCP se definen en la RFC 2132. Consulte “Opciones DHCP” en la página 567 si desea obtener una descripción de las opciones y sus respectivos 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 de caracteres ASCII para formatos específicos definidos en la RFC 2132.
- Conversión hexadecimal en el momento de la inicialización. Los datos se deben entrar como *hex: 01 aa 04*.
- Serie de caracteres. Los datos se deben entrar 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 fin-rango [nombre_grupo_subred] [prioridad_grupo_subred] [lista_políticas]*
Define una subred.

nombre-subred

Indica el nombre de la subred.

Valores válidos: Cualquier serie ASCII de 10 caracteres

Valor por omisión: Ninguno

dirección de subred
Especifica la dirección de la subred. La dirección se especifica en formato decimal de puntos.

Valores válidos: Cualquier dirección de subred IP válida.

Valor por omisión: Ninguno

máscara de subred
Especifica la máscara de la dirección de subred. La dirección de subred debe estar dentro de la máscara de subred y no puede contener un número mayor de bits que la máscara.

Valores válidos: Cualquier máscara IP válida en formato decimal de puntos

Valor por omisión: Se calcula en base a la dirección de subred

inicio-rango
Especifica la dirección IP de inicio de la agrupación de direcciones IP que el servidor administrará para esta subred. Si no se especifica *inicio-rango*, el servidor administra todas las direcciones de la subred.

Valores válidos: Cualquier dirección de sistema principal IP válida dentro de la subred especificada en formato decimal de puntos.

Valor por omisión: La primera dirección IP de la subred

fin-rango Especifica la dirección IP final de la agrupación de direcciones IP que el servidor administrará para esta subred.

Valores válidos: Cualquier dirección de sistema principal IP válida dentro de la subred especificada en formato decimal de puntos.

Valor por omisión: inicio-rango más 50. Si la dirección IP resultante ya no se encuentra dentro de la subred, el valor por omisión será la última dirección IP de la subred.

nombre de grupo de subredes
Especifica el nombre del grupo de subredes al que pertenece la subred.

Valores válidos: Cualquier serie ASCII de hasta 64 caracteres

Valor por omisión: Ninguno

prioridad de grupo de subredes
Especifica la prioridad de esta subred dentro del grupo de subredes. Esta prioridad se utiliza para determinar el orden en el que se asignan las direcciones dentro de un grupo de subredes específico.

Valores válidos: 1 - 65535

Valor por omisión: 1

lista de políticas
Identifica la lista de direcciones de política, Balance o Inorder, a la que se añadirá el grupo de subredes. Si el

grupo de subredes ya existe en una de las listas y se especifica la otra, el grupo de subredes se moverá a la nueva lista.

Valores válidos: Inorder o Balance

Valor por omisión: Si se trata de una nueva subred, el valor por omisión es Inorder. De lo contrario, es la lista de política actual a la que pertenece el grupo de subredes.

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 de proveedor. Existen dos maneras de proporcionar datos de opción de proveedor:

- Entrar datos hex cuando se solicita
- Añadir opciones específicas del proveedor mediante el mandato **add option vendor**. Consulte la página 594 si desea obtener información de opciones.

nombre_proveedor

Especifica el nombre del proveedor.

Valores válidos: Una serie ASCII de hasta 40 caracteres

Valor por omisión: Ninguno

valor_hex Especifica la serie de caracteres ASCII hexadecimal que representa el valor hexadecimal de la parte destinada a datos de la opción.

Valores válidos: Cualquier serie de caracteres hexadecimales válida en el siguiente formato: *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, un cliente, una subred o una opción de proveedor.

Sintaxis:

change class

client

subnet

vendor-option

class *ámbito [nombre_subred] nombre_clase nuevo_nombre_clase [nuevo_inicio_rango] [nuevo_fin_rango]*
Modifica una clase.

ámbito Especifica el ámbito de la clase que se está modificando.

Valores válidos: global o subnet

Valor por omisión: Ninguno

nombre-subred
Sólo es válido si el **ámbito** es *subnet*. 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: El nombre de una clase existente

Valor por omisión: Ninguno

nuevo nombre de clase
Indica el nuevo nombre de la clase.

Valores válidos: Una serie ASCII de hasta 40 caracteres

Valor por omisión: El nombre de la clase existente

nuevo inicio de rango
Sólo es válido si el **ámbito** es *subnet*. Especifica la nueva dirección IP de inicio de 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 del rango existente

nuevo fin de rango
Especifica la nueva dirección IP final de la agrupación de direcciones IP a la que se asignarán clientes.

Valores válidos: Cualquier dirección IP válida dentro del rango de subredes y superior a **nuevo-fin-rango**

Valor por omisión: El 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_id_tipo nuevo_id_valor nueva_dirección*
Modifica un cliente

ámbito Especifica el ámbito del cliente que se está modificando.

Valores válidos: global o subnet

Valor por omisión: Ninguno

nombre-subred
Sólo es válido si el **ámbito** es *subnet*. 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 de cliente
Indica el nuevo nombre del cliente.

Valores válidos: Una serie ASCII de hasta 10 caracteres

Valor por omisión: El nombre del cliente existente

nuevo tipo de id
Indica el nuevo tipo de hardware del cliente.

Valores válidos: 0 - 21. Consulte la página 593.

Valor por omisión: El tipo existente de hardware del cliente

nuevo valor de id
Especifica el nuevo identificador del cliente.

Valores válidos: 0 o cualquier dirección MAC válida (12 dígitos hexadecimales)

Valor por omisión: El tipo existente de id del cliente

Nota: Un **tipo-id** *0* y un **valor-id** *0* indican que el servidor no debe distribuir la dirección IP especificada.

nueva dirección
Especifica la nueva dirección IP a proporcionar al cliente o una serie de caracteres que indica que el cliente no recibirá

servicio o que se le puede proporcionar cualquier dirección de la agrupación de direcciones IP.

Valores válidos:

Cualquier dirección IP válida

none Indica que el cliente coincidente no recibirá servicio

any Indica que se puede proporcionar al cliente cualquier dirección IP de la agrupación de subredes.

Valor por omisión: Ninguno

Nota: Un **tipo-id** *0* y un **valor-id** *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_fin_rango*
Modifica una subred.

nombre_subred
Indica el nombre de la red específica a modificar.

Valores válidos: Un nombre de subred existente

Valor por omisión: Ninguno

nuevo nombre de subred
Indica el nuevo nombre de la subred especificada.

Valores válidos: Cualquier serie ASCII de 10 caracteres

Valor por omisión: El nombre de subred original

nueva dirección de subred
Especifica la nueva dirección de la subred. La dirección se especifica en notación decimal de puntos.

Valores válidos: Cualquier dirección de subred IP válida.

Valor por omisión: La dirección de subred existente

nueva máscara de subred
Especifica la nueva máscara de la dirección de subred. La dirección de subred debe estar dentro de la máscara de

subred y no puede contener un número mayor de bits que la máscara.

Valores válidos: Cualquier máscara IP válida

Valor por omisión La máscara de subred existente

nuevo inicio de rango
Especifica la nueva dirección IP de inicio de la agrupación de direcciones IP que el servidor administrará para esta subred. Si no se especifica *inicio-rango*, el servidor administra todas las direcciones de la subred.

Valores válidos: Cualquier dirección IP válida dentro del rango de subredes

Valor por omisión: La dirección de inicio de la agrupación existente

nuevo fin de rango
Especifica la nueva dirección IP final de la agrupación de direcciones IP que el servidor administrará para esta subred.

Valores válidos: Cualquier dirección IP válida dentro del rango de subredes y superior a la dirección de inicio de la agrupación.

Valor por omisión: La 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]?
```

opción de proveedor *nombre_proveedor nuevo_nombre_proveedor [nuevo_valor_hex]*
Modifica una opción de proveedor.

nombre de proveedor
Especifica el nuevo nombre de la opción de proveedor.

Valores válidos: Un nombre de proveedor existente

Valor por omisión: Ninguno

nuevo nombre de proveedor
Especifica el nuevo nombre de la opción de proveedor.

Valores válidos: Una serie ASCII de hasta 40 caracteres

Valor por omisión: El nombre de la opción de proveedor existente

nuevo valor hex
Especifica la nueva serie de caracteres ASCII hexadecimal que representa el valor hexadecimal de la parte destinada a

datos de la opción. No se puede añadir un valor hex si se han añadido opciones específicas a esta opción de proveedor.

Valores válidos: Cualquier serie de caracteres hexadecimales válida

Valor por omisión: La serie de caracteres hexadecimales 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, un cliente, una opción, una subred, un grupo de subredes o una opción de 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 en su ámbito.

ámbito Especifica el ámbito en el que se está suprimiendo la clase.

Valores válidos: global o subnet

Valor por omisión: Ninguno

nombre_subred

Sólo es válido si el **ámbito** es *subnet*. Especifica el nombre de la subred de donde se está suprimiendo la clase.

Valores válidos: Cualquier nombre de subred existente

Valor por omisión: Ninguno

nombre-clase

Indica el nombre de la clase a suprimir.

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 en su ámbito.

ámbito Especifica el ámbito en el que se está suprimiendo el cliente.

Valores válidos: global o subnet

Valor por omisión: Ninguno

nombre_subred

Sólo es válido si el **ámbito** es *subnet*. Especifica el nombre de la subred de donde se está suprimiendo el cliente.

Valores válidos: Un nombre de subred existente

Valor por omisión: Ninguno

nombre de cliente

Indica el nombre del cliente a suprimir.

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 dentro del ámbito especificado.

ámbito Especifica el ámbito en el que se está suprimiendo la opción.

Valores válidos:

- class-global
- class-subnet
- client-global
- client subnet
- global
- subnet
- vendor-option

Valor por omisión: Ninguno

nombre-subred
Sólo es válido si el **ámbito** es *subnet, class-subnet,* o *client-subnet*. Especifica el nombre de la subred de donde se está suprimiendo el cliente.

Valores válidos: Cualquier nombre de subred existente

Valor por omisión: Ninguno

nombre-clase
Sólo es válido si el **ámbito** es *class-global* o *class-subnet*. Indica el nombre de la clase de donde se está suprimiendo la opción.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

nombre-cliente
Sólo es válido si el **ámbito** es *client-global* o *client-subnet*. Indica el nombre del cliente de donde se está suprimiendo la opción.

Valores válidos: Cualquier nombre de cliente existente

Valor por omisión: Ninguno

nombre-proveedor
Sólo es válido si el **ámbito** es *vendor-option*. Indica el nombre del proveedor de donde se está suprimiendo la opción.

Valores válidos: Cualquier nombre de proveedor existente

Valor por omisión: Ninguno

código Especifica el código de la opción. Las opciones DHCP se definen en la RFC 2132. Consulte “Opciones DHCP” en la página 567 si desea obtener una descripción de las opciones y sus respectivos 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 un subred y todas las clases, clientes y opciones que se definen en su ámbito.

nombre_subred

Especifica el nombre de la subred que se está suprimiendo.

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 concreto y todas las clases, clientes y opciones definidas en los ámbitos de subred.

nombre de grupo de subredes

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 de proveedor y todas las opciones definidas en su ámbito.

nombre_proveedor

Especifica el nombre del proveedor.

Valores válidos: Una serie ASCII de hasta 40 caracteres

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 una clase, un cliente, parámetros globales, subredes u opciones de proveedor y sus opciones asociadas.

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 a visualizar.

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 todas las clases configuradas o los detalles de un cliente específico.

nombre-cliente

Indica el nombre del cliente a visualizar.

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 los 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 que se está listando la opción.

Valores válidos:

- class-global
- class-subnet
- client-global
- client subnet
- global
- subnet
- vendor-option

Valor por omisión: Ninguno

nombre-subred
Sólo es válido si el **ámbito** es *subnet*, *class-subnet* o *client-subnet*. Especifica el nombre de la subred a la que pertenece la opción que se está listando.

Valores válidos: Cualquier nombre de subred existente

Valor por omisión: Ninguno

nombre-clase
Sólo es válido si el **ámbito** es *class-global* o *class-subnet*. Indica el nombre de la clase a la que pertenece la opción que se está listando.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

nombre-cliente
Sólo es válido si el **ámbito** es *client-global* o *client-subnet*. Indica el nombre del cliente al que pertenece la opción que se está listando.

Valores válidos: Cualquier nombre de cliente existente

Valor por omisión: Ninguno

nombre-proveedor
Sólo es válido si el **ámbito** es *vendor-option*. Indica el nombre del proveedor al que pertenece la opción que se está listando.

Valores válidos: Cualquier nombre de proveedor existente

Valor por omisión: Ninguno

código Especifica el código de la opción. Las opciones DHCP se definen en la RFC 2132. Consulte “Opciones DHCP” en la página 567 si desea obtener una descripción de las opciones y sus respectivos 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 a visualizar.

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 de proveedor específica.

nombre-proveedor

Indica el nombre de la opción de proveedor a visualizar.

Valores válidos: Un nombre de 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 los valores de los parámetros globales y para añadir grupos de subredes a las listas Balance e Inorder.

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_subredes*

Añade o mueve un grupo de subredes a la lista Balance. Las direcciones se asignarán de modo rotatorio desde todas las subredes asociadas con los grupos definidos dentro de un grupo de subredes, en función de su prioridad.

nombre de grupo de subredes
Especifica el nombre del grupo de subredes al que 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*
Indica si el servidor DHCP especifica o no un servidor bootstrap para clientes. Si desea que el servidor DHCP especifique un servidor bootstrap, deberá definir la dirección IP del servidor. Este parámetro se puede especificar dentro del ámbito global, de subred, de clase o de cliente.

ámbito Especifica el ámbito del parámetro bootstrapserver.

Valores válidos:

- class-global
- class-subnet
- client-global
- client-subnet
- global
- subnet

Valor por omisión: Ninguno

nombre-subred
Sólo es válido si el ámbito es *subnet*, *class-subnet* o *client-subnet*. Indica el nombre de la subred para la que se está especificando el servidor bootstrap.

Valores válidos: Un nombre de subred existente

Valor por omisión: Ninguno

nombre-clase
Sólo es válido si el ámbito es *class-global* o *class-subnet*. Indica el nombre de la clase para la que se está especificando el servidor bootstrap.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

nombre-cliente
Sólo es válida si el ámbito es *client-global* o *client-subnet*. Indica el nombre del cliente para el que se está especificando el servidor bootstrap.

Valores válidos: Un nombre de cliente existente

Valor por omisión: Ninguno

dirección IP del servidor

Especifica la dirección IP del servidor bootstrap.

Valores válidos: Cualquier dirección IP válida en formato decimal de puntos

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 MAC en direcciones de formato canónico.

Las direcciones MAC de los clientes Ethernet/802.3 se almacenan en formato canónico (el byte empieza con el bit menos significativo). Las direcciones MAC para clientes de red en anillo se almacenan en el formato no canónico (el byte empieza con el bit más significativo). Este parámetro se debe utilizar cuando el servidor DHCP se encuentra en un tipo de medio (red en anillo o Ethernet/802.3), el cliente en otro tipo de medio y existe un puente de conversión entre ambos. Cuando este parámetro se establece en *yes* (sí), el servidor DHCP hará que la dirección MAC del cliente se transforme de canónica a no canónica o, al contrario, de no canónica a canónica. Puesto que el servidor DHCP no conoce el formato en el que estaba originalmente la dirección MAC, al establecer este parámetro en *yes* (sí) la dirección cambiará simplemente de una a otra. Una dirección canónica se puede establecer dentro del ámbito global, de subred, de clase o de cliente.

ámbito Especifica el ámbito del parámetro bootstrapserver.

Valores válidos:

- class-global
- class-subnet
- client-global
- client-subnet
- global
- subnet

Valor por omisión: Ninguno

nombre-subred
Sólo es válida si el ámbito es *subnet*, *class-subnet* o *client-subnet*. Indica el nombre de la subred para la que se está especificando la dirección canónica.

Valores válidos: Un nombre de subred existente

Valor por omisión: Ninguno

nombre-clase
Sólo es válida si el ámbito es *class-global* o *class-subnet*. Indica el nombre de la clase para la que se está especificando la dirección canónica.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

nombre-cliente
Sólo es válida si el ámbito es *client-global* o *client-subnet*. Indica el nombre del cliente para el que se está especificando la dirección canónica.

Valores válidos: Un nombre de cliente existente

Valor por omisión: Ninguno

valor Especifica si las direcciones MAC se deben transformar a formato canónico

Valores válidos: yes, no

Valor por omisión: no, si el **ámbito** es *global*. De lo contrario, el valor por omisión se determina mediante la jerarquía de ámbitos. Consulte “Conceptos y terminología” en la página 564 se desea obtener una descripción del concepto 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 Inorder. Las direcciones se asignarán desde las subredes de un grupo de subredes en el orden de prioridad asignado a dicha subred.

nombre de grupo de subredes

Especifica el grupo de subredes al que 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 al cabo del cual se examina la condición de cesión de todas las direcciones de la agrupación de direcciones para determinar las cesiones que han caducado. El intervalo de caducidad de la cesión sólo se puede establecer a nivel global.

tiempo Especifica la unidad de medida de tiempo.

Valores válidos: segundos, minutos, horas

Valor por omisión: Ninguno

duración Especifica la duración del intervalo.

Valores válidos: 15 segundos - 12 horas

Valor por omisión:

- 15 (si la unidad de tiempo es el segundo)
- 1 (si la unidad de tiempo es el minuto)
- 1 (si la unidad de tiempo es la hora)

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 de la cesión por omisión para las cesiones ejecutadas por el servidor DHCP. Un intervalo infinito significa que las cesiones nunca caducarán. El valor por omisión del tiempo de cesión sólo se puede establecer a nivel global.

tiempo Especifica la unidad de medida de tiempo.

Valores válidos: minutos, horas, días, semanas, meses, años, infinito

Valor por omisión: Ninguno

duración Especifica la duración del intervalo.

Valores válidos: 3 minutos - infinito

Valor por omisión:

- 3 (si la unidad de tiempo es el minuto)
- 1 (si la unidad de tiempo es la hora)
- 1 (si la unidad de tiempo es el día)
- 1 (si la unidad de tiempo es el mes)
- 1 (si la unidad de tiempo es el año)

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 efectúa una prueba para asegurarse de que la dirección IP no está en uso. Este valor especifica el intervalo durante el que el servidor DHCP esperará una respuesta ping antes de marcar la dirección disponible. Un valor de 0 inhabilita los pings, lo que hace que el servidor DHCP no pruebe una dirección antes de asignarla.

tiempo Especifica la unidad de medida de tiempo.

Valores válidos: segundos

Valor por omisión: Ninguno

duración Especifica la duración del 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 peticiones de clientes BOOTP. Si el servidor DHCP no se ha configurado previamente para ofrecer soporte a clientes BOOTP y se ha reconfigurado para no ofrecer soporte a clientes BOOTP, el enlace de direcciones de los clientes BOOTP que se haya establecido antes de la reconfiguración se man-

tendrá hasta que el cliente BOOTP envíe otra petición (cuando se está iniciando). En ese momento, el servidor no responderá y se eliminará el enlace. Este parámetro sólo se puede establecer a nivel global.

Valores válidos: yes 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 que no sean aquéllos cuyos ID se listan de manera específica en esta configuración. Este parámetro dispone de varios valores posibles:

ámbito Especifica el ámbito del parámetro **support-unlisted-clients**.

Valores válidos:

- class-global
- class-subnet
- global
- subnet

Valor por omisión: Ninguno

nombre-subred

Sólo es válida si el ámbito es *subnet*, *class-subnet* o *client-subnet*. Indica el nombre de la subred para la que se está especificando este parámetro.

Valores válidos: Un nombre de subred existente

Valor por omisión: Ninguno

nombre-clase

Sólo es válida si el ámbito es *class-global* o *class-subnet*. Indica el nombre de la clase para la que se está especificando este parámetro.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

valor

yes El servidor DHCP debe responder a cualquier cliente sin tener en cuenta el tipo al que pertenece o si está configurado.

no El servidor DHCP responderá sólo a las peticiones de clientes DHCP que estén configurados.

bootp El servidor DHCP ofrecerá soporte a clientes BOOTP no listados pero no lo ofrecerá a clientes DHCP no listados.

dhcp El servidor DHCP responderá a clientes DHCP no listados pero no lo hará a clientes BOOTP no listados.

Valores válidos: yes, no, bootp, dhcp

Valor por omisión: yes, si el **ámbito** es *global*. De lo contrario, el valor por omisión se determina mediante la jerarquía de ámbitos. Consulte “Conceptos y terminología” en la página 564 se desea obtener una descripción del concepto 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 que el servidor mantendrá una dirección IP en uso antes de ponerla a disposición para su asignación. Antes de que el servidor asigne una dirección IP, éste ejecuta ping en la dirección para asegurarse de que no se está utilizando ya en la red. Si es así, marca la dirección en uso como reservada. Este parámetro especifica el intervalo durante el que se mantiene como reservada una dirección en uso antes de ponerla a disposición para su asignación. Este parámetro sólo se puede establecer a nivel global.

tiempo Especifica la unidad de medida de tiempo.

Valores válidos: segundos, minutos, horas, días, semanas, meses, años, infinito

Valor por omisión: Ninguno

duración Especifica la duración del intervalo.

Valores válidos: 30 segundos - infinito

Valor por omisión:

- 30 (si la unidad de tiempo es el segundo)
- 15 (si la unidad de tiempo es el minuto)
- 1 (si la unidad de tiempo es la hora)
- 1 (si la unidad de tiempo es el día)
- 1 (si la unidad de tiempo es el mes)
- 1 (si la unidad de tiempo es el año)

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. Entre **talk 5** en el indicador OPCON. Por ejemplo:

   ```
   * talk 5
   Config>
   ```

   Después de entrar el mandato **talk 5**, el indicador CONFIG (+) aparece en el terminal. Si el indicador no aparece cuando se entra por primera vez la configuración, pulse **Intro** de nuevo.

2. En el indicador +, entre el mandato **feature dhcp-server** para acceder al indicador `DHCP Server>`.

Mandatos de supervisión del servidor DHCP

Tabla 61. 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 xxxii.
Disable	Inhabilita dinámicamente el servidor DHCP.
Enable	Habilita dinámicamente el servidor DHCP.
List	Visualiza los parámetros de clases, de clientes, globales, de subredes y de opciones de 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 xxxiii.

Disable

Utilice el mandato **disable** para inhabilitar de manera dinámica al 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 de una clase, un cliente, de parámetros globales, de subredes o de una opción de proveedor y sus opciones asociadas. Consulte “List” en la página 608 para obtener ejemplos del mandato **list**.

Sintaxis:

list class
client
global
option
subnet
vendor-option

Reset

Utilice el mandato **reset** para restablecer de manera dinámica la configuración del servidor DHCP.

Sintaxis:

res**et**	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 de administración.

Sintaxis:

req**uest**	clientid
	delete
	ipquery
	poolquery
	stats
	status

clientid *id_cliente*

Visualiza información de un cliente.

client_id 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 una cesión de una dirección específica IP del cliente.

dirección Indica la dirección IP del cliente que se debe suprimir.

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 de 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 de una agrupación de direcciones IP.

dirección Indica una dirección IP de la agrupación a visualizar.

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 estadística sobre la agrupación de direcciones administradas por el servidor. Dichas estadísticas incluyen: los paquetes de descubrimiento procesados, los paquetes de descubrimiento sin respuesta, las ofertas efectuadas, las cesiones concedidas, las peticiones sin acuse de recibo (NAK), los informes procesados (incluyendo los informes más los acuses de recibo, ACK), las renovaciones, las entregas, los clientes BOOTP procesados, los proxyARec actualizados intentados y los paquetes sin soporte. 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

En este apartado se describe la reconfiguración dinámica (DR) y cómo afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

El protocolo DHCP (Dynamic Host Configuration Protocol) no da soporte al mandato **delete interface** de CONFIG (Talk 6).

Mandato activate interface de GWCON (Talk 5)

El mandato **activate interface** de GWCON (Talk 5) no es aplicable al protocolo DHCP (Dynamic Host Configuration Protocol). La configuración de DHCP no se basa en ninguna interfaz concreta.

Mandato reset interface de GWCON (Talk 5)

El mandato **reset interface** de GWCON (Talk 5) no es aplicable al protocolo DHCP. La configuración del protocolo DHCP no se basa en ninguna interfaz concreta.

Mandatos de restablecimiento de componente de GWCON (Talk 5)

El protocolo DHCP (Dynamic Host Configuration Protocol) da soporte a los mandatos **reset** de GWCON (Talk 5) específicos del protocolo DHCP:

Mandato GWCON, feature DHCP, reset DHCP

Descripción: Restablece el servidor DHCP y lo inicializa con la nueva configuración.

Efecto en la red: Si la nueva configuración da soporte a los mismos clientes, se les ofrecerá nuevos tiempos de cesión y de renovación. Si la nueva configuración no da soporte a los mismos clientes, expirará su tiempo de cesión.

Limitaciones:

- En los direccionadores que no tienen disco fijo ni tarjeta de almacenamiento flash, después de una operación de restablecimiento, los clientes DHCP continuarán funcionando con sus cesiones, pero el servidor DHCP ya no las conocerá.
- En los direccionadores que no tienen disco fijo ni tarjeta de almacenamiento flash, las direcciones IP cedidas con anterioridad por el servidor DHCP, se marcarán como “USED” en el mandato “GWCON, feature DHCP, request status” no fuera caso que las direcciones se intentarán ceder de nuevo.

En la tabla siguiente se resumen los cambios en la configuración del protocolo de configuración dinámica de sistemas principales (DHCP) que se activan cuando se ejecuta el mandato **GWCON, feature DHCP, reset dhcp**:

Mandatos cuyos cambios se activan al ejecutar 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 protocolo de configuración dinámica de sistemas principales (DHCP) da soporte a los siguientes mandatos de GWCON que cambian temporalmente el estado operativo del dispositivo. Estos cambios se perderán si el dispositivo se reinicia, si se vuelve a cargar, o si se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
GWCON, feature DHCP, disable dhcp
GWCON, feature DHCP, enable dhcp

Mandatos no reconfigurables dinámicamente

Todos los parámetros de configuración del protocolo DHCP pueden cambiarse dinámicamente.

Utilización de la función Thin Server

En este capítulo se describe el modo de utilización de la función Thin Server (TSF) en el IBM 2212.

Visión general de la Network Station

Una Network Station es similar a un PC ya que dispone de un teclado, una pantalla y un ratón. La principal diferencia entre una Network Station y un PC es que los archivos de la Network Station residen en un servidor de red en lugar de en una unidad de disco duro de la máquina. La Network Station dispone de una interfaz gráfica de usuario (GUI), que proporciona acceso a muchos recursos, incluidos emuladores, aplicaciones X remotas, navegadores de Web, aplicaciones e impresoras.

La Network Station se comunica mediante TCP/IP a través de una conexión de red en anillo o Ethernet con el servidor. El proceso de encendido de la Network Station es el que sigue:

- Se inicia un programa supervisor de arranque residente en la memoria de acceso aleatorio no volátil y se ejecutan autopruebas de encendido.
- La Network Station contacta con un servidor BootP o DHCP que proporciona a la Network Station información tal como su dirección IP, las direcciones de servidor y la vía de acceso y el nombre del archivo de arranque. Como alternativa, la Network Station puede recuperar esta información a partir de los valores almacenados en su memoria de acceso aleatorio no volátil.
- La Network Station utiliza el protocolo de transferencia de archivos trivial (TFTP), el sistema de archivos remoto/400 (RFS/400) o el sistema de archivos de red (NFS) para bajar del servidor de código base el código base, como puede ser el sistema operativo, los archivos de configuración de hardware y los programas de aplicaciones.
- La Network Station baja del servidor de configuración del terminal la información de configuración basada en el terminal, como puede ser la configuración de una impresora conectada a la Network Station o el idioma del teclado de la Network Station.
- La Network Station muestra una pantalla de inicio de sesión. En ese momento, puede entrar un id de usuario y una contraseña.
- El servidor de autenticación valida el id de usuario y la contraseña y permite acceder a los archivos de usuario personales.
- Se bajan las preferencias de entorno del usuario.
- La Network Station visualiza el escritorio personalizado del usuario.

Consulte la publicación *IBM Network Station Manager Instalación y utilización*, si desea más información sobre las Network Station.

Visión general de la función Thin Server

Un dispositivo físico puede funcionar como servidor BootP/DHCP, servidor de arranque, servidor de configuración del terminal y servidor de autenticación o cada uno de estos servidores puede ser un dispositivo independiente. Por ejemplo, se puede disponer de una Network Station conectada a un AS/400® y que el AS/400 funcione como servidor BootP, servidor de código base, servidor de configuración del terminal y servidor de autenticación. Como alternativa, cada servidor puede ser una caja física independiente. Por ejemplo, la Network Station puede estar conectada a una red en la que un servidor Windows® NT es su servidor DHCP, un AS/400 es su servidor de código base, otro AS/400 es su servidor de configuración del terminal y otro AS/400 es su servidor de autenticación.

La función Thin Server permite que el 2212 se convierta en servidor de código base. Un ejemplo de por qué sería deseable utilizar TSF queda ilustrado en la Figura 50 en la página 633 y la Figura 51 en la página 633. En la Figura 50 en la página 633, cualquier archivo que la Network Station necesite se bajará de un único servidor. Cuando se enciende la Network Station, la bajada supone la utilización de bastantes megabytes. Ello puede suponer una notable exigencia para una infraestructura de red, así como también para un dispositivo que actúe de servidor de código base/configuración de terminal o como servidor de autenticación, especialmente si hay muchas Network Station encendidas. La Figura 51 en la página 633 muestra la red con un Thin Server utilizado en el sitio remoto. El Thin Server guardará en la antememoria muchos de los archivos asociados con el código de arranque de la Network Station. Cuando se enciende la Network Station, la mayor parte del código de arranque se cargará a partir del Thin Server y sólo será necesario que una pequeña cantidad de datos sea transportada por la infraestructura de la red. Este proceso reducido en cualquier servidor individual disminuye el tráfico de red y reduce el tiempo necesario para completar el encendido de una Network Station.

Puesto que los archivos almacenados en antememoria por el Thin Server son copias de archivos que residen en el servidor de archivos maestro, si la versión que reside en el servidor de archivos maestro se modifica, es necesario que el Thin Server actualice la versión de este archivo. El Thin Server verificará que todos los archivos almacenados en antememoria sean idénticos a la versión del servidor de archivos maestro de aquellos archivos cuando:

1. Se enciende el IBM 2212
2. Se vuelve a cargar o se reinicia el IBM 2212
3. Se reinicia TSF
4. Se alcanza el intervalo de tiempo especificado en la configuración de TSF
5. Un parámetro de acción de la MIB de SNMP lo desencadena
6. Se ejecuta el mandato `talk 5` **refresh** de TSF
7. Siempre que se accede a un archivo (excepto TFTP). TSF verificará que cada archivo al que se accede coincida con la versión del servidor de archivos maestro. Cuando se detecte una diferencia, dicho archivo se actualizará. A continuación, TSF verificará que los archivos restantes coincidan también con el servidor de archivos maestro.

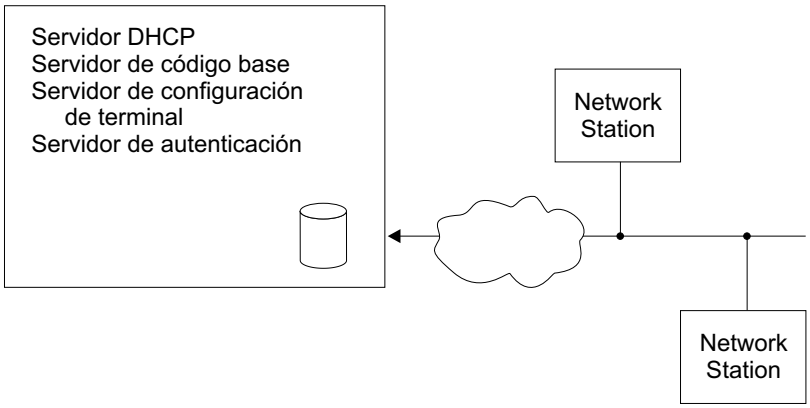


Figura 50. Estación de red remota sin Thin Server

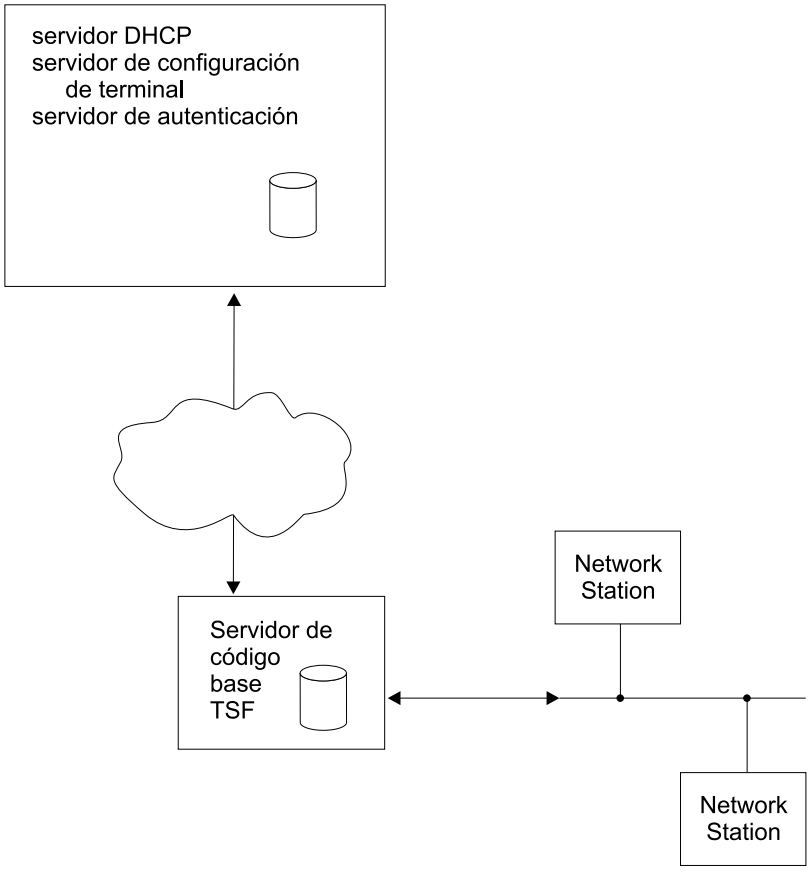


Figura 51. Estación de red remota con un Thin Server

Soporte de BootP/DHCP

Existen dos opciones de soporte para servidores BootP/DHCP:

- Utilizar el soporte del servidor DHCP del IBM 2212. Consulte “Utilización del servidor DHCP” en la página 559.
- Configurar el IBM 2212 para que funcione como agente de retransmisión para las peticiones BootP/DHCP. Si necesita más información, consulte el apartado

Configuración del proceso de reenvío BOOTP/DHCP del capítulo Utilización de IP de la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 1*.

Consulte la publicación *IBM Network Station Manager Instalación y utilización*, si desea obtener más información sobre entornos multiservidor.

Protocolos utilizados para comunicar con Network Station

Los protocolos que se utilizan para establecer comunicación entre la Network Station y sus servidores están determinados por la configuración BootP/DHCP o la configuración NVRAM de la Network Station. En cualquiera de los dos casos, los protocolos que la Network Station utiliza deben ser compatibles con la configuración de TSF.

Si TSF está configurada para utilizar el sistema de archivos remoto (RFS) para comunicarse con el servidor de archivos maestro, responderá a las peticiones RFS y TFTP provenientes de las Network Station, pero no responderá a las peticiones del sistema de archivos de red (NFS) provenientes de las Network Station.

NFS El sistema de archivos de red es un sistema de archivos distribuidos que permite acceder de forma transparente a discos remotos.

RFS El sistema de archivos remoto (específico del AS/400) se utiliza fundamentalmente para transferir archivos entre sistemas.

De manera similar, si TSF está configurada para utilizar NFS para comunicarse con el servidor de archivos maestro, responderá a las peticiones NFS y TFTP provenientes de las Network Station, pero no responderá a las peticiones RFS provenientes de las Network Station.

Utilización de RFS

TSF establece una conexión con el AS/400 mediante RFS. Cuando una Network Station efectúa una petición para abrir un archivo, TSF reenvía esa petición al AS/400 para su autorización. Si la Network Station no está autorizada, TSF no enviará el archivo solicitado a la Network Station. Si la Network Station está autorizada y la versión de AS/400 del archivo solicitado difiere de la versión almacenada en TSF del IBM 2212, la petición de la Network Station se retransmite al AS/400. Si el archivo de AS/400 tiene la misma versión que el archivo que TSF ha guardado en antememoria, TSF servirá dicho archivo a la Network Station.

Si TSF está configurada para funcionar en modalidad desconectada, manejará de forma local todo el tráfico de las Network Station y servirá los archivos que tenga guardados en antememoria o, si no los tiene guardados, responderá con un mensaje de "archivo no encontrado". Por lo tanto, es imperativo que todos los archivos que solicita la Network Station se guarden en antememoria. TSF se conecta con el servidor de archivos maestro para llevar a cabo las renovaciones, pero no abre ningún archivo o la autenticación por cada archivo se retransmite al servidor de archivos maestro.

Si la conexión TSF con el AS/400 no está disponible, o TSF está en modalidad desconectada, TSF servirá a la Network Station los archivos que tiene almacenados actualmente en antememoria.

Utilización de TFTP

Si se utiliza TFTP para comunicar entre la Network Station y TSF, TSF atenderá las peticiones de archivos de la Network Station si dichos archivos están disponibles. No se efectúa ninguna verificación de versión entre TSF y el servidor de archivos maestro. Si el archivo no está disponible en la antememoria de TSF, la petición de la Network Station se reenvía al servidor de archivos maestro.

Si TSF está configurada para funcionar en la modalidad desconectada, manejará de forma local todas las peticiones provenientes de las Network Station. Si un archivo no está disponible en la antememoria de TSF, en lugar de reenviar la petición al servidor de archivos maestro, responderá con un mensaje de "archivo no encontrado".

Utilización de NFS

Si NSF se utiliza para comunicarse entre la Network Station y TSF, cuando una Network Station solicite un archivo, TSF empezará a servir dicho archivo si está almacenado en antememoria. Simultáneamente, verificará que la versión del archivo sea la misma que la del servidor de archivos maestro. En caso contrario, TSF dejará de servir el archivo para empezar a bajar de inmediato la nueva versión del servidor de archivos maestro.

Si TSF está configurada para funcionar en la modalidad desconectada, no verificará los archivos que se soliciten.

Si TSF no tiene almacenado el archivo en antememoria, responderá con un mensaje de "archivo no encontrado". Asimismo, si el archivo solicitado reside en un directorio para el que se ha configurado TSF con *include subdirectories* o reside en un subdirectorio de dicho directorio configurado, TSF empezará a guardar en antememoria el archivo, si el archivo existe en el servidor de archivos maestro.

Actualizaciones de antememorias de archivos

El protocolo utilizado para guardar en antememoria archivos en el dispositivo de red lo determina la configuración de TSF. Los servidores maestros se designan mediante el mandato **add master-file-server**.

TSF contempla la posibilidad de configurar dos servidores de archivos maestros, un servidor de archivos y un servidor de archivos secundario. El servidor de archivos secundario es un servidor de archivos de reserva.

Para ambos tipos de servidores de archivos maestros, RFS y NFS, se le solicitará la dirección de un servidor de archivos y de servidor de archivos secundario. La dirección del servidor de archivos es obligatoria; la dirección del servidor de archivos secundario es opcional. El servidor de archivos debe ser el servidor de archivos maestro principal de esta TSF. En caso de que más de un servidor esté ejecutando NSM y que se quiera especificar un servidor de archivos de reserva o alternativo que utilice TSF si el servidor especificado como servidor de archivos no está disponible, se puede especificar un servidor de archivos secundario. Si no existe ningún servidor de archivos secundario, establezca la dirección del servidor de archivos secundario como 0.0.0.0. Se recomienda que ambos servidores de archivos maestros ejecuten la misma versión de NSM y, si se utiliza RFS, se recomienda que ambas listas de precarga sean idénticas; en caso contrario, el compor-

tamiento de la Network Station puede ser distinto cuando TSF conmute al servidor de archivos maestro secundario.

La conmutación o selección del servidor de archivos o del servidor de archivos secundario se controla mediante el mandato **set selection** de Talk 6. Se pueden establecer las opciones de selección principal, secundario o automática. Si se elige la opción principal, se hará caso omiso del servidor de archivos secundario; TSF se pondrá en contacto solamente con el principal. Si no es posible ponerse en contacto con el servidor principal después del número configurado de reintentos, TSF dejará de intentar ponerse en contacto hasta el próximo proceso de renovación. Si se elige la opción secundario, se hará caso omiso de la dirección del servidor de archivos principal; TSF se pondrá en contacto solamente con el servidor de archivos secundario. Si no es posible ponerse en contacto con el servidor secundario después del número configurado de reintentos, TSF dejará de intentar ponerse en contacto hasta el próximo proceso de renovación. Si se elige la opción automática, TSF intentará ponerse en contacto con el servidor de archivos principal.Si no lo consigue después del número configurado de reintentos, TSF automáticamente intentará ponerse en contacto con el servidor de archivos secundario.

Si especifica *rfs*, se le solicitará que especifique un nombre de archivo de lista de precarga. La lista de precarga es un archivo ASCII que especifica el nombre de archivo totalmente calificado de todos los archivos que TSF almacenará en antememoria.

Si especifica *nfs*, se le solicitarán los nombres de los directorios que se almacenarán en antememoria (puede que se ofrezcan algunos valores por omisión). Cuando especifique un directorio, se le solicitará si desea incluir o no los subdirectorios. Si especifica que *no* (no incluir subdirectorios), TSF precargará todos los archivos en el directorio especificado de la antememoria de TSF. Si se especifica *yes* (incluir subdirectorios), TSF *NO* precargará ningún archivo de ese directorio, sino que recuperará dinámicamente archivos de ese directorio y de sus subdirectorios a medida que las Network Station soliciten dichos archivos.

Los archivos que están en proceso de renovación no se enviarán a la Network Station durante este proceso.

Configuración del entorno del Thin Server

Cuando TSF está instalada, existen varias configuraciones además de la configuración de la propia TSF que se deben tener en cuenta. En este apartado se comentan los cambios que puede ser necesario realizar en la configuración del servidor BootP/DHCP, del servidor de archivos maestro, del BootP Relay del IBM 2212, de la dirección IP interna del IBM 2212 y de TSF del IBM 2212. En el apartado “Ejemplo de configuración” en la página 639 se puede ver un ejemplo de Thin Server conectado con un AS/400 que está ejecutando Network Station Manager (NSM) Release 2.5.

En los apartados siguientes se describe el proceso de configuración del entorno Thin Server:

Recomendaciones de configuración

A continuación encontrará algunas recomendaciones de configuración que le ayudarán a sacar el máximo partido al TSF:

- Utilizar un disco fijo.

  Aunque TSF no requiere un disco fijo, éste mejorará el rendimiento si la antememoria de TSF se ha configurado en un valor demasiado bajo (o no se puede configurar lo suficientemente grande a causa de otras funciones del 2212) y también mejorará el rendimiento si TSF o el 2212 se reinicia o se vuelve a cargar.

- Número máximo de Network Station.

  TSF permitirá hasta 200 conexiones de Network Station RFS a la vez. Encender de manera simultánea más de 30 a 40 Network Station puede ocasionar retrasos que hagan superar los valores de tiempo de espera de la Network Station. Puede que sea necesario volver a poner en marcha la Network Station para la recuperación.

- El servidor de archivos maestro debe ser un servidor que ejecute Network Station Manager (NSM). Los servidores de archivos maestros principal y secundario deben utilizar la misma versión de NSM.

  Aunque TSF permite que la dirección IP del servidor de archivos maestro sea cualquier valor, se recomienda que sea la dirección de un dispositivo que ejecute NSM, de tal manera que la estructura de archivos sea compatible con la Network Station y, por consiguiente, con TSF, y pueda servir los archivos que TSF le solicite.

- Definir suficiente memoria para contener todos los archivos guardados en antememoria.

  Esto es necesario si no se dispone de un disco fijo. Si no dispone de un disco fijo, el acceso a la memoria es mucho más rápido que el acceso al disco fijo. La cantidad de memoria necesaria variará en función del entorno específico. Utilice el mandato `Talk 5` **list config** para determinar el tamaño del conjunto de archivos en un momento determinado. El valor que se visualiza en *Hard File storage being used for Thin Server* es el tamaño del conjunto de archivos en kilobytes. De todos modos, si se añaden diferentes tipos de Network Station al entorno o se eliminan de él, este valor puede cambiar.

- Si está utilizando NFS, TSF averigua qué archivos que necesita.

  Este proceso de averiguación puede necesitar varias secuencias de encendido de la Network Station para que TSF identifique todos los archivos necesarios.

- Si TSF está configurada para funcionar en la modalidad desconectada, asegúrese de que almacena en antememoria todos los archivos necesarios.

  Si TSF está configurada para funcionar en modalidad desconectada, todos los archivos que solicite la Network Station desde TSF, el Thin Server deberá

guardarlos en antememoria. Si se utiliza RFS, la lista de precarga debe contener todos los archivos necesarios.Si se utiliza NFS, TSF debe estar configurada para que guarde en antememoria los directorios apropiados. (TSF seguirá averiguando/bajando archivos, si es necesario). Si la lista de precarga o los directorios apropiados no están configurados correctamente, las Network Station no arrancarán correctamente. Una forma de asegurarse de que la configuración es correcta es ejecutar TSF en modalidad habilitada y supervisar los mensajes ELS y los contadores TSF apropiados antes de ejecutarla en modalidad desconectada.

Configuración del servidor BootP/DHCP

Cuando se ejecuta el Network Station Manager Release 3, DHCP es obligatorio si se está utilizando un Thin Server. Si está utilizando un AS/400 como servidor de archivos maestro, se puede utilizar el Network Station Manager Release 2.5, en cuyo caso se puede utilizar BootP en lugar de DHCP.

En el caso de BootP, sólo se puede especificar una dirección de servidor. Dicha dirección se especifica mediante el identificador **sa**. Puede que dicho identificador exista o no en el registro BootP de una Network Station determinada. Si no existe, créelo y establezca el valor en la dirección IP interna del 2212. Si existe ya, cámbielo por la dirección IP interna del 2212.

En el caso de DHCP, es probable que sea necesario modificar los campos cuando el Thin Server se utiliza del modo siguiente:

- Opción 66 o servidor bootstrap - dirección IP del servidor de código base

  Este valor se debe establecer en la dirección IP interna del IBM 2212

- Opción 211 - protocolo a utilizar para el servidor de código base

  Si el Thin Server se está configurando para NFS de tipo servidor de archivos maestro, debe ser *nfs* o *tftp*. Si el Thin Server se está configurando para RFS de tipo servidor de archivos maestro, debe ser *rfs/400* o *tftp*.

- Opción 212 - servidor de configuración de terminal

  Esta dirección debe ser la misma que la dirección IP del servidor de archivos maestro.

Para obtener más detalles sobre cómo interactúan las NS con BootP y DHCP, consulte la publicación *IBM Network Station Manager Instalación y utilización*.

Configuración del servidor para el entorno del Thin Server

En el caso de RFS, la lista de precarga debe estar instalada en el AS/400. La lista de precarga está disponible en la dirección de internet `http://www.networking.ibm.com/netprod.html#routers`. Debe ejecutar ftp para el archivo LoadList.file desde dicho sitio y ubicarlo en `/QIBM/ProdData/OS400/NetStationRmtController` del AS/400. Puede que sea necesario crear el directorio NetStationRmtController.

En el caso de NFS, no es necesario hacer ningún cambio especial en el servidor maestro para el Thin Server.

Configuración de BootP Relay

Se debe habilitar el agente BootP Relay del IBM 2212 y se deben configurar los servidores BootP y DHCP para que el BootP Relay reenvíe a dichos servidores. Consulte la publicación *Access Integration Services Guía del usuario de software* si desea obtener más información.

Configuración de la dirección IP interna

Si ya existe una dirección IP interna, no es necesario ningún cambio especial. Si hay ninguna dirección IP interna especificada actualmente, se deberá especificar una. Consulte la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 1* si desea obtener más información.

Configuración de TSF

Utilice los mandatos descritos en el “Configuración y supervisión de la función Thin Server” en la página 645 para configurar el Thin Server.

Como mínimo, se deben entrar los siguientes mandatos:

1. **load add package thin-server**
2. **set mode enable** o **set mode disconnected**
3. **add master-server**

Ejemplo de configuración

El siguiente ejemplo muestra cómo configurar una TSF destinada a un AS/400 en el que se ejecuta Network Station Manager R2.5.

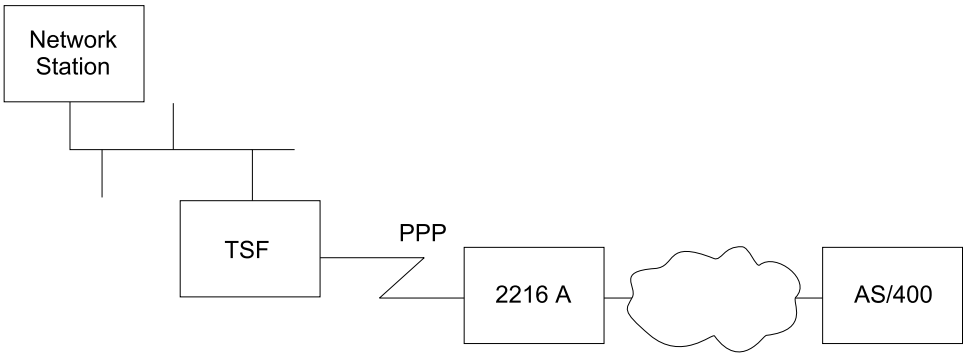


Figura 52. Ejemplo de configuración de TSF

Esta descripción de la configuración de la función Thin Server está basada en la red anterior y utiliza los siguientes supuestos:

- El AS/400 será el servidor BootP.
- El 2216 A es un direccionador (sin ninguna TSF configurada ni ninguna configuración especial para TSF).
- La conectividad IP de la red se ha validado, es decir, el AS/400 puede ejecutar PING en el IBM 2212 (TSF) y el IBM 2212 puede ejecutar PING en el AS/400.
- BootP Relay NO está habilitado en la actualidad en el IBM 2212 (TSF)
- No hay configurada una dirección IP interna en el IBM 2212 (TSF)

Configuración del AS/400

BootP (NSM Release 2.5)

1. Utilice NSM para definir la NS
2. Ejecute ftp para transferir la tabla BootP a un sistema que disponga de un editor ASCII

```
c:\>ftp as400a
Connected to as400a.raleigh.ibm.com.
220-QTCP at AS400A.RALEIGH.IBM.COM.
220 Connection will close if idle more than 5 minutes.
Name (as400a:goofy): qsecofr
331 Enter password. Password:
230 QSECOFR logged on.
ftp> ascii
ftp> get qusrsys/qatodbtp.bootptab bootp.tab
ftp> quit
```

3. Edite el archivo con un editor ASCII, añadiendo un identificador "sa" con la dirección IP interna del 2212 (TSF) especificada:

```
LÍNEA ANTIGUA
--------
NSEN106:ip=192.9.250.36:bt=IBMNSM:ht=1:ha=00.00.A7.01.2E.35:
sm=255.255.248.0:gw=192.9.250.6:bf=KERNEL:
hd=/QIBM/PRODDATA/NETWORKSTATION

LÍNEA MODIFICADA
-------------
NSEN106:ip=192.9.250.36:bt=IBMNSM:ht=1:ha=00.00.A7.01.2E.35:
sm=255.255.248.0:gw=192.9.250.6:bf=KERNEL:
hd=/QIBM/PRODDATA/NETWORKSTATION:sa=192.9.250.6
```

   donde 192.9.250.6 es la dirección IP interna del 2212 (TSF)

4. Ejecute ftp para transferir la tabla BootP otra vez al AS/400

```
c:\> ftp as400a
Connected to as400a.raleigh.ibm.com.
220-QTCP at AS400A.RALEIGH.IBM.COM.
220 Connection will close if idle more than 5 minutes.
Name (as400a:goofy): qsecofr
331 Enter password.
 Password:
230 QSECOFR logged on.
ftp> ascii
ftp> put bootp.tab qusrsys/qatodbtp.bootptab
ftp> quit
```

Preparación de la lista de precarga

Puede obtener una lista de precarga de internet:
`http://www.networking.ibm.com/netprod.html#routers`

Una vez disponga de la lista de precarga, puede ejecutar ftp para transferirla al AS/400.

1. Asegúrese de que el directorio local se ha establecido en la ubicación del archivo "LoadList.file".
2. Ejecute ftp hacia el AS/400 - "test400" es el nombre del AS/400 en este ejemplo.

```
ftp test400
Connected to test400.raleigh.ibm.com.
Name (test400:root): qsecofr
Enter password.
Password:
QSECOFR logged on.
```

3. Cambie al directorio correcto del AS/400 de destino:

```
ftp> cd /
Current directory changed to /.
ftp> cd qibm/proddata/os400/
Current directory changed to /qibm/proddata/os400.
ftp> dir
 PORT subcommand request successful.
 List started.
QTCP            34816 04/30/97 02:50:36 *DIR     REXEC/
QSECOFR         33792 07/24/98 08:04:55 *DIR     NetStationRmtController/
 List completed.
```

4. Si el directorio "NetStationRmtController" no existe, deberá crearlo.

```
ftp> MKD
(directory - name) NetStationRmtController
Created directory /qibm/proddata/os400/netstationrmtcontroller
```

5. Cambie al directorio NetStationRmtController:

```
ftp> cd NetStationRmtController
Current directory changed to /qibm/proddata/os400/Netstationrmtcontroller.
```

6. Transfiera el archivo al AS/400:

```
ftp> ascii
Representation type is ASCII nonprint.
ftp> put LoadList.file
 PORT subcommand request successful.
 Sending file to /qibm/proddata/os400/Netstationrmtcontroller
 File transfer completed successfully.
```

Configuración de TCP/IP

La configuración TCP/IP dependerá del entorno específico.

Configuración del IBM 2212 (TSF)

BootP Relay

1. Determine si el BootP Relay ya está configurado:

```
*
*
t 6
 Config>protocol ip
 Internet protocol user configuration
IP config>list bootp
BOOTP forwarding: enabled
Max number of BOOTP forwarding hops: 4
Min secs of retry before forwarding: 0
Configured BOOTP servers:      192.9.220.21
IP config>
```

2. Si todavía no está habilitado, habilítelo:

```
IP config>enable bootp
Maximum number of forwarding hops [4]?
Minimum seconds before forwarding [0]?
IP config>
```

3. Si el servidor BootP o DHCP de Network Station no está en la lista de servidores configurados, añádalo.

```
IP
config>add bootp-server
BOOTP server address [0.0.0.0]? 9.37.121.6
IP config>
```

Dirección IP interna

1. Determine si ya se ha configurado una dirección IP interna:

```
 Config>protocol ip
 Internet protocol user configuration
 IP config>list addresses
IP addresses for each interface:
    intf     0   9.37.177.97      255.255.248.0    Local wire...
    intf     1   192.9.220.2      255.255.255.0    Local wire...
    intf     2   192.9.250.6      255.255.255.0    Local wire...
    intf     3   192.9.222.2      255.255.255.0    Local wire...
    intf     4                                     IP disabled...
    intf     5                                     IP disabled...
    intf     6   192.9.223.2      255.255.255.0    Local wire...
IP config>
```

2. Configure la dirección IP interna.

```
IP config>set internal-ip-address
Internal IP address [192.9.223.2]? 192.9.250.6
IP config>
```

3. Liste las direcciones de nuevo.

```
IP config>list addresses
IP addresses for each interface:
   intf     0   9.37.177.97      255.255.248.0    Local wire
   intf     1   192.9.220.2      255.255.255.0    Local wire
   intf     2   192.9.250.6      255.255.255.0    Local wire
   intf     3   192.9.222.2      255.255.255.0    Local wire
   intf     4                                     IP disabled
   intf     5                                     IP disabled
   intf     6   192.9.223.2      255.255.255.0    Local wire
Internal IP address: 192.9.250.6
IP config>
```

Función Thin Server

1. Añada el paquete de carga del Thin Server.

   Para poder configurar la función Thin Server, debe añadir el paquete de carga.

   En primer lugar, asegúrese de que el paquete del Thin Server está disponible.

```
Config>load list available Available Packages
------------------
appn package
tn3270e package
thin-server package
Config>
```

   Si no está disponible, es necesario que obtenga la versión de software correcta antes de continuar.

   Si está disponible, verifique que el paquete no se haya cargado ya.

```
Config>load list configured
Configured Packages
-------------------
thin-server package
Config>
```

   Si ya está cargado/configurado (como muestra el ejemplo anterior), puede continuar con la configuración de TSF. Si todavía no se ha cargado, deberá añadir el paquete del Thin Server:

```
Config>load add package thin-server
thin-server package configured successfully
This change requires a reload.
Config>
```

2. Vuelva a cargar

   Si ha tenido que añadir el paquete del Thin Server, deberá escribir ahora la configuración y volver a cargar el IBM 2212.

3. Establezca la modalidad

   Cuando se carga el paquete, Thin Server está inicialmente inhabilitado. La modalidad se debe establecer como habilitada, desconectada o de paso a través para poder configurar cualquier otro parámetro del Thin Server.

```
*
*
t 6
Config>feature tsf
Thin server config>set mode enable

Thin server feature (TSF) is fully enabled once
you have entered a Master File Server for either
RFS or NFS. Please add a master-file-server if
one is not already configured.
Thin server config>
```

4. Añada un servidor de archivos maestro.

   Una vez que se ha habilitado la función Thin Server, se debe configurar el servidor de archivos maestro. En ese ejemplo, el servidor de archivos maestro es un AS/400, de manera que añadiremos un servidor de archivos maestro RFS. En el caso de esta red, los parámetros de reintento y tiempo de espera TFTP por omisión son los adecuados.

```
Thin server
config>add master-file-server rfs-as400
File Server IP address [0.0.0.0]? 192.9.221.21
Secondary File Server IP address [0.0.0.0]? 192.9.225.20
Master Server Refresh Retry Limit (1 - 20) [10]?
TFTP Packet Timeout in seconds (5 - 10) [5]?
TFTP Max Retry Limit (1 - 10) [1]? 7
TFTP Max Segment Size in bytes (valid values are 512, 1024, 2048, 4096, 8192)
                                                          [8192]?
Pre-load File name
   [/QIBM/ProdData/OS400/NetstationRmtController/Load list.file]?
Thin server config>
```

   La dirección IP del AS/400 en la interfaz de red en anillo es 9.37.100.68. Cuando hemos instalado el archivo de lista de precarga en el AS/400 hemos asignado su nombre para que coincida con el nombre por omisión del Thin Server a fin de que no tenga que ser modificado.

5. Establezca la hora de renovación de la lista de precarga (opcional)

   El valor por omisión de la hora del día para llevar a cabo la renovación es la 1:00 AM. Se eligió esta hora para minimizar cualquier impacto de rendimiento si se han modificado archivos grandes y el Thin Server debe bajarlos.

6. Establezca el intervalo de la lista de precarga (opcional)

   El intervalo por omisión para verificar que los archivos guardados en la antememoria están al mismo nivel que el servidor de archivos maestro es cada día. El valor de este parámetro y el parámetro de hora de renovación de la lista de precarga determinan la frecuencia con la que se verifican los archivos. Si los archivos de la Network Station cambian de manera poco frecuente, es

posible que desee que éstos sólo se renueven una vez a la semana o una vez al mes.

7. Establezca la memoria (opcional)

   La memoria por omisión de una antememoria RAM de 16 MB para guardar archivos debe ser suficiente. En cuanto varias Network Station utilicen TSF, en el apartado “Recomendaciones de configuración” en la página 637 consulte cuáles son los valores recomendados.

8. Establezca el disco fijo (opcional)

   Se recomienda un disco fijo. Si no dispone de un disco fijo, este parámetro se debe establecer en *no*.

9. Establezca la selección (opcional)

   El valor por omisión es principal. Si tiene un servidor de archivos maestro secundario, puede que quiera especificar la selección automática. Consulte el apartado “Actualizaciones de antememorias de archivos” en la página 635 para obtener detalles.

Configuración y supervisión de la función Thin Server

En este capítulo se describe cómo utilizar los mandatos de configuración y de funcionamiento de la función Thin Server (TSF) y consta de los apartados siguientes:

Acceso al entorno de configuración de TSF

Utilice el procedimiento siguiente para acceder al proceso de configuración de TSF.

1. En el indicador OPCON, entre **talk 6**. (Si desea obtener más detalles sobre este mandato, consulte "El proceso y los mandatos de OPCON" en la publicación *Access Integration Services Guía del usuario de software*.) Por ejemplo:

   ```
   * talk 6
   Config>
   ```

   Después de entrar el mandato **talk 6**, el indicador CONFIG (`Config>`) aparece en el terminal. Si el indicador no aparece cuando se entra por primera vez en la configuración, pulse **Intro** de nuevo.

2. Entre el mandato **feature tsf** en el indicador CONFIG para acceder al indicador `Thin server config>`.

Mandatos de configuración de TSF

Para configurar TSF, entre los mandatos en el indicador `Thin server config>`.

Tabla 62. Resumen de mandatos de configuración de TSF

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 xxxii.
Add	Añade un servidor de archivos maestro—sistema de archivos remoto (RFS) o sistemas de archivos de red (NFS).
Delete	Suprime un servidor de archivos maestro (RFS o NFS).
List	Lista la configuración del Thin Server.
Modify	Modifica el servidor de archivos maestro (RFS o NFS).
Set	Establece los parámetros del Thin Server.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxiii.

Add

Utilice el mandato **add** para añadir la configuración de un servidor de archivos maestro.

Si selecciona *nfs* como tipo de servidor de archivos maestro, el Thin Server utilizará NFS para comunicar con el servidor de archivos maestro y sincronizar archivos y las NS se pueden comunicar con el Thin Server mediante TFTP o NFS. Si selecciona *rfs* como tipo de servidor maestro, el Thin Server utilizará RFS para comunicar con el servidor de archivos maestro y sincronizar archivos y las NS se pueden comunicar con el Thin Server mediante TFTP o RFS.

Sintaxis:

add master-file-server nfs-s390
nfs-nt
nfs-aix
nfs-other
rfs-as400

nfs-s390 Se utiliza cuando TSF se conecta a un S/390®.

File Server IP address
Especifica la dirección IP del servidor de archivos maestro.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

Secondary File Server IP address
Especifica la dirección IP de un servidor de archivos maestro de reserva. Consulte el apartado “Actualizaciones de antememorias de archivos” en la página 635 para obtener más información. Consulte el mandato **set selection** para obtener una descripción de cómo se utiliza este parámetro.

Nota: No puede establecerse como 0.0.0.0 si el mandato **set selection** especifica secundario o automática.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

Master Server Refresh Retry Limit
Especifica el número de veces que TSF intentará conectarse con el servidor de archivos maestro antes de declararlo inaccesible.

Rango: de 1 a 20

Valor por omisión: 10

tftp packet timeout

Valores válidos: de 5 a 10 segundos

Valor por omisión: 5

tftp maximum retry limit

Valores válidos: de 1 a 10

Valor por omisión: 1

maximum segment size
Especifica el tamaño máximo de segmentos de paquetes.

Valores válidos: 512, 1024, 2048, 4096, 8192 (bytes)

Valor por omisión: 8192

additional Include subdirectories
Especifica si deben añadirse subdirectorios Include adicionales. Se pueden especificar subdirectorios adicionales si TSF necesita guardar en antememoria archivos que no se encuentran en los directorios por omisión.

Valores válidos: yes o no

Valor por omisión: yes

additional Include subdirectory path
Especifica la vía de acceso del subdirectorio Include que se debe añadir.

Valores válidos: a-z, A-Z, 0-9, ., _, —, /

Valor por omisión: ninguno

include all subdirectories under this directory
Especifica si se incluirán todos los subdirectorios anidados de la vía de acceso del subdirectorio adicional especificado.

Valores válidos:

- No

  TSF precargará todos los archivos del directorio especificado.

- Yes

  TSF no precargará ningún archivo del directorio especificado. TSF cargará, en cambio, archivos del directorio y de cualquiera de sus subdirectorios, según convenga.

Valor por omisión: no

nfs-nt Se utiliza cuando TSF se conectada a Windows NT.

File Server IP address
Especifica la dirección IP del servidor de archivos maestro.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

Secondary File Server IP address
Especifica la dirección IP de un servidor de archivos maestro de reserva. Consulte el apartado “Actualizaciones de antememorias de archivos” en la página 635 para obtener más información. Consulte el mandato **set selection** para obtener una descripción de cómo se utiliza este parámetro.

Nota: No puede establecerse como 0.0.0.0 si el mandato **set selection** especifica secundario o automática.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

Master Server Refresh Retry Limit
Especifica el número de veces que TSF intentará conectarse con el servidor de archivos maestro antes de declararlo inaccesible.

Rango: de 1 a 20

Valor por omisión: 10

tftp packet timeout

Valores válidos: de 5 a 10 segundos

Valor por omisión: 5

tftp max retry limit

Valores válidos: de 1 a 10

Valor por omisión: 1

maximum segment size
Especifica el tamaño máximo de segmentos de paquetes.

Valores válidos: 512, 1024, 2048, 4096, 8192 (bytes)

Valor por omisión: 8192

additional Include subdirectories
Especifica si deben añadirse subdirectorios Include adicionales.

Valores válidos: yes o no

Valor por omisión: yes

additional Include subdirectory path
Especifica la vía de acceso del subdirectorio Include que se debe añadir.

Valores válidos: a-z, A-Z, 0-9, ., _, —, /

Valor por omisión: ninguno

include all subdirectories under this directory
Especifica si se incluirán todos los subdirectorios anidados de la vía de acceso del subdirectorio adicional especificado.

Valores válidos:

- No

  TSF precargará todos los archivos del directorio especificado.

- Yes

  TSF no precargará ningún archivo del directorio especificado. TSF cargará, en cambio, archivos del directorio y de cualquiera de sus subdirectorios, según convenga.

Valor por omisión: no

nfs-aix Se utiliza cuando TSF se conecta a AIX®.

File Server IP address
Especifica la dirección IP del servidor de archivos maestro.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

Secondary File Server IP address
Especifica la dirección IP de un servidor de archivos maestro de reserva. Consulte el apartado “Actualizaciones de antememorias de archivos” en la página 635 para obtener más información. Consulte el mandato **set selection** para obtener una descripción de cómo se utiliza este parámetro.

Nota: No puede establecerse como 0.0.0.0 si el mandato **set selection** especifica secundario o automática.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

Master Server Refresh Retry Limit
Especifica el número de veces que TSF intentará conectarse con el servidor de archivos maestro antes de declararlo inaccesible.

Rango: de 1 a 20

Valor por omisión: 10

tftp packet timeout

Valores válidos: de 5 a 10 segundos

Valor por omisión: 5

tftp maximum retry limit

Valores válidos: de 1 a 10

Valor por omisión: 1

maximum segment size
Especifica el tamaño máximo de segmentos de paquetes.

Valores válidos: 512, 1024, 2048, 4096, 8192 (bytes)

Valor por omisión: 8192

additional Include subdirectories
Especifica si deben añadirse subdirectorios Include adicionales.

Valores válidos: yes o no

Valor por omisión: yes

additional Include subdirectory path
Especifica la vía de acceso del subdirectorio Include que se debe añadir.

Valores válidos: a-z, A-Z, 0-9, ., _, —, /

Valor por omisión: ninguno

include all subdirectories under this directory
Especifica si se incluirán todos los subdirectorios anidados de la vía de acceso del subdirectorio adicional especificado.

Valores válidos:

- No

  TSF precargará todos los archivos del directorio especificado.

- Yes

  TSF no precargará ningún archivo del directorio especificado. TSF cargará, en cambio, archivos del directorio y de cualquiera de sus subdirectorios, según convenga.

Valor por omisión: no

nfs-other Se utiliza cuando se desean designar manualmente todos los subdirectorios.

File Server IP address
Especifica la dirección IP del servidor de archivos maestro.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

Secondary File Server IP address
Especifica la dirección IP de un servidor de archivos maestro de reserva. Consulte el apartado “Actualizaciones de antememorias de archivos” en la página 635 para obtener más información. Consulte el mandato **set selection** para obtener una descripción de cómo se utiliza este parámetro.

Nota: No puede establecerse como 0.0.0.0 si el mandato **set selection** especifica secundario o automática.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

Master Server Refresh Retry Limit
Especifica el número de veces que TSF intentará conectarse con el servidor de archivos maestro antes de declararlo inaccesible.

Rango: de 1 a 20

Valor por omisión: 10

tftp packet timeout

Valores válidos: de 5 a 10 segundos

Valor por omisión: 5

tftp maximum retry limit

Valores válidos: de 1 a 10

Valor por omisión: 1

maximum segment size
Especifica el tamaño máximo de segmentos de paquetes.

Valores válidos: 512, 1024, 2048, 4096, 8192 (bytes)

Valor por omisión: 8192

additional Include subdirectories
Especifica si deben añadirse subdirectorios Include adicionales.

Valores válidos: yes o no

Valor por omisión: yes

additional Include subdirectory path
Especifica la vía de acceso del subdirectorio Include que se debe añadir.

Valores válidos: a-z, A-Z, 0-9, ., _, —, /

Valor por omisión: ninguno

include all subdirectories under this directory
Especifica si se incluirán todos los subdirectorios anidados de la vía de acceso del subdirectorio adicional especificado.

Valores válidos:

- No

  TSF precargará todos los archivos del directorio especificado.

- Yes

  TSF no precargará ningún archivo del directorio especificado. TSF cargará, en cambio, archivos del directorio y de cualquiera de sus subdirectorios, según convenga.

Valor por omisión: no

rfs-as400 Se utiliza cuando TSF se conecta a un AS/400.

File Server IP address
Especifica la dirección IP del servidor de archivos maestro.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

Secondary File Server IP address
Especifica la dirección IP de un servidor de archivos maestro de reserva. Consulte el apartado “Actualizaciones de antememorias de archivos” en la página 635 para obtener más información. Consulte el mandato **set selection** para obtener una descripción de cómo se utiliza este parámetro.

Nota: No puede establecerse como 0.0.0.0 si el mandato **set selection** especifica secundario o automática.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

Master Server Refresh Retry Limit
Especifica el número de veces que TSF intentará conectarse con el servidor de archivos maestro antes de declararlo inaccesible.

Rango: de 1 a 20

Valor por omisión: 10

tftp packet timeout

Valores válidos: de 5 a 10 segundos

Valor por omisión: 5

tftp maximum retry limit

Valores válidos: de 1 a 10

Valor por omisión: 1

maximum segment size
Especifica el tamaño máximo de segmentos de paquetes.

Valores válidos: 512, 1024, 2048, 4096, 8192 (bytes)

Valor por omisión: 8192

pre-load file name
Especifica el nombre y la vía de acceso del archivo de precarga.

Valores válidos: a-z, A-Z, 0-9, ., _, —, /

Valor por omisión:
/QIBM/ProdData/OS400/NetStationRmtController/LoadList.file

Ejemplo: para NFS

```
Thin server config> add master-file-server nfs-nt
 File Server IP address [0.0.0.0]? 10.22.55.94
 Secondary File Server IP address [0.0.0.0]? 10.22.55.96

 Master Server Refresh Retry Limit (1-20) [10]?

TFTP Packet Timeout in seconds (5 - 10) ][5]?

 TFTP Max Retry Limit (1 - 10) [1]?

 TFTP Max Segment Size in bytes (valid values are 512, 1024, 2048, 4096, 8192) [8192]?

Default Include Directories:

  Include Directory List Follows:

  Include
    all
  Subdirs?   Directory Names
    --------   ----------------------------------
       N       /netstation/prodbase
       Y       /netstation/prodbase/mods
       Y       /netstation/prodbase/nls
       Y       /netstation/prodbase/fonts
       Y       /netstation/prodbase/java
       Y       /netstation/prodbase/keyboards
       Y       /netstation/prodbase/proms
       Y       /netstation/prodbase/X11
       Y       /netstation/prodbase/configs
       Y       /netstation/prodbase/SysDef
       Y       /netstation/prodbase/zoneinfo

   Do you want additional Include Subdirectories (Y)es (N)o [N]? y

Include Subdirectory [   ]? /netstation/prodbase/another
Include all subdirectories under this directory (Y)es or (N)o [N]?

Do you want additional Include Subdirectories (Y)es (N)o [N]?
```

Ejemplo: para RFS

```
Thin server config> add master-file-server rfs
 File Server IP address [0.0.0.0]? 192.9.225.21
 Secondary File Server IP address [0.0.0.0]? 192.9.225.20
 Master Server Refresh Retry Limit (1-20) [10]?
TFTP Packet Timeout in seconds (5 - 10) [5]?
 TFTP Max Retry Limit (1-10) [1]?
 TFTP Max Segment Size in bytes (valid values are 512, 1024, 2048, 4096, 8192) ][8192]?

 Pre-Load File name
 [/QIBM/ProdData/OS400/NetStationRmtController/LoadList.file]?
```

Delete

Utilice el mandato **delete** para eliminar la configuración de un servidor de archivos maestro.

Sintaxis:

delete master-file-server nfs
rfs

nfs Se utiliza cuando alguno de los servidores de archivos maestro NFS está configurado.

rfs Se utiliza cuando TSF está configurada para el servidor de archivos maestro RFS.

List

Utilice el mandato **list** para visualizar la configuración de TSF.

Sintaxis:

list all

Ejemplo: para NFS

```
Thin server config> list all

Thin Server Feature configuration:

     Mode:                          ENABLED
     Master File Server Selection: PRIMARY
     Interval to refresh cache in day(s): 1
     Time of day (military time) to refresh cache: 0100
     Megabytes used for Thin Server RAM cache: 16
     Use Hard File: YES


Master Thin Server list:
     Server IP Address: 192.9.221.21
     Secondary Server IP Address: 192.9.225.20
     Server Protocol: NFS

     Master Server Refresh Retry Limit value: 10
     TFTP Packet Timeout value: 5
     TFTP Maximum Retry Limit value: 6
     TFTP Maximum Segment Size value: 512

     Initial directories setup for server type: NFS-AIX

 NFS Include Directory List follows:

  Include
    all
     subdirs?    Directory Names
     --------    ---------------------------------------

     N       /usr/netstation
     Y       /usr/netstation/mods
     Y       /usr/netstation/nls
     Y       /usr/netstation/fonts
     Y       /usr/netstation/java
     Y       /usr/netstation/keyboards
     Y       /usr/netstation/proms
     Y       /usr/netstation/X11
     Y       /usr/netstation/configs
     Y       /usr/netstation/SysDef
     Y       /usr/netstation/zoneinfo
```

Ejemplo: para RFS

```
Thin server config> list all

Thin Server Feature configuration:

     Mode:                          DISCONNECTED
     Master File Server Selection: PRIMARY
     Interval to refresh cache in day(s): 1
     Time of day (military time) to refresh cache: 0100
     Megabytes used for Thin Server RAM cache: 16
     Use Hard File: YES


Master Thin Server list:
     Server IP Address: 192.9.221.21
     Secondary Server IP Address: 192.9.225.20
     Server Protocol: RFS

     Master Server Refresh Retry Limit value: 10
     TFTP Packet Timeout value: 5
     TFTP Maximum Retry Limit value: 1
     TFTP Maximum Segment Size value: 8192

 Protocol RFS List:
     Pre-load File:  /QIBM/ProdData/OS400/NetStationRmtcontroller/Loadlist.file
```

Modify

Utilice el mandato **modify** para modificar la configuración de un servidor de archivos maestro.

Sintaxis:

modify master-file-server nfs
rfs

nfs Se utiliza cuando alguno de los servidores de archivos maestro NFS se ha configurado.

rfs Se utiliza cuando TSF está configurada para el servidor de archivos maestro RFS.

Ejemplo: para NFS

```
Thin server config> modify master-file-server nfs
File Server IP address [1.1.1.1]?
Secondary File Server IP address [1.1.1.2]?

Master Server Refresh Retry Limit (1 - 20) [10]?

TFTP Packet timeout in seconds (5 - 10) [5]?

TFTP Max retry limit value (1 - 10) [1]?

TFTP Max Segment Size in bytes (valid values are 512, 1024, 2048, 4096, 8192) [8192]?
Include directory /netstation/prodbase, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [N]?
Include directory /netstation/prodbase/mods, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?
Include directory /netstation/prodbase/nls, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?
Include directory /netstation/prodbase/fonts, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?
Include directory /netstation/prodbase/java, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?
Include directory /netstation/prodbase/keyboards, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?
Include directory /netstation/prodbase/proms, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?
Include directory /netstation/prodbase/X11, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?
Include directory /netstation/prodbase/configs, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?
Include directory /netstation/prodbase/SysDef, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?
Include directory /netstation/prodbase/zoneinfo, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?

Do you want additional Include Subdirectories (Y)es (N)o [N]?
Thin server config>
```

Ejemplo: para RFS

```
Thin server config> modify master-file-server rfs
File Server IP address [192.9.225.21]? 192.9.225.23
Secondary File Server IP address [192.9.225.20]? 192.9.225.22
Master Server Refresh Retry Limit (1-20) [10]? 8
TFTP Packet Timeout in seconds (5-10) [5]? 7
TFTP Max Retry Limit (1-10) [1]? 15
TFTP Max Segment Size in bytes (valid values are 512, 1024, 2048, 4096, 8192) [8192]? 4096

 Pre-Load File name [/QIBM/ProdData/OS400/NetStationRmtController/LoadList.file]?
```

Set

Utilice el mandato **set** para establecer los parámetros de configuración de TSF.

Sintaxis:

set
- mode
- selection
- interval-pre-load-list
- time-to-refresh-pre-load-list
- memory-cache
- hard-file

mode Especifica la modalidad de TSF.

Valores válidos:

enable Indica que TSF es totalmente funcional y que servirá archivos guardados en la antememoria a las Network Stations.

disable Indica que TSF no está activa y que no responderá a ninguna Network Station. Las Network Stations deben estar configuradas para comunicar directamente con el servidor.

passthru La modalidad "passthru" sólo es válida si se utiliza RFS. La modalidad "passthru" permite que la Network Station se ponga en contacto con TSF, pero siempre obtiene los archivos del servidor de archivos maestro.

disconnected Indica que TSF funciona y que servirá archivos guardados en la antememoria a las Network Stations. Sin embargo, el tráfico dirigido al servidor de archivos maestro se minimiza. Consulte el apartado “Protocolos utilizados para comunicar con Network Station” en la página 634 para obtener más detalles.

Valor por omisión: disable

selection Especifica si para renovar la antememoria de TSF, ésta se pondrá en contacto con la dirección IP del servidor de archivos o con la dirección IP del servidor de archivos secundario.

Valores válidos:

primary Indica que cuando TSF intenta renovar la antememoria, sólo utilizará la dirección IP especificada como dirección IP del servidor de archivos. Se hace caso omiso de la dirección IP del servidor de archivos secundario.

secondary Indica que cuando TSF intenta renovar la antememoria, sólo utilizará la dirección IP especificada como dirección IP del servidor de archivos secundario. Se hace caso omiso de la dirección IP del servidor de archivos.

automatic Indica que TSF intentará ponerse en contacto con la dirección IP especificada como dirección IP del servidor de archivos. Si no lo consigue después del número configurado de reintentos, TSF intentará ponerse en contacto con la dirección IP especificada como dirección IP del servidor de archivos secundario. Consulte el apartado “Actualizaciones de antememorias de archivos” en la página 635 para obtener más información.

Valor por omisión: primary

interval-pre-load-list
Indica el intervalo (en días) que tardará TSF en renovar la lista de precarga de la antememoria.

Valores válidos: de 00 a 365

Valor por omisión: 01

time-to-refresh-pre-load-list

Indica la hora del día (en formato de 24 horas) en que se renovarán los archivos almacenados en la antememoria.

Valores válidos: de 0001 a 2400

Valor por omisión: 0100

memory-cache

Especifica la cantidad de memoria en megabytes de la antememoria RAM del Thin Server. Cuando se utiliza un disco fijo, se debe elegir este valor para equilibrar el rendimiento de TSF con otras funciones del IBM 2212. Cuando no se utiliza un disco fijo, dicho valor debe ser lo suficientemente grande para contener todos los archivos guardados en memoria. Si desea obtener más información, consulte “Recomendaciones de configuración” en la página 637.

Valores válidos: de 8 a 64 Megabytes

Valor por omisión: 16

hard-file Especifica si se debe utilizar o no el disco fijo.

Valores válidos: yes o no

Valor por omisión: yes

Ejemplo:

```
Thin server config> set mode passthru
This server feature (TSF) is passthru
Thin server config> set interval-pre-load-list
Interval to refresh the Pre-Load list in days (00-365) [01]? 1
Thin server config> set time-to-refresh-pre-load-list
Time of day to refresh cache in military time (0001-2400) [0100] 0800
Thin server config> set memory-cache
Amount of memory in megabytes for Thin Server RAM cache (8-64MB) [8]
Thin server config> set hard-file
Use the Hard File  (Y)ex N(o) [Y]? yes
```

Acceso al entorno de supervisión de TSF

Utilice el procedimiento siguiente para acceder a los mandatos de supervisión de TSF. Este proceso le proporciona acceso al proceso de *supervisión* de TSF.

1. Entre **talk 5** en el indicador OPCON. (Si desea obtener más información sobre este mandato, consulte *The OPCON Process and Commands* en la publicación Access Integration Services Guía del usuario de software.) Por ejemplo:

   ```
   * talk 5
   +
   ```

   Después de entrar el mandato **talk 5**, el indicador GWCON (+) aparece en el terminal. Si el indicador no aparece cuando se entra por primera vez en la configuración, pulse **Intro** de nuevo.

2. Entre el mandato **f tsf** en el indicador + para acceder al indicador `Thin-Server>`.

   Ejemplo:

   ```
   + f tsf
   Thin-Server>
   ```

Mandatos de supervisión de TSF

En este apartado se describen los mandatos de supervisión de TSF.

Tabla 63. Resumen de mandatos de supervisión de TSF

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 xxxii.
Delete	Suprime un archivo de la antememoria de archivos de la función Thin Server.
Flush	Vacía la antememoria de archivos de la función Thin Server.
List	Visualiza la configuración y los valores del Thin Server.
Refresh	Renueva la antememoria.
Reset	Restablece los contadores.
Restart	Reinicia el proceso del Thin Server.
Set	Cambia los valores de la función Thin Server.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiii.

Delete

Utilice el mandato **delete** para eliminar un archivo de la antememoria de archivos de la función Thin Server.

Sintaxis:

d**elete** *nombre_archivo*

nombre_archivo

Especifica el nombre del archivo que se debe eliminar de la antememoria de archivos.

Valores válidos:

Valor por omisión: ninguno

Ejemplo:

```
Thin-Server> delete
Enter filename to delete from the File Cache: /ibm/prod/ns/5494.dat
Are you sure that you want to delete this file? (Y/ [N]): y
File successfully deleted
```

Flush

Utilice el mandato **flush** para vaciar la memoria de TSF y el espacio de antememoria del disco duro. El mandato **flush** borrará todos los archivos guardados en la antememoria. La antememoria del Thin Server se actualizará en la próxima renovación a partir del servidor maestro. Las Network Stations pueden experimentar retrasos hasta que la renovación se complete.

Sintaxis:

f**lush**

Ejemplo:

```
Thin-Server> flush
The FLUSH command will erase all cached files.
  The Thin Server cache will be updated on the next refresh
  from the Master Server.  Network Stations may experience
  delays until the refresh is completed.
Are you sure you really want to do this? (Y/ [N]: y
All Thin Server cached files have been flushed
```

List

Utilice el mandato **list** para visualizar los valores de los parámetros de TSF.

Sintaxis:

list cached-files
config
file-access-counters
file-refresh-counters
pre-load-list
tftp-counters
ts-counters

Ejemplo:

```
Thin-Server> list cached-files

Cached
File Name     File Size  Time Stamp         Flags  Host File Name
------------  ---------  -----------------  -----  -----------------
00000026.DAT      2729   04/08/98 13:35:07   RYY   /QIBM/ProdData/OS400/Netstat
ionRmtController/Loadlist.file
00000002.DAT   2049220   09/16/97 08:55:39   RYU   /QIBM/PRODDATA/NETWORKSTATIO
N/KERNEL
                 10060   03/04/97 16:12:44   RY-   /QIBM/PRODDATA/NETWORKSTATIO
N/FONTS/PCF/MISC/7X14B.PCF
    List is Complete
```

Los identificadores tienen el siguiente significado:

- WhereFrom
  - R = Cliente RFS
  - N = Cliente NFS
  - - = Ninguno
- InTable
  - - = No en tabla
  - u (o m) = A punto de actualizarse
  - Y = En tabla
- FileState
  - - = No en disco
  - D = Sucio
  - A = Actualización cancelada anormalmente
  - u = A punto de actualizarse

- U = Actualización en proceso
- Y = En el disco y disponible

Las combinaciones habituales de los dos últimos identificadores (se muestran los tres identificadores para que resulte más claro) son:

- RYY - archivo bueno
- RuY - renovación completa en proceso, este archivo no se ha verificado todavía
- RYU - este archivo se está actualizando

Ejemplo de RFS

```
Thin-Server> list config
Thin Server Configuration
  Thin Server feature mode is:                        Disconnected
  Thin Server feature state is:                       Active, all files up-to-date
  Interval to refresh Pre-Load List (#days):          1
  Time of day (Military) to refresh Pre-Load List:    01:00:00
  Memory (KB) currently using for RAM cache:          16384
  Maximum memory (KB) configured for RAM cache:       16384
  Currently using Hard File?:                         Yes
  Hard File storage defined for Thin Server:          817664
  Hard File storage being used for Thin Server:       27328
  Number of Files Cached:                             82
  Master Server IP address:                           192.9.225.21
  Secondary Master Server IP address:                 192.9.225.20
  Master Server Retry Limit:                          10
  Master Server Selection:                            primary
  TFTP Packet Timeout Value:                          5
  TFTP Max Retries:                                   1
  TFTP Max Segment Size:                              8192

  Thin Server Sync Protocol:                          RFS
  Name of Pre-Load List file:
      /QIBM/ProdData/OS400/NetstationRmtController/Loadlist.file
Thin Server>
```

Ejemplo de NFS

```
Thin-Server> list config

Thin Server Configuration
  Thin Server feature is:                          Enabled
  Thin Server Feature state is:                    Active, initializing file structure
  Interval to refresh Pre-Load List (#days):       1
  Time of day (Military) to refresh Pre-Load List: 01:00:00
  Memory (KB) currently using for RAM cache:       25600
  Maximum memory (KB) configured for RAM cache:    25600
  Currently using Hard File?:                      Yes
  Hard File storage defined for Thin Server:       915424
  Hard File storage being used for Thin Server:    27328
  Number of Files Cached:                          82
  Master Server IP address:                        192.9.225.21
  Secondary Master Server IP address:              192.9.225.20
  Master Server Retry Limit:                       10
  Master Server Selection:                         primary
  TFTP Packet Timeout Value:                       5
  TFTP Max Retries:                                1
  TFTP Max Segment Size:                           8192

  Thin Server Sync Protocol:                       NFS
  Include Directory List Follows:

  Include
    all
  Subdirs?   Directory Names
  --------   -----------------------------------
     N       /usr/netstation
     Y       /usr/netstation/mods
     Y       /usr/netstation/nls
     Y       /usr/netstation/fonts
     Y       /usr/netstation/java
     Y       /usr/netstation/keyboards
     Y       /usr/netstation/proms
     Y       /usr/netstation/X11
     Y       /usr/netstation/configs
     Y       /usr/netstation/SysDef
     Y       /usr/netstation/zoneinfo
Thin Server>
```

Ejemplo:

```
Thin-Server> list file-access-counters

Disk Statistics/Counters:
    Number of files currently open:               20
    Number of Total File Opens:                   23
    Number of Open Fails when File is Locked:      1
    Number of Read misses - Version Mismatch:      4
    Number of Read misses - File Not Present:      3
    Number of Write misses - Hard File Full:       4
```

Ejemplo:

```
Thin-Server> list file-refresh-counters

File Refresh Statistics/Counters
    Last Successful refresh Master Server IP address:  192.9.225.20
    Current refresh Master Server IP address:          192.9.225.21
    Number of Files Updated during last refresh:       0
    Number of Update Failures during last refresh:     0
    Number of Refreshes:                               0
    Number of Refresh Failures:                        1
    Number of Refreshes - Primary Master Server:       0
    Number of Refresh Failures - Primary Server:       0
    Number of Refreshes - Secondary Master Server:     0
    Number of Refresh Failures - Secondary Server:     0
    Number of Files Refreshed:                         249
    Date/Time of Last File Update:                     02/17/1999 01:00:36
    Date/Time of Last File Download:                   02/16/1999 15:57:05

Thin Server>
```

Ejemplo:

```
Thin-Server> list pre-load-list
 <display of pre-load list raw file>
List of Pre-Load List File is Complete
```

Ejemplo:

```
Thin-Server> list tftp-counters

TFTP Server Statistics/Counters
    Relay to Master File Server:                          Available
    Number of Total TFTP Requests:                         3
    Number of Current TFTP Requests:                       2
    Number of Files Served:                               22
    Number of Files Served by Master Server:              22
    Number of Files Served by Primary Master Server:      22
    Number of Files Served by Secondary Master Server:     0

Thin Server>
```

Ejemplo de RFS

```
Thin-Server> list ts-counters

Thin Server Statistics/Counters
    Relay to Master File Server:                        Available
    Number of Total RFS Clients:                        0
    Number of Current RFS Clients:                      0
    Number of Files Served:                             0
    Number of Files Served by Master Server:            0
    Number of NS Port Mapper socket accepts:            0
    Number of NS Port Mapper sockets currently active/open: 0
    Number of NS Server socket accepts:                 0
    Number of NS 8473 sockets currently active/open:    0
    Number of NS Login sock accepts:                    0
    Number of NS 8476 sockets currently active/open:    0
    Number of RFS writes to a Thin Server cached file:  0
Thin Server>
```

Ejemplo de NFS

```
Thin-Server> list ts-counters

Thin Server Statistics/Counters
    Number of NFS Server Reads:                          13
    Number of NFS Server Read Directories:                8
    Number of Unsupported NFS Requests:                   2
    Number of total NFS Mounts:                          22
    Number of current NFS Mounts:                         7
    Number of total NFS clients:                         15
    Number of current NFS Clients:                        4
```

Refresh

Utilice el mandato **refresh** para forzar una renovación de la antememoria.

Sintaxis:

ref**resh**

Ejemplo:

```
Thin-Server> refresh

Force a refresh of the cache (Y/N) [N]? y

Thin Server cache has been refreshed
```

Reset

Utilice el mandato **reset** para restablecer dinámicamente contadores.

Sintaxis:

res**et** all | file-access-counters | file-refresh | tftp-counters | ts-counters

Ejemplo:

```
Thin-Server> reset all

All Thin Server feature counters have been reset
```

Restart

Utilice el mandato **restart** para reiniciar el proceso de TSF.

Sintaxis:

rest**art**

Ejemplo:

```
Thin-Server> restart

Restart Thin Server? (Y/ [N]): y

Thin Server has been restarted
```

Set

Utilice el mandato **set** para establecer la modalidad de antememoria de TSF.

Sintaxis:

s**et** mode

mode Especifica la modalidad de TSF. Consulte “Set” en la página 656.

Valores válidos:

- enable
- disable
- passthru
- disconnected

Ejemplo:

```
Thin-Server> set mode disconnected

Thin Server caching is now disconnected
```

Soporte de reconfiguración dinámica de TSF

En este apartado se describe la reconfiguración dinámica (DR) y cómo afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

TSF no da soporte al mandato **delete interface** de CONFIG (Talk 6).

Mandato activate interface de GWCON (Talk 5)

El mandato **activate interface** de GWCON (Talk 5) no es aplicable a TSF. Activar una interfaz no afecta directamente al Thin Server; sin embargo, sí que puede afectar a las conexiones con el cliente o con el servidor de archivos maestro.

Mandato reset interface de GWCON (Talk 5)

El mandato **reset interface** de GWCON (Talk 5) no es aplicable a TSF. Restablecer una interfaz no afecta directamente al Thin Server; sin embargo, sí que puede afectar a las conexiones con el cliente o con el servidor de archivos maestro.

Mandatos de restablecimiento de componente de GWCON (Talk 5)

La función Thin Server da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos de TSF:

Mandato GWCON, feature TSF, restart

Descripción: Reinicia el Thin Server.

Efecto en la red: Durante el reinicio, los clientes no pueden acceder al Thin Server para obtener archivos.

Limitaciones:

No se recomienda modificar el tipo de servidor de archivos maestro (de rfs a nfs, o viceversa). Si se hiciera, afectará a la cantidad de memoria disponible como antememoria de archivos y podría producirse una anomalía durante el proceso de reinicio si no hay suficiente memoria.

Todos los cambios en la configuración de TSF se activan automáticamente, excepto estos:

Mandatos cuyos cambios no se activan al ejecutar el mandato GWCON, feature tsf, restart
CONFIG, feature tsf, set memory-cache

Mandatos de cambio temporal de GWCON (Talk 5)

TSF da soporte a los siguientes mandatos de GWCON que cambian temporalmente el estado operativo del dispositivo. Estos cambios se perderán si el dispositivo se reinicia, si se vuelve a cargar, o si se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
GWCON, feature tsf, set mode **Nota:** Se cambia la modalidad de la función thin server.

Mandatos no reconfigurables dinámicamente

La tabla siguientes describe los mandatos de configuración de TSF que no pueden modificarse dinámicamente. Para activarlos es necesario reiniciar o volver a cargar el dispositivo.

Mandatos
CONFIG, feature tsf, set memory-cache **Nota:** Si se va a aumentar la cantidad de antememoria especificada, para que el cambio surta efecto hay que reiniciar o volver a cargar el direccionador.
CONFIG, feature tsf, set mode **Nota:** Si la modalidad del Thin Server era inhabilitada cuando el direccionador se reinició o se volvió a cargar, hay que reiniciar o volver a cargar el direccionador después de cambiar la modalidad del Thin Server a habilitada. La modalidad del Thin Server se establece al valor por omisión de inhabilitada la primera vez que se carga el paquete Thin Server.

Configuración y supervisión de VCRM

El gestor de recursos de circuito virtual (VCRM) es una función que da soporte al protocolo de reserva de recursos (RSVP), el cual se describe en " Utilización de RSVP" y en "Configuración y supervisión de RSVP" en la publicación *Configuración y supervisión de protocolos - Manual de consulta, volumen 1*. A partir de la petición de reserva de RSVP, VCRM crea la conexión del flujo de datos en la interfaz física. Para llevar a cabo esto, VCRM debe determinar en primer lugar si existe suficiente ancho de banda para dar cabida a la reserva.

Nota: Si está utilizando interfaces WAN, como pueden ser Frame Relay o X.25, es necesario que establezca una velocidad de línea para que VCRM sepa cuánto ancho de banda hay disponible. El procedimiento para establecer la velocidad de línea se describe en los capítulos de configuración y de supervisión de las interfaces Frame Relay y X.25 de la publicación *Access Integration Services Guía del usuario de software*.

Si la interfaz es un enlace PPP, una LAN o una WAN, VCRM pone en colas por software los paquetes QoS y los paquetes optimizados para dar prioridad a los paquetes del enlace de salida.

Este capítulo consta de los apartados siguientes:

- "Acceso al entorno de configuración de VCRM"
- "Acceso al entorno de supervisión de VCRM"
- "Mandatos de supervisión de VCRM" en la página 668

Acceso al entorno de configuración de VCRM

Para acceder al entorno de configuración de VCRM, entre el mandato siguiente en el indicador `Config>`:

```
Config> feature vcrm
VC & Resource Management config console
  --Currently no configurable objects.
Config>
```

El propósito del mensaje que se visualiza es indicar que VCRM no se puede configurar de manera independiente. Al habilitar RSVP, se habilita VCRM, que obtiene sus parámetros de la configuración de RSVP.

Acceso al entorno de supervisión de VCRM

Para acceder al entorno de supervisión de VCRM, escriba

```
* t 5
```

A continuación, entre el mandato siguiente en el indicador **+**:

```
+ feature VCRM
VCRM console
VCRM Console>
```

Aparece el indicador `VCRM Console>`.

Mandatos de supervisión de VCRM

En este apartado se describen los mandatos de supervisión de VCRM. Entre estos mandatos en el indicador `VCRM Console>`.

Tabla 64. 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 xxxii.
Clear	Restablece las estadísticas sobre colas.
Queue	Muestra las estadísticas de las colas por software.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiii.

Clear

Utilice el mandato **clear** para restablecer las estadísticas de la cola por software.

Sintaxis:

c**lear**

Consulte el mandato **queue** para ver un ejemplo del mandato **clear**.

Queue

Utilice el mandato **queue** para mostrar las colas por software de los flujos de tráfico .

Sintaxis:

q**ueue**

La lista siguiente define los términos que se utilizan en la visualización de las colas por software :

Quota
La cantidad de ancho de banda reservado. En un principio, optimizado (B.E.) dispone de todas las cuotas. Cuando se lleva a cabo una reserva, el ancho de banda (b/w) reservado se desplaza de la cuota B.E. a la cuota QoS.

Max-q
Longitud máxima de la cola, especificada en paquetes.

Curr-q
Longitud actual de la cola, especificada en paquetes.

In quota
Paquetes o kilobytes enviados dentro del ancho de banda asignado.

Outside quota
Paquetes o kilobytes enviados que superan el ancho de banda asignado, cuando no había ancho de banda desocupado disponible.

Packets/bytes dropped
Paquetes o bytes descartados por las colas por software.

DLC packets/bytes dropped

Paquetes o bytes descartados por DLC después de que los paquetes hayan pasado por la cola por 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>
```

Utilización de la función de voz

En este capítulo se describen las capacidades, los adaptadores soportados y las opciones de configuración de voz del 2212.

Este capítulo consta de los apartados siguientes:

Visión general del adaptador de voz

El 2212 puede dar soporte a un máximo de cuatro adaptadores de voz. Cada adaptador tiene dos interfaces de voz. Se da soporte a los adaptadores siguientes:

- Adaptador CPCI de voz y fax FXS analógico de dos puertos
- Adaptador CPCI de voz y fax FXO analógico de dos puertos
- Adaptados CPCI de voz y fax E&M analógico de dos puertos

Estos adaptadores permiten conectarse con una centralita telefónica privada (PBX), con un teléfono o con un sistema con teclado. El 2212 da soporte a conexiones de voz sobre Frame Relay (VoFR) con cualquiera de esos adaptadores.

Funciones de voz

El 2212 con un adaptador de voz da soporte a conexiones de voz sobre Frame Relay. Con VoFR se puede configurar el 2212 para comunicarse con un IBM 9783, otro direccionador (de direccionador a direccionador), o entre las interfaces de voz del propio 2212 (direccionamiento de llamadas locales). Con VoFR también se puede configurar el 2212 para reenviar paquetes de voz (no se precisa un adaptador de voz). Para obtener más información sobre el reenvío de voz, consulte el apartado titulado "Voice Forwarding Over Frame Relay" del capítulo "Using Frame Relay Interfaces" de la publicación *MRS Guía del usuario de software*

Conceptos sobre la configuración

Existen 4 grupos principales de parámetros de voz que sirven para configurar las funciones de voz del 2212.

Parámetros de la función de voz Estos parámetros se definen una vez y se aplican a todas las interfaces del 2212. Ejemplos de estos parámetros son los valores del temporizador y del tono, y de las reglas de salida de la compañía telefónica.

Parámetros de la interfaz de voz Estos parámetros son exclusivos de cada interfaz de voz. Entre estos parámetros se incluyen: velocidad del fax, tipo de protocolo del

codificador vocal, valores de ganancia de transmisión y de recepción, etc.

Parámetros de voz sobre Frame Relay Estos parámetros se utilizan para configurar las conexiones de voz sobre Frame Relay (incluyendo las conexiones de direccionador a direccionador, con un IBM 9783 y las de direccionamiento de llamadas locales). Aquí también se definen las reglas de marcación, los planes de proceso de llamada, etc.

Para configuraciones de voz sobre Frame Relay (solamente para conexiones de direccionador a direccionador y con un IBM 9783), o para configuraciones de VoIP que incluyan comunicarse con un IBM 9783, tendrá que configurar Frame Relay en una interfaz. Hallará más información en el capítulo “Configuración y supervisión de interfaces Frame Relay” de la publicación *AIS Guía del usuario de software*.

Información de configuración de la función voz sobre Frame Relay

Para que el 2212 se comunique con la función voz sobre Frame Relay, se deben configurar los puntos siguientes:

- Reglas de proceso de llamada
- Habilitar Frame Relay en la interfaz
- Regla de salida de la compañía telefónica (si se conecta con una PBX o con un sistema con teclado)

Puede definir hasta ocho reglas de proceso de llamada para cada interfaz de voz. Cada regla consta de un conjunto de parámetros de conexión que determina el modo en que se establece una conexión. Para conexiones remotas (es decir, para direccionamiento local de llamadas), la regla de proceso de llamada consta de la información siguiente:

- DLCI de proceso (16 a 1007)
- DLCI de carga útil (16 a 1007)
- Subcanal de proceso (4 a 254)
- Subcanal de carga útil (4 a 254)
- Número de regla de comparación de dígitos de marcación (1 a 64)
- Número de regla de salida de la red (1 a 64)

Nota: Los parámetros de carga útil y de proceso definidos para una interfaz de voz deben corresponderse con los parámetros de carga útil y de proceso definidos para los IBM 9783 que están configurados para comunicarse con esta interfaz de voz (si se utilizan IBM 9783 en la red).

Para el direccionamiento de llamadas locales, la regla de proceso de llamada consta de:

- Número de regla de comparación de dígitos de marcación (1 a 64)
- Número de regla de salida de la red (1 a 64)

La regla de comparación de dígitos de marcación permite especificar el rango de dígitos aceptables en cada posición de una secuencia de dígitos de marcación.

Puede especificar comodines de varios dígitos. así como una secuencia que establezca una conexión inmediata durante una condición de “descolgar”. Puede definir una agrupación de hasta 64 reglas y especificar una reglas de dígitos de marcación en cada regla de proceso de llamada.

La regla de salida de la red le permite especificar el modo en que el número de destino debe aparecer en el paquete Frame Relay de establecimiento de la llamada. Dicha regla consta de una combinación de dígitos de número de destino y constantes.

Las reglas de salida de la compañía telefónica determinan el modo en que los dígitos de marcación se transmiten en la interfaz de la compañía telefónica. Cada regla de la compañía telefónica consta de una combinación de dígitos de marcación de destino, dígitos de números de origen, constantes y pausas. Una regla de salida de la compañía telefónica debe configurarse para marcar de salida mediante pulsos para las interfaces FXO y E&M. Para cada 2212, se pueden definir hasta ocho reglas de salida de la compañía telefónica.

Cuando una interfaz de voz del 2212 realiza una llamada, el número de destino se compara con las reglas de comparación de dígitos de marcación de esa interfaz. Dichas reglas se definen en las reglas de proceso de llamada de esa interfaz. Cuando se da una coincidencia, el DLCI y el subcanal (para las conexiones de direccionador a direccionador y con un IBM 9783) o el número local (para el direccionamiento de llamadas locales) de la regla de comparación determinan el nodo de destino. Si hay que modificar el número de destino, la regla de salida de la red determina el modo en que debe ser modificado.

Cuando un 2212 recibe una llamada, el DLCI y el subcanal, para las conexiones de direccionador a direccionador y con un IBM 9783, o el número local, para el direccionamiento de llamadas locales, determinan cuál es la interfaz de voz que recibirá la llamada. Cada interfaz de voz acepta llamadas de cualquier par de DLCI y subcanal que esté definido en una de sus reglas de proceso de llamada. La regla de salida de la compañía telefónica de la interfaz de voz de destino se utiliza con el número de destino para generar la secuencia de pulsos de marcación de salida, si ésta es necesaria.

Comunicarse con un IBM 9783

La Figura 53 en la página 674 muestra una red en la que dos 2212 están conectados a un IBM 9783. La definición de esta red de voz es un proceso de configuración de dos pasos. El primero consiste en configurar el IBM 9783 para que se comunique con la interfaz de voz del 2212. El segundo, en definir la interfaz de voz del 2212 con la información que corresponda.

Configuración del IBM 9783 para comunicarse con un 2212

Para configurar el IBM 9783 para que se comunique con una interfaz de voz de un 2212, hay que definir un conjunto de parámetros llamado un plan de marcación. El plan de marcación de un IBM 9783 consta de la información siguiente:

- Grupos de circuitos
- Descriptores de circuitos

La Figura 54 en la página 675 muestra la información de direccionamiento necesaria para la comunicación entre las interfaces de voz en 2212A y en 2212B.

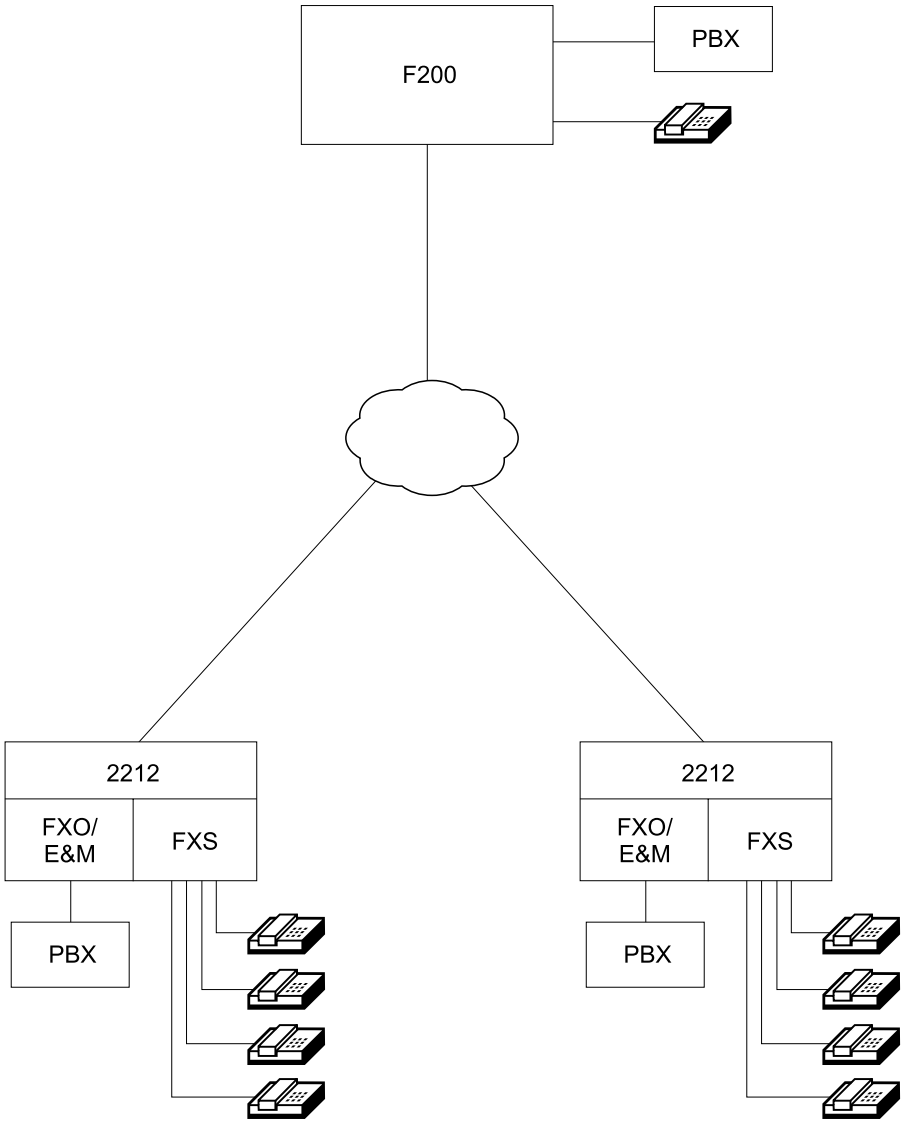


Figura 53. Comunicación entre un IBM 9783 y varias interfaces de voz de 2212

Un grupo de circuitos IBM 9783 define un *tronco de red de voz virtual* entre un IBM 9783 y un nodo remoto. Aunque un grupo de circuitos entre IBM 9783 e IBM 9783 puede contener muchos circuitos individuales, un grupo de circuitos de interfaces de voz entre IBM 9783 y 2212 sólo contiene un circuito (PVC). El grupo de circuitos se conecta con el nodo remoto (la interfaz de voz del IBM 9783 o del 2212). En la Figura 54 en la página 675; el grupo de circuitos 1 se conecta con la interfaz de voz del 2212A que tiene el ID de nodo 1.1.1.5., El grupo de circuitos 2 se conecta con la interfaz de voz del 2212B que tiene el ID de nodo 2.1.1.5., y el grupo de circuitos 3 se conecta con la interfaz de voz del 2212B que tiene el ID de nodo 2.1.1.7. Cada interfaz de voz del 2212, incluso las interfaces del propio 2212, deben tener un ID de nodo exclusivo. Por lo tanto, se debe definir un grupo de circuitos exclusivo en el IBM 9783 para cada interfaz de voz de cada 2212.

Un descriptor de circuitos IBM 9783 define los circuitos individuales dentro de cada grupo de circuitos. En el caso de un grupo de circuitos entre IBM 9783 y IBM 9783, pueden existir varios descriptores de circuitos; uno por cada circuito del grupo. Puesto que un grupo de circuitos de interfaces de voz entre IBM 9783 y 2212 sólo

F200 0.0.0.1 Grupo de circuitos (Plan marcación)

Grupo de circuitos #	Circuito (Descripción)	DLCI	Subcanal
1	Proceso 5	16 16	4 5
2	Proceso 5	17 17	4 5
3	Proceso 7	17 17	6 7

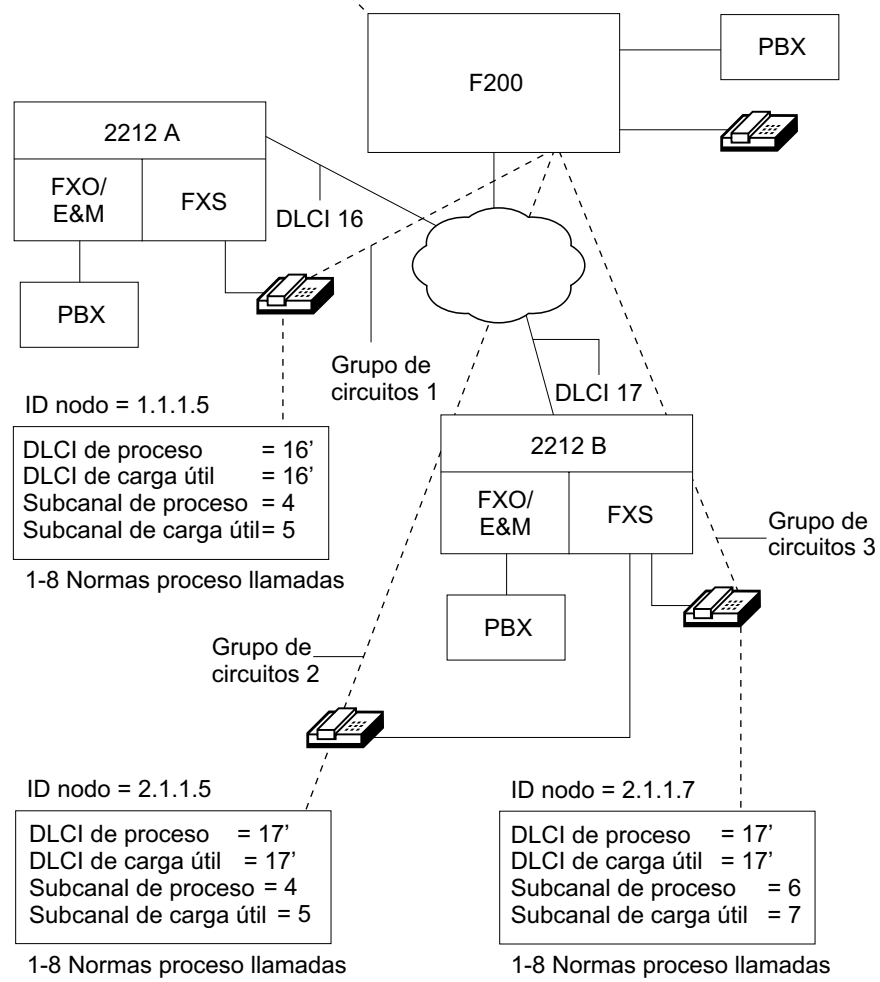


Figura 54. Configuración de la información del proceso de llamada del puerto de voz

contiene un circuito, un grupo de circuitos de interfaces de voz entre IBM 9783 y 2212 sólo contiene un descriptor de circuitos.

Los descriptores de circuitos contienen información tanto del circuito de proceso como del circuito de carga útil. El circuito de proceso se utiliza para transferir paquetes necesarios para establecer la llamada e interrumpirla. Dichos paquetes son los paquetes propietarios CALL SETUP, CONNECT, ANSWER y RELEASE de Nuera. El circuito de carga útil se utiliza para transferir paquetes que contienen los datos reales de voz comprimidos.

En la Figura 54, el IBM 9783 tiene un plan de marcación que contiene tres grupos de circuitos, uno para cada interfaz de voz del 2212 con el que ha de conectarse. Cuando un IBM 9783 recibe una petición para establecer comunicación con un ID de nodo específico, utiliza el grupo de circuitos para localizar el dispositivo de destino. Un grupo de circuitos IBM 9783 consta de la información siguiente:

- El número del grupo de circuitos
- Nodo de conexión (nodo con el que se está conectando)
- Descriptores de circuitos (proceso y carga útil)
  - DLCI (16-991)
  - Subcanales (proceso y carga útil)

Nota: Cuando se define un descriptor de circuitos para un circuito de una interfaz de voz entre IBM 9783 y 2212, el descriptor de circuitos y el número del subcanal de carga útil deben coincidir. El valor mínimo de subcanal que se puede especificar es 4. Todos los grupos de circuitos entre un IBM 9783 y un 2212 pueden utilizar el mismo DLCI.

Configuración de un plan de marcación: Un plan de marcación de un IBM 9783 consta de 1 a 4 reglas de conversión. Dichas reglas controlan el modo en que los dispositivos se conectan y se comunican con el IBM 9783. Cada regla de conversión consta de cierto número de casos ordenados (de 1 a 100). Cada grupo de circuitos IBM 9783 se asocia con una regla de conversión específica. Cada regla de conversión está compuesta de los siguientes elementos:

Regla de comparación de origen Un patrón de comparación de dígitos de marcación para un número de origen

Regla de comparación de destino Un patrón de comparación de dígitos de marcación para un número de destino

Regla de ruta Una lista de grupos de circuitos, subconjuntos de grupos de circuitos o puertos locales.

Regla de salida de origen Una regla para convertir el número de origen durante el establecimiento de la llamada.

Regla de salida de destino Una regla para convertir el número de destino durante el establecimiento de la llamada o durante la transmisión de datos.

Durante el establecimiento de la llamada, los números de origen y destino se comparan con las reglas de comparación correspondientes de cada caso de regla de conversión. Las comparaciones de efectúan en orden ascendente hasta que se encuentra una coincidencia. Cuando se encuentra una coincidencia, la regla de ruta del caso que ha coincidido direcciona la llamada. La regla de salida del caso que ha coincidido modifica la información del establecimiento de la llamada o genera dígitos de marcación.

Configuración de la interfaz de voz del 2212 para comunicarse con el IBM 9783

Para configurar una interfaz de voz de 2212 para que se comunique con un IBM 9783, es necesario definir la información siguiente:

- Reglas de proceso de llamada - hasta ocho reglas para cada interfaz de voz
- ID de nodo - uno por cada interfaz de voz.

Configuración de red sin un IBM 9783

Si sólo es necesario un acceso limitado a la red, se puede establecer comunicación entre dos interfaces de voz sin utilizar un IBM 9783 aplicando los métodos siguientes:

- Comunicación entre interfaces de voz en 2212 diferentes (de direccionador a direccionador).
- Comunicación entre interfaces de voz en el mismo 2212 (direccionamiento de llamadas locales).

Configuraciones de direccionador a direccionador

Si se definen las correspondientes reglas de proceso de llamada para cada interfaz de voz, se pueden efectuar llamadas entre dos interfaces de voz de 2212 diferentes sin utilizar un IBM 9783. Cada una de dichas reglas debe especificar los mismos subcanales de carga útil y de proceso de llamada, así como los DLCI de carga útil y de proceso de llamada correspondientes. Cuando se establece comunicación sin un IBM 9783, el campo de ID de nodo no se utiliza. Si una interfaz de voz se conecta con una PBX o con un sistema de teclado, debe configurarse una regla de salida de compañía telefónica para la interfaz de voz.

Nota: Sin conexión con un IBM 9783, cada interfaz de voz se puede conectar a un máximo de ocho interfaces de voz remotas. Si se habilita el direccionamiento de llamadas locales para una interfaz de voz, esa interfaz de voz se podrá conectar como máximo a siete interfaces de voz.

Direccionamiento de llamadas locales

Se pueden realizar llamadas entre dos interfaces de voz del mismo 2212 sin utilizar un IBM 9783. Esto se puede llevar a cabo configurando una de las ocho reglas de proceso de llamada de cada interfaz para direccionamiento de llamadas locales. El direccionamiento de llamadas locales compara el número de destino con el número local configurado para las interfaces de voz para las que se ha definido una regla de llamada local. Se puede especificar el número de los dígitos iniciales que se deben comparar en el número local de cada interfaz.

La regla de salida de la red, especificada en una regla de llamada local, debe especificar los dígitos del número de destino necesarios para direccionar de manera correcta la llamada.

Ya que la interfaz de voz de origen y de destino se encuentran en el mismo 2212, una regla de direccionamiento de llamadas locales no contiene información de DLCI ni de subcanal.

Configuración y supervisión de la función de voz

En este capítulo se describe como utilizar los mandatos de configuración y de funcionamiento de la función de voz. Consta de los apartados siguientes:

Acceso a los mandatos de la función de voz

Utilice el procedimiento siguiente para acceder al proceso de configuración de la función de voz.

1. En el indicador OPCON, escriba **talk 6** (si desea obtener más información sobre este mandato, consulte *El proceso y los mandatos de OPCON* en Access Integration Services Guía del usuario de software). Por ejemplo:

   ```
   * talk 6
   Config>
   ```

   Después de escribir el mandato **talk 6**, aparecerá el indicador CONFIG (`Config>`) en la línea de mandatos. Si el indicador no aparece cuando se entra por primera vez la configuración, pulse **Intro** de nuevo.

2. En el indicador CONFIG escriba el mandato **feat voice** para acceder al indicador `Voice Config>`.

Mandatos de la función de voz

En este apartado se describen los parámetros de la función de voz y los mandatos utilizados para configurarlos.

Tabla 65. Resumen de mandatos de la función de voz

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 xxxii.
Add	Añade una regla de salida de la compañía telefónica.
Delete	Suprime una regla de salida de la compañía telefónica.
List	Lista todos los temporizadores y tonos aplicables a todas las interfaces de voz, además de las reglas de salida de la compañía telefónica.
Modify	Actualiza una regla de salida de la compañía telefónica.
Set	Establece los temporizadores y los tonos aplicables a todas las interfaces de voz.
VoFR	Accede a los mandatos de configuración de la función voz sobre Frame Relay.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiii.

Add

Utilice el mandato **add** para añadir una regla de salida de la compañía telefónica. Después de añadir la regla de salida de la compañía telefónica, se puede aplicar a una interfaz de voz utilizando el mandato de configuración **set telco-output-rule** de Voice Net.

Sintaxis:

a**dd** telco-output-rule

telco-output-rule

Especifica la secuencia de dígitos de marcación que se enviarán desde la interfaz de la compañía telefónica cuando ésta sea el destino de una llamada. La secuencia se especifica como una combinación de constantes, de caracteres de pausa y de los dígitos de marcación de los números de origen y de destino enviados durante el establecimiento de llamada.

Nota: La regla de salida de la compañía telefónica es equivalente a la regla de salida de destino del IBM 9783 para una interfaz de voz.

Ejemplo:

```
Voice config>add telco

Define Telco Output Rule #1

Digit  1 : (Source/Destination/Constant/Pause/End) [Destination]?
         (1-20) [1]?
Digit  2 : (Source/Destination/Constant/Pause/End) [Destination]?
         (1-20) [2]?
Digit  3 : (Source/Destination/Constant/Pause/End) [Destination]? e
Voice Config>a t

Define Telco Output Rule #2

Digit  1 : (Source/Destination/Constant/Pause/End) [Destination]?
           (1-20) [1]?
Digit  2 : (Source/Destination/Constant/Pause/End) [Destination]? s
           (1-20) [2]?
Digit  3 : (Source/Destination/Constant/Pause/End) [Destination]? c
           (0-9, A-D, *, #) [0]? a
Digit  4 : (Source/Destination/Constant/Pause/End) [Destination]? p
Digit  5 : (Source/Destination/Constant/Pause/End) [Destination]? e
```

Digit núm.

Especifica cómo se determina el dígito de marcación concreto.

Source Se ha de utilizar el dígito de la posición especificada del número de teléfono de origen.

Destination
Se ha de utilizar el dígito de la posición especificada del número de teléfono de destino.

Constant Se ha de utilizar siempre el dígito constante siguiente (0–9, A—D, #, *) en la posición especificada.

Pause En este punto de la secuencia de dígitos de marcación, se ha de insertar un intervalo de pausa.

End Especifica el final de la secuencia de dígitos.

Delete

Utilice el mandato **delete** para suprimir una regla de salida de la compañía telefónica.

Sintaxis:

delete telco-output-rule

Para obtener una explicación de la regla de salida de la compañía telefónica, consulte “Add” en la página 680.

List

Utilice el mandato **list** para mostrar los temporizadores y tonos aplicables a todas las interfaces de voz, además de las reglas de salida de la compañía telefónica.

Sintaxis:

list telco-output-rule ...
timers
tones

telco-output-rule
Lista la regla de salida de la compañía telefónica que se especifique. Si no se especifica ningún número de regla, aparecerá el indicador `Rule #`.

timers Lista todos los retardos y tiempos de espera (en milisegundos). Estos parámetros se describen en la página 682.

Ejemplo:

```
Voice config>list timers

Seize Detect Delay    :50   ms   First Digit Timeout     :10000 ms
Answer Detect Delay   :10   ms   Inter Digit Timeout     :5000  ms
Discon Detect Delay   :200  ms   Start Dial Delay        :500   ms
Glare Detect Delay    :500  ms   Ring No Answer Timeout  :30000 ms
Wink Detect Timeout   :2000 ms   Ring on Detect Timeout  :400   ms
Wink Start Delay      :50   ms   Ring Off Detect Timeout :6000  ms
Wink Duration         :200  ms   Warble Timeout          :10000 ms
```

tones Lista todos los tonos asociados con esta función de voz. Estos parámetros se describen en la página 684.

Ejemplo:

```
Voice config>list tones

Tone         On1    Off1    On2   Off2   Freq1 Freq2   Level1 Level2
             ms     ms      ms    ms     Hz    Hz      dB     dB
Dial         0      0       0     0      350   440     -16    -16
Ring Back    2000   4000    2000  4000   440   480     -22    -22
Busy         500    500     500   500    480   620     -20    -20
Fast Busy    300    300     300   300    480   620     -16    -16
Warble       100    100     100   100    1400  2060    -16    -16
Dtmf         100    100                                -7     -7
```

Modify

Utilice el mandato **modify** para actualizar las reglas de salida de la compañía telefónica de la función de voz.

Sintaxis:

m**odify** telco-output-rule

En “Add” en la página 680 hallará una explicación de la regla de salida de la compañía telefónica.

Set

Utilice el mandato **set** para especificar los valores de los retardos y tiempos de espera.

Sintaxis:

s**et** timer . . .
tone . . .

timer Utilice el mandato **set timer** para establecer los siguientes parámetros de un temporizador.

answer-detect-delay
Tiempo (en milisegundos) que transcurrirá antes de que se reconozca una señal de respuesta.

Valores válidos: de 0 a 500 ms

Valor por omisión: 10 ms

disconnect-detect-delay
Tiempo (en milisegundos) que transcurrirá antes de que se reconozca una señal de desconexión.

Valores válidos: de 0 a 500 ms

Valor por omisión: 200 ms

first-digit-timeout
Tiempo (en milisegundos) durante el que debe recibirse el primer dígito.

Valores válidos: de 0 a 10 000 ms

Valor por omisión: 10 000 ms

glare-detect-delay
Tiempo (en milisegundos) que transcurrirá antes de que una interfaz pueda tomar un canal.

Valores válidos: de 0 a 500 ms

Valor por omisión: 500 ms

inter-digit-timeout
Tiempo (en milisegundos) durante el que debe recibirse un dígito *después* de haber recibido el primero.

Valores válidos: de 0 a 10 000 ms

Valor por omisión: 5000 ms

ring-no-answer-timeout
Tiempo (en milisegundos) que esperará respuesta un canal de voz que llame a una interfaz FXO, antes de renunciar a la llamada.

Valores válidos: de 0 a 64 000 ms

Valor por omisión: 30 000 ms

ring-off-detect-timeout
Tiempo (en milisegundos) durante el que no debe haber señal de llamada en una interfaz FXO, para que el servidor determine que la llamada se ha interrumpido.

Valores válidos: de 0 a 64 000 ms

Valor por omisión: 6000 ms

ring-on-detect-timeout
Tiempo (en milisegundos) durante el que ha de haber señal de llamada en una interfaz FXO, para que se reconozca la llamada.

Valores válidos: de 0 a 64 000 ms

Valor por omisión: 400 ms

start-dial-delay
Tiempo (en milisegundos) que transcurrirá después de recibir una señal de marcación, pero antes de transmitir los dígitos.

Valores válidos: de 0 a 64 000 ms

Valor por omisión: 500 ms

seize-detect-delay
Tiempo (en milisegundos) que transcurrirá antes de que se reconozca una señal de toma.

Valores válidos: de 0 a 500 ms

Valor por omisión: 50 ms

warble-timeout
Tiempo (en milisegundos) de silencio que debe transcurrir después de una desconexión, para poder generar una señal de frecuencia variable.

Valores válidos: de 0 a 64 000 ms

Valor por omisión: 10 000 ms

wink-detect-timeout
Tiempo (en milisegundos) que debe transcurrir sin recibir una señal de guiño, antes de que se interrumpa la llamada.

Valores válidos: de 0 a 64 000 ms

Valor por omisión: 2000 ms

wink-duration
Duración (en milisegundos) de la señal de guiño.

Valores válidos: de 0 a 1000 ms

Valor por omisión: 200 ms

wink-start-delay
Tiempo (en milisegundos) transcurrido después de recibir una señal entrante de toma antes de generar una señal de guiño.

Valores válidos: de 0 a 64 000 ms

Valor por omisión: 50 ms

tone Utilice el mandato **set tone** para establecer los parámetros de tono siguientes.

busy Especifica las características de hasta dos frecuencias, utilizadas para generar la señal de ocupado. Al entrar el mandato set tone busy, se le pedirá la información siguiente:

on1 Tiempo (en milisegundos) que la frecuencia *freq1* estará "activa". Si el valor especificado es cero, el tono asociado estará siempre activado, lo que produce un tono continuo.

Valores válidos: de 0 a 32 767 ms

Valor por omisión: 500

off1 Tiempo (en milisegundos) que la frecuencia *freq1* estará "inactiva". Si el valor especificado es cero, el tono asociado estará siempre activado, lo que produce un tono continuo.

Valores válidos: de 0 a 32 767 ms

Valor por omisión: 500

on2 Tiempo (en milisegundos) que la frecuencia *freq2* estará "activa". Si el valor especificado es cero, el tono asociado estará siempre activado, lo que produce un tono continuo.

Valores válidos: de 0 a 32 767 ms

Valor por omisión: 500

off2 Tiempo (en milisegundos) que la frecuencia *freq2* estará "inactiva". Si el valor especificado es cero, el tono asociado estará siempre activado, lo que produce un tono continuo.

Valores válidos: de 0 a 32 767 ms

Valor por omisión: 500

freq1 Frecuencia (en hercios) del primer tono de la señal de ocupado.

Valores válidos: de 300 a 3000 hercios

Valor por omisión: 480 hercios

freq2 Frecuencia (en hercios) del segundo tono de la señal de ocupado.

Valores válidos: de 300 a 3000 hercios

Valor por omisión: 620 hercios

level1 Nivel de ganancia, en decibelios, de la frecuencia *freq1*, en incrementos de 0,5 dB.

Valore válidos: de –9 dB a –22 dB

Valor por omisión: –20 dB

level2 Nivel de ganancia, en decibelios, de la frecuencia *freq2*, en incrementos de 0,5 dB.

Valore válidos: de –9 dB a –22 dB

Valor por omisión: –20 dB

dial Especifica las características de hasta dos frecuencias utilizadas para generar un tono de marcación. Cuando se entra el mandato **set tone dial**, se le pedirán los datos siguientes: *on1, off1, on2, off2, freq1, freq2, level1 y level2*. Estos parámetros se describen en la página 684. En la nota a pie de página [1] encontrará más información.

dtmf Especifica las características de la señal de multifrecuencia de dos tonos (DTMF). Cuando se entra el mandato **set tone dtmf**, se le pedirá la información siguiente:

ontime Especifica el "tiempo que estará activada" (en milisegundos) la señal DTMF. Si el valor que se especifica es cero, no se generará ninguna señal DTMF. Normalmente no debe especificarse un *tiempo que estará activada* inferior a 40 milisegundos. Esto produciría una señal de 12,5 tonos por segundo.

[1] Los valores por omisión de dial, fast busy, ring-back y warble no son iguales que los que se utilizan para busy. Si quiere más información, consulte dial 685, fast busy 686, ring-back 686 y warble 686.

Valores válidos: de 0 a 32767 ms

Valor por omisión: 100 ms

offtime Especifica el "tiempo que estará desactivada" (en milisegundos) la señal DTMF. Si el valor que se especifica es cero, no se generará ninguna señal DTMF.

Valores válidos: de 0 a 32767 ms

Valor por omisión: 100 ms

level low tone
Especifica el nivel de ganancia, en decibelios, de la señal baja de DTMF, en incrementos de 0,5 dB.

Valores válidos: de –7 dB a –31 dB

Valor por omisión: –7 dB

level high tone
Especifica el nivel de ganancia, en decibelios, de la señal alta de DTMF, en incrementos de 0,5 dB.

Valores válidos: de –7 dB a –31 dB

Valor por omisión: –7 dB

fast busy Especifica las características de hasta dos frecuencias utilizadas para generar la señal rápida de ocupado. Cuando se entra el mandato **set tone fast busy**, se le pedirán los datos siguientes *on1, off1, on2, off2, freq1, freq2, level1 y level2*. Estos parámetros se describen en la página 684. Para obtener más información, lea la nota a pie de página [1].

ring-back
Especifica las características de hasta dos frecuencias utilizadas para generar un eco. Cuando se entra el mandato **set tone ring-back**, se le pedirán los datos siguientes: *on1, off1, on2, off2, freq1, freq2, level1 y level2*. Estos parámetros se describen en la página 684. Para obtener más información, lea la nota a pie de página [1].

warble Especifica las características de hasta dos frecuencias utilizadas para generar un tono de marcación. Cuando se entra el mandato **set tone warble**, se le pedirán los datos siguientes: *on1, off1, on2, off2, freq1, freq2, level1 y level2*. Estos parámetros se describen en la página 684. Para obtener más información, lea la nota a pie de página [1].

VoFR

En el apartado “Acceso a los mandatos de la función voz sobre Frame Relay (VoFR)” en la página 692 se dan más detalles sobre este mandato.

Acceso a los mandatos de la interfaz de voz

Utilice el procedimiento siguiente para acceder al proceso de configuración de la interfaz de voz.

1. En el indicador OPCON, escriba **talk 6** (si desea obtener más información sobre este mandato, consulte “El proceso y los mandatos de OPCON” en *Access Integration Services Guía del usuario de software*).
2. Por ejemplo:

```
* talk 6
Config>
```

   Después de escribir el mandato **talk 6**, aparecerá el indicador CONFIG (`Config>`) en la línea de mandatos. Si el indicador no aparece cuando se entra por primera vez la configuración, pulse **Intro** de nuevo.
3. En el indicador `CONFIG>`, escriba **net x**, donde x es el número de la interfaz de voz.

Mandatos de la interfaz de voz

En este apartado se describen los parámetros de la interfaz de voz y los mandatos utilizados para configurarlos.

Tabla 66. Resumen de mandatos de la interfaz de voz

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 xxxii.
List	Lista distintos valores de la interfaz de voz.
Set	Establece varios parámetros de la interfaz de voz.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiii.

List

Utilice el mandato **list** para visualizar los valores actuales de una interfaz de voz.

Sintaxis:

list

Por ejemplo, para listar la configuración actual de la interfaz de voz, escriba:

Ejemplo:

```
Voice 8 config>list

NodeID: 1.2.3.4

Local Phone Number:1234567

Telco Output Rule Number: 0

Telco Parameters

Tx Gain   :-4 dB       E&M Type :1
Rx Gain   :-4 dB       E&M Wire :4
OOS Signal:Busy        E&M Start:Immediate

Dsp Parameters

Vocoder Suite :Nuera   VAD Mode      :Off
Vocoder Rate  :9600    VAD Hangover  :255 ms
Frame Packing :1       VAD Threshold :-45 dB

Echo Cancel   :On      Fax   :On
NLP           :On      NSF   :On
2100Hz Detect :On      Max Fax Rate: Vocoder Rate
```

Node ID Indica el ID de nodo del IBM 9783 de la interfaz de voz.

Local Telephone Number
Indica el número de teléfono local de la interfaz de voz.

Telco Output Rule
Indica la regla de salida de la compañía telefónica que está utilizando actualmente la interfaz de voz.

Tx Gain Indica la ganancia actual de transmisión, en decibelios.

Rx Gain Indica la ganancia actual de recepción, en decibelios.

OOS Signal
Indica el tipo de señal que se utilizará si la interfaz no funciona.

E&M Type
Indica el tipo de interfaz de la compañía telefónica que utiliza la interfaz de voz.

E&M Wire
Indica si esta interfaz de voz es de dos cables o de cuatro cables.

E&M Start
Indica cómo iniciará la transmisión la interfaz de voz.

Vocoder Suite
Indica el tipo de protocolo del codificador vocal (ITU o NUERA) actualmente disponible en la interfaz de voz.

Vocoder Rate
Indica la cadencia actual del codificador vocal.

VAD Mode
Indica el tipo de VAD que se está utilizando. Se pueden especificar los valores fixed, adaptative u off.

VAD Hangover
Indica el tiempo que el nivel de la señal de entrada debe permanecer por debajo del valor umbral de VAD antes de considerar que el enlace está mudo.

VAD Threshold
Indica el nivel de la señal (en decibelios) que se utilizará para determinar cuándo está mudo un enlace.

NLP Indica si el proceso no lineal está habilitado (On) o inhabilitado (Off).

2100Hz Detect
Indica si la detección de los 2100Hz está habilitada (On) o inhabilitada (Off).

FAX Indica si la función FAX Relay está habilitada (On) o inhabilitada (Off).

NSF Indica si los recursos no estándar están habilitados (On) o inhabilitados (Off).

Max Fax Rate
Velocidad máxima a la que se conectará el fax.

Consulte el mandato “Set” para obtener la descripción de otros parámetros.

Set

Utilice el mandato **set** para especificar los valores de una determinada interfaz de voz.

Sintaxis:

set
- echo-cancel
- fax
- frame-packing
- local-number
- node-id
- oos
- rate
- rx-gain
- start
- suite
- telco-output-rule
- tx-gain
- type (E&M-only)
- vad
- wire

Se pueden especificar los parámetros siguientes para el mandato **set**:

echo-cancel
Especifica si se habilita o no la cancelación de eco, el proceso no lineal, o la detección de los 2100 Hz.

Valores válidos: on, off, nlp o detect-2100Hz

Valor por omisión: on

nlp

Valores válidos: on u off

Valor por omisión: on

detect-2100Hz

Valores válidos: on u off

Valor por omisión: on

Ejemplo:

```
Voice 8 Config>s e on
```

fax Especifica si se habilita o no el fax, los recursos no estándar, y la velocidad máxima a la que se conectará el fax.

Valores válidos: on, off, nsf o max-rate

Valor por omisión: on

nsf Especifica si se han de habilitar o no los recursos no estándar.

Valores válidos: on u off

Valor por omisión: on

max-rate Especifica la velocidad máxima.

Valores válidos: Vocoder Rate, 4,8 Kb ó 9,6 Kb

Valor por omisión: Vocoder Rate

Ejemplo:

```
Voice 8 Config>s fa on
```

frame-packing

Especifica el número de tramas de voz que se empaquetarán en un único paquete Frame Relay.

Valores válidos: de 1 a 5

Valor por omisión: 1

Ejemplo:

```
Voice 8 Config>s fr
Frame Packing (1 to 5) [1]?
```

local-number

Especifica el número de teléfono local de la interfaz de voz especificada.

Valores válidos: cualquier número de 20 dígitos (de 0 a 9, de A a D, *, #)

Valor por omisión: 0

Ejemplo:

```
Voice 8 Config>s l
Local Phone Number (1 to 20 digits, range 0-9, A-D, *, #) [0]? 524
Number of leading digits used for local call routing (1 to 3) [3]?
```

node-id Especifica el ID de nodo de la interfaz.

Valores válidos: cualquier ID de nodo válido (dirección IP)

Valor por omisión: 0.0.0.0

Ejemplo:

```
Voice 8 Config>s n
Node ID (IP Address) [0.0.0.0]? 1.2.4.2
```

oos Especifica el tipo de tono que se quiere utilizar para indicar que la interfaz de voz especificada no funciona.

Valores válidos: idle o busy

Valor por omisión: busy

Ejemplo:

```
Voice 8 Config>s o busy
```

rate Especifica la velocidad de transmisión de la interfaz de voz.

Valores válidos: Si se especifica Nuera como parámetro suite, se pueden elegir los valores siguientes: 4,8 KB; 7,47 KB; 9,6 KB o 32 KB. Si se especifica ITU como parámetro suite, se pueden elegir los valores siguientes: 8 KB, 16 KB o 32 KB.

Valor por omisión: 9,6 KB

rx-gain Especifica el valor en que la interfaz de voz atenúa (o amplifica) la señal recibida.

Valores válidos: de –16 dB a +7 dB

Valor por omisión: 0 dB

Ejemplo:

```
Voice 8 Config>s rx
Gain (-16 to +7 dB) [0]?
```

start (E&M-only)
Especifica cómo iniciará las transmisiones la interfaz de voz.

Valores válidos: immediate start o wink start

Valor por omisión: immediate start

Ejemplo:

```
Voice 8 Config>s st immediate
```

suite Especifica el tipo de protocolo que quiere que utilice la interfaz puerto de voz.

Valores válidos: NUERA – ECELP/G.726 o ITU – G.729/G728/G.726

Valor por omisión: NUERA

Ejemplo:

```
Voice 8 Config>s su I
```

telco-output-rule
Especifica qué regla de salida de la compañía telefónica se utilizará.

Valores válidos: de 0 a 8. El límite superior depende del número de reglas de salida de la compañía telefónica definidas.

Valor por omisión: 0

Ejemplo:

```
Voice 8 Config>s te
Telco Output Rule Number (0 to 1) [0]? 1
```

tx-gain Especifica el valor en que la interfaz de voz atenúa (o amplifica) la señal transmitida.

Valores válidos: de –16 dB a +7 dB

Valor por omisión: 0 dB

Ejemplo:

```
Voice 8 Config>s tx
Gain (-16 to +7 dB) [0]?
```

type (E&M-only)
Especifica la interfaz E&M de la compañía telefónica para la interfaz de voz especificada.

Valores válidos: 1,2 ó 5

Valor por omisión: 1

Ejemplo:

```
Voice 8 Config>s ty
E&M Type (1,2,5) [1]?
```

vad Especifica los valores siguientes:

mode Especifica el tipo de vad.

Valores válidos: fixed, adaptive u off

Valor por omisión: off

hangover Especifica el tiempo que tarda en colgar vad.

Valores válidos: de 1 a 500 ms

Valor por omisión: 255 ms

umbral Especifica el umbral de vad.

Valores válidos: de –15 a –60 dB

Valor por omisión: –45 dB

wire (E&M-only)
Especifica si se está utilizando una conexión de la compañía telefónica de dos cables o de cuatro cables.

Valores válidos: 2 (de dos cables) o 4 (de cuatro cables)

Valor por omisión: 4

Ejemplo:

```
Voice 8 Config>s w
E&M Wire (2,4) [4]?
```

Acceso a los mandatos de la función voz sobre Frame Relay (VoFR)

Utilice el procedimiento siguiente para acceder a los mandatos de la función voz sobre Frame Relay.

1. En el indicador OPCON, escriba **talk 6** (si desea obtener más información sobre este mandato, consulte *El proceso y los mandatos de OPCON* en Access Integration Services Guía del usuario de software). Por ejemplo:

   ```
   * talk 6
   Config>
   ```

   Después de escribir el mandato **talk 6**, aparecerá el indicador CONFIG (`Config>`) en la línea de mandatos. Si el indicador no aparece cuando se entra por primera vez la configuración, pulse **Intro** de nuevo.

2. En el indicador CONFIG, escriba el mandato **feat voice** para acceder al indicador `voice config>`.
3. En el indicador `voice config>`, escriba **VoFR** para acceder al indicador `VoFR config>`.

Mandatos de la función voz sobre Frame Relay (VoFR)

En este apartado se describen los mandatos de la función voz sobre Frame Relay y los parámetros configurables del menú VoFR.

Tabla 67. Resumen de mandatos de configuración de VoFR

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 xxxii.
Add	Añade una regla de proceso de llamada, una regla de comparación de marcación o una regla de salida de la red.
Delete	Suprime una regla de salida de la red, una regla de comparación de marcación o una regla de proceso de llamada.
Disable	Inhabilita la función voz sobre Frame Relay en la interfaz de la red de voz especificada.
Enable	Habilita la función voz sobre Frame Relay en la interfaz de la red de voz especificada.
List	Lista la red de frame relay, las interfaces, las reglas de salida de la red, las reglas de comparación de marcación, las reglas de proceso de llamada, o todos los elementos.
Modify	Actualiza una regla de proceso de llamada, una regla de comparación de marcación o una regla de salida de la red.
Reorder-call-rule	Vuelve a ordenar las reglas de llamada.
Set	Establece fr-net (red frame relay).
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxiii.

Add

Este mandato añade una regla de salida de la red, una regla de comparación de marcación o una regla de proceso de llamada a la configuración de VoFR.

Sintaxis:

add call-processing-rule
dial-matching-rule
network-output-rule

call-processing-rule

Especifica las reglas de proceso de llamada. Para las llamadas de salida, las reglas de proceso de llamada se evalúan en orden ascendente, comparando los dígitos marcados con la regla de comparación de dígitos de marcación asociada con cada regla de proceso de llamada. Si se detecta una coincidencia, para procesar la llamada se utilizarán las reglas de salida de la red y de información de

direccionamiento de llamada de la regla de proceso de llamada. Puesto que una interfaz de voz puede aceptar llamadas de cualquiera de los destinos especificados en cualquiera de sus reglas de direccionamiento de llamada asociadas, esta regla no tiene ningún efecto. Se pueden definir hasta ocho reglas de proceso de llamadas para cada interfaz de voz.

Nota: La regla de proceso de llamadas es equivalente a la regla de conversión del IBM 9783, que combina una regla de salida de la red y una regla de comparación de marcación con la información de direccionamiento de llamada (la especificación DLCI y de subcanal, en caso de que la ruta de llamada sea remota, o los dígitos del número de destino que se han de comparar con los números locales, en caso de que la ruta de llamada sea local).

Ejemplo:

```
VoFR Config>a c
Voice Net [0]? 8

Define Call Processing Rule #2

Destination Type (Local or Remote) [Remote]?
Call Processing DLCI (16 to 1007) [16]?
Payload         DLCI (16 to 1007) [16]?
Call Processing Subchannel (4 to 254) [4]?
Payload         Subchannel (4 to 254) [4]? 5
Dial Digit Matching Rule Number (0 to 3) [0]? 2
Network Output Rule Number (0 to 3) [0]? 1


VoFR Config>a c
Voice Net [0]? 8

Define Call Processing Rule #3

Destination Type (Local or Remote) [Remote]? l
Dial Digit Matching Rule Number (0 to 3) [0]? 1
Network Output Rule Number (0 to 2) ]0]? 1
```

Destination Type

Especifica si el nodo de destino está en otro 2212/IBM 9783 (remoto) o en otra interfaz de voz del mismo 2212 (local).

Call Processing DLCI

Especifica el DLCI que se utilizará para establecer e interrumpir la llamada.

Payload DLCI

Especifica el DLCI que se utilizará para enviar y recibir los paquetes de datos de voz comprimidos.

Call Processing Subchannel

Especifica el subcanal que se utilizará para establecer e interrumpir la llamada.

Payload Subchannel

Especifica el subcanal que se utilizará para enviar y recibir los paquetes de datos de voz comprimidos.

Dial Digit Matching Rule

Especifica el número de la regla de comparación de dígitos de marcación que utilizará esta regla de proceso de llamada.

Network Output Rule

Especifica el número de la regla de salida de la red que utilizará esta regla de proceso de llamada.

dial-matching-rule

Especifica una secuencia de patrones de comparación de dígitos de marcación, en la que cada elemento de la secuencia especifica un rango de dígitos aceptables en esa posición.

Nota: La regla de comparación de marcación es equivalente a la regla de comparación de destino del IBM 9783.

Ejemplo:

```
VoFR Config>a d

Define Dial Digit Matching Rule #3

Dial Mask  1 : Digit String (0-9,A-D,*,#), [W]ildcard, [N]umeric Wildcard,
                                           [M]ultiDigit Wildcard.
               [MultiDigit Wildcard]?

Dial Mask  2 : Digit String (0-9,A-D,*,#), [W]ildcard, [N]umeric Wildcard,
                                           [M]ultiDigit Wildcard, or [E]nd.
               [End]?

Matching Rule contains MultiDigit Wildcard(s).
Minimum number of digits accepted for MultiDigit Wildcard (0,1) [1]?
```

Dial Mask núm.

Especifica una de las veinte máscaras de dígitos de marcación posibles. Cada máscara indica el rango aceptable del dígito en esta posición de la secuencia de marcación de 20 dígitos.

Digit String

Especifica un conjunto de dígitos del que debe elegirse el dígito.

Wildcard Especifica que el dígito debe ser uno de los siguientes: 0-9, A-D, # o *.

Numeric Wildcard

Especifica que el dígito debe estar comprendido entre el 0 y el 9

Multidigit Wildcard

Especifica que en la posición especificada se puede aceptar más de un dígito. Si la máscara de comodín de varios dígitos es la última de la regla de comparación de marcación, se podrá entrar cualquier dígito (0–9, A—D, #, *) en este punto de la secuencia. En este caso, la interfaz de voz continuará reuniendo dígitos hasta que se entren los 20 dígitos o hasta que se agote el tiempo de espera entre dígitos sin que se haya entrado ningún otro dígito. Si hay una máscara después del comodín de varios dígitos, la interfaz de voz continuará reuniendo dígitos que satisfagan la máscara de varios dígitos hasta que se entre un dígito que satisfaga la máscara que hay después del comodín de varios dígitos.

network-output-rule

Especifica los dígitos del número de destino que se pasarán en el paquete de establecimiento de llamada Frame Relay. La secuencia se especifica como una combinación de constantes y de los dígitos marcados recibidos en la interfaz de la compañía telefónica de origen.

Nota: La regla de salida de la red es equivalente a la regla de salida de destino del IBM 9783 para una interfaz Frame Relay.

Ejemplo:

```
VoFR Config>a n

Define Network Output Rule #2

Digit  1 : (Destination/Constant/End) [Destination]?
         (1-20) [1]?
Digit  2 : (Destination/Constant/End) [Destination]? e
```

Digit núm.

Especifica cómo se determina el dígito de marcación concreto.

Destination
Se ha de utilizar el dígito de la posición especificada del número de teléfono de destino.

Constant Se ha de utilizar siempre el dígito constante siguiente (0–9, A—D, #, *) en la posición especificada.

End Especifica el final de la secuencia de dígitos.

Delete

Este mandato suprime una regla de salida de la red, una regla de comparación de marcación o una regla de proceso de llamada de la configuración de VoFR.

Sintaxis:

de**lete**	call-processing-rule dial-matching-rule network-output-rule

Para obtener una explicación de las reglas de salida de la red, de las reglas de comparación de marcación y de las reglas de proceso de llamada, consulte el mandato “Add” en la página 693.

Disable

Este mandato inhabilita la función voz sobre Frame Relay en la interfaz de la red de voz especificada. Para interfaces nuevas, VoFR está habilitada.

Sintaxis:

di**sable**	interface *número-interfaz*

Ejemplo:

```
disable interface 5
```

Enable

Este mandato habilita la función voz sobre Frame Relay en la interfaz de red de voz especificada. Para interfaces nuevas, VoFR está habilitada.

Sintaxis:

e**nable**	interface *número-interfaz*

Ejemplo:

```
enable interface 5
```

List

Este mandato puede listar toda la información de configuración de VoFR, de la red frame relay, de reglas de salida de la red, de reglas de comparación de marcación, o de reglas de proceso de llamada.

Sintaxis:

list	all call-processing-rule dial-matching-rule fr-net interfaces network-output-rule

all Lista la información de la red Frame Relay, las interfaces de voz en las que VoFR está habilitado o inhabilitado, las reglas de salida de la compañía telefónica, las reglas de salida de la red, las reglas de comparación de dígitos de marcación y las reglas de proceso de llamada.

call processing rule

Lista la regla de llamada de la interfaz de voz especificada. Si no se especifica un número de interfaz concreta, aparecerá el indicador `Voice Net [0]`, donde podrá especificarla.

Ejemplo:

```
VoFR config>list call 7

Call Processing Rule #1

Call Processing      DLCI         = 16
Payload              DLCI         = 16
Call Processing Subchannel = 4
Payload         Subchannel = 5
Dial Digit Matching  Rule #       = 1
Network Output       Rule #       = 1


Call Processing Rule #2

Call Processing      DLCI          = 16
Payload              DLCI          = 16
Call Processing      Subchannel    = 6
Payload              Subchannel    = 7
Dial Digit Matching  Rule #        = 2
Network Output       Rule #        = 2
```

Call processing DLCI

Indica el DLCI de proceso de llamada definido para esta interfaz.

Payload DLCI

Indica el DLCI de carga útil definido para esta interfaz.

Call processing subchannel

Indica el subcanal de proceso de llamada definido para esta interfaz.

Payload subchannel

Indica el subcanal de carga útil definido para esta interfaz.

Dial digit matching rule
Indica la regla de comparación de dígitos de marcación que está utilizando actualmente esta interfaz.

Network output rule
Indica la regla de salida de red que está utilizando actualmente esta interfaz.

dial matching rule
Lista la regla de comparación de dígitos de marcación de la interfaz de voz especificada. Si no se especifica ningún número de regla, aparecerá el indicador `Rule #`.

Ejemplo:

```
Voice config>list dial

Rule # (0 to 2) or all [all]? 1

Dial Digit Matching Rule #1

Dial Mask  1 : Match Digits = 0123456789
Dial Mask  2 : Match Digits = 0123456789
Dial Mask  3 : Match Digits = 0123456789
Dial Mask  4 : Match Digits = 0123456789
```

fr-net Lista el número de la red Frame Relay a través de la que se dirigirán los paquetes VoFR.

interfaces
Lista si la función voz sobre Frame Relay está habilitada o inhabilitada para las interfaces de voz, donde:

- La columna Net especifica el número de interfaz de la red de voz.
- La columna VoFR especifica si la función voz sobre Frame Relay está habilitada o inhabilitada en la red de voz.

Ejemplo:

```
VoFR Config>list interface
Net   VoFR
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Enabled
9     Disabled
```

network-output-rule
Lista la regla de salida de la red especificada. Si no se especifica ningún número de regla, aparecerá el indicador `Rule #`.

Ejemplo:

```
VoFR Config>l n
Rule # (0 to 1) or all [all]? 1

Destination Number Generation Rule #1

Dial Digit  1 : Digit  1 from Destination Number
```

Modify

Este mandato actualiza una regla de salida de la red, una regla de comparación de marcación o una regla de proceso de llamada en la configuración de VoFR.

Sintaxis:

modify call-processing-rule

dial-matching-rule
network-output-rule

Para obtener una explicación de las reglas de proceso de llamada, de las reglas de comparación de marcación y de las reglas de salida de red, consulte el mandato “Add” en la página 693.

Ejemplo:

```
VoFR Config>modify call-processing-rule
Voice Net [0]? 8
Rule # (1 to 2) [1]?

Define Call Processing Rule #1

Destination Type (Local or Remote) [Remote]?
Call Processing DLCI (16 to 1007) [16]?
Payload         DLCI (16 to 1007) [16]?
Call Processing Subchannel (4 to 254) [4]?
Payload         Subchannel (4 to 254) [5]?
Dial Digit Matching Rule Number (0 to 2) [0]? 2
Network Output Rule Number (0 to 1) [0]? 1
```

Ejemplo:

```
VoFR Config>modify dial-matching-rule
Rule # (1 to 2) [1]?

Define Dial Digit Matching Rule #1

Dial Mask  1 : Digit String (0-9,A-D,*,#), [W]ildcard, [N]umeric Wildcard,
                                           [M]ultiDigit Wildcard.
               [0123456789]?

Dial Mask  2 : Digit String (0-9,A-D,*,#), [W]ildcard, [N]umeric Wildcard,
                                           [M]ultiDigit Wildcard, or [E]nd.
               [0123456789]?

Dial Mask  3 : Digit String (0-9,A-D,*,#), [W]ildcard, [N]umeric Wildcard,
                                           [M]ultiDigit Wildcard, or [E]nd.
               [0123456789]?

Dial Mask  4 : Digit String (0-9,A-D,*,#), [W]ildcard, [N]umeric Wildcard,
                                           [M]ultiDigit Wildcard, or [E]nd.
               [0123456789]?

Dial Mask  5 : Digit String (0-9,A-D,*,#), [W]ildcard, [N]umeric Wildcard,
                                           [M]ultiDigit Wildcard, or [E]nd.
               [End]?
```

Ejemplo:

```
VoFR Config>modify network-output-rule
Rule # (1 to 1) [1]?

Define Network Output Rule #1

Digit  1 : (Destination/Constant/End) [Destination]?
           (1-20) [1]?
Digit  2 : (Destination/Constant/End) [Destination]?
           (1-20) [2]?
Digit  3 : (Destination/Constant/End) [Destination]?
           (1-20) [3]?
Digit  4 : (Destination/Constant/End) [Destination]?
           (1-20) [4]?
Digit  5 : (Destination/Constant/End) [Destination]?
           (1-20) [5]?
Digit  6 : (Destination/Constant/End) [Destination]?
           (1-20) [6]?
Digit  7 : (Destination/Constant/End) [Destination]?
           (1-20) [7]?
Digit  8 : (Destination/Constant/End) [Destination]? e
```

Reorder-call-rule

Este mandato cambia el orden en que se procesan las reglas de proceso de llamada de la interfaz de voz (si la función VoFR está habilitada).

Sintaxis:

reorder-call-rule

Para el mandato **reorder-call-rule** hay que especificar el número de la interfaz de voz. En caso contrario, se le pedirá cuando entre el mandato.

Ejemplo:

```
VoFR Config>r
Voice Net [0]? 8
Current Rule # (1 to 2) [1]?
New Rule # (1 to 2) [1]? 2
```

Set

Este mandato establece una red de Frame Relay para la configuración de VoFR.

Sintaxis:

set fr-net

fr-net Utilice el mandato **set fr-net** para especificar el número de la red Frame Relay a través de la que se dirigirán los paquetes VoFR. Especifique un número de red configurado.

Ejemplo:

```
VoFR Config>s f
Frame Relay Net for Voice Traffic [65535]? 2
```

Acceso al entorno de supervisión de la interfaz de voz

Utilice el procedimiento siguiente para acceder a los mandatos de supervisión de la interfaz de voz.

1. Entre **talk 5** en el indicador OPCON (si desea obtener más información sobre este mandato, consulte “El proceso y los mandatos de OPCON” en *Access Integration Services Guía del usuario de software*).
2. Por ejemplo:

```
* talk 5
+
```

   Después de entrar el mandato **talk 5**, aparecerá el indicador GWCON (+) en la línea de mandatos.

3. Entre el mandato **network n** en el indicador + para acceder al indicador `Voice n Console >`.

   Ejemplo:

```
+ network 2
Voice 2 Console>
```

Mandatos de supervisión de la interfaz de voz

En este apartado se describen los mandatos de supervisión de la interfaz de voz.

Tabla 68. Resumen de mandatos de supervisión de la interfaz de voz

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 xxxii.
Calls	Muestra varios contadores de sucesos y de mensajes asociados con la interfaz de voz especificada.
Status	Muestra distintos valores de la interfaz de voz, así como información sobre los errores de transmisión o recepción.
Trace call	Muestra información de rastreo sobre una interfaz de destino.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiii.

Calls

Utilice el mandato **calls** para visualizar los mensajes de proceso de llamada y los contadores de sucesos.

Sintaxis:

calls

Ejemplo:

```
Voice 1 Console> calls

Event Counters

Seize Detected               5            Digit Detected        4
Seize Applied                0            Digit Generated      0

Message Counters

Setup Sent                   1            Setup Received        0
Connect Sent                 0            Connect Received      1
Answer Sent                  0            Answer Received       1
Release Sent                 2            Release Received      0

Release Cause Counters

Normal                       1             Response             0
Busy                         1             OOS                  0
Local Bandwidth              0             Incompatible         0
Remote Bandwidth             0
```

Event Counters Indican el número de sucesos producidos en la interfaz de la compañía telefónica.

Seize Detected
Indica el número de sucesos Seize In (el teléfono conectado a la interfaz de voz se desconecta—cuelga).

Seize Applied
Indica el número de sucesos Seize Out (la propia interfaz de voz se desconecta—cuelga).

Digit Detected
Indica el número de dígitos de marcación recibidos del abonado en la interfaz de la compañía telefónica.

Digit Generated
Indica el número de dígitos de marcación enviados al abonado en la interfaz de la compañía telefónica.

Message Counters
Indican el número de mensajes de proceso de llamadas enviados a una interfaz de voz o recibidos por ésta, a través del circuito Frame Relay. Cuando se establece una llamada, se envían mensajes de Establecimiento, Conexión y Respuesta entre los dos nodos. El iniciador de la llamada envía un mensaje de Establecimiento al extremo remoto, que responde con un mensaje de Conexión seguido de un mensaje de Respuesta, si la llamada es satisfactoria. Si la llamada no puede realizarse, el nodo remoto enviará un mensaje de Liberación. Cada extremo también envía mensajes de Liberación cuando una llamada satisfactoria finaliza normalmente (ambos nodos se conectan y cuelgan).

Setup Sent
Indica el número de mensajes de Establecimiento enviados.

Connect Sent
Indica el número de mensajes de Conexión enviados.

Answer Sent
Indica el número de mensajes de Respuesta enviados.

Release Sent
Indica el número de mensajes de Liberación enviados.

Setup Received
Indica el número de mensajes de Establecimiento recibidos.

Connect Received
Indica el número de mensajes de Conexión recibidos.

Answer Received
Indica el número de mensajes de Respuesta recibidos.

Release Received
Indica el número de mensajes de Liberación recibidos.

Release Cause Counters
Indican las causas del mensaje de Liberación.

Normal Indica el número de señales de colgar normales iniciadas por el nodo local.

Busy Indica el número de señales de colgar causadas por un canal ocupado.

Local Bandwidth
Indica el número de señales de colgar causadas por un ancho de banda local insuficiente.

Remote Bandwidth
Indica el número de señales de colgar causadas por un ancho de banda remota insuficiente.

Response
Indica el número de señales de colgar normales iniciadas por el nodo remoto.

OOS Indica el número de señales de colgar causadas porque el nodo remoto no funciona.

Incompatible
Indica el número de señales de colgar causadas por incompatibilidad con el nodo remoto.

Status

Utilice el mandato **status** para mostrar información sobre una interfaz de voz en concreto.

Sintaxis:

s**tatus**

Ejemplo:

```
Voice 1 Config> status

Voice Over Frame Relay   :Enabled
Node ID             :0.0.0.0
Absolute interface Address    :01

Vocoder Suite         Nuera           Echo Canceller      Filter
Vocoder Active        ECELP           Fax Demodulation    Idle
Vocoder Rate           9600           Fax Modulation      Idle
Vocoder Packet Size      18           Fax Type            V.27 at 9600 bps
Vocoder Frame Size      120           Fax Last FCF        0

Last Received    Dial Sequence       :8675309
Last Transmitted Dial Sequence       :911

Transmit Packets                Receive Packets

Total           179             Total       184
Voice           169             Voice       167
CAS               0             CAS          11
DTMF              0             DTMF          0
FAX               0             FAX           0
Lost              0             Lost          0
```

Voice over Frame Relay
Indica si la función voz sobre Frame Relay está habilitada o inhabilitada en esta interfaz.

Node ID Indica el ID de nodo del IBM 9783 de la interfaz de voz.

Absolute Interface Address
Indica el identificador de la interfaz de voz del 2212 utilizado por el sistema de contabilidad de llamadas del IBM 9783. El software del 2212 genera esta dirección automáticamente y es exclusiva para cada interfaz de voz de un determinado 2212.

Vocoder Suite
Indica el tipo de protocolo del codificador vocal (ITU o NUERA) actualmente disponible en la interfaz de voz.

Vocoder Active
Indica el codificador vocal que está actualmente activo en la interfaz.

Vocoder Rate
Indica la cadencia actual del codificador vocal.

Vocoder Packet Size
Indica el número de bytes de cada paquete del codificador vocal. Éste es el tamaño de la salida de compresión en bruto y no incluye la cabecera Frame Relay.

Vocoder Frame Size
Indica el número de muestras PCM de cada trama de codificador vocal.

Echo Canceller
Indica el estado actual del cancelador de eco.

FAX Demodulation
Indica el estado actual de desmodulación de FAX. El estado puede ser Activo o Desocupado.

FAX Modulation
Indica el estado actual de modulación de FAX. El estado puede ser Activo o Desocupado.

FAX Type
Indica el tipo de modulación que se está utilizando.

FAX Last FCF
Indica el último campo de control de FAX desmodulado.

Last Received Dial Sequence
Indica la última secuencia de dígitos de marcación recibida del abonado a través de la interfaz de la compañía telefónica.

Last Transmitted Dial Sequence
Indica la última secuencia de dígitos de marcación enviada al abonado a través de la interfaz de la compañía telefónica.

Transmit Packets/ Receive Packets
Muestra información sobre los paquetes Frame Relay transmitidos y recibidos. Los paquetes transmitidos son los paquetes generados por la interfaz de voz y enviados a través del enlace Frame Relay. Los paquetes recibidos son los paquetes recibidos por la interfaz de voz a través del enlace Frame Relay.

Total Indica el número total de paquetes recibidos y transmitidos.

Voice Indica el número de paquetes de voz comprimidos recibidos y transmitidos.

CAS Indica el número de paquetes CAS recibidos y transmitidos.

DTMF Indica el número de paquetes DTMF recibidos y transmitidos.

FAX Indica el número de paquetes FAX recibidos y transmitidos.

Lost Muestra el número de paquetes enviados por el nodo local pero que no ha recibido el nodo remoto (paquetes transmitidos) y el número de paquetes enviados por el nodo remoto pero que no ha recibido el nodo local (paquetes recibidos).

Trace Call

Utilice el mandato **trace call** para rastrear todos los mensajes de establecimiento o los mandatos de control de configuración de la interfaz de destino. Los sucesos de rastreo pueden verse con el mandato ELS (Talk 2).

Sintaxis:

trace call

Soporte de reconfiguración dinámica de la función de voz

En este apartado se describe la reconfiguración dinámica (DR) y cómo afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

La función de voz da soporte al mandato **delete interface** de CONFIG (Talk 6) sin restricciones.

Mandato activate interface de GWCON (Talk 5)

La función de voz no da soporte al mandato **activate interface** de GWCON (Talk 5).

Mandato reset interface de GWCON (Talk 5)

La función de voz da soporte al mandato **reset interface** de GWCON (Talk 5), tendiendo en cuenta que:

- Todos los parámetros de la función de voz, excepto FR-NET, pueden modificarse dinámicamente. Los parámetros de la función de voz se definen para cada direccionador y se aplican a todas las interfaces del direccionador. Después de cambiar un parámetro de la función de voz, todas las interfaces de voz deben restablecerse manualmente para que se les aplique el cambio.

Soporte de reconfiguración dinámica de las interfaces de voz

En este apartado se describe la reconfiguración dinámica (DR) y cómo afecta a los mandatos de Talk 6 y Talk 5.

Mandato delete interface de CONFIG (Talk 6)

Las interfaces de voz dan soporte al mandato **delete interface** de CONFIG (Talk 6), teniendo en cuenta que:

- Si se suprime uno de los puertos de voz de un adaptador de voz de dos puertos, el otro puerto del adaptador se suprimirá automáticamente, puesto que existe una restricción que obliga a que ambos puertos de un adaptador de voz de dos puertos estén configurados como presentes.

Mandato activate interface de GWCON (Talk 5)

Las interfaces de voz no dan soporte al mandato **activate interface** de GWCON (Talk 5).

Mandato reset interface de GWCON (Talk 5)

Las interfaces de voz dan soporte al mandato **reset interface** de GWCON (Talk 5). Todos los parámetros de la interfaz de voz pueden modificarse dinámicamente.

Apéndice A. Atributos de la seguridad AAA remota

En este apartado se identifican los atributos de la seguridad AAA remota que utilizan los servidores Radius, TACACS y TACACS+.

Radius

ID de proveedor de IBM: 211

Atributos de autorización

Del 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		integer
	1	PPTP
	2	L2F
	3	L2TP
TUNNEL_MEDIUM_TYPE		integer
	1	IP
TUNNEL_SERVER_EP		string
		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
SUBNETMASK	215
PRIVILEGE	216

Palabras clave

Los servidores Radius que permiten la entrada de campos específicos del proveedor utilizan palabras clave `<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_SUBNETMASK SNM
| KWD_PRIVILEGE PRV

Valores

| CALLBACK_FLAGS
REQ devolución de llamada obligatoria
ROAM devolución de llamada itinerante

PRIVILEGE:
ADMIN
OPER
MONITOR

| Ejemplo de archivo de configuración de RADIUS

| El siguiente es un ejemplo de archivo de configuración de RADIUS:

```
| VENDOR IBM 211
| ATTRIBUTE   User-Name            1   string
| ATTRIBUTE   User-Password        2   string
| ATTRIBUTE   CHAP-Password        3   string
| ATTRIBUTE   NAS-IP-Address       4   ipaddr
| ATTRIBUTE   NAS-Port             5   integer
| ATTRIBUTE   Service-Type         6   integer
| ATTRIBUTE   Framed-Protocol      7   integer
| ATTRIBUTE   Framed-IP-Address    8   ipaddr
| ATTRIBUTE   Framed-IP-Netmask    9   ipaddr
| ATTRIBUTE   Framed-Routing       10  integer
| ATTRIBUTE   Filter-Id            11  string
| ATTRIBUTE   Framed-MTU           12  integer
| ATTRIBUTE   Framed-Compression   13  integer
| ATTRIBUTE   Login-IP-Host        14  ipaddr
| ATTRIBUTE   Login-Service        15  integer
| ATTRIBUTE   Login-TCP-Port       16  integer #
| ATTRIBUTE   Old-Password         17  string
| ATTRIBUTE   Reply-Message        18  string
| ATTRIBUTE   Callback-Number      19  string
| ATTRIBUTE   Callback-Id          20  string #
| ATTRIBUTE   Unassigned           21  string
| ATTRIBUTE   Framed-Route         22  string
| ATTRIBUTE   Framed-IPX-Network   23  integer
| ATTRIBUTE   State                24  string
| ATTRIBUTE   Class                25  string
| ATTRIBUTE   Vendor-Specific      26  string
| ATTRIBUTE   Session-Timeout      27  integer
| ATTRIBUTE   Idle-Timeout         28  integer
| ATTRIBUTE   Termination-Action   29  integer
| ATTRIBUTE   Called-Station-Id    30  string
| ATTRIBUTE   Calling-Station-Id   31  string
| ATTRIBUTE   NAS-Identifier       32  string
```

```
| ATTRIBUTE                Proxy-State                33              string
| ATTRIBUTE                Login-LAT-Service          34              string
| ATTRIBUTE                Login-LAT-Node             35              string
| ATTRIBUTE                Login-LAT-Group            36              string
| ATTRIBUTE                Framed-Appletalk-Link      37              integer
| ATTRIBUTE                Framed-Appletalk-Net       38              integer
| ATTRIBUTE                Framed-Appletalk-Zone      39              string
| ATTRIBUTE                Acct-Status-Type           40              integer
| ATTRIBUTE                Acct-Delay-Time            41              integer
| ATTRIBUTE                Acct-Input-Octets          42              integer
| ATTRIBUTE                Acct-Output-Octets         43              integer
| ATTRIBUTE                Acct-Session-Id            44              string
| ATTRIBUTE                Acct-Authentic             45              integer
| ATTRIBUTE                Acct-Session-Time          46              integer
| ATTRIBUTE                Acct-Input-Packets         47              integer
| ATTRIBUTE                Acct-Output-Packets        48              integer
| ATTRIBUTE                Acct-Terminate-Cause       49              integer
| ATTRIBUTE                Acct-Multi-Session-Id      50              string
| ATTRIBUTE                Acct-Link-Count            51              integer
| ATTRIBUTE                CHAP-Challenge             60              string
| ATTRIBUTE                NAS-Port-Type              61              integer
| ATTRIBUTE                Port-Limit                 62              integer
| ATTRIBUTE                Login-LAT-Port             63              string
| ---------- START IBM ----------
| ATTRIBUTE                Tunnel-Type                64              integer
| ATTRIBUTE                Tunnel-Medium              65              integer
| ATTRIBUTE                Tunnel-Client-EP           66              string
| ATTRIBUTE                Tunnel-Server-EP           67              string
| ATTRIBUTE                Tunnel-Conn-ID             68              string
| ATTRIBUTE                Tunnel-Password            69              string
| ATTRIBUTE                Tunnel-NAS-Password        101             string
| ATTRIBUTE                VC-ACTIVE                  177             integer
| ATTRIBUTE                VC-IDLETIME                179             integer
| ATTRIBUTE                VC-SUSPENDTIME             180             integer
| ATTRIBUTE                IBM-Callback-Flags         210             string
| ATTRIBUTE                IBM-Encryption             211             string
| ATTRIBUTE                IBM-DialOut                214             string
| ATTRIBUTE                IBM-Hostname               213             string
| ATTRIBUTE                IBM-Subnetmask             215             string
| ATTRIBUTE                IBM-Privilege              216             string
| ATTRIBUTE                IBM-ipsec-inb-ah           110             integer
| ATTRIBUTE                IBM-ipsec-inb-esp          111             integer
| ATTRIBUTE                IBM-ipsec-ob-ah            112             integer
| ATTRIBUTE                IBM-ipsec-ob-esp           113             integer
| ATTRIBUTE                IBM-ipsec-ip-bad           114             integer
| ATTRIBUTE                IBM-ipsec-op-bad           115             integer
| ATTRIBUTE                IBM-ipsec-ip-bad-ah        116             integer
| ATTRIBUTE                IBM-ipsec-ip-bad-esp       117             integer
| ATTRIBUTE                IBM-ipsec-op-bad-ah        118             integer
| ATTRIBUTE                IBM-ipsec-op-bad-esp       119             integer
| ATTRIBUTE                IBM-ipsec-ip-ah            120             integer
| ATTRIBUTE                IBM-ipsec-ip-esp           121             integer
| ATTRIBUTE                IBM-ipsec-op-ah            122             integer
| ATTRIBUTE                IBM-ipsec-op-esp           123             integer
| ATTRIBUTE                IBM-ipsec-ip-bad-ah-r      124             integer
| ATTRIBUTE                IBM-ipsec-ip-bad-esp-r     125             integer
| ATTRIBUTE                IBM-ipsec-inb-wrap         128             integer
| ATTRIBUTE                IBM-ipsec-ob-wrap          129             integer
| ATTRIBUTE                IBM-ipsec-ib-ah-wrap       130             integer
| ATTRIBUTE                IBM-ipsec-ib-esp-wrap      131             integer
```

ATTRIBUTE	IBM-ipsec-ob-ah-wrap	132	integer
ATTRIBUTE	IBM-ipsec-ob-esp-wrap	133	integer
ATTRIBUTE	IBM-ipsec-policy-name	135	string
ATTRIBUTE	IBM-ipsec-p1-id	136	string
ATTRIBUTE	IBM-ipsec-p1-name	143	string
ATTRIBUTE	IBM-ipsec-esp-algo	140	string
ATTRIBUTE	IBM-ipsec-ah-algo	141	string
ATTRIBUTE	IBM-ipsec-esp-algo	142	string
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+

Autenticación

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 de supervisor), 1 (privil. operador), 15 (privil. administrador)
- callback-dialinteger

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 limítrofe de área
ack	Acuse de recibo
AIX	Advanced Interactive Executive
AMA	Direccionamiento del MAC arbitrario
AMP	Supervisor presente activo
ANSI	Instituto Nacional de Normalización de los Estados Unidos
AP2	AppleTalk Phase 2
APPN	Red de igual a igual
ARE	Trama exploradora de todas las rutas
ARI/FCI	Indicador de dirección reconocida/indicador de trama copiada
ARP	Address Resolution Protocol
AS	Sistema autónomo
ASBR	Direccionador limítrofe de sistema autónomo
ASCII	American National Standard Code for Information Interchange
ASN.1	Notación de sintaxis de abstracción 1
ASRT	Direccionamiento transparente de origen adaptable
ASYNC	Asíncrono
ATCP	AppleTalk Control Protocol
ATP	AppleTalk Transaction Protocol
AUI	Interfaz de unidad de conexión
ayt	¿Hay alguien ahí?
BAN	Nodo de acceso de límites
BBCM	Bridging Broadcast Manager
BECN	Notificación de congestión explícita hacia atrás
BGP	Border Gateway Protocol
BNC	Bayonet Niell-Concelman
BNCP	Bridging Network Control Protocol
BOOTP	Protocolo BOOT
BPDU	Unidad de datos de protocolo de puente
bps	Bits por segundo
BR	Función de puente/direccionamiento
BRS	Reserva de ancho de banda
BSD	Distribución de software de Berkeley

BTP Agente de relay de BOOTP

BTU Unidad básica de transmisión

CAM Memoria dirigible a través del contenido

CCITT Comisión Consultiva de la Telefonía y Telegrafía Internacionales

CD Detección de colisión

CGWCON Consola de pasarela

CIDR Direccionamiento entre dominios sin clase

CIP Classical IP

CIR Velocidad de información comprometida

CLNP Connectionless-Mode Network Protocol

CPU Unidad central de proceso

CRC Comprobación de redundancia cíclica

CRS Configuration Report Server

CTS Preparado para transmitir

CUD Datos de usuario de llamada

DAF Filtración de direcciones de destino

DB Base de datos

DBsum Resumen de la base de datos

DCD Detector de señal de línea recibida de canal de datos

DCE Equipo de terminación de circuito de datos

DCS Servidor conectado directamente

DDLC Controlador de enlace de datos dual

DDN Defense Data Network

DDP Datagram Delivery Protocol

DDT Dynamic Debugging Tool

DHCP Dynamic Host Configuration Protocol

dir Conectado directamente

DL Enlace de datos

DLC Control de enlace de datos

DLCI Identificador de conexión de enlace de datos

DLS Conmutación del enlace de datos

DLSw Conmutación del enlace de datos

DMA Acceso de memoria directo

DNA Digital Network Architecture

DNCP DECnet Protocol Control Protocol

DNIC Código de identificador de red de datos

DdD Departamento de Defensa

DOS Disk Operating System

DR Direccionador designado

DRAM Memoria de acceso aleatorio dinámica

DSAP Punto de acceso a servicios de destino

DSE Equipo de conmutación de datos

DSE Intercambio de conmutaciones de datos

DSR Aparato de datos preparado

DSU Unidad de servicio de datos

DTE Equipo terminal de datos

DTR Terminal de datos preparado

Dtype Tipo de destino

DVMRP Distance Vector Multicast Routing Protocol

E&M Ear & Mouth

E1 Velocidad de transmisión de 2,048 Mbps

EDEL Delimitador de final

EDI Indicador de errores detectados

EGP Exterior Gateway Protocol

EIA Electronics Industries Association

ELAN LAN emulada

ELAP EtherTalk Link Access Protocol

ELS Sistema para el registro cronológico de sucesos

ELSCon Consola secundaria de ELS

ESI Identificador de sistema final

EST Horario Estándar del Este de los EE.UU

Eth Ethernet

fa-ga Dirección funcional-dirección de grupo

FCS Secuencia de comprobación de trama

FECN Notificación de congestión explícita hacia adelante

FIFO Primero en entrar, primero en salir

FLT Biblioteca de filtros

FR Frame Relay

FRL Frame Relay

FTP File Transfer Protocol

FXO Foreign Exchange Office

FXS Foreign Exchange Station

GMT Hora Media de Greenwich

GOSIP Perfil de Interconexión de Sistemas Abiertos del Gobierno

GTE Compañía Telefónica General

GWCON Consola de pasarela

HDLC Control de enlace de datos de alto nivel

HEX Hexadecimal

HPR Direccionamiento de alto rendimiento

HST TCP/IP Host Services

HTF Formato de tabla de sistema principal

IBD Dispositivo de arranque integrado

ICMP Internet Control Message Protocol

ICP Internet Control Protocol

ID Identificación

IDP Parte de dominio inicial

IDP Internet Datagram Protocol

IEEE Institute of Electrical and Electronics Engineers

Ifc# Número de interfaz

IGP Interior Gateway Protocol

InARP Inverse Address Resolution Protocol

IP Internet Protocol

IPCP IP Control Protocol

IPPN IP Protocol Network

IPX Internetwork Packet Exchange

IPXCP IPX Control Protocol

RDSI Red digital de servicios integrados

ISO Organización Internacional de Normalización

Kbps Kilobits por segundo

LAN Red de área local

LAPB Protocolo de acceso a enlace equilibrado

LAT Transporte de área local

LCS Estación de canal de LAN

LCP Link Control Protocol

LED Diodo emisor de luz

LF Trama mayor; salto de línea

LIS Subred IP lógica

LLC Control de enlace lógico

LLC2 Control de enlace lógico 2

LMI Interfaz de gestión local

LRM LAN Reporting Mechanism

LS Estado de enlace

LSA Anuncio de estado de enlace

LSA Link Services Architecture

LSB Bit menos significativo

LSI Interfaz de métodos abreviados de LAN

LSreq Petición de estado de enlace

LSrxl Lista de retransmisión de estado de enlace

LU Unidad lógica

MAC Control del acceso al medio

Mb Megabit

MB Megabyte

Mbps Megabits por segundo

MBps Megabytes por segundo

MC Multidifusión

MCF Filtración del MAC

MIB Base de la información de gestión

MIB II Base de la información de gestión II

MILNET Red militar

MOS Micro Operating System

MOSDBG Micro Operating System Debugging Tool

MOSPF Open Shortest Path First con extensiones de multidifusión

MPC Canal de diversas vías de acceso

MPC+ Canal de diversas vías de acceso de transferencia de datos de alto rendimiento (HPDT)

MSB Bit más significativo

MSDU Unidad de datos de servicio MAC

MRU Unidad máxima de recepción

MTU Unidad máxima de transmisión

nak Sin acuse de recibo

NAS Estación Nways Switch Administration

NBMA Acceso múltiple sin difusión

NBP Name Binding Protocol

NBR Direccionador vecino

NCP Network Control Protocol

NCP Network Core Protocol

NDPS Conmutación de vías de acceso sin interrupciones

NetBIOS Network Basic Input/Output System

NHRP Next Hop Resolution Protocol

NIST National Institute of Standards and Technology

NPDU Unidad de datos de protocolo de red

NRZ No retorno a cero

NRZI No retorno a cero invertido

NSAP Punto de acceso a servicios de red

NSF National Science Foundation

NSFNET National Science Foundation NETwork

NVCNFG Configuración permanente

OOS fuera de servicio

OPCON Consola del operador

OSI Interconexión de sistemas abiertos

OSICP OSI Control Protocol

OSPF Open Shortest Path First

OUI Identificador exclusivo de organización

PC Personal Computer

PCR Velocidad mayor de célula

PDN Red de datos pública

PING Sonda de paquetes InterNet

PDU Unidad de datos de protocolo

PID Identificación de proceso

P-P Punto a punto

PPP Point-to-Point Protocol

PROM Memoria de sólo lectura programable

PU Unidad física

PVC Circuito virtual permanente

RAM Memoria de acceso aleatorio

RD Descriptor de ruta

REM Ring Error Monitor

REV Recepción

RFC Request for Comments

RI Indicador de llamada; información de direccionamiento

RIF Campo de información de direccionamiento

RII Indicador de información de direccionamiento

RIP Routing Information Protocol

RISC Sistema de juego reducido de instrucciones

RNR Recepción no preparada

ROM Memoria de sólo lectura

ROpcon Consola del operador remota

RPS Ring Parameter Server

RTMP Routing Table Maintenance Protocol

RTP RouTing update Protocol

RTS Petición de emisión

Rtype Tipo de ruta

rxmits Retransmisiones

rxmt Retransmisión

s Segundo

SAF Filtración de direcciones de origen

SAP Punto de acceso a servicios

SAP Service Advertising Protocol

SCR Velocidad sostenida de célula

SCSP Server Cache Synchronization Protocol

sdel Delimitador de inicio

SDLC Relay de SDLC, control síncrono de enlace de datos

seqno Número de secuencia

SGID Identificación de grupo de servidores

SGMP Simple Gateway Monitoring Protocol

SL Línea serie

SMP Supervisor presente en espera

SMTP Simple Mail Transfer Protocol

SNA Systems Network Architecture

SNAP Subnetwork Access Protocol

SNMP Simple Network Management Protocol

SNPA Punto de conexión de subred

SPF Ruta intraárea OSPF

SPE1 Ruta externa OSPF de tipo 1

SPE2 Ruta externa OSPF de tipo 2

SPIA Tipo de ruta inter-área OSPF

SPID Identificación de perfil de servicio

SPX Sequenced Packet Exchange

SQE Error en calidad de señal

SRAM Memoria de acceso aleatorio estática

SRB Puente de direccionamiento en origen

SRF Trama específicamente direccionada

SRLY Relay de SDLC

SRT Transparente de direccionamiento en origen

SR-TB Puente transparente-direccionamiento en origen

STA Estático

STB Puente de árbol de extensión

STE Trama exploradora del árbol de extensión

STP Par trenzado y apantallado; protocolo de árbol de extensión

SVC Circuito virtual conmutado

TB Puente transparente

TCN Notificación de cambio de topología

TCP Transmission Control Protocol

TCP/IP Transmission Control Protocol/Internet Protocol

TEI Identificador de punto de terminal

TFTP Trivial File Transfer Protocol

TKR Red en anillo

TMO Tiempo de espera excedido

TOS Tipo de servicio

TSF Tramas de extensión transparentes

TTL Período de duración

TTY Teletipo

TX Transmisión

UA Acuse de recibo no numerado

UDP User Datagram Protocol

UI Información no numerada

UTP Par trenzado y no apantallado

VCC Conexión de canal virtual

VINES VIrtual NEtworking System

VIR Velocidad de información variable

VL Enlace virtual

VNI Virtual Network Interface

VoFR Voz sobre Frame Relay

VR Ruta virtual

WAN Red de área amplia

WRS Redireccionamiento/restauración de WAN

X.25 Redes de paquetes conmutados

X.251 Capa física de X.25

X.252 Capa de trama de X.25

X.253 Capa de paquetes de X.25

XID Identificación de intercambio

XNS Xerox Network Systems

XSUM Suma de comprobación

ZIP AppleTalk Zone Information Protocol

ZIP2 AppleTalk Zone Information Protocol 2

ZIT Tabla de información de zonas

Glosario

En este glosario figuran términos y definiciones extraídos de los documentos y publicaciones siguientes:

- *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 propiedad del Instituto Nacional de Normalización de los Estados Unidos (ANSI). Si desea adquirir un ejemplares de esta publicación, diríjase a American National Standards Institute, 11 West 42nd Street, New York, New York 10036, Estados Unidos. Las definiciones se identifican mediante el símbolo (A) que aparece después de la definición.
- ANSI/EIA Standard—440-A, *Fiber Optic Terminology*. Si desea adquirir una copia de este documento, diríjase a Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006, Estados Unidos. Las definiciones se identifican mediante el símbolo (E) que aparece después de la definición.
- *Information Technology Vocabulary* redactado por la Subcomisión 1 (SC1), Comisión Técnica Mixta 1 (JTC1), de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). Las definiciones de las secciones publicadas de este vocabulario se identifican mediante el símbolo (I) que aparece después de la definición; las definiciones de los borradores de normas internacionales, borradores de comisiones y documentos de trabajo que está desarrollando la JTC1/SC1 de la ISO/IEC se identifican mediante el símbolo (T) que aparece después de la definición, símbolo que indica que las Corporaciones Nacionales de la SC1 participantes todavía no han llegado a un acuerdo definitivo.
- *IBM Dictionary of Computing*, New York: McGraw-Hill, 1994.
- Internet Request for Comments: 1208, *Glossary of Networking Terms*
- Internet Request for Comments: 1392, *Internet Users' Glossary*
- *Object-Oriented Interface Design: IBM Common User Access Guidelines*, Carmel, Indiana: Que, 1992.

En este glosario, se utilizan las siguientes referencias cruzadas:

Compárese con: Se refiere a un término que tiene un significado opuesto o esencialmente distinto.

Equivale a: Indica que el término tiene el mismo significado que un término preferente, el cual está definido en el lugar que le corresponde dentro del glosario.

Sinónimo de: Es una referencia inversa de un término definido a los demás términos que tienen el mismo significado.

Véase: Remite al lector a términos de diversas palabras que tienen la misma palabra al principio.

Véase también: Remite al lector a términos que tienen un significado relacionado, pero no sinónimo.

A

acceso de memoria directo (DMA). Recurso del sistema que permite que un dispositivo del bus Micro Channel obtenga acceso directo a la memoria del sistema o a la memoria del bus sin la intervención del procesador del sistema.

acceso múltiple con detección de portadora y detección de colisión (CSMA/CD). Protocolo que necesita detección de portadora y en el que una estación de datos transmisora que detecta otra señal mientras transmite detiene la emisión, envía una señal de atasco y luego espera durante un período variable antes de volver a intentar la acción. (T) (A)

ACCESS. En el protocolo Simple Network Management Protocol (SNMP), cláusula de un módulo de la Base de la información de gestión (MIB) que define el nivel mínimo de soporte que proporciona un nodo gestionado para un objeto.

activo. (1) Operativo. (2) Perteneciente a un nodo o dispositivo que está conectado o está disponible para la conexión con otro nodo o dispositivo.

actualización de base de datos de topología (TDU). Mensaje sobre un nodo o enlace nuevo o modificado que se difunde entre los nodos de red APPN para mantener la base de datos de topología de red, que está reproducida en su totalidad en cada nodo de red. Una TDU contiene información para identificar lo siguiente:

- El nodo emisor.
- Las características de nodo y enlace de diversos recursos de la red.
- El número de secuencia de la actualización más reciente para cada uno de los recursos descritos.

acuse de recibo. (1) Transmisión, por parte de un receptor, de caracteres de acuse de recibo como respuesta afirmativa a un remitente. (T) (2) Indicación de que se ha recibido un elemento enviado.

Address Resolution Protocol (ARP). (1) En el conjunto de protocolos de Internet, protocolo que corre-

laciona dinámicamente una dirección IP con una dirección utilizada por una red de área metropolitana o local de soporte, como, por ejemplo, Ethernet o Red en Anillo. (2) Véase también *Reverse Address Resolution Protocol (RARP)*.

agencia operativa privada reconocida (RPOA). Cualquier individuo, empresa o corporación (que no sea un departamento o servicio del gobierno) que realiza operaciones en un servicio de telecomunicaciones y está sujeta a las obligaciones definidas en el Convenio de la unión de telecomunicaciones internacionales y en la legislación; por ejemplo, una empresa de telecomunicación.

agente. Sistema que asume el cometido de agente.

alerta. Mensaje enviado a un punto focal de servicios de gestión de una red para identificar un problema o un problema inminente.

analógico. (1) Perteneciente a datos compuestos por cantidades físicas continuamente variables. (A) (2) Compárese con *digital*.

ancho de banda. El ancho de banda de un enlace óptico designa la capacidad de contener información del enlace y está relacionado con la máxima velocidad en bits a la que puede dar soporte un enlace de fibra.

anillo. Véase *red de tipo anillo*.

anomalía en la autenticación. En el protocolo Simple Network Management Protocol (SNMP), detección (de condición de excepción) que una entidad de autenticación puede haber generado cuando un cliente peticionario no es miembro de la comunidad de SNMP.

antememoria. (1) Almacenamiento intermedio de fines especiales más pequeño y rápido que el almacenamiento principal; se utiliza para que contenga una copia de instrucciones y datos obtenidos del almacenamiento principal y que probablemente necesitará a continuación el procesador. (T) (2) Almacenamiento intermedio que contiene instrucciones y datos a los que se accede frecuentemente; se utiliza para reducir el tiempo del acceso. (3) Parte opcional de la base de datos de directorios existente en los nodos de red donde puede almacenarse información de directorios de uso frecuente para acelerar las búsquedas en directorios. (4) Colocar, ocultar o almacenar en antememoria.

aparato de datos preparado (DSR). Equivale a *DCE preparado*.

AppleTalk. Protocolo de red desarrollado por Apple Computer, Inc. Este protocolo se utiliza para la interconexión de dispositivos de red, que pueden ser una mezcla de productos Apple y productos que no son Apple.

AppleTalk Address Resolution Protocol (AARP). En redes AppleTalk, protocolo que (a) convierte las direcciones de nodo AppleTalk en direcciones de hardware y (b) soluciona las discrepancias de direccionamiento en las redes que dan soporte a más de un conjunto de protocolos.

AppleTalk Transaction Protocol (ATP). En redes AppleTalk, protocolo que proporciona funciones de petición y respuesta de cliente/servidor a los sistemas principales que acceden al protocolo Zone Information Protocol (ZIP) para la información de zonas.

árbol de extensión. En contextos de LAN, método mediante el cual los puentes desarrollan automáticamente una tabla de direccionamiento y actualizan esta tabla en respuesta a un cambio de la topología para asegurarse de la existencia de una sola ruta entre dos LAN cualesquiera en la red con puentes. Este método evita bucles de paquetes, donde un paquete vuelve en una ruta de circuito al direccionador emisor.

archivo de configuración. Archivo que especifica las características de un dispositivo del sistema o una red.

área. En los protocolos de direccionamiento de Internet y DECnet, subconjunto de una red o pasarela que se ha agrupado por definición del administrador de red. Cada área es independiente; la información sobre la topología de un área permanece oculta respecto a las otras áreas.

arquitectura de red. Estructura lógica y principios operativos de una red de sistema. (T)

Nota: Los principios operativos de una red incluyen los principios de los servicios, funciones y protocolos.

arquitectura interconexión de sistemas abiertos (OSI). Arquitectura de red que se ajusta al conjunto particular de normas ISO relacionado con interconexión de sistemas abiertos. (T)

arreglo temporal del programa (PTF). Solución o ajuste temporal de un problema diagnosticado por IBM del release actual no modificado del programa.

asequibilidad. Capacidad de un nodo o recurso para comunicarse con otro nodo o recurso.

asíncrono (ASYNC). Perteneciente a dos o más procesos que no dependen de la aparición de sucesos específicos, como, por ejemplo, señales comunes de temporización. (T)

B

base de datos de configuración (CDB). Base de datos que almacena los parámetros de configuración de uno o diversos dispositivos. Se prepara y actualiza utilizando el programa de configuración.

base de la información de gestión (MIB). (1) Conjunto de objetos a los que se puede acceder por medio de un protocolo de gestión de red. (2) Definición de información de gestión que especifica la información disponible de un sistema principal o una pasarela y las operaciones permitidas. (3) En OSI, depósito conceptual de información de gestión dentro de un sistema abierto.

baudio. En la transmisión asíncrona, unidad de velocidad de modulación correspondiente al intervalo de una unidad por segundo; es decir, si la duración del intervalo de la unidad es de 20 milisegundos, la velocidad de modulación es de 50 baudios. (A)

bit D. Bit de confirmación de entrega. En comunicaciones X.25, bit de un paquete de datos o paquete de petición de llamada que se establece en 1 si el destinatario necesita acuse de recibo (confirmación de entrega) de extremo a extremo.

Border Gateway Protocol (BGP). Protocolo IP utilizado entre dominios y sistemas autónomos.

bucle de direccionamiento. Situación que ocurre cuando los direccionadores hacen circular información entre ellos hasta que se produce la convergencia o hasta que se consideran inasequibles las redes implicadas.

C

cabecera. (1) Información de control definida por el sistema que precede a los datos de usuario. (2) Parte de un mensaje que contiene información de control para el mismo, como, por ejemplo, uno o más campos de destino, el nombre de la estación de origen, el número de secuencia de entrada, una serie que indica el tipo de mensaje y el nivel de prioridad del mensaje.

cabecera de transmisión (TH). Información de control, seguida opcionalmente de una unidad básica de información (BIU) o de un segmento de BIU, que crea y utiliza el control de la vía de acceso para direccionar unidades de mensajes y controlar su flujo dentro de la red. Véase también *unidad de información de vía de acceso*.

canal. (1) Vía de acceso por la que pueden enviarse señales, como, por ejemplo, canal de datos, canal de salida. (A) (2) Unidad funcional, controlada por el procesador, que maneja la transferencia de datos entre el almacenamiento del procesador y el equipo de periféricos local.

canal de diversas vías de acceso (MPC). Protocolo de canal que utiliza diversos subcanales unidireccionales para la comunicación bidireccional de VTAM a VTAM.

canal de entrada/salida. En un sistema de proceso de datos, unidad funcional que maneja la transferencia de datos entre el equipo interno y el equipo de periféricos. (I) (A)

canal lógico. En el funcionamiento en modalidad de paquete, canal de emisión y canal de recepción que se utilizan conjuntamente para enviar y recibir datos sobre un enlace de datos al mismo tiempo. Pueden establecerse varios canales lógicos en el mismo enlace de datos si se intercala la transmisión de paquetes.

canalización. Proceso consistente en romper el ancho de banda de una línea de comunicaciones en varios canales, posiblemente de diferentes tamaños. También se denomina ***multiplexación de la división del tiempo*** (TDM).

capa. (1) En una arquitectura de red, grupo de servicios que está completo desde un punto de vista conceptual, que es uno de los grupos de un conjunto de grupos ordenados jerárquicamente y que se extiende por todos los sistemas que se ajustan a la arquitectura de red. (T) (2) En el modelo de referencia interconexión de sistemas abiertos, uno de los siete grupos de servicios, funciones y protocolos ordenados jerárquicamente y completos conceptualmente que se extienden por todos los sistemas abiertos. (T) (3) En SNA, agrupación de funciones relacionadas que están separadas lógicamente de las funciones de otros grupos. La implementación de las funciones de una capa puede cambiar sin que ello afecte a las funciones de otras capas.

capa de control de enlace de datos (DLC). En SNA, capa que está compuesta por las estaciones de enlace que planifican la transferencia de datos sobre un enlace entre dos nodos y realizan un control de errores para el enlace. Ejemplos de control de enlace de datos son: el SDLC para la conexión de enlaces serie por bit y el control de enlace de datos para el canal de System/370.

Nota: Normalmente, la capa de DLC es independiente del mecanismo de transporte físico y asegura la integridad de los datos que alcanzan las capas superiores.

capa de enlace de datos. En el modelo de referencia de OSI (interconexión de sistemas abiertos), capa que proporciona servicios para la transferencia de datos entre las entidades de la capa de red sobre un enlace de comunicaciones. La capa de enlace de datos

detecta los errores que puedan producirse en la capa física y posiblemente los corrige. (T)

capa de red. En la arquitectura interconexión de sistemas abiertos (OSI), capa que es responsable del direccionamiento, de la conmutación y del acceso a la capa de enlace a lo largo del entorno de OSI.

capa de transporte. En el modelo de referencia interconexión de sistemas abiertos, capa que proporciona un servicio fiable de transferencia de datos de extremo a extremo. Puede haber sistemas abiertos del tipo Relay en la vía de acceso. (T) Véase también *modelo de referencia interconexión de sistemas abiertos*.

capa física. En el modelo de referencia interconexión de sistemas abiertos, capa que proporciona los medios mecánicos, eléctricos, funcionales y de procedimiento para establecer, mantener y liberar conexiones físicas sobre el medio de transmisión. (T)

carácter comodín. Equivale a *carácter de coincidencia con el patrón*.

carácter de coincidencia con el patrón. Carácter especial, como, por ejemplo, un asterisco (*) o un signo de interrogación (?), que puede utilizarse para representar uno o más caracteres. Cualquier carácter o conjunto de caracteres puede sustituir a un carácter de coincidencia con el patrón. Sinónimo de *carácter global* y *carácter comodín*.

CCITT. Comisión consultiva de la telefonía y telegrafía Internacionales. Era una organización de la Unión de Telecomunicaciones Internacionales (ITU). El 1 de marzo de 1993 se reorganizó la ITU y las responsabilidades de la normalización recayeron en una organización subordinada que se denomina Sector de normalización de telecomunicaciones de la unión de telecomunicaciones (ITU-TS). La “CCITT” sigue funcionando para las recomendaciones que se aprobaron antes de la reorganización.

central privada (PBX). Central telefónica privada para la transmisión de llamadas desde y hacia la red telefónica pública.

centro de información de la red (NIC). En comunicaciones de Internet, grupos locales, regionales y nacionales de todo el mundo que proporcionan ayuda, documentación, formación y otros servicios a los usuarios.

circuito de datos. (1) Par de canales de transmisión y recepción asociados que proporcionan un medio de comunicación de datos de dos direcciones. (I) (2) En SNA, sinónimo de *conexión de enlace*. (3) Véase también *circuito físico* y *circuito virtual*.

Notas:

1. Entre los intercambios de conmutaciones de datos, el circuito de datos puede incluir un equipo de terminación de circuito de datos (DCE) de acuerdo con el tipo de interfaz que se utilice en el intercambio de conmutaciones de datos.
2. Entre una estación de datos y un intercambio de conmmutaciones de datos o concentrador de datos, el circuito de datos incluye el equipo de terminación de circuito de datos en el extremo de la estación de datos y puede incluir un equipo similar a un DCE en el intercambio de conmutaciones de datos o en la ubicación del concentrador de datos.

circuito físico. Circuito establecido sin multiplexación. Véase también *circuito de datos*. Compárese con *circuito virtual*.

circuito huérfano. Circuito no configurado cuya disponibilidad se averigua dinámicamente.

circuito virtual. (1) En la conmutación de paquetes, recursos proporcionados por una red que ofrecen el aspecto de una conexión real ante el usuario. (T) Véase también *circuito de datos*. Compárese con *circuito físico*. (2) Conexión lógica establecida entre dos DTE.

circuito virtual conmutado (SVC). Circuito X.25 que se establece dinámicamente cuando es necesario. El equivalente, en X.25, de una línea conmutada. Compárese con *circuito virtual permanente (PVC)*.

circuito virtual permanente (PVC). En comunicaciones de X.25 y Frame-Relay, circuito virtual que tiene un canal lógico asignado permanentemente al mismo en cada equipo terminal de datos (DTE). No son necesarios protocolos de establecimiento de llamada. Compárese con *circuito virtual conmutado (SVC)*.

clase de productividad. En la conmutación de paquetes, velocidad a la que circulan los paquetes de un equipo terminal de datos (DTE) por la red de conmutación de paquetes.

clase de servicio (COS). Conjunto de características (como, por ejemplo, seguridad de ruta, prioridad de transmisión y ancho de banda) utilizadas para crear una ruta entre los asociados a una sesión. La clase de servicio deriva de un nombre de modalidad especificado por el iniciador de una sesión.

cliente. (1) Unidad funcional que recibe servicios compartidos de un servidor. (T) (2) Usuario.

cliente/servidor. En comunicaciones, modelo de interacción en el proceso de datos distribuidos en el que un programa de un sitio envía una petición a un programa de otro sitio y espera una respuesta. El programa

peticionario se denomina cliente; el programa que responde se denomina servidor.

codificar. Convertir datos mediante el uso de un código de manera que sea posible la reconversión al formato original. (T)

colisión. Condición no deseada que deriva de la existencia de transmisiones simultáneas en un canal. (T)

compresión. (1) Proceso consistente en eliminar claros, campos vacíos, redundancias y datos innecesarios para disminuir la longitud de los registros o los bloques. (2) Cualquier codificación destinada a reducir el número de bits utilizados para representar un mensaje o un registro determinado.

comunidad. En el protocolo Simple Network Management Protocol (SNMP), relación administrativa entre las entidades.

concentrador (inteligente). Concentrador de cableado, como, por ejemplo, el IBM 8260, que proporciona funciones de puente y direccionamiento a las LAN con diferentes cables y protocolos.

conectado mediante enlace. (1) Perteneciente a dispositivos que están conectados a una unidad de control por medio de un enlace de datos. (2) Compárese con *conectado mediante canal*. (3) Sinónimo de *remoto*.

conexión. En la comunicación de datos, asociación establecida entre unidades funcionales para comunicar información. (I) (A)

conexión de enlace. (1) Equipo físico que proporciona comunicación en dos direcciones entre una estación de enlace y otra u otras estaciones de enlace; por ejemplo, un equipo de terminación de circuito de datos (DCE) y una línea de telecomunicaciones. (2) En SNA, sinonimia con *circuito de datos*.

conexión Rapid Transport Protocol (RTP). En el direccionamiento de alto rendimiento (HPR), conexión establecida entre los puntos finales de la ruta para transportar tráfico de sesión.

conexión virtual. En Frame Relay, vía de acceso de vuelta de una conexión potencial.

configuración. (1) Manera en que están organizados e interconectados el hardware y el software de un sistema de proceso de información. (T) (2) Dispositivos y programas que componen un sistema, un subsistema o una red.

configuración del sistema. Proceso que especifica los dispositivos y programas que componen un sistema de proceso de datos determinado.

Configuration Report Server (CRS). En IBM Token-Ring Network Bridge Program, servidor que acepta mandatos de LAN Network Manager (LNM) para obtener información de estaciones, establecer parámetros de estación y eliminar estaciones de su anillo. Este servidor también recoge y reenvía informes de configuración generados por las estaciones de su anillo. Los informes de configuración son informes de nuevo supervisor activo e informes de vecino ascendente activo más próximo (NAUN).

congestión. Véase *congestión de la red*.

congestión de la red. Condición no deseada de carga excesiva causada por la presencia de más tráfico del que puede manejar una red.

conmutación de la línea. Equivale a *conmutación del circuito*.

conmutación de paquetes. (1) Proceso consistente en direccionar y transferir datos por medio de paquetes dirigidos de manera que un canal esté ocupado durante la transmisión de un paquete solamente. Cuando se completa la transmisión, el canal queda disponible para la transferencia de otros paquetes. (I) (2) Sinónimo de *funcionamiento en modalidad de paquete*. Véase también *conmutación del circuito*.

conmutación del circuito. (1) Proceso que, a petición, conecta dos o más equipos terminales de datos (DTE) y permite el uso exclusivo de un circuito de datos entre ellos hasta que se libera la conexión. (I) (A) (2) Sinónimo de *conmutación de la línea*.

conmutación del enlace de datos (DLSw). Método para transportar protocolos de red que utilizan el tipo 2 de control de enlace lógico (LLC) de IEEE 802.2. SNA y NetBIOS son ejemplos de protocolos que utilizan el tipo 2 de LLC. Véase también *encapsulación* y *simulación*.

consola remota. Estación que ejecuta OS/2, TCP/IP y el programa Nways Switch Resource Control remoto. Puede conectarse con cualquier estación de soporte de red para realizar operaciones en Nways Switch y darle servicio técnico remotamente.

La conexión puede ser mediante:

- Una línea conmutada que utilice un módem

Cualquier estación de soporte de red puede utilizarse como consola remota de otra estación de soporte de red.

control de enlace de datos (DLC). Conjunto de normas utilizado por los nodos de un enlace de datos (como, por ejemplo, un enlace de SDLC o una Red en Anillo) para efectuar un intercambio de información ordenado.

control de enlace de datos de alto nivel (HDLC). En la comunicación de datos, utilización de una serie de bits especificada para controlar enlaces de datos de acuerdo con las normas internacionales respecto al HDLC: la estructura de trama de ISO 3309 y los elementos de procedimientos de ISO 4335.

control de enlace lógico (LLC). Subcapa de LAN de control de enlace de datos (DLC) que proporciona dos tipos de operaciones de DLC para el intercambio ordenado de información. El primer tipo es el servicio sin conexiones, que permite enviar y recibir información sin establecer un enlace. La subcapa de LLC no efectúa recuperación de errores ni control del flujo para el servicio sin conexiones. El segundo tipo es el servicio orientado a las conexiones, que requiere el establecimiento de un enlace antes del intercambio de información. El servicio orientado a las conexiones proporciona transferencia de información en secuencia, control del flujo y recuperación de errores.

control de la vía de acceso (PC). Función que direcciona unidades de mensajes entre las unidades de red accesibles de la red y proporciona las vías de acceso entre éstas. Convierte las unidades básicas de información (BIU) del control de transmisión (posiblemente segmentándolas) en unidades de información de vía de acceso (PIU) e intercambia unidades básicas de transmisión que contienen una o más PIU con el control de enlace de datos. El control de la vía de acceso difiere según el tipo de nodo: algunos nodos (los nodos APPN, por ejemplo) utilizan identificadores de sesión generados localmente para el direccionamiento y otros (los nodos de subárea) utilizan direcciones de red para el direccionamiento.

control del acceso al medio (MAC). En las LAN, subcapa de la capa de control de enlace de datos que da soporte a funciones dependientes del medio y utiliza los servicios de la capa física para proporcionar servicios a la subcapa de control de enlace lógico (LLC). La subcapa del MAC incluye el método para determinar cuándo un dispositivo tiene acceso al medio de transmisión.

control del flujo. (1) En SNA, proceso consistente en gestionar la velocidad a la que pasa el tráfico de datos entre los componentes de la red. La finalidad del control del flujo es optimizar la velocidad del flujo de unidades de mensajes con la congestión mínima de la red; es decir, ni desbordar los almacenamientos intermedios del receptor o de nodos de direccionamiento intermedio ni dejar al receptor esperando más unidades de mensajes. (2) Véase también *ritmo*.

Control síncrono de enlace de datos (SDLC). (1) Disciplina que se ajusta a los subconjuntos de los Advanced Data Communication Control Procedures (ADCCP) del American National Standards Institute (ANSI) y del High-level Data Link Control (HDLC) de la organización internacional para la normalización, y está destinada a la gestión de la transferencia síncrona de información serie por bit de código transparente sobre una conexión de enlace. Los intercambios de transmisiones pueden ser dúplex o semi-dúplex sobre enlaces conmutados o no conmutados. La configuración de la conexión de enlace puede ser de punto a punto, de multipunto o de bucle. (I) (2) Compárese con *comunicación síncrona en binario (BSC)*.

correlación. Proceso consistente en convertir datos que el emisor transmite con un formato determinado en el formato de datos que puede aceptar el receptor.

corriente de datos general (GDS). Corriente de datos utilizada para las conversaciones en sesiones de LU 6.2.

coste de la vía de acceso. En los protocolos de direccionamiento de estado de los enlaces, suma de los costes de enlace a lo largo de la vía de acceso entre dos nodos o redes.

cronometraje. (1) En la comunicación síncrona en binario, utilización de pulsaciones de reloj para controlar la sincronización de los datos y caracteres de control. (2) Método para controlar el número de bits de datos enviados en una línea de telecomunicaciones en un momento determinado.

cuenta de saltos. (1) Métrica o medida de distancia entre dos puntos. (2) En comunicaciones de Internet, número de direccionadores por los que pasa un datagrama cuando se dirige a su destino. (3) En SNA, medida consistente en el número de enlaces por los que se debe pasar en la vía de acceso a un destino.

D

daemon. Programa que se ejecuta desatendido para realizar un servicio estándar. Algunos daemon se desencadenan de manera automática para realizar su tarea; otros realizan las operaciones periódicamente.

Datagram Delivery Protocol (DDP). En redes AppleTalk, protocolo que proporciona conectividad de red por medio de un servicio de entrega de socket a socket sin conexiones de la capa de internet.

datagrama. (1) En la conmutación de paquetes, paquete individual e independiente de otros paquetes que contiene información suficiente para el direccionamiento desde el equipo terminal de datos (DTE) de origen al DTE de destino sin apoyarse en intercambios anteriores entre los DTE y la red. (I) (2) En TCP/IP, unidad básica de información que pasa a través del entorno de Internet. Un datagrama contiene direcciones de origen y de destino junto con los datos. Un datagrama de Internet Protocol (IP) está compuesto

por una cabecera de IP seguida de los datos de capa de transporte. (3) Véase también *paquete* y *segmento*.

datagrama de IP. En el conjunto de protocolos de Internet, unidad básica de información transmitida a través de una internet. Contiene direcciones de origen y de destino, datos de usuario e información de control, como, por ejemplo, la longitud del datagrama, la suma de comprobación de cabecera y distintivos que indican si el datagrama puede fragmentarse o si se ha fragmentado.

DCE preparado. En la norma EIA 232, señal que indica al equipo terminal de datos (DTE) que el equipo de terminación de circuito de datos (DCE) local está conectado al canal de comunicaciones y se encuentra preparado para enviar datos. Sinónimo de *aparato de datos preparado (DSR)*.

DECnet. Arquitectura de red que define el funcionamiento de una familia de módulos de software, bases de datos y componentes de hardware que se utilizan normalmente con el fin de conectar entre sí sistemas Digital Equipment Corporation para el compartimiento de recursos, cálculo distribuido o configuración de sistemas remotos. Las implementaciones de la red DECnet siguen el modelo Digital Network Architecture (DNA).

detección (de condición de excepción). En Simple Network Management Protocol (SNMP), mensaje enviado por un nodo gestionado (la función de agente) a una estación de gestión para informarle de una condición de excepción.

detección de colisión. En el acceso múltiple con detección de portadora y detección de colisión (CSMA/CD), señal que indica que dos o más estaciones están transmitiendo simultáneamente.

detección de portadora. En una red de área local, actividad continua de una estación de datos para detectar si otra estación está transmitiendo. (T)

detector de portadora. Equivale a *detector de señal de línea recibida (RLSD)*.

detector de portadora de datos (DCD). Equivale a *detector de señal de línea recibida (RLSD)*.

detector de señal de línea recibida (RLSD). En la norma EIA 232, señal que indica al equipo terminal de datos (DTE) que está recibiendo una señal del equipo de terminación de circuito de datos (DCE) remoto. Sinónimo de *detector de portadora* y *detector de portadora de datos (DCD)*.

determinación de problemas. Proceso consistente en determinar el origen de un problema; por ejemplo, un componente de un programa, una anomalía en una máquina, recursos de telecomunicaciones, programas o equipos instalados por el contratista o por el usuario, una anomalía del entorno, como, por ejemplo, pérdida de alimentación, o un error del usuario.

difusión. (1) Transmisión de los mismos datos a todos los destinos. (T) (2) Transmisión simultánea de datos a más de un destino. (3) Compárese con *multidifusión*.

digital. (1) Perteneciente a datos compuestos por dígitos. (T) (2) Perteneciente a datos con formato de dígitos. (A) (3) Compárese con *analógico*.

Digital Network Architecture (DNA). Modelo para todas las implementaciones de hardware y software DECnet.

dirección. En la comunicación de datos, código exclusivo asignado a cada dispositivo, estación de trabajo o usuario conectado a una red.

dirección administrada localmente. En una red de área local, dirección de adaptador que el usuario puede asignar para alterar temporalmente la dirección administrada universalmente. Compárese con *dirección administrada universalmente*.

dirección administrada universalmente. En una red de área local, dirección codificada de forma permanente en un adaptador en el momento de la fabricación. Todas las direcciones administradas universalmente son exclusivas. Compárese con *dirección administrada localmente*.

dirección canónica. En las LAN, formato de IEEE 802.1 de la transmisión de direcciones del control del acceso al medio (MAC) para adaptadores de Red en Anillo y Ethernet. En el formato canónico, el bit menos significativo (situado más a la derecha) de cada byte de dirección se transmite en primer lugar. Compárese con *dirección no canónica*.

dirección de difusión. En comunicaciones, dirección de estación (ocho números 1) reservada como dirección común a todas las estaciones de un enlace. Sinónimo de *dirección de todas las estaciones*.

dirección de red. Según ISO 7498-3, nombre que no es ambiguo en el entorno de OSI y que identifica a un conjunto de puntos de acceso a servicios de red.

dirección de subred. En comunicaciones de Internet, extensión del esquema básico de direccionamiento de IP donde una parte de la dirección de sistema principal se interpreta como dirección de red local.

dirección de todas las estaciones. En comunicaciones, sinónimo de *dirección de difusión*.

dirección de usuario de red (NUA). En comunicaciones de X.25, dirección X.121 que contiene hasta 15 dígitos en código binario.

dirección Internet. Véase *dirección IP*.

dirección IP. Dirección de 32 bits definida en el documento RFC 791, que contiene las especificaciones del protocolo IP, estándar 5. Normalmente, se representa mediante formato decimal con puntos.

dirección no canónica. En las LAN, formato de la transmisión de direcciones del control del acceso al medio (MAC) para adaptadores de Red en Anillo. En el formato no canónico, el bit más significativo (situado más a la izquierda) de cada byte de dirección se transmite en primer lugar. Compárese con *dirección canónica*.

direccionador. (1) Sistema que determina la vía de acceso del flujo de tráfico de red. La selección de vía de acceso se realiza entre diversas vías de acceso sobre la base de la información obtenida a partir de protocolos específicos, algoritmos que intentan identificar la vía de acceso mejor o la más corta, y otros criterios, como, por ejemplo, direcciones de destino específicas de los protocolos o la métrica. (2) Dispositivo de conexión que conecta dos segmentos de LAN, los cuales utilizan arquitecturas similares o diferentes, en la capa de red del modelo de referencia. (3) En terminología de OSI, función que determina una vía de acceso mediante la cual puede accederse a una entidad. (4) En TCP/IP, sinonimia con *pasarela*. (5) Compárese con *puente*.

direccionador de IP. Dispositivo de una internet IP que tiene la responsabilidad de tomar decisiones acerca de las vías de acceso por las que fluirá tráfico de red. Los protocolos de direccionamiento se utilizan para obtener información sobre la red y para determinar la mejor ruta por la que debe reenviarse el datagrama hacia el destino final. Los datagramas se direccionan sobre la base de direcciones de destino IP.

direccionador designado. Direccionador que informa a los nodos finales de la existencia y la identidad de los otros direccionadores. La selección del direccionador designado se basa en el direccionador con la prioridad superior. Cuando diversos direccionadores comparten la prioridad superior, se selecciona el direccionador con la dirección de estación superior.

direccionador generador. En redes AppleTalk, direccionador que mantiene datos de configuración (números de red de rango y listas de zonas, por ejemplo) para la red. Cada red debe tener, como mínimo, un direccionador generador. El direccionador generador debe configurarse inicialmente por medio de la herramienta configuradora. Compárese con *direccionador no generador*.

direccionador limítrofe. En comunicaciones de Internet, direccionador que está situado en el borde de un sistema autónomo y que se comunica con un direccionador que está situado en el borde de un sistema autónomo diferente.

direccionador no generador. En redes AppleTalk, direccionador que obtiene información del rango de números de red y de la lista de zonas de un direccionador generador conectado a la misma red.

direccionador troncal. (1) Direccionador utilizado para transmitir datos entre áreas. (2) Direccionador de una serie que se utiliza para interconectar redes de manera que formen una internet mayor.

direccionamiento. (1) Asignación de la vía de acceso mediante la cual un mensaje va a alcanzar su destino. (2) En SNA, reenvío de una unidad de mensaje por una vía de acceso determinada a través de una red tal como lo determinan los parámetros contenidos en la unidad de mensaje, como, por ejemplo, la dirección de red de destino de una cabecera de transmisión.

direccionamiento. En la comunicación de datos, manera que tiene una estación de seleccionar la estación a la que va a enviar datos.

direccionamiento de alto rendimiento (HPR). Adición para la arquitectura Advanced Peer-to-Peer Networking (APPN) que mejora el rendimiento y la fiabilidad del direccionamiento de datos, especialmente en la utilización de enlaces de gran velocidad.

direccionamiento de sesiones intermedias (ISR). Tipo de función de direccionamiento de un nodo de red APPN que proporciona información de indisponibilidad y control del flujo de nivel de sesión para todas las sesiones que pasan por el nodo pero cuyos puntos finales están en otra parte.

direccionamiento dinámico. Direccionar utilizando rutas averiguadas en lugar de las rutas configuradas estáticamente durante la inicialización.

direccionamiento en origen. En las LAN, método mediante el cual la estación emisora determina la ruta que la trama seguirá e incluye la información de direccionamiento en la trama. A continuación, los puentes leen la información de direccionamiento para determinar si deben reenviar la trama.

direccionamiento intraárea. En comunicaciones de Internet, direccionamiento de datos dentro de un área.

direcciones MAC arbitrarias (AMA). En la arquitectura DECnet, esquema de direcciones utilizado por DECnet Phase IV-Prime que da soporte a direcciones administradas universalmente y direcciones administradas localmente.

directorio. Tabla de identificadores y referencias para los elementos de datos correspondientes. (I) (A)

dispositivo. Aparato mecánico, eléctrico o electrónico con un fin específico.

dominio. (1) Parte de una red de sistema en la que los recursos de proceso de datos están bajo un control común. (T) (2) En interconexión de sistemas abiertos (OSI), parte de un sistema distribuido o conjunto de objetos gestionados a los que se aplica una política común. (3) Véase *Dominio administrativo* y *nombre de dominio*.

Dominio administrativo. Conjunto de sistemas principales y direccionadores, y las redes de interconexión, que gestiona una sola autoridad administrativa.

dominio de direccionamiento. En comunicaciones de Internet, grupo de sistemas intermedios que utilizan un protocolo de direccionamiento para que la representación de la red en un conjunto sea la misma en cada sistema intermedio. Los dominios de direccionamiento se conectan entre sí mediante enlaces exteriores.

E

eco. En la comunicación de datos, señal de un canal de comunicaciones reflejada. Por ejemplo, en un terminal de comunicaciones, cada señal se visualiza dos veces, una cuando entra en el terminal local y otra cuando vuelve sobre el enlace de comunicaciones. Esto permite comprobar la exactitud de las señales.

EIA 232. En la comunicación de datos, especificación de la Electronic Industries Association (EIA) que define la interfaz entre el equipo terminal de datos (DTE) y el equipo de terminación de circuito de datos (DCE), que utiliza el intercambio de datos binarios serie.

Electronic Industries Association (EIA). Organización de fabricantes del campo de la electrónica que anticipa el crecimiento tecnológico de la industria, representa los puntos de vista de sus miembros y desarrolla normas para la industria.

encapsulación. (1) En comunicaciones, técnica utilizada por protocolos de capa mediante la cual una capa añade a la unidad de datos de protocolo (PDU) información de control de la capa a la que da soporte. A este respecto, la capa encapsula los datos de la capa soportada. En el conjunto de protocolos de Internet, por ejemplo, un paquete contendrá información de control de la capa física, a continuación información de control de la capa de red y a continuación los datos de protocolo de la aplicación. (2) Véase también *conmutación del enlace de datos*.

enlace. Combinación de la conexión de enlace (el medio de transmisión) y dos estaciones de enlace, una a cada extremo de la conexión de enlace. Una conexión de enlace puede estar compartida entre diversos enlaces en una configuración de multipunto o Red en Anillo.

enlace lógico. Par de estaciones de enlace, una en cada uno de dos nodos adyacentes, y su conexión de enlace subyacente que proporcionan una sola conexión de capa de enlace entre los dos nodos. Pueden distinguirse diversos enlaces lógicos mientras comparten el uso del mismo medio físico de conexión de dos nodos. Ejemplos son los enlaces lógicos de 802.2 utilizados en recursos de red de área local (LAN) y los enlaces lógicos de LAP E del mismo enlace físico punto a punto entre dos nodos. El término enlace lógico también incluye los diversos canales lógicos de X.25 que comparten el uso del enlace de acceso de un DTE con una red X.25.

enlace virtual. En OSPF (Open Shortest Path First), interfaz punto a punto que conecta direccionadores limítrofes separados por un área de tránsito no troncal. Puesto que los direccionadores de área forman parte de la red troncal OSPF, el enlace virtual conecta la red troncal. Los enlaces virtuales garantizan que la red troncal OSPF no se vuelva discontinua.

equipo de terminación de circuito de datos (DCE). En una estación de datos, equipo que proporciona la conversión de señal y la codificación entre el equipo terminal de datos (DTE) y la línea. (I)

Notas:

1. El DCE puede ser un equipo independiente o parte integral del DTE o del equipo intermedio.
2. Un DCE puede realizar otras funciones que normalmente se llevan a cabo al final de red de la línea.

equipo terminal de datos (DTE). Parte de una estación de datos que funciona como origen y/o destino de datos. (I) (A)

esfera de control (SOC). Conjunto de dominios de punto de control servidos por un solo punto focal de servicios de gestión.

estación. Punto de entrada o salida de un sistema que utiliza recursos de telecomunicaciones; por ejemplo, uno o más sistemas, terminales, dispositivos y programas asociados de una ubicación determinada que pueden enviar o recibir datos sobre una línea de telecomunicaciones.

estación de configuración Nways Switch. Estación de OS/2 dedicada que ejecuta una versión autónoma de la herramienta Nways Switch Configuration Tool (NCT). Se utiliza para generar una base de datos de configuración de red y debe instalarse como consola remota.

estación de enlace. (1) Componentes de hardware y software de un nodo que representan una conexión con un nodo adyacente sobre un enlace específico. Por ejemplo, si el nodo A es el extremo primario de una línea multipunto que se conecta con tres nodos adyacentes, el nodo A tendrá tres estaciones de enlace que representarán las conexiones con los nodos adyacentes. (2) Véase también *estación de enlace adyacente (ALS)*.

estación de gestión. En comunicaciones de Internet, sistema responsable de la gestión de toda una red o de parte de la misma. La estación de gestión se comunica con agentes de gestión de red que residen en el nodo gestionado por medio de un protocolo de gestión de red, como, por ejemplo, Simple Network Management Protocol (SNMP).

estación de gestión de red. En el protocolo Simple Network Management Protocol (SNMP), estación que ejecuta programas de aplicación de gestión que supervisan y controlan elementos de red.

estación de soporte de red. Procesador utilizado para realizar operaciones en Nways Switch y darle servicio técnico localmente. Lo utilizan el administrador o el personal de servicio encargados de Nways Switch.

estado de los enlaces. En los protocolos de direccionamiento, información anunciada sobre las interfaces utilizables y los vecinos a los que se puede llegar de un direccionador o una red. La base de datos topológica del protocolo se forma a partir de los anuncios reunidos sobre el estado de los enlaces.

estructura de la información de gestión (SMI). (1) En el protocolo Simple Network Management Protocol (SNMP), normas utilizadas para definir los objetos a los que puede accederse por medio de un protocolo de gestión de red. (2) En OSI, conjunto de normas relativas a la información de gestión. El conjunto incluye el *Management Information Model* y las *Guidelines for the Definition of Managed Objects.*

Ethernet. Red de área local de banda base de 10 Mbps que permite que diversas estaciones accedan al medio de transmisión a voluntad sin coordinación previa, evita la contención utilizando la detección y deferencia de portadora y resuelve la contención utilizando la detección de colisión y la retransmisión retardada. Ethernet utiliza el acceso múltiple con detección de portadora y detección de colisión (CSMA/CD).

excepción. Condición anormal, como, por ejemplo, un error de E/S encontrado durante el proceso de un conjunto de datos o archivo.

extensión de ruta (REX). En SNA, componentes de red de control de la vía de acceso, incluido un enlace periférico, que componen la parte de una vía de acceso que está entre un nodo de subárea y una unidad de red dirigible (NAU) de un nodo periférico adyacente. Véase también *ruta explícita (ER)*, *vía de acceso* y *ruta virtual (VR)*.

Exterior Gateway Protocol (EGP). En el conjunto de protocolos de Internet, protocolo utilizado entre dominios y sistemas autónomos que permite anunciar e intercambiar información sobre la asequibilidad de la red. Las direcciones de red IP de un sistema autónomo se anuncian en otro sistema autónomo por medio de direccionadores que participan de EGP. Un ejemplo de EGP es Border Gateway Protocol (BGP). Compárese con Interior Gateway Protocol (IGP).

F

fax. Copia impresa que se recibe de una máquina de facsímil. Sinónimo de ***telecopia.***

File Transfer Protocol (FTP). En el conjunto de protocolos de Internet, protocolo de capa de aplicación que utiliza servicios de TCP y Telnet para transferir archivos de datos generales entre máquinas o sistemas principales.

fluctuación. (1) Variaciones no acumulativas a corto plazo de los instantes significativos de una señal digital respecto a sus posiciones ideales en el tiempo. (2) Variaciones no deseadas de una señal digital transmitida. (3) Variaciones en el retardo de la red.

formato decimal con puntos. Representación sintáctica de un entero de 32 bits que consta de cuatro números de 8 bits escritos en base 10 con puntos que los separan. Se utiliza para representar direcciones IP.

fragmentación. (1) Proceso consistente en dividir un datagrama en partes más pequeñas, o fragmentos, para que se ajuste a las posibilidades del medio físico por el que se va a transmitir. (2) Véase también *segmentación*.

fragmento. Véase *fragmentación*.

Frame Relay. (1) Norma de interfaz que describe el límite entre el equipo de un usuario y una red de paquetes rápidos. En los sistemas Frame-Relay, se eliminan las tramas defectuosas; la recuperación se produce de extremo a extremo en lugar de efectuarse salto a salto. (2) Técnica derivada de la norma de canal D de red digital de servicios integrados (RDSI). Supone que las conexiones son fiables y prescinde de la actividad general de control y detección de errores en la red.

función de puente. En las LAN, el reenvío de una trama de un segmento de LAN a otro. El destino está especificado mediante la dirección de subcapa del control del acceso al medio (MAC) codificada en el

campo de dirección de destino de la cabecera de la trama.

función de puente local. Función de un programa de puente que permite que un solo puente conecte diversos segmentos de LAN sin la utilización de un enlace de telecomunicaciones. Compárese con *función de puente remota*.

función de puente remota. Función de un puente que permite que dos puentes conecten diversas LAN utilizando un enlace de telecomunicaciones. Compárese con *función de puente local*.

función de puente transparente. En las LAN, método para relacionar redes de área local individuales entre sí en el nivel del control del acceso al medio (MAC). Un puente transparente almacena las tablas que contienen direcciones del MAC para que las tramas que ve el puente puedan reenviarse a otra LAN si las tablas lo indican así.

funcionamiento en modalidad de paquete. Equivale a *conmutación de paquetes*.

G

gestión de red. Proceso consistente en planificar, organizar y controlar un proceso de datos o sistema de información orientado a las comunicaciones.

gestor de red. Programa o grupo de programas que se utiliza para supervisar y gestionar una red así como para diagnosticar los problemas de la misma.

grupo de transmisión (TG). (1) Conexión entre nodos adyacentes que se identifica mediante un número de grupo de transmisión. (2) En una red de subárea, enlace o grupo de enlaces entre nodos adyacentes. Cuando un grupo de transmisión está compuesto por un grupo de enlaces, los enlaces se ven como un solo enlace lógico y el grupo de transmisión se denomina *grupo de transmisión multienlace (MLTG)*. Un *grupo de transmisión multienlace de mezcla de medios (MMMLTG)* contiene enlaces de diferentes tipos de medios (por ejemplo, Red en Anillo, SDLC conmutado, SDLC no conmutado y enlaces Frame-Relay). (3) En una red APPN, enlace entre nodos adyacentes. (4) Véase también *grupos de transmisión paralelo*.

grupos de transmisión paralelo. Diversos grupos de transmisión entre nodos adyacentes, teniendo cada grupo un número de grupo de transmisión distinto.

H

Hello. Protocolo utilizado por un grupo de direccionadores que cooperan y se apoyan entre sí para poder descubrir rutas de retardo mínimo.

heurístico. Perteneciente a métodos exploratorios para la resolución de problemas en los que se descubren soluciones mediante una evaluación del progreso realizada respecto al resultado final.

histéresis. Cantidad que indica cuánto debe cambiar la temperatura una vez pasado el umbral del establecimiento de alerta y antes de que se elimine la condición de alerta.

horizonte dividido. Técnica destinada a minimizar el tiempo para conseguir la convergencia en la red. Un direccionador registra la interfaz sobre la que ha recibido una ruta en particular y no propaga su información sobre la ruta otra vez sobre la misma interfaz.

I

identificación de intercambio (XID). Tipo específico de unidad básica de enlace que se utiliza para la comunicación de características de nodo y enlace entre nodos adyacentes. Los XID se intercambian entre estaciones de enlace antes de la activación del enlace y durante la misma para establecer y negociar las características de enlace y nodo, y después de la activación del enlace para comunicar los cambios de estas características.

identificador de conexión de enlace de datos (DLCI). Identificador numérico de un subpuerto Frame-Relay o segmento de PVC en una red Frame-Relay. Cada subpuerto de un puerto Frame-Relay individual tiene un DLCI exclusivo. La tabla siguiente, extraída de la norma T1.618 del American National Standards Institute (ANSI) y la norma Q.922 de la Comisión Consultiva de la telefonía y telegrafía internacionales (ITU-T/CCITT), indica las funciones asociadas con determinados valores de DLCI:

Valores de DLCI	Función
0	Señalización de canal de entrada
1–15	Se reserva
16–991	Se asigna utilizando procedimientos de conexión de Frame-Relay
992–1007	Gestión de capa 2 de servicio portador de Frame-Relay
1008–1022	Se reserva
1023	Gestión de capa de canal de entrada

identificador de puente. Campo de 8 bytes que se utiliza en un protocolo de árbol de extensión y está compuesto por la dirección MAC del puerto con el identificador de puerto más bajo y un valor definido por el usuario.

identificador de red. (1) En TCP/IP, parte de la dirección IP que define a una red. La longitud del identificador de red depende del tipo de la clase de red (A, B o C). (2) Nombre de 1 a 8 bytes seleccionado por el cliente o nombre de 8 bytes registrado por IBM que identifica de manera exclusiva a una subred específica.

inhabilitado. (1) Perteneciente a un estado de una unidad de proceso que evita la aparición de determinados tipos de interrupciones. (2) Perteneciente al estado en el cual una unidad de control de transmisión o unidad de respuestas audibles no puede aceptar llamadas de entrada de una línea.

inhabilitar. Convertir en no funcional.

Instituto Nacional de Normalización de los Estados Unidos (ANSI). Organización compuesta por productores, clientes y grupos con intereses generales que establece los procedimientos mediante los cuales organizaciones acreditadas crean y mantienen normas voluntarias de la industria en los Estados Unidos. (A)

Integrated Digital Network Exchange (IDNX). Procesador que integra aplicaciones a base de voz, datos e imágenes. También gestiona los recursos de transmisión y se conecta a multiplexores y sistemas de soporte de gestión de redes. Permite la integración de equipos de diferentes proveedores.

intercalación. (1) Alternancia de dos o más operaciones o funciones por medio del uso superpuesto de un programa de utilidad informático. (2) En transmisión de datos, alternancia de los paquetes de una corriente de datos con los de otra.

intercambio de conmutaciones de datos (DSE). Equipo instalado en una ubicación individual para proporcionar funciones de conmutación, como, por ejemplo, conmutación del circuito, conmutación de mensajes y conmutación de paquetes. (I)

interconexión de sistemas abiertos (OSI). (1) Interconexión de sistemas abiertos que sigue las normas de la organización internacional para la normalización (ISO) para el intercambio de información. (T) (A) (2) Utilización de procedimientos normalizados para permitir la interconexión de sistemas de proceso de datos.

Nota: La arquitectura OSI establece una infraestructura para coordinar el desarrollo de normas actuales y futuras de cara a la interconexión de sistemas. Las funciones de red se dividen en siete capas. Cada capa representa un grupo de funciones relacionadas de proceso de datos y comunicación que pueden llevarse a cabo de una manera estándar para dar soporte a diferentes aplicaciones.

interfaz. (1) Límite compartido entre dos unidades funcionales en cuya definición entran características funcionales, características de señalización u otras características según lo que corresponda. El concepto incluye la especificación de la conexión de dos dispositivos que tienen funciones diferentes. (T) (2) Hardware y/o software para el enlace de sistemas, programas o dispositivos.

interfaz de gestión local (LMI). Véase *protocolo de interfaz de gestión local (LMI)*.

interfaz de unidad de conexión (AUI). En una red de área local, interfaz entre la unidad de conexión al medio y el equipo terminal de datos de una estación de datos. (I) (A)

Interior Gateway Protocol (IGP). En el conjunto de protocolos de Internet, protocolo utilizado para propagar información sobre la asequibilidad y direccionamiento de la red dentro de un sistema autónomo. Ejemplos de IGP son Routing Information Protocol (RIP) y Open Shortest Path First (OSPF).

Internet. Red internet administrada por la Internet Architecture Board (IAB) y compuesta por grandes redes troncales nacionales así como por muchas redes regionales y de campus en todo el mundo. Internet utiliza el conjunto de protocolos de Internet.

internet. Conjunto de redes interconectadas por una serie de direccionadores que les permiten funcionar como una sola red grande. Véase también *Internet*.

Internet Architecture Board (IAB). Corporación técnica que supervisa el desarrollo del conjunto de protocolos de Internet conocidos como TCP/IP.

Internet Control Message Protocol (ICMP). Protocolo utilizado para manejar mensajes de control y errores en la capa de Internet Protocol (IP). Los informes sobre problemas y destinos incorrectos de datagramas se devuelven al origen del datagrama. ICMP forma parte de Internet Protocol.

Internet Control Protocol (ICP). Protocolo de VIrtual NEtworking System (VINES) que proporciona notificaciones de excepciones, notificaciones sobre métrica y el soporte del programa PING. Véase también *RouTing update Protocol (RTP)*.

Internet Engineering Task Force (IETF). Grupo de operaciones de la Internet Architecture Board (IAB) que es responsable de la resolución de las necesidades técnicas de la Internet a corto plazo.

Internet Protocol (IP). Protocolo sin conexiones que direcciona datos a través de una red o redes interconectadas. IP actúa como intermediario entre las capas de protocolos superiores y la red física. No obstante, este protocolo no proporciona recuperación de errores ni control del flujo ni garantiza la fiabilidad de la red física.

Internetwork Packet Exchange (IPX). (1) Protocolo de red utilizado para conectar servidores Novell, o cualquier estación de trabajo o direccionador que implemente IPX, con otras estaciones de trabajo. Aunque es similar a Internet Protocol (IP), IPX utiliza unos formatos de paquete y una terminología diferentes. (2) Véase también *Xerox Network Systems (XNS)*.

interoperatividad. Posibilidad de comunicarse, ejecutar programas o transferir datos entre diversas unidades funcionales de tal forma que el usuario necesite tener poco conocimiento, o ninguno, de las características exclusivas de estas unidades. (T)

Inverse Address Resolution Protocol (InARP). En el conjunto de protocolos de Internet, protocolo utilizado para ubicar una dirección de protocolo mediante la dirección de hardware conocida. En un contexto de Frame-Relay, identificador de conexión de enlace de datos (DLCI) es sinónimo de dirección de hardware conocida.

IPPN. Interfaz que otros protocolos pueden utilizar para transportar datos sobre IP.

IPXWAN. Protocolo de Novell que se utiliza para intercambiar información de direccionador a direccionador antes de intercambiar información de direccionamiento de Internetwork Packet Exchange (IPX) estándar y tráfico sobre redes de área amplia (WAN).

L

LAN Network Manager (LNM). Programa bajo licencia de IBM que permite que un usuario gestione y supervise recursos de LAN desde una estación de trabajo central.

línea tronco. Línea de gran velocidad que conecta dos Nways Switch. Puede ser un cable coaxial, un cable de fibra u ondas de radio, por ejemplo, y puede alquilarse en empresas de telecomunicación.

local. (1) Perteneciente a un dispositivo al que se accede directamente sin utilizar una línea de telecomunicaciones. (2) Compárese con *remoto*. (3) Equivale a *conectado mediante canal*.

M

mandato ping. Mandato que envía un paquete de petición con eco de Internet Control Message Protocol (ICMP) a una pasarela, direccionador o sistema principal esperando recibir una respuesta.

máscara. (1) Patrón de caracteres utilizado para controlar la retención o eliminación de partes de otro patrón de caracteres. (I) (A) (2) Utilizar un patrón de caracteres para controlar la retención o eliminación de partes de otro patrón de caracteres. (I) (A)

máscara de dirección. Respecto a las subredes de internet, máscara de 32 bits utilizada para identificar los bits de dirección de subred de la parte del sistema principal de una dirección IP. Sinónimo de *máscara de subred* y *máscara de subred (grupo de nodos)*.

máscara de subred. Equivale a *máscara de dirección*.

máscara de subred (grupo de nodos). Equivale a *máscara de dirección*.

memoria de almacenamiento dinámico. Cantidad de RAM utilizada para asignar estructuras de datos dinámicamente.

memoria de sólo lectura (ROM). Memoria en la que el usuario no puede modificar los datos almacenados salvo en condiciones especiales.

memoria instantánea. Dispositivo de almacenamiento de datos que puede programarse y borrarse y que no necesita alimentación continua. La ventaja principal de la memoria instantánea sobre otros dispositivos de almacenamiento de datos que pueden programarse y borrarse es que puede volver a programarse sin quitarla de la placa de circuitos.

mensaje hello. (1) Mensaje enviado periódicamente para establecer y probar la asequibilidad entre direccionadores o entre direccionadores y sistemas principales. (2) En el conjunto de protocolos de Internet, mensaje definido por el protocolo Hello como Interior Gateway Protocol (IGP).

métrica. En comunicaciones de Internet, valor asociado con una ruta que se utiliza para establecer diferencias entre los múltiples puntos de entrada o salida respecto al mismo sistema autónomo. Se prefiere la ruta con la métrica inferior.

MIB. (1) Módulo de la MIB. (2) Base de la información de gestión.

MIB estándar. En el protocolo Simple Network Management Protocol (SNMP), módulo de la MIB que se ubica bajo la rama de gestión de la estructura de la

información de gestión (SMI) y que se considera una norma en Internet Engineering Task Force (IETF).

MILNET. Red militar que formaba parte de ARPANET en un principio. Quedó separada de ARPANET en 1984. MILNET proporciona un servicio de red fiable para las instalaciones militares.

modelo de referencia interconexión de sistemas abiertos (OSI). Modelo que describe los principios generales de interconexión de sistemas abiertos así como la finalidad y la ordenación jerárquica de sus siete capas. (T)

módem (modulador/demodulador). (1) Unidad funcional que modula y demodula señales. Una de las funciones de un módem es permitir que los datos digitales se transmitan sobre recursos de transmisión analógicos. (T) (A) (2) Dispositivo que convierte los datos digitales de un sistema en una señal analógica que pueda transmitirse en una línea de telecomunicaciones, y convierte la señal analógica recibida en datos para el sistema.

modulación en código de pulsaciones (PCM). Norma adoptada para la digitalización de una señal de voz analógica. En la PCM, se realiza un muestreo de la voz a una velocidad de ocho kHz y cada muestra se codifica en una trama de 8 bits.

módulo. (1) Perteneciente a un módulo matemático; por ejemplo, 9 equivale a 4 módulo 5. (2) Véase también *módulo (diferencia)*.

módulo. En Nways Switch, unidad de hardware funcional empaquetada que contiene tarjetas lógicas, conectores y luces. Los módulos se utilizan para empaquetar adaptadores, acopladores de interfaz de línea, extensiones de servidor de voz y otros componentes. Todos los módulos pueden ***conectarse en caliente*** en los subbastidores lógicos.

módulo (diferencia). Número, como por ejemplo un entero positivo, de una relación que divide la diferencia entre dos números relacionados sin dejar un resto; por ejemplo, 9 y 4 tienen un módulo de 5 (9 - 4 = 5; 4 - 9 = -5; y 5 divide tanto 5 como -5 sin dejar un resto).

multiplexación de la división del tiempo (TDM). Véase ***canalización***.

N

Name Binding Protocol (NBP). En redes AppleTalk, protocolo que proporciona la función de conversión de nombre a partir del nombre (serie) de una entidad (recurso) AppleTalk en una dirección IP AppleTalk (número de 16 bits) en la capa de transporte.

NetBIOS. Network Basic Input/Output System. Interfaz estándar para redes, IBM PC (Personal Computer) y PC compatibles que se utiliza en las LAN para proporcionar funciones de mensajes, de servidor de impresión y de servidor de archivos. Los programas de aplicación que utilizan NetBIOS no necesitan manejar los detalles de protocolos de control de enlace de datos (DLC) de la LAN.

nivel de enlace. (1) Parte de la recomendación X.25 que define el protocolo de enlace utilizado para entrar datos en la red y sacarlos de la misma a través del enlace dúplex que conecta la máquina del abonado con el nodo de red. LAP y LAPB son los protocolos de acceso de enlace recomendados por la CCITT. (2) Véase *nivel de enlace de datos*.

nivel de enlace de datos. (1) En la estructura jerárquica de una estación de datos, nivel conceptual de control o lógica de proceso entre la lógica de alto nivel y el enlace de datos que mantiene el control del enlace de datos. El nivel de enlace de datos realiza funciones tales como la inserción de bits de transmisión y supresión de bits de recepción; interpretación de campos de dirección y control; generación, transmisión e interpretación de mandatos y respuestas; y cálculo e interpretación de secuencias de comprobación de trama. Véase también *nivel de paquete* y *nivel físico*. (2) En comunicaciones de X.25, sinónimo de *nivel de trama*.

nivel de trama. Sinónimo de *nivel de enlace de datos*. Véase *nivel de enlace*.

nodo. (1) En una red, punto donde una o más unidades funcionales conectan canales o circuitos de datos. (I) (2) Cualquier dispositivo conectado a una red que transmite y recibe datos.

nodo Advanced Peer-to-Peer Networking (APPN). Nodo de red APPN o nodo final APPN.

nodo de destino. Nodo al que se envían datos o una petición.

nodo de esfera de control (SOC). Nodo que está incluido directamente en la esfera de control de un punto focal. Un nodo de SOC ha intercambiado elementos de habilitación de los servicios de gestión con su punto focal. Un nodo final APPN puede ser un nodo de SOC si da soporte a la función de intercambio de elementos de habilitación de los servicios de gestión.

nodo de red (NN). Véase *nodo de red Advanced Peer-to-Peer Networking (APPN)*.

nodo de red Advanced Peer-to-Peer Networking (APPN). Nodo que ofrece un amplio rango de servicios de usuario final y que puede proporcionar lo siguiente:

- servicios de directorios distribuidos, incluido el registro de los recursos del dominio con un servidor de directorios central
- Intercambios de bases de datos de topología con otros nodos de red APPN, lo que permite que los nodos de red de la red seleccionen las rutas óptimas para sesiones de LU-LU basándose en las clases de servicio solicitadas
- Servicios de sesiones para los nodos finales clientes y las LU locales
- Servicios de direccionamiento intermedio de una red APPN

nodo de red APPN. Véase *nodo de red Advanced Peer-to-Peer Networking (APPN)*.

nodo de red de entrada baja (LEN). Nodo que proporciona un rango de servicios de usuario final, se conecta directamente con otros nodos utilizando protocolos de igual a igual y hace derivar servicios de red de un nodo de red APPN adyacente implícitamente, es decir, sin el uso directo de sesiones de CP-CP.

nodo final (EN). (1) Véase *nodo final Advanced Peer-to-Peer Networking (APPN)* y *nodo final de red de entrada baja (LEN)*. (2) En comunicaciones, nodo que se conecta frecuentemente a un solo enlace de datos y no puede realizar funciones de direccionamiento intermedio.

nodo final Advanced Peer-to-Peer Networking (APPN). Nodo que proporciona un amplio rango de servicios de usuario final y da soporte a las sesiones entre su punto de control (CP) local y el CP de un nodo de red adyacente. Utiliza estas sesiones con el fin de registrar dinámicamente sus recursos con el CP adyacente (su servidor de nodos de red) para enviar y recibir peticiones de búsqueda en directorios y obtener servicios de gestión. Un nodo final APPN también puede conectarse a una red de subárea como nodo periférico o a otros nodos finales.

nodo final de red de entrada baja (LEN). Nodo LEN que recibe servicios de red de un nodo de red APPN adyacente.

nodo intermedio. Nodo que está al final de más de una rama. (T)

nodos adyacentes. Dos nodos conectados conjuntamente por una vía de acceso, como mínimo, que no conecta ningún otro nodo. (T)

nombre de comunidad. En el protocolo Simple Network Management Protocol (SNMP), serie de octetos que identifica a una comunidad.

nombre de dominio. En el conjunto de protocolos de Internet, nombre de un sistema principal. Un nombre de dominio está compuesto por una secuencia de subnombres separados por un carácter delimitador. Por ejemplo, si el nombre de dominio calificado al completo (FQDN) de un sistema principal es `ralvm7.vnet.ibm.com`, cada uno de los siguientes es un nombre de dominio:

- `ralvm7.vnet.ibm.com`
- `vnet.ibm.com`
- `ibm.com`

notación de sintaxis de abstracción 1 (ASN.1). Método de Interconexión de Sistemas Abiertos (OSI) para la sintaxis de abstracción que se especifica en las normas siguientes:

- ITU-T recomendación X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T recomendación X.680 (1994) | ISO/IEC 8824-1: 1994

Véase también *normas básicas de codificación (BER)*.

número de puerto. En comunicaciones de Internet, identificación de una entidad de aplicación para el servicio de transporte.

número de secuencia. En comunicaciones, número asignado a una trama o paquete en particular para controlar el flujo de la transmisión y la recepción de datos.

número de sistema autónomo. En TCP/IP, número asignado a un sistema autónomo por la misma autorización central que también asigna direcciones IP. El número de sistema autónomo hace posible que los algoritmos de direccionamiento automatizado distingan los sistemas autónomos.

Nways Switch. Sinónimo de IBM 2220 Nways BroadBand Switch.

O

objeto de la MIB. Equivale a *variable de la MIB*.

Open Shortest Path First (OSPF). En el conjunto de protocolos de Internet, función que proporciona transferencia de información intradominio. Como alternativa al protocolo Routing Information Protocol (RIP), OSPF permite el direccionamiento de menor coste y lo maneja en grandes redes regionales o corporativas.

Organización Internacional de Normalización (ISO). Organización de corporaciones nacionales de normas de varios países establecida para promocionar el desarrollo de normas con el fin de facilitar el intercambio internacional de artículos y servicios además de desarrollar la cooperación en la actividad intelectual, científica, tecnológica y económica.

origen. Unidad lógica (LU) externa o programa de aplicación de donde parten un mensaje u otros datos. Véase también *destino*.

P

paquete. En la comunicación de datos, secuencia de dígitos binarios, con inclusión de señales de control y datos, que se transmite y se conmuta como un todo compuesto. Los datos, las señales de control y, posiblemente, la información de control de errores se ordenan siguiendo un formato específico. (I)

paquete de datos. En comunicaciones de X.25, paquete utilizado para la transmisión de datos de usuario dentro de un circuito virtual en la interfaz DTE/DCE.

paquete de petición de llamada. (1) Paquete de supervisión de llamada que un equipo terminal de datos (DTE) transmite con el fin de solicitar que se establezca una conexión para una llamada en la red. (2) En comunicaciones de X.25, paquete de supervisión de llamada transmitido por un DTE para solicitar el establecimiento de una llamada en la red.

paquete de petición de restablecimiento. En comunicaciones X.25, paquete transmitido por el equipo terminal de datos (DTE) al equipo de terminación de circuito de datos (DCE) para solicitar que se restablezca una llamada virtual o un circuito virtual permanente. En el paquete también puede especificarse la razón de la petición.

paquete de recepción no preparada (RNR). Véase *paquete de RNR*.

paquete de RNR. Paquete utilizado por un equipo terminal de datos (DTE) o por un equipo de terminación de circuito de datos (DCE) con el fin de indicar una incapacidad temporal para aceptar paquetes adicionales de petición de llamada virtual o circuito virtual permanente.

paquete explorador. En las LAN, paquete que está generado por el sistema principal de origen y que atraviesa toda la parte de direccionamiento en origen de una LAN con el fin de recoger información sobre las posibles vías de acceso que se encuentran disponibles para el sistema principal.

parámetro de configuración. Variable de una definición de configuración cuyos valores pueden caracterizar la relación de un producto con otros productos de la misma red o pueden definir características del producto en sí.

pasarela. (1) Unidad funcional que interconecta dos redes de sistema con arquitecturas de red diferentes. Una pasarela conecta redes o sistemas de arquitecturas diferentes. Un puente interconecta redes o sistemas con la misma arquitectura o con arquitecturas similares. (T) (2) En la Red en Anillo de IBM, dispositivo y software asociado que conectan una red de área local a otra red de área local o sistema principal que utiliza protocolos de enlace lógico diferentes. (3) En TCP/IP, sinónimo de *direccionador*.

pasarela exterior. En comunicaciones de Internet, pasarela de un sistema autónomo que comunica con otro sistema autónomo. Compárese con *pasarela interior*.

pasarela interior. En comunicaciones de Internet, pasarela que sólo comunica con su propio sistema autónomo. Compárese con *pasarela exterior*.

período de duración (TTL). Técnica utilizada por los protocolos de entrega de mayor eficacia para impedir que los paquetes se repitan en bucle de manera interminable. El paquete se elimina si el contador de TTL alcanza el valor de 0.

peticionario de LU dependientes (DLUR). Nodo final APPN o nodo de red APPN que posee LU dependientes pero solicita que un servidor de LU dependientes proporcione los servicios del SSCP para estas LU dependientes.

Point-to-Point Protocol (PPP). Protocolo que proporciona un método para encapsular y transmitir paquetes sobre enlaces serie punto a punto.

portadora. Tren de pulsaciones u ondas eléctricas o electromagnéticas que puede variar según una señal con información a transmitir sobre un sistema de comunicaciones. (T)

procesador de componente frontal. Procesador, como, por ejemplo, el IBM 3745 oel 3174, que releva a un sistema principal de las tareas de control de comunicaciones.

proceso a tiempo real. Manipulación de los datos que un proceso necesita o genera mientras el proceso está en funcionamiento. Normalmente, los resultados se utilizan para influir en el proceso y quizá en procesos relacionados, mientras se está desarrollando.

proporción de pérdida de un paquete. Probabilidad que tiene un paquete de no alcanzar su destino o de no alcanzarlo dentro del período especificado.

protocolo. (1) Conjunto de normas semánticas y sintácticas que determinan el comportamiento de las unidades funcionales a la hora de conseguir la comunicación. (I) (2) En la arquitectura interconexión de sistemas abiertos, conjunto de normas semánticas y sintácticas que determinan el comportamiento de las entidades de la misma capa a la hora de desempeñar funciones de comunicación. (T) (3) En SNA, signifi-

cados y normas de puesta en secuencia de las peticiones y respuestas que se utilizan para gestionar la red, transferir datos y sincronizar los estados de los componentes de la red. Sinónimo de *disciplina de control de línea* y *disciplina de línea*. Véase *protocolo delimitador* y *protocolo de enlace*.

protocolo de acceso de enlace equilibrado (LAPB). Protocolo utilizado para acceder a una red X.25 en el nivel de enlace. LAPB es un protocolo simétrico, asíncrono y dúplex que se utiliza en la comunicación punto a punto.

protocolo de control de enlace lógico (LLC). En una red de área local, protocolo que dirige el intercambio de tramas de transmisión entre estaciones de datos independientemente de cómo está compartido el medio de transmisión. (T) El protocolo de LLC se desarrolló en la comisión de IEEE 802 y es común a todas las normas de LAN.

protocolo de control del acceso al medio (MAC). En una red de área local, protocolo que dirige el acceso al medio de transmisión, teniendo en cuenta los aspectos topológicos de la red, con el fin de permitir el intercambio de datos entre estaciones de datos. (T)

protocolo de direccionamiento. Técnica utilizada por un direccionador para encontrar otros direccionadores y mantener información actualizada sobre la mejor manera de acceder a las redes asequibles.

protocolo de interfaz de gestión local (LMI). En un NCP, conjunto de procedimientos y mensajes de gestión de red Frame-Relay utilizados por nodos Frame-Relay adyacentes para intercambiar información de estado de línea sobre el DLCI X'00'. Un NCP da soporte tanto a la versión del protocolo de LMI del American National Standards Institute (ANSI) como a la de la Comisión Consultiva de la Telefonía y Telegrafía Internacionales (ITU-T/CCITT). Estas normas se refieren al protocolo de LMI como *pruebas de verificación de integridad de enlace (LIVT)*.

prueba de bucle de retorno. Prueba donde las señales de un comprobador se repiten en bucle en un módem u otro elemento de red hacia el comprobador para tomar medidas que determinen o verifiquen la calidad de la vía de acceso de comunicaciones.

puente. Unidad funcional que interconecta diversas LAN (local o remotamente) que utilizan el mismo protocolo de control de enlace lógico pero que pueden utilizar diferentes protocolos de control del acceso al medio. Un puente reenvía una trama a otro puente basándose en la dirección del control del acceso al medio (MAC).

puente de direccionamiento en origen. En las LAN, método de función de puente que utiliza el campo de información de direccionamiento de la cabecera del control del acceso al medio (MAC) de IEEE 802.5 de una trama para determinar los anillos o segmentos de Red en Anillo que debe recorrer la trama. El nodo de origen inserta el campo de información de direccionamiento en la cabecera del MAC. La información del campo de información de direccionamiento deriva de los paquetes exploradores generados por el sistema principal de origen.

puente de ruta. Función de un programa de puente de IBM que permite que dos sistemas de puente utilicen un enlace de telecomunicaciones para conectar dos LAN. Cada sistema de puente se conecta directamente a una de las LAN y el enlace de telecomunicaciones conecta los dos sistemas de puente.

puente raíz. Puente que es la raíz de un árbol de extensión formado entre otros puentes activos de la red de funciones de puente. El puente raíz origina y transmite unidades de datos de protocolo de puente (BPDU) a otros puentes activos para mantener la topología de árbol de extensión. Es el puente con la prioridad superior de la red.

puentes paralelo. Par de puentes conectados al mismo segmento de LAN que crean vías de acceso redundantes para el segmento.

puerto. (1) Punto de acceso para la entrada o salida de datos. (2) Conector de un dispositivo al que se conectan cables para otros dispositivos, como, por ejemplo, estaciones de pantalla o impresoras. (3) Representación de una conexión física con el hardware de enlace. A veces, un puerto viene referido como adaptador; no obstante, en un adaptador puede haber más de un puerto. Un solo proceso de DLC puede controlar uno o más puertos. (4) En el conjunto de protocolos de Internet, número de 16 bits utilizado para la comunicación entre TCP o el protocolo User Datagram Protocol (UDP) y una aplicación o protocolo de nivel superior. Algunos protocolos, como, por ejemplo, File Transfer Protocol (FTP) y Simple Mail Transfer Protocol (SMTP), utilizan el mismo número de puerto conocido en todas las implementaciones de TCP/IP. (5) Abstracción utilizada por protocolos de transporte para establecer diferencias entre los diversos destinos en una máquina de sistema principal. (6) Sinónimo de *socket*.

puerto de destino. Adaptador asíncrono de 8 puertos que sirve de punto de conexión con un servicio serie.

punto de acceso a servicios (SAP). (1) En la arquitectura interconexión de sistemas abiertos (OSI), punto en el que una entidad de una capa proporciona los servicios de esta capa a una entidad de la capa superior más próxima. (T) (2) Punto lógico que queda disponible mediante un adaptador y donde puede recibirse y

transmitirse información. Muchos enlaces pueden terminar en un solo punto de acceso a servicios.

punto de acceso a servicios de destino (DSAP). En SNA y TCP/IP, dirección lógica que permite que un sistema direccione datos desde un dispositivo remoto al soporte de comunicaciones correspondiente. Compárese con *punto de acceso a servicios de origen (SSAP)*.

punto de acceso a servicios de origen (SSAP). En SNA y TCP/IP, dirección lógica que permite que un sistema envíe datos a un dispositivo remoto desde el soporte de comunicaciones correspondiente. Compárese con *punto de acceso a servicios de destino (DSAP)*.

punto de control (CP). (1) Componente de un nodo APPN o LEN que gestiona los recursos de dicho nodo. En un nodo APPN, el CP puede dedicarse a establecer sesiones de CP-CP con otros nodos APPN. En un nodo de red APPN, el CP también proporciona servicios a nodos finales adyacentes de la red APPN. (2) Componente de un nodo que gestiona los recursos de dicho nodo y, opcionalmente, proporciona servicios a otros nodos de la red. Pueden citarse como ejemplos el punto de control de servicios del sistema (SSCP) de un nodo de subárea de tipo 5, el punto de control de nodo de red (NNCP) de un nodo de red APPN y el punto de control de nodo final (ENCP) de un nodo final APPN o LEN. Un SSCP y un NNCP pueden proporcionar servicios a otros nodos.

punto de control de servicios del sistema (SSCP). Componente de una red de subárea destinado a gestionar la configuración, coordinar las peticiones del operador de red y las de determinación de problemas y proporcionar servicios de directorios además de otros servicios de sesiones para los usuarios de la red. Diversos SSCP, cooperando como iguales entre sí, pueden dividir la red en dominios de control y tener, cada uno de los SSCP, una relación de control jerárquica con las unidades físicas y las unidades lógicas de su propio dominio.

punto de entrada (EP). En SNA, nodo de tipo 2.0, tipo 2.1, tipo 4 otipo 5 que proporciona soporte de gestión de redes distribuidas. Envía datos de gestión de redes sobre sí mismo y los recursos que controla a un punto focal para el proceso centralizado, y recibe y ejecuta los mandatos iniciados por el punto focal para gestionar y controlar sus recursos.

R

rastreo. (1) Registro de la ejecución de un programa de sistema. Muestra las secuencias en que se han ejecutado las instrucciones. (A) (2) Para los enlaces de datos, registro de las tramas y bytes transmitidos o recibidos.

recepción no preparada (RNR). En comunicaciones, mandato o respuesta de enlace de datos que indica una condición temporal de incapacidad para aceptar tramas de entrada.

reconfiguración dinámica (DR). Proceso consistente en cambiar la configuración de una red (las PU y LU periféricas) sin regenerar las tablas de configuración al completo ni desactivar el nodo principal afectado.

recurso. En Nways Switch, elemento de hardware o entidad lógica creados por Control Program. Por ejemplo, los adaptadores, LIC y líneas son recursos físicos. Los puntos de control y conexiones son recursos lógicos.

red. (1) Configuración de software y dispositivos de proceso de datos conectados para el intercambio de información. (2) Grupo de nodos y los enlaces que los interconectan.

red Advanced Peer-to-Peer Networking (APPN). Conjunto de nodos de red interconectados y sus nodos finales clientes.

red APPN. Véase *red Advanced Peer-to-Peer Networking (APPN)*.

red de área amplia (WAN). (1) Red que proporciona servicios de comunicación a un área geográfica mayor que la servida por una red de área local o una red de área metropolitana, y que puede utilizar o proporcionar recursos públicos de comunicación. (T) (2) Red de comunicación de datos diseñada para servir a un área de cientos o miles de kilómetros; por ejemplo, las redes públicas y privadas de conmutación de paquetes y las redes telefónicas nacionales. (3) Compárese con *red de área local (LAN)* y *red de área metropolitana (MAN)*.

red de área local (LAN). (1) Red de sistema ubicada en el lugar de un usuario dentro de un área geográfica limitada. La comunicación dentro de una red de área local no está sujeta a reglamentos externos; no obstante, la comunicación más allá del límite de una LAN puede estar sujeta a alguna forma de reglamento. (T) (2) Red en la que un conjunto de dispositivos están conectados entre sí para la comunicación y que puede conectarse a una red mayor. (3) Véase también *Ethernet* y *Red en Anillo*. (4) Compárese con *red de área metropolitana (MAN)* y *red de área amplia (WAN)*.

red de área metropolitana (MAN). Red formada por la interconexión de dos o más redes que puede funcionar a una velocidad mayor que éstas, puede atravesar límites administrativos y puede utilizar diversos métodos de acceso. (T) Compárese con *red de área local (LAN)* y *red de área amplia (WAN)*.

red de clase A. En comunicaciones de Internet, red en la que el bit situado más a la izquierda (más significativo) de la dirección IP está establecido en 0 y el identificador de sistema principal ocupa los tres octetos situados más a la derecha.

red de clase B. En comunicaciones de Internet, red en la que los dos bits situados más a la izquierda (más significativo y próximo al más significativo) de la dirección IP están establecidos en 1 y 0, respectivamente, y el identificador de sistema principal ocupa los dos octetos situados más a la derecha.

red de entrada baja (LEN). Posibilidad de los nodos de conectarse directamente entre sí utilizando protocolos básicos de igual a igual para dar soporte a sesiones múltiples y en paralelo entre unidades lógicas.

Red de igual a igual (APPN). Extensión de SNA que ofrece (a) un control superior de las redes distribuidas que evita las dependencias jerárquicas críticas y, por lo tanto, aisla los efectos de puntos anómalos individuales; (b) intercambio dinámico de información de topología de red para facilitar la conexión, reconfiguración y selección de rutas adaptables; (c) definición dinámica de recursos de red; y (d) automatización en el registro de recursos y la búsqueda en directorios. APPN hace extensiva la orientación de igual de la LU 6.2 para los servicios de usuario final al control de redes y da soporte a diversos tipos de LU, incluidas la LU 2, la LU 3 y la LU 6.2.

red de tipo anillo. (1) Red en la que cada nodo tiene exactamente dos ramas conectadas y en la que hay exactamente dos vías de acceso entre dos nodos cualesquiera. (T) (2) Configuración de red en la que los dispositivos están conectados mediante enlaces de transmisión unidireccional para formar una vía de acceso cerrada.

red digital de servicios integrados (RDSI). Red digital de telecomunicaciones de extremo a extremo que da soporte a diversos servicios, los cuales incluyen voz y datos pero no se limitan a ello.

Nota: Las RDSI se utilizan en arquitecturas de red públicas y privadas.

red en anillo. (1) Red que permite la transmisión de datos unidireccional entre estaciones de datos, mediante un procedimiento consistente en pasar señales, de tal manera que los datos transmitidos vuelven a la estación transmisora. (T) (2) Red que utiliza una topología de anillo, según la cual pasan señales en un circuito de nodo a nodo. Un nodo que está preparado para emitir puede capturar la señal e insertar datos para la transmisión.

Red en Anillo. (1) Según la norma IEEE 802.5, tecnología de red que controla el acceso al medio pasando una señal (paquete o trama especial) entre las estaciones conectadas al medio. (2) IEEE 802.5 con una topología de anillo que pasa señales de una estación de anillo de conexión (nodo) a otra. (3) Véase también *red de área local (LAN)*.

red óptica síncrona (SONET). Norma de los EE.UU. para la transmisión de información digital sobre interfaces ópticas. Está estrechamente relacionada con la recomendación sobre la jerarquía digital síncrona (SDH).

red troncal. Red central a la que se conectan redes más pequeñas, casi siempre de menor velocidad. Normalmente, la red troncal tiene una capacidad muy superior a las redes a las que ayuda a interconectarse o es una red de área amplia (WAN), como, por ejemplo, una red pública de datagramas de paquetes conmutados.

reensamblaje. En comunicaciones, proceso consistente en volver a juntar paquetes segmentados después de haberlos recibido.

Registro de no retorno a cero y con cambios en los unos (NRZ-1). Método de registro donde los unos están representados mediante un cambio en la condición de magnetización y los ceros están representados mediante la ausencia de cambio. Sólo se registran explícitamente las señales de los unos. (Denominado anteriormente registro ***no retorno a cero invertido***, NRZI.)

Remote Execution Protocol (REXEC). Protocolo que permite la ejecución de un mandato o programa en cualquier sistema principal de la red. El sistema principal local recibe los resultados de la ejecución del mandato.

remoto. (1) Perteneciente a un sistema, programa o dispositivo al que se accede mediante una línea de telecomunicaciones. (2) Equivale a *conectado mediante enlace*. (3) Compárese con *local*.

Request for Comments (RFC). En comunicaciones de Internet, serie de documentos que describe una parte del conjunto de protocolos de Internet y experimentos relacionados. Todas las normas de Internet están documentadas como RFC.

resolución de direcciones. (1) Método para correlacionar direcciones de capa de red con direcciones específicas de los medios. (2) Véase también *Address*

Resolution Protocol (ARP) y *AppleTalk Address Resolution Protocol (AARP)*.

resolución de nombres. En comunicaciones de Internet, proceso consistente en correlacionar un nombre de máquina con la dirección Internet Protocol (IP) correspondiente. Véase también *Sistema de nombres de dominio (DNS)*.

respuesta a excepción (ER). En SNA, protocolo solicitado en el campo de formato de respuesta solicitado de la cabecera de una petición que indica al receptor que devuelva una respuesta sólo si la petición no es aceptable tal como se recibe o si no puede procesarse; es decir, puede devolverse una respuesta negativa, pero no una respuesta positiva. Compárese con *respuesta definida* y *sin respuesta*.

restablecimiento. En un circuito virtual, reinicialización del control del flujo de datos. En el restablecimiento, se eliminan todos los datos en tránsito.

ritmo. (1) Técnica mediante la cual un componente de recepción controla la velocidad de transmisión de un componente de emisión para evitar un desbordamiento o una congestión. (2) Véase también *control del flujo*, *ritmo de recepción*, *ritmo de emisión*, *ritmo de nivel de sesión* y *ritmo de ruta virtual (VR)*.

rlogin (inicio de sesión remoto). Servicio ofrecido por los sistemas de Berkeley basados en UNIX que permite que los usuarios autorizados de una máquina se conecten con otros sistemas UNIX en una internet e interactúen como si sus terminales estuvieran conectados directamente. El software rlogin pasa información sobre el entorno del usuario (por ejemplo, el tipo de terminal) a la máquina remota.

Routing Information Protocol (RIP). En el conjunto de protocolos de Internet, protocolo de pasarela interior utilizado para intercambiar información de direccionamiento intradominio y para determinar las rutas óptimas entre los sistemas principales de internet. RIP determina las rutas óptimas sobre la base de la métrica de ruta y no sobre la base de la velocidad de transmisión de un enlace.

Routing Table Maintenance Protocol (RTMP). En redes AppleTalk, protocolo que proporciona generación y mantenimiento de información de direccionamiento en la capa de transporte por medio de la tabla de direccionamiento AppleTalk. La tabla de direccionamiento AppleTalk dirige la transmisión de paquetes por la internet de socket de origen a socket de destino.

RouTing update Protocol (RTP). Protocolo de VIrtual NEtworking System (VINES) que mantiene la base de datos de direccionamiento y permite el intercambio de información de direccionamiento entre nodos VINES. Véase también *Internet Control Protocol (ICP)*.

rsh. Variante del mandato rlogin que invoca un interpretador de mandatos en una máquina remota UNIX y pasa los argumentos de línea de mandatos al interpretador de mandatos saltándose completamente el paso de inicio de sesión.

ruta. (1) Secuencia ordenada de nodos y grupos de transmisión (TG) que representan una vía de acceso de un nodo de origen a un nodo de destino por la que pasa el tráfico intercambiado entre éstos. (2) Vía de acceso que el tráfico de red utiliza para ir del origen al destino.

ruta estática. Ruta entre sistemas principales y/o redes que se entra manualmente en una tabla de direccionamiento.

ruta explícita (ER). En SNA, serie de uno o más grupos de transmisión que conectan dos nodos de subárea. Una ruta explícita se identifica mediante una dirección de subárea de origen, una dirección de subárea de destino, un número de ruta explícita y un número de ruta explícita inversa. Compárese con *ruta virtual (VR)*.

ruta virtual (VR). (1) En SNA, (a) conexión lógica entre dos nodos de subárea que se realiza físicamente como una ruta explícita en particular o (b) conexión lógica contenida en su totalidad dentro de un nodo de subárea para las sesiones intranodo. Una ruta virtual entre nodos de subárea distintos impone una prioridad de transmisión sobre la ruta explícita subyacente, proporciona control del flujo mediante el ritmo de ruta virtual y proporciona la integridad de los datos mediante la numeración en secuencia de las unidades de información de vía de acceso (PIU). (2) Compárese con *ruta explícita (ER)*. Véase también *vía de acceso* y *extensión de ruta (REX)*.

rutina de carga. (1) Secuencia de instrucciones cuya ejecución hace que se carguen y se ejecuten unas instrucciones adicionales hasta que se haya almacenado todo el programa de sistema. (T) (2) Técnica o dispositivo diseñado para que entre en un estado determinado por medio de su propia acción, por ejemplo, una rutina de máquina cuyas primeras instrucciones sean suficientes para que el resto de la misma entre en el sistema desde un dispositivo de entrada. (A)

S

salto. (1) En APPN, parte de una ruta que no tiene nodos intermedios. Está compuesto por un solo grupo de transmisión que conecta nodos adyacentes. (2) Para la capa de direccionamiento, distancia lógica entre dos nodos en una red.

SAP. Véase punto de acceso a servicios.

segmentación. En OSI, función realizada por una capa para correlacionar una unidad de datos de protocolo (PDU) de la capa a la que da soporte con diversas PDU.

segmento. (1) Sección de cable entre componentes o dispositivos. Un segmento puede estar compuesto por un solo cable provisional, diversos cables provisionales conectados o una combinación de cables provisionales y de construcción conectados. (2) En comunicaciones de Internet, unidad de transferencia entre funciones de TCP en diferentes máquinas. Cada segmento contiene campos de control y de datos; la posición de corriente de bytes actual y los bytes de datos reales se identifican conjuntamente con una suma de comprobación para validar los datos recibidos.

segmento de anillo. Parte de un anillo que puede aislarse (desenchufando conectores) del resto del anillo. Véase *segmento de LAN*.

segmento de LAN. (1) Cualquier parte de una LAN (por ejemplo, un bus o un anillo) que puede funcionar independientemente pero está conectada a otras partes de la red por medio de puentes. (2) Red de tipo bus o anillo sin puentes.

señal. (1) En una red de área local, símbolo de autorización pasado sucesivamente de una estación de datos a otra para indicar la estación que tiene temporalmente el control del medio de transmisión. Cada estación de datos tiene una oportunidad de obtener y utilizar la señal para controlar el medio. Una señal es un mensaje o patrón de bits determinado que significa el permiso para transmitir. (T) (2) En las LAN, secuencia de bits pasada de un dispositivo a otro por el medio de transmisión. Cuando la señal tiene datos añadidos, se convierte en una trama.

Serial Line Internet Protocol (SLIP). Protocolo utilizado sobre una conexión punto a punto entre dos sistemas principales de IP de una línea serie, como, por ejemplo, un cable serie o una conexión RS232 con un módem, de una línea telefónica.

Service Advertising Protocol (SAP). En Internetwork Packet Exchange (IPX), protocolo que proporciona lo siguiente:

- Un mecanismo que permite que los servidores IPX de una internet anuncien sus servicios por el nombre y el tipo. Los servidores que utilizan este protocolo tienen registrados su nombre, tipo de servicios y dirección en todos los servidores de archivos que ejecutan NetWare.
- Un mecanismo que permite que una estación de trabajo difunda una consulta para descubrir las identidades de todos los servidores de todos los tipos, todos los servidores de un tipo específico o el servidor más cercano de un tipo específico.
- Un mecanismo que permite que una estación de trabajo consulte cualquier servidor de archivos que ejecute NetWare para descubrir nombre y dirección de todos los servidores de un tipo específico.

servicio de directorios (DS). Elemento de servicio de aplicaciones que convierte los nombres simbólicos utilizados por procesos de aplicaciones en direcciones de red completas utilizadas en un entorno de OSI. (T)

servicios de directorios (DS). Componente del punto de control de un nodo APPN que mantiene la información sobre la ubicación de los recursos de red.

servicios de gestión de punto de control (CPMS). Componente de un punto de control que consta de conjuntos de funciones de servicios de gestión y proporciona recursos de ayuda para realizar la gestión de problemas, gestión del rendimiento y de la contabilidad, gestión de los cambios y gestión de la configuración. Las posibilidades proporcionadas por los CPMS incluyen el envío de peticiones a los servicios de gestión de unidad física (PUMS) para probar recursos del sistema, la reunión de información estadística (por ejemplo, datos de errores y del rendimiento) de los PUMS sobre los recursos del sistema y el análisis y presentación de los resultados de las pruebas y la información estadística reunida sobre los recursos del sistema. Las responsabilidades del análisis y de la presentación para la determinación de problemas y la supervisión del rendimiento pueden distribuirse entre los diversos CPMS.

servicios de gestión de SNA (SNA/MS). Servicios proporcionados como ayuda para la gestión de las redes SNA.

servidor. Unidad funcional que proporciona servicios compartidos a estaciones de trabajo sobre una red; por ejemplo, un servidor de archivos, un servidor de impresión, un servidor de correo. (T)

servidor de acceso a red (NAS). Dispositivo que proporciona a los usuarios acceso a red temporal a petición. Este acceso es punto a punto por medio de líneas PSTN o RDSI.

servidor de nombres. En el conjunto de protocolos de Internet, sinónimo de *servidor de nombres de dominio*.

servidor de nombres de dominio. En el conjunto de protocolos de Internet, programa servidor que suministra la conversión de nombres en direcciones correlacionando nombres de dominio con direcciones IP. Sinónimo de *servidor de nombres*.

servidor de puentes de LAN (LBS). En el programa Bridge para la Red en Anillo de IBM, servidor que mantiene información estadística sobre las tramas reenviadas entre dos o más anillos (mediante un puente). LBS envía estas estadísticas a los gestores de LAN correspondientes mediante LAN Reporting Mechanism (LRM).

sesión. (1) En la arquitectura de red, con el fin de la comunicación de datos entre unidades funcionales, todas las actividades que tienen lugar durante el establecimiento, mantenimiento y liberación de la conexión. (T) (2) Conexión lógica entre dos unidades de red accesibles (NAU) que puede activarse, adaptarse, para proporcionar varios protocolos y desactivarse de la manera solicitada. Cada sesión está identificada de manera exclusiva en la cabecera de transmisión (TH) que acompaña a cualquier transmisión intercambiada durante la sesión.

Simple Network Management Protocol (SNMP). En el conjunto de protocolos de Internet, protocolo de gestión de red que se utiliza para supervisar direccionadores y redes conectadas. SNMP es un protocolo de capa de aplicación. La información sobre los dispositivos gestionados está definida y almacenada en la base de la información de gestión (MIB) de la aplicación.

simulación. Para los enlaces de datos, técnica mediante la cual un protocolo iniciado en una estación final se reconoce con acuse de recibo y se procesa en un nodo intermedio en nombre del destino final. En la conmutación del enlace de datos del IBM 6611, por ejemplo, las tramas de SNA se encapsulan en paquetes de TCP/IP para el transporte a través de una red de área amplia diferente de SNA, se desempaquetan en otro IBM 6611 y pasan al destino final. Una ventaja de la simulación es que se evitan tiempos de espera excedidos de sesión de final a final.

síncrono. (1) Perteneciente a dos o más procesos que dependen de la aparición de sucesos específicos, como, por ejemplo, señales comunes de temporización. (T) (2) Que se produce con una relación temporal regular o previsible.

sintaxis de abstracción. Especificación de datos que incluye todas las distinciones necesarias en las transmisiones de datos, pero que omite (excluye) otros detalles, como, por ejemplo, los que dependen de las arquitecturas específicas de los sistemas. Véase también *notación de sintaxis de abstracción 1 (ASN.1)* y *normas básicas de codificación (BER)*.

sistema. En el proceso de datos, conjunto de personas, máquinas y métodos organizados para llevar a cabo un conjunto de funciones específicas. (I) (A)

sistema autónomo. En TCP/IP, grupo de redes y direccionadores bajo una sola autorización administrativa. Estas redes y estos direccionadores cooperan estrechamente para propagar la información de asequibilidad (y direccionamiento) de la red entre ellos utilizando un protocolo de pasarela interior de su elección.

sistema de juego reducido de instrucciones (RISC). Sistema que utiliza un juego pequeño y simplificado de instrucciones de uso frecuente para la ejecución rápida.

sistema de nombres de dominio (DNS). En el conjunto de protocolos de Internet, sistema de bases de datos distribuidas utilizado para correlacionar nombres de dominio con direcciones IP.

sistema principal. En el conjunto de protocolos de Internet, sistema final. El sistema final puede ser cualquier estación de trabajo; no es necesario que sea un sistema principal.

socket. (1) Punto final para la comunicación entre procesos o programas de aplicación. (2) Abstracción proporcionada por la Distribución de software de Berkeley de la Universidad de California (software que suele recibir el nombre de UNIX de Berkeley o UNIX de BSD) que funciona como punto final para la comunicación entre procesos o aplicaciones.

sonda de paquetes Internet (PING). (1) En comunicaciones de Internet, programa utilizado en redes TCP/IP para probar la capacidad de alcanzar destinos enviando a los mismos una petición con eco de Internet Control Message Protocol (ICMP) y esperando una respuesta. (2) En comunicaciones, prueba de asequibilidad.

sondeo. (1) En una conexión multipunto o conexión punto a punto, proceso consistente en invitar a las estaciones de datos a transmitir, una por una. (I) (2) Interrogar a dispositivos con el fin de evitar contenciones, determinar el estado operativo o determinar la disposición para enviar o recibir datos. (A)

soporte de diversos dominios (MDS). Técnica para transportar datos de servicios de gestión entre conjuntos de funciones de servicios de gestión sobre sesiones de LU-LU y CP-CP. Véase también *unidad de mensaje de soporte de diversos dominios (MDS-MU)*.

StreetTalk. En VIrtual NEtworking System (VINES), sistema exclusivo de denominación y direccionamiento de red amplia que permite que los usuarios ubiquen cualquier recurso de la red y accedan al mismo sin conocer la topología de la red. Véase también *Internet Control Protocol (ICP)* y *RouTing update Protocol (RTP)*.

subárea. Parte de la red SNA compuesta por un nodo de subárea, nodos periféricos conectados y recursos asociados. En un nodo de subárea, todas las unidades de red accesibles (NAU), enlaces y estaciones de enlace adyacentes (de nodos de subárea o nodos periféricos conectados) que son dirigibles dentro de la subárea comparten una dirección de subárea común y tienen direcciones de elementos distintas.

subcapa del control del acceso al medio (MAC). En una red de área local, parte de la capa de enlace de datos que aplica un método de acceso al medio. La subcapa del MAC da soporte a funciones dependientes de la topología y utiliza los servicios de la capa física para proporcionar servicios a la subcapa de control de enlace lógico. (T)

Subnetwork Access Protocol (SNAP). En las LAN, protocolo encargado de establecer diferencias entre protocolos de 5 bytes que identifica la familia de protocolos estándares distintos de IEEE a la que pertenece un paquete. El valor de SNAP se utiliza para diferenciar los protocolos que utilizan `$AA` como valor de punto de acceso a servicios (SAP).

subred. (1) En TCP/IP, parte de una red que se identifica mediante una parte de la dirección IP. (2) Equivale a *subred (grupo de nodos)*.

subred (grupo de nodos). (1) Cualquier grupo de nodos que tienen un conjunto de características comunes, como, por ejemplo, el mismo identificador de red. (2) Sinónimo de *subred*.

subsistema. Sistema secundario o subordinado que a menudo puede funcionar de manera independiente o asíncrona respecto a un sistema de control. (T)

suma de comprobación. (1) Suma de un grupo de datos que se asocia con el grupo y se utiliza con fines de comprobación. (T) (2) En la detección de errores, función de todos los bits de un bloque. Si las sumas grabadas y las calculadas no coinciden, se indica que hay un error. (3) En un disquete, datos grabados en un sector con fines de detección de errores; una suma de comprobación calculada que no coincide con la suma de comprobación de los datos grabados en el sector indica que hay un sector anómalo. Los datos son numéricos u otras series de caracteres consideradas numéricas con el fin de calcular la suma de comprobación.

supervisor. (1) Dispositivo que observa y registra actividades seleccionadas en un sistema de proceso de datos para el análisis. Sus usos posibles son para indicar cualquier desviación significativa de la norma o para determinar los niveles de utilización de unidades funcionales en particular. (T) (2) Software o hardware que observa, supervisa, controla o verifica operaciones de un sistema. (A) (3) Función necesaria para iniciar la transmisión de una señal del anillo y para proporcionar recuperación de errores de software en el caso de que se pierdan señales, tramas en circulación u otras dificultades. La posibilidad está presente en todas las estaciones de anillo.

supervisor activo. En una Red en Anillo, función realizada en cualquier momento por una estación de anillo que inicia la transmisión de señales y proporciona recursos de recuperación de errores de señales. Cualquier adaptador activo del anillo tiene la posibilidad de proporcionar la función de supervisor activo si falla el supervisor activo actual.

SYNTAX. En el protocolo Simple Network Management Protocol (SNMP), cláusula del módulo de la MIB que define la estructura de datos abstracta correspondiente a un objeto gestionado.

Systems Network Architecture (SNA). Descripción de la estructura lógica, formatos, protocolos y secuencias operativas para la transmisión de unidades de información a través de las redes y para el control de la configuración y del funcionamiento de las mismas. La estructura de capas de SNA permite que los orígenes y destinos finales de la información, es decir, los usuarios, sean independientes de los servicios y recursos de red SNA específicos utilizados para el intercambio de información y que no se vean afectados por dichos servicios y recursos.

T

T1. En los Estados Unidos, línea de acceso público de 1,544 Mbps. Está disponible en veinticuatro canales de 64 Kbps. La versión europea (E1) transmite a 2,048 Mbps.

tabla de correlación de direcciones (AMT). Tabla mantenida en el direccionador AppleTalk que proporciona la correlación actual de las direcciones de nodo con las direcciones de hardware.

tabla de direccionamiento. Conjunto de rutas utilizadas para dirigir el reenvío de datagramas o para establecer una conexión. La información pasa entre direccionadores para identificar la topología de red y la factibilidad de los destinos.

tabla de información de zonas (ZIT). Listado de números de red y sus correlaciones con los nombres de zonas asociadas de internet. Cada direccionador de internet mantiene este listado en una internet AppleTalk.

TCP/IP. (1) Transmission Control Protocol/Internet Protocol. (2) Protocolo de interconexión de sistemas basado en Ethernet/de tipo UNIX que desarrolló originalmente el Departamento de Defensa de los EE.UU. TCP/IP facilitó ARPANET (Advanced Research Projects

Agency Network), una red de paquetes conmutados para la investigación en que la capa 4 era TCP y la capa 3, IP.

Telnet. En el conjunto de protocolos de Internet, protocolo que proporciona un servicio de conexión de terminales remotos. Permite que los usuarios de un sistema principal se conecten con un sistema principal remoto e interactúen como usuarios de terminal conectado directamente de este sistema principal.

terminal de datos preparado (DTR). Señal para el módem que se utiliza con el protocolo EIA 232.

tiempo de espera excedido. (1) Suceso que se produce al final de un período predeterminado de tiempo que ha empezado al aparecer otro suceso especificado. (I) (2) Intervalo de tiempo asignado para que tengan lugar determinadas operaciones; por ejemplo, la respuesta a un sondeo o direccionamiento antes de que se interrumpa el funcionamiento del sistema y deba reiniciarse.

topología. En comunicaciones, ordenación física o lógica de los nodos de una red, especialmente las relaciones de un nodo con otro nodo y los enlaces entre los mismos.

trama. (1) En la arquitectura interconexión de sistemas abiertos, estructura de datos perteneciente a un área particular de información y compuesta por ranuras que pueden aceptar los valores de atributos específicos y de las que pueden deducirse inferencias mediante conexiones apropiadas de procedimiento. (T) (2) Unidad de transmisión en algunas redes de área local, incluida la Red en Anillo de IBM. Incluye delimitadores, caracteres de control, información y caracteres de comprobación. (3) En SDLC, vehículo para cada mandato, cada respuesta y toda información transmitida con procedimientos de SDLC.

trama de información (I). Trama de formato I que se utiliza para la transferencia de información numerada.

trama exploradora. Véase *paquete explorador*.

trama I. Trama de información.

transceptor (transmisor-receptor). En las LAN, dispositivo físico que conecta una interfaz de sistema principal a una red de área local, como, por ejemplo, Ethernet. Los transceptores de Ethernet contienen elementos electrónicos que aplican señales al cable y que detectan colisiones.

Transmission Control Protocol (TCP). Protocolo de comunicaciones utilizado en Internet y en cualquier red que siga las normas del Departamento de Defensa de los EE.UU. para el protocolo interredes. TCP proporciona un protocolo fiable de sistema principal a sistema principal entre sistemas principales en redes de comunicaciones de paquetes conmutados y en los sistemas interconectados de dichas redes. Utiliza Internet Protocol (IP) como protocolo subyacente.

Transmission Control Protocol/Internet Protocol (TCP/IP). Conjunto de protocolos de comunicaciones que dan soporte a funciones de conectividad de igual a igual para redes de área local y amplia.

transporte de vector de gestión de red (NMVT). Unidad de petición/respuesta (RU) de servicios de gestión que fluye sobre una sesión activa entre servicios de gestión de unidad física y servicios de gestión de punto de control (sesión de SSCP-PU).

troncal. (1) En una configuración de anillo de diversos puentes de una red de área local, enlace de gran velocidad al que se conectan los anillos por medio de puentes o direccionadores. Un troncal puede configurarse como bus o como anillo. (2) En una red de área amplia, enlace de gran velocidad al que se conectan nodos o intercambios de conmutaciones de datos (DSE).

U

umbral. (1) En programas de puente de IBM, valor asignado al número máximo de tramas que no se reenvían por un puente debido a errores antes de que se cuente una aparición de “umbral sobrepasado” y se indique en los programas de gestión de red. (2) Valor inicial a partir del cual un contador disminuye hasta 0 o valor hasta el que aumenta o disminuye un contador a partir de un valor inicial.

unidad básica de transmisión (BTU). En SNA, unidad de datos e información de control que pasa entre los componentes del control de la vía de acceso. Una BTU puede constar de una o más unidades de información de vía de acceso (PIU).

unidad de datos de protocolo (PDU). Unidad de datos especificada en un protocolo de una capa determinada y compuesta por información de control de protocolo de esta capa además de, posiblemente, datos de usuario de esta capa. (T)

unidad de datos de protocolo de control de enlace lógico (LLC). Unidad de información intercambiada entre estaciones de enlace de diferentes nodos. La unidad de datos de protocolo de LLC contiene un punto de acceso a servicios de destino (DSAP), un punto de acceso a servicios de origen (SSAP), un campo de control y datos de usuario.

unidad de información de vía de acceso (PIU). Unidad de mensaje compuesta por una sola cabecera de transmisión (TH) o por una TH seguida de una unidad básica de información (BIU) o un segmento de BIU.

unidad de mensaje de soporte de diversos dominios (MDS-MU). Unidad de mensaje utilizada en el soporte de diversos dominios que contiene datos de servicios de gestión y fluye entre conjuntos de funciones de servicios de gestión sobre las sesiones de LU-LU y CP-CP. Esta unidad de mensaje, así como los datos reales de servicios de gestión que contiene, tiene el formato de corriente de datos general (GDS). Véase también *unidad de servicios de gestión de punto de control (CP-MSU)*, *unidad de servicios de gestión (MSU)* y *transporte de vector de gestión de red (NMVT)*.

unidad de red accesible (NAU). Unidad lógica (LU), unidad física (PU), punto de control (CP) o punto de control de servicios del sistema (SSCP). Es el origen o el destino de la información transmitida por la red de control de la vía de acceso. Sinónimo de *unidad de red direccionable*.

unidad de red direccionable (NAU). Equivale a *unidad de red accesible*.

unidad de servicio de canal (CSU). Unidad que proporciona la interfaz a una red digital. La CSU proporciona funciones de acondicionamiento (o igualación) de línea, que mantienen la uniformidad del rendimiento de la señal a lo largo del ancho de banda de canal; remodelación de señal, que constituye la corriente de pulsaciones binarias; y prueba de bucle de retorno, que incluye la transmisión de señales de prueba entre la CSU y la unidad de canal de oficina de la portadora de red. Véase también *unidad de servicio de datos (DSU)*.

unidad de servicio de datos (DSU). Dispositivo que proporciona una interfaz de servicio de datos digital al equipo terminal de datos de manera directa. La DSU proporciona igualación de bucle y posibilidades de pruebas locales y remotas, así como una interfaz EIA/CCITT estándar.

unidad de servicios de gestión de punto de control (CP-MSU). Unidad de mensaje que contiene datos de servicios de gestión y fluye entre los conjuntos de funciones de servicios de gestión. Esta unidad de mensaje tiene el formato de corriente de datos general (GDS). Véase también *unidad de servicios de gestión (MSU)* y *transporte de vector de gestión de red (NMVT)*.

unidad EIA. Unidad de medida que ha establecido la Electronic Industries Association y es igual a 44,45 milímetros (1,75 pulgadas).

unidad física (PU). (1) Componente que gestiona y supervisa los recursos (como, por ejemplo, enlaces conectados y estaciones de enlace adyacentes) asociados con un nodo tal como lo solicita un SSCP mediante una sesión de SSCP-PU. Un SSCP activa una sesión con la unidad física con el fin de gestionar indirectamente, a través de la PU, recursos del nodo, como, por ejemplo, enlaces conectados. Este término sólo se aplica a los nodos de tipo 2.0, tipo 4 y tipo 5. (2) Véase también *PU periférica* y *PU de subárea*.

unidad lógica (LU). Tipo de unidad de red accesible que permite que los usuarios obtengan acceso a recursos de red y se comuniquen entre sí.

unidad máxima de transmisión (MTU). En las LAN, la mayor unidad de datos posible que puede enviarse por un medio físico determinado en una sola trama. Por ejemplo, la MTU para Ethernet tiene 1500 bytes.

unión de telecomunicaciones internacionales (ITU). Agencia de telecomunicaciones especializada de las Naciones Unidas que se ha establecido con el fin de proporcionar procedimientos y prácticas para la normalización de las comunicaciones, lo cual incluye asignación de frecuencia y regulaciones de la radio universales.

User Datagram Protocol (UDP). En el conjunto de protocolos de Internet, protocolo que proporciona un servicio no fiable de datagramas sin conexiones. Permite que un programa de aplicación de una máquina o proceso envíe un datagrama a un programa de aplicación de otra máquina o proceso. UDP utiliza Internet Protocol (IP) para entregar datagramas.

V

V.24. En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito de datos (DCE).

V.25. En la comunicación de datos, especificación de la CCITT que define el equipo de respuesta automática y el equipo de llamada automática paralelo de la red telefónica general conmutada, incluidos los procedimientos de inhabilitación de dispositivos controlados con eco para las llamadas establecidas de manera manual y automática.

V.34. Recomendación del ITU-T para la comunicación por módem sobre canales estándares de transmisión de voz de 33,6 Kbps (y más lentos) disponibles comercialmente.

V.35. En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito de datos (DCE) con varias velocidades de datos.

V.36. En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito

de datos (DCE) con las velocidades de 48, 56, 64 ó 72 kilobits por segundo.

valor por omisión. Perteneciente a un atributo, condición, valor u opción que se supone cuando no se especifica nada de forma explícita. (I)

variable de corriente de datos general (GDS). Tipo de subestructura de RU que va precedida de un identificador y un campo de longitud e incluye datos de aplicación, datos de control de usuario o datos de control definidos según SNA.

variable de la MIB. En el protocolo Simple Network Management Protocol (SNMP), instancia específica de datos definida en un módulo de la MIB. Sinónimo de *objeto de la MIB*.

vecino. Direccionador de una subred común designado por un administrador de red para recibir información de direccionamiento.

vecino ascendente activo más próximo (NAUN). En la Red en Anillo de IBM, estación que envía datos directamente a una estación determinada del anillo.

vector de control de selección de ruta (RSCV). Vector de control que describe una ruta de una red APPN. El RSCV consta de una secuencia ordenada de vectores de control que identifican los TG y nodos que componen la vía de acceso de un nodo de origen a un nodo de destino.

velocidad de información comprometida. Cantidad máxima de datos en bits que la red acepta entregar.

velocidad de transferencia de datos. Promedio de los bits, caracteres o bloques por unidad de tiempo que pasan entre los miembros del equipo correspondiente en un sistema de transmisión de datos. (I)

Notas:

1. La velocidad se expresa en bits, caracteres o bloques por segundo, minuto u hora.
2. Debe indicarse el equipo correspondiente; por ejemplo, módems, equipo intermedio u origen y destino.

versión. Programa bajo licencia independiente que a menudo tiene un nuevo código o una nueva función significativos.

vertimiento múltiple. (1) Transmisión de los mismos datos a un grupo seleccionado de destinos. (T) (2) Forma especial de difusión en que se entregan copias de un paquete a un subconjunto de todos los destinos posibles solamente.

vía de acceso. (1) En una red, cualquier ruta entre dos nodos cualesquiera. Una vía de acceso puede incluir más de una rama. (T) (2) Serie de componentes de red de transporte (control de la vía de acceso y control de enlace de datos) por los que pasa la información intercambiada entre dos unidades de red accesibles. Véase también *ruta explícita (ER)*, *extensión de ruta* y *ruta virtual (VR)*.

VINES. VIrtual NEtworking System.

VIrtual NEtworking System (VINES). Sistema operativo de red y software de red de Banyan Systems, Inc. En una red VINES, la función de enlace virtual permite que todos los dispositivos y servicios aparenten estar conectados directamente entre sí cuando en realidad pueden encontrarse a miles de kilómetros de distancia. Véase también *StreetTalk*.

vista de la MIB. En el protocolo Simple Network Management Protocol (SNMP), conjunto de objetos gestionados, conocidos por el agente, que es visible en una comunidad en particular.

vuelco. (1) Datos que se han volcado. (T) (2) Copiar el contenido de la totalidad o de parte del almacenamiento virtual con el fin de reunir información de errores.

X

X.21. recomendación de la comisión consultiva de la telefonía y telegrafía internacionales (CCITT) relativa a una interfaz de fines generales entre un equipo terminal de datos y un equipo de terminación de circuito de datos para las operaciones síncronas en una red pública de datos.

X.25. (1) recomendación de la comisión consultiva de la telefonía y telegrafía internacionales (CCITT) relativa a la interfaz entre un equipo terminal de datos y las redes de datos de paquetes conmutados. (2) Véase también *conmutación de paquetes*.

Xerox Network Systems (XNS). Conjunto de protocolos de internet desarrollados por Xerox Corporation. Aunque es similar a los protocolos TCP/IP, XNS utiliza unos formatos de paquete y una terminología diferentes. Véase también *Internetwork Packet Exchange (IPX)*.

Z

zona. En redes AppleTalk, subconjunto de nodos dentro de una internet.

Zone Information Protocol (ZIP). En redes AppleTalk, protocolo que proporciona un servicio de gestión de zonas manteniendo una correlación de los nombres de zonas y los números de red de la internet en la capa de sesión.

Índice

CH

D

E

F

G

H

I

L

LL

M

N

O

P

Q

R

S

T

U

V

W

Hoja de Comentarios

Access Integration Services
Utilización y configuración
de las funciones
Versión 3.4

Número de Publicación SC10-3437-01

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
SC10-3437-01

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

SC10-3437-01

Corte o Doble
Por la Línea

SC10-3437-01