



# **APX 8000<sup>TM</sup>/MAX TNT<sup>®</sup>/DSL TNT<sup>TM</sup>**

Guía de configuración, ruteo y túnel para WAN

**Copyright© 2000 Lucent Technologies. Todos los derechos reservados.**

Este material está protegido por las leyes de derechos de autor (copyright) de los Estados Unidos y otros países. No se puede reproducir, distribuir ni modificar en modo alguno por ninguna entidad (ajena o vinculada a Lucent Technologies), con excepción de lo estipulado en los acuerdos, contratos y licencias aplicables, sin la autorización expresa por escrito de Lucent Technologies. Para obtener permiso de reproducción o distribución, envíe su petición por correo electrónico a [techpubs@ascend.com](mailto:techpubs@ascend.com).

#### **Aviso**

Se ha hecho todo lo posible para garantizar que la información contenida en este documento esté completa y sea correcta en el momento de su impresión, pero la información está sujeta a posibles cambios.

#### **Información sobre seguridad, cumplimiento de normativas y garantía**

Antes de manipular cualquier producto de hardware de redes de acceso de Lucent, lea la *Guía de seguridad y cumplimiento de normativas de redes de acceso* incluida en el embalaje del producto. Consulte, asimismo, dicha guía para determinar si los productos cumplen los requisitos de Interferencia electromagnética (EMI) y compatibilidad de redes vigentes en su país. Consulte la tarjeta de la garantía incluida en el embalaje del producto para ver las condiciones de la garantía limitada que Lucent Technologies proporciona con sus productos.

#### **Declaración de seguridad**

En raras ocasiones, personas no autorizadas realizan conexiones a la red de telecomunicaciones mediante el uso de las funciones de acceso.

#### **Marcas comerciales**

4ESS, 5ESS, A Network of Expertise, AnyMedia, AqueView, AUDIX, B-STDx 8000, B-STDx 9000, ...Beyond Compare, CaseView, Cajun, CajunDocs, CAJUNVIEW, Callmaster, CallVisor, CBX 500, CellPipe, ChoiceNet, ClearReach, ComOS, cvMAX, DACScan, Dacsmate, Datakit, DEFINITY, Definity One, DSLMAX, DSL Terminator, DSLPipe, DSLTNT, Elemedia, Elemedia Enhanced, EMMI, End to End Solutions, EPAC, ESS, EVEREST, Gigabit-scaled campus networking, Globalview, GRF, GX 250, GX 550, HyperPATH, Inferno, InfernoSpaces, Intragy, IntragyAccess, IntragyCentral, Intuity, IP Navigator, IPWorX, LineReach, LinkReach, MAX, MAXENT, MAX TNT, Multiband, Multiband PLUS, Multiband RPM, MultiDSL, MultiVoice, MultiVPN, Navis, NavisAccess, NavisConnect, NavisCore, NavisRadius, NavisXtend, NetCare, NetLight, NetPartner, OneVision, Open Systems Innovations, OpenTrunk, P550, PacketStar, PathStar, Pinnacle, Pipeline, PMVision, PortMaster, SecureConnect, Selectools, Series56, SmoothConnect, Stinger, SYSTIMAX, True Access, WaveLAN, WaveMANAGER, WaveMODEM, WebXtend y Where Network Solutions Never End son marcas comerciales de Lucent Technologies. Advantage Pak, Advantage Services, AnyMedia, ...Beyond Compare, End to End Solutions, Inter.NetWorking, MAXENT y NetWork Knowledge Solutions son marcas de servicio de Lucent Technologies. Las demás marcas comerciales, marcas de servicio y nombres comerciales que aparecen en esta publicación pertenecen a sus propietarios respectivos.

#### **Copyrights del software de terceros incluido en los productos de software de redes de acceso de Lucent**

Software C++ Standard Template Library copyright© 1994 Hewlett-Packard Company y copyright© 1997 Silicon Graphics. Se otorga autorización para usar, copiar, modificar, distribuir y vender este software y su documentación gratuitamente, con la condición de que el aviso de copyright anterior aparezca en todas las copias y que tanto el copyright como esta autorización aparezcan en la documentación de soporte. Ni Hewlett-Packard ni Silicon Graphics hacen ninguna declaración sobre la idoneidad de este software para cualquier propósito. Se proporciona "tal cual" sin garantía expresa o implícita.

Software para UNIX Berkeley Software Distribution (BSD) copyright© 1982, 1986, 1988, 1993 Los miembros del consejo rector de California. Todos los derechos reservados. Se autoriza la redistribución y el uso en forma fuente y binaria, con o sin modificaciones, siempre que se cumplan las siguientes condiciones. 1. Las redistribuciones del código fuente deben incluir el aviso de copyright anterior, esta lista de condiciones y la siguiente exención de responsabilidad. 2. Las redistribuciones en forma binaria deben reproducir el aviso de copyright anterior, esta lista de condiciones y la siguiente exención de responsabilidad en la documentación u otros materiales proporcionados con la distribución. 3. Todos los materiales publicitarios que mencionen características o el uso de este software deben incluir el siguiente reconocimiento: Este producto incluye software desarrollado por University of California, Berkeley y sus colaboradores. 4. Ni el nombre de la universidad ni el de sus colaboradores puede ser usado para recomendar o promocionar productos derivados de este software sin previa autorización por escrito.

LOS MIEMBROS DEL CONSEJO RECTOR Y COLABORADORES PROPORCIONAN ESTE SOFTWARE "TAL CUAL" Y RECHAZAN CUALQUIER GARANTÍA EXPRESA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN E IDONEIDAD PARA UN PROPÓSITO ESPECÍFICO. EN NINGÚN CASO SERÁN RESPONSABLES LOS MIEMBROS DEL CONSEJO RECTOR NI LOS COLABORADORES DE DAÑOS DIRECTOS, INDIRECTOS, FORTUITOS, ESPECIALES O RESULTANTES (INCLUIDAS, PERO SIN LIMITARSE A, LA OBTENCIÓN O SUSTITUCIÓN DE BIENES O SERVICIOS; PÉRDIDA DE USO O DATOS O LUCRO CESANTE; O INTERRUPCIÓN DE ACTIVIDADES EMPRESARIALES), CUALESQUIERA SEAN SUS CAUSAS NI DE CUALQUIER SUPUESTO DE RESPONSABILIDAD, YA SEA POR CONTRATO, RESPONSABILIDAD ESTRUCTA O AGRAVIO (POR NEGLIGENCIA U OTROS SUPUESTOS), QUE DERIVEN EN CUALQUIER MANERA DEL USO DE ESTE SOFTWARE, AUNQUE SE HAYA ADVERTIDO DE LA POSIBILIDAD DE DICHOS DAÑOS.

#### **Solicitud de información**

Puede solicitar la información más actualizada del producto y formación en línea por computadora en la dirección <http://www.lucent.com/ins/bookstore>.

#### **Comentarios**

Lucent Technologies aprecia los comentarios, positivos o negativos, sobre este manual. Envíelos a [techpubs@ascend.com](mailto:techpubs@ascend.com).

---

## ***Servicio de atención al cliente***

El servicio de atención al cliente proporciona diferentes opciones para obtener información sobre los servicios y productos de Lucent, las actualizaciones de software y la asistencia técnica.

### **Buscar información y software en Internet**

Visite el sitio Web <http://www.lucent.com/ins> si desea obtener información técnica, información sobre los productos y descripciones de los servicios disponibles.

Visite el sitio FTP <ftp://ftp.ascend.com> si desea obtener actualizaciones de software, notas sobre la versión y suplementos.

### **Asistencia técnica**

Puede obtener asistencia técnica por teléfono, correo electrónico, fax, módem o correo postal, así como mediante Internet.

#### ***Recopilación de la información necesaria***

Si necesita ponerse en contacto con Lucent para obtener ayuda y resolver algún problema, cerciórese de disponer de la siguiente información cuando haga la llamada o, si escribe, inclúyala en su correspondencia:

- Nombre del producto y modelo
- Opciones de software y hardware
- Versión del software
- Si los suministra la compañía portadora, los SPID (Identificadores de perfil de servicios) asociados a su línea
- Tipo de conmutación de su compañía telefónica local y modo operativo como, por ejemplo, 5ESS Custom de AT&T o National ISDN-1 de Northern Telecom
- Si utiliza un sistema de ruteo o de puenteo con el producto Lucent
- Tipo de computadora que usa
- Descripción del problema

#### ***Llamar a Lucent desde los Estados Unidos***

Si reside en los Estados Unidos, puede beneficiarse de la Asistencia técnica prioritaria o de un contrato de servicios avanzados. También puede llamar para solicitar asistencia.

##### ***Asistencia técnica prioritaria***

Si necesita ponerse en contacto con un técnico de manera inmediata, llame al (900) 555-2763 y su llamada se pondrá a la cola de las llamadas prioritarias. El precio de la llamada es de 2,95 dólares por minuto y no comenzará a aplicarse hasta que haya sido puesto al habla con un técnico. El tiempo medio de espera es inferior a tres minutos.

---

## *Servicios avanzados*

Servicios avanzados ofrece una amplia selección de servicios. Los servicios de instalación le ayudan a instalar correctamente su WAN (Red de área amplia) de Lucent. Los servicios continuos de mantenimiento y de soporte proporcionan soluciones de hardware y software que permiten que la red funcione a pleno rendimiento. Si desea obtener más información al respecto, llame al teléfono de los Estados Unidos (800) 272-3634.

## *Otros números de teléfono*

Si desea escuchar un menú de los servicios de Lucent, llame al teléfono de los Estados Unidos (800) 272-3634. O llame al (510) 769-6001 si desea hablar con un operador.

## *Llamar a Lucent desde fuera de los Estados Unidos*

Puede ponerse en contacto con Lucent por teléfono desde otros países llamando a uno de los números siguientes:

Teléfono para llamar desde fuera de los Estados Unidos	(510) 769-8027
Austria, Alemania, Suiza	(+33) 492 96 5672
Benelux	(+33) 492 96 5674
Francia	(+33) 492 96 5673
Italia	(+33) 492 96 5676
Japón	(+81) 3 5325 7397
Oriente Medio, África	(+33) 492 96 5679
Países escandinavos	(+33) 492 96 5677
España, Portugal	(+33) 492 96 5675
Reino Unido	(+33) 492 96 5671

Podrá encontrar recursos adicionales de soporte para la zona del Pacífico y Asia en <http://www.lucent.com/ins/international/apac/>.

## *Obtener asistencia por correspondencia*

Envíe sus preguntas sobre asistencia técnica a una de las siguientes direcciones de correo electrónico. También se puede poner en contacto por fax, BBS o correo postal con la oficina de Servicio de atención al cliente de Lucent en los Estados Unidos en Alameda, California:

- Por correo electrónico desde los Estados Unidos: [support@ascend.com](mailto:support@ascend.com)
- Por correo electrónico desde Europa, Oriente Medio y África: [EMEAsupport@ascend.com](mailto:EMEAsupport@ascend.com)
- Por correo electrónico desde la zona del Pacífico y Asia: [apac.support@ascend.com](mailto:apac.support@ascend.com)
- Por fax: (510) 814-2312

- 
- Por BBS de soporte al cliente (vía módem): (510) 814-2302
  - Dirija su correspondencia con Lucent a:

Attn: Customer Service  
Lucent Technologies  
1701 Harbor Bay Parkway  
Alameda, CA 94502-3002  
EE.UU.



# Índice

Servicio de atención al cliente .....	iii
---------------------------------------	-----

## **Acerca de esta guía ..... xxv**

Contenido de esta guía .....	xxv
Lo que debería saber .....	xxv
Convenciones utilizadas en la documentación.....	xxvi
Documentación .....	xxvii

## **Capítulo 1 Conexiones WAN ..... 1-1**

Introducción a las conexiones WAN .....	1-1
Tipos de protocolos de encapsulación .....	1-2
PPP, MP y MP+ .....	1-2
Otros protocolos de encapsulación .....	1-2
Cómo responde y autentica llamadas de entrada el sistema .....	1-2
Cómo inicia el sistema las llamadas de salida .....	1-3
Cómo establece y supervisa sesiones el sistema.....	1-3
Perfiles generales del sistema .....	1-3
Perfil Answer-Defaults .....	1-3
Ajustes de RADIUS predeterminados .....	1-4
Petición de la autenticación en llamadas PPP .....	1-4
Ajustes de V.120.....	1-4
Perfil Terminal-Server .....	1-5
Perfil External-Auth.....	1-6
Perfiles de autenticación locales y externos.....	1-7
Utilización de perfiles Connection .....	1-7
Utilización compartida de perfiles para cada usuario .....	1-7
Utilización de RADIUS .....	1-8
Especificación de límites de tiempo de sesión.....	1-8
Ajustes del límite de tiempo en un perfil Connection .....	1-9
Ajustes del límite de tiempo en un perfil RADIUS.....	1-9
Ejemplos de definición de límites de tiempo.....	1-10
Utilización de la contabilidad de sesiones .....	1-11
Especificación de velocidades de recepción y transmisión de datos en RADIUS .....	1-11
Configuración de conexiones de marcación conmutadas .....	1-12
Conexiones PPP de un único canal.....	1-12
Ajustes de un perfil Connection .....	1-12
Ajustes de un perfil RADIUS .....	1-13
Autenticación de la contraseña .....	1-14
Métodos de compresión de enlaces .....	1-14
Supervisión de la calidad del enlace.....	1-14
Ejemplos de una conexión PPP síncrona.....	1-15
Ejemplos de una conexión PPP asíncrona .....	1-15

Conexiones de protocolo multienlace (MP) .....	1-16
Ajustes de un perfil Connection .....	1-16
Ajustes de un perfil RADIUS .....	1-17
Ejemplos de una conexión MP .....	1-18
Vinculación de llamadas analógicas mediante MP .....	1-18
Conexiones del protocolo multienlace Plus (MP+) .....	1-19
Cómo agregan ancho de banda las unidades TAOS .....	1-19
Ajustes de un perfil Connection .....	1-21
Ajustes de un perfil RADIUS .....	1-22
Ejemplos de una configuración MP+ .....	1-23
Protocolo de control de asignación de ancho de banda (BACP) .....	1-24
Conexiones TCP-Clear .....	1-25
Mejoras de rendimiento para llamadas TCP-Clear (sólo perfiles locales) .....	1-25
Ajustes de un perfil Connection .....	1-25
Ajustes de un perfil RADIUS .....	1-27
Ejemplos de conexiones TCP-Clear .....	1-28
Ejemplo de TCP-Clear con almacenamiento de paquetes en el búfer (sólo perfiles locales) .....	1-28
Aplicación de un perfil IPsec a una sesión TCP-Clear .....	1-29
Modo de túnel y modo de transporte .....	1-30
Ejemplo de una configuración ESP de IPsec para TCP-Clear .....	1-31
Conexiones X.75 .....	1-32
Configuración de conexiones permanentes y permanentes MP+ .....	1-33
Conexiones permanentes .....	1-34
Ajustes de un perfil Connection .....	1-34
Ajustes de un perfil RADIUS .....	1-35
Ejemplos de una conexión permanente .....	1-36
Conexiones permanentes MP+ .....	1-37
Ajustes de un perfil Connection .....	1-37
Ajustes de un perfil RADIUS .....	1-38
Ejemplos de una conexión permanente MP+ .....	1-38
Interfaces de reserva para conexiones permanentes .....	1-39
Ajustes de un perfil Connection .....	1-40
Ajustes de un perfil RADIUS .....	1-40
Ejemplos de una interfaz de reserva conmutada .....	1-40
Configuración de conexiones de salida .....	1-42
Acerca de los perfiles RADIUS de llamadas de salida .....	1-43
Temporizador de llamadas de salida que se puede configurar .....	1-43
Perfiles de llamada de salida PPP y PPP multicanal .....	1-44
Ajustes de un perfil Connection .....	1-44
Ajustes de un perfil RADIUS .....	1-45
Autenticación de la contraseña .....	1-45
Ejemplos de una conexión PPP de llamadas de salida .....	1-46
Conexiones de llamada de salida por módem .....	1-47
Necesidad de reiniciar el sistema .....	1-47
Activación de Direct-Access del módem .....	1-47
Ejemplo de Direct-Access utilizando una contraseña global .....	1-48
Conexiones de llamadas de salida por módem que requieren perfiles .....	1-49



<b>Capítulo 2</b>	<b>Ruteo IP .....</b>	<b>2-1</b>
	Información general sobre el ruteo .....	2-1
	Rutas e interfaces .....	2-1
	Visualización de la tabla de ruteo.....	2-2
	Visualización de la tabla de interfaces .....	2-3
	Sintaxis de las direcciones IP.....	2-4
	Configuración de interfaces IP LAN .....	2-6
	Información general sobre los ajustes de una interfaz LAN.....	2-6
	Ejemplo de configuración de una interfaz IP LAN .....	2-7
	Activación de ARP de proxy .....	2-8
	Activación de RIP.....	2-9
	Ejemplo de definición de interfaces LAN virtuales.....	2-9
	Ejemplo de definición de la interfaz software .....	2-10
	Ejemplo de desactivación de difusiones generales dirigidas .....	2-11
	Ejemplo de definición de una interfaz de sólo gestión .....	2-12
	Configuración de interfaces IP WAN .....	2-12
	Información general sobre los ajustes de una interfaz WAN .....	2-12
	Ajustes de los perfiles Connection .....	2-13
	Ajustes de los perfiles RADIUS.....	2-15
	Ejemplos de una conexión a otro ruteador IP .....	2-18
	Ejemplos de una conexión de ruta de host.....	2-19
	Ejemplos de una conexión de interfaz numerada .....	2-20
	Ejemplos de una conexión IP-Direct .....	2-21
	Ejemplos de creación de la ruta hacia una conexión privada .....	2-22
	Ejemplos de gateways predeterminados de cliente.....	2-23
	Ejemplos de verificación de la dirección de origen por sesión.....	2-23
	Ejemplos de definición de la política QoS y TOS .....	2-24
	Configuración de rutas IP estáticas .....	2-25
	Información general sobre los ajustes de rutas estáticas.....	2-26
	Ajustes de los perfiles IP-Route .....	2-26
	Ajustes de un perfil de ruta RADIUS .....	2-27
	Ajustes de ruta en un perfil de usuario RADIUS .....	2-28
	Rutas estáticas privadas específicas de la conexión (sólo RADIUS).....	2-29
	Ejemplos de configuración de rutas predeterminadas .....	2-29
	Ejemplos de una ruta predeterminada basada en LAN.....	2-29
	Ejemplos de una ruta predeterminada en un enlace WAN .....	2-30
	Ejemplos de configuración de una ruta hacia una subred remota.....	2-31
	Ejemplos de configuración de una ruta de varios trayectos.....	2-31
	Configuración de tablas de ruteo privado .....	2-32
	Información general sobre los ajustes de un perfil local .....	2-33
	Información general sobre los atributos RADIUS para hacer referencia a una tabla de ruteo privado.....	2-34
	Información general sobre los atributos RADIUS para definir una tabla de ruteo privado .....	2-35
	Ejemplos de configuración de una tabla de ruteo privado.....	2-36
	Ejemplos de utilización de tablas de ruteo privado .....	2-37
	Ejemplos de rutas estáticas privadas.....	2-38
	Definición de políticas de ruteo TCP/IP .....	2-39
	Definición de una dirección IP de origen del sistema .....	2-39
	Definición de políticas de seguridad del ruteador .....	2-40
	Requisito de aceptación de asignación dinámica de direcciones.....	2-41
	Perfiles compartidos .....	2-41

Especificación de un perfil User predeterminado para el acceso Telnet .....	2-42
Restricción del acceso Telnet al sistema: .....	2-43
Definición de políticas de ruteo general del sistema .....	2-43
Cómo pasar por alto paquetes ICMP .....	2-44
Descarte de paquetes de ruteados en origen .....	2-44
Definición de preferencias de ruta estática .....	2-45
Definición de opciones de protocolo de ruteo .....	2-45
Política RIP para propagar las actualizaciones de vuelta a la subred de origen ....	2-46
Activación de RIP .....	2-47
Definición de los valores de preferencia para rutas obtenidas de actualizaciones de RIP .....	2-47
Veto de rutas para forzar el uso de una unidad TAOS redundante .....	2-48
Limitación del tamaño de las colas de paquetes UDP .....	2-48
Cómo pasar por alto rutas predeterminadas al actualizar la tabla de ruteo .....	2-49
Supresión de anuncios de ruta de host .....	2-49
Definición de opciones de caché de ruta IP y puerto IP .....	2-49
Cachés de ruta .....	2-50
Cachés de puerto .....	2-50
Activación de opciones de protocolo .....	2-51
Activación del protocolo Boot y Reverse-ARP .....	2-52
Activación de sumas de comprobación UDP .....	2-52
Definición de un tiempo de espera TCP .....	2-53
Activación de respuestas a consultas Finger .....	2-53
Activación de BOOTP-Relay .....	2-55
Utilización de SNTP para ajustar y mantener la hora del sistema .....	2-55
Configuración de una redirección de puerto .....	2-56
Información general sobre los ajustes del perfil Connection .....	2-56
Información general sobre los ajustes de RADIUS .....	2-57
Ejemplo de configuración de una redirección de puerto .....	2-58
Configuración de DNS .....	2-58
Configuración de búsquedas DNS y la lista DNS .....	2-59
Especificación de nombres de dominio para las búsquedas .....	2-59
Especificación de direcciones de servidor DNS local .....	2-60
Soporte a la lista DNS .....	2-60
Configuración de una tabla DNS local .....	2-61
Coincidencia de nombres de host .....	2-62
Definición de la tabla local .....	2-62
Utilización de la función Auto-Update .....	2-63
Utilización del DNS de cliente .....	2-64
Información general sobre los ajustes de un DNS de cliente .....	2-65
Ejemplo de configuración de servidores DNS de cliente en el nivel del sistema..	2-66
Ejemplos de configuración de un DNS de cliente en el nivel de la conexión .....	2-66
Configuración de la asignación de WINS de Microsoft .....	2-67
Ajustes de un perfil Connection .....	2-67
Ajustes de un perfil RADIUS .....	2-68
Ejemplos de configuración de servidores WINS de cliente .....	2-68
Configuración y utilización de agrupaciones de direcciones .....	2-69
Información general sobre los ajustes para definir agrupaciones .....	2-69
Ajustes de los perfiles IP-Global .....	2-69
Ajustes de los perfiles de pseudousuario RADIUS .....	2-70
Agrupaciones RADIUS globales (RADIPAD) .....	2-70
Ejemplos de configuración de agrupaciones de direcciones .....	2-72

Ejemplos de configuración de agrupaciones de direcciones resumidas .....	2-73
Activación del indicador Pool-Summary .....	2-73
Definición de agrupaciones con alineación de red .....	2-73
Ejemplos de asignación de una dirección desde una agrupación .....	2-75
Encadenamiento de agrupaciones IP .....	2-76
Encadenamiento de agrupaciones en perfiles locales .....	2-77
Encadenamiento de agrupaciones en RADIUS .....	2-79
Configuración del envío de difusión múltiple.....	2-81
Ajustes globales para activar el envío por difusión múltiple.....	2-82
Especificación de un tiempo de espera para miembros de un grupo.....	2-83
Control del pulso del tráfico de difusión múltiple.....	2-84
Configuración de la interfaz MBONE .....	2-85
Información general sobre los ajustes de la interfaz MBONE .....	2-86
Ejemplo de un ruteador MBONE local .....	2-86
Ejemplo de un ruteador MBONE en una interfaz WAN.....	2-87
Configuración de interfaces de cliente de difusión múltiple .....	2-87
Ajustes de los perfiles IP-Interface y Connection locales .....	2-87
Ajustes de los perfiles RADIUS .....	2-88
Definición del límite de velocidad de difusión múltiple .....	2-89
Especificación de un retardo para la eliminación de grupos IGMP .....	2-89
Ejemplo de configuración de una interfaz LAN de cliente de difusión múltiple ..	2-90
Ejemplos de configuración de interfaces WAN de cliente de difusión múltiple...	2-90

## Capítulo 3      **Ruteo OSPF ..... 3-1**

Introducción a OSPF .....	3-1
Limitaciones de RIP resueltas por OSPF.....	3-1
Métrica de distancia-vector .....	3-1
Limitación de 15 saltos.....	3-2
Exceso de tráfico de ruteo y convergencia lenta .....	3-2
Implementación TAOS de OSPF.....	3-2
Funciones limitadas de ruteador de frontera.....	3-2
Autenticación.....	3-2
Una interfaz IP activa por puerto.....	3-3
Comandos de diagnóstico de OSPF.....	3-3
Capturas OSPF.....	3-3
Características de OSPF.....	3-3
Seguridad .....	3-4
Soporte para máscaras de subred de longitud variable.....	3-4
Intercambio de información de ruteo.....	3-4
Ruteadores designados y ruteadores designados de reserva.....	3-5
Métrica configurable del coste .....	3-6
Ruteo jerárquico (áreas).....	3-6
Algoritmo de ruteo de estado de enlaces .....	3-8
Adición de una unidad TAOS a una red OSPF.....	3-10
Información general de los ajustes OSPF de LAN y WAN .....	3-10
Ejemplo de configuración de una interfaz OSPF de LAN.....	3-13
Ejemplo de configuración de interfaces OSPF de WAN.....	3-14
Ejemplo de integración de una interfaz RIP-v2.....	3-15
Configuración de opciones de ruta.....	3-16
Ejemplo de importación de una agrupación resumida como ASE .....	3-17
Ejemplo de definición de preferencias ASE .....	3-18
Configuración de información de ruta estática OSPF.....	3-18

Ejemplo de configuración de un LSA de tipo 7 en una NSSA .....	3-19
Ejemplo de asignación de un coste a una ruta estática .....	3-20
Ejemplo de especificación de una ruta de terceros .....	3-20
Soporte multiacceso de no difusión (NBMA) de OSPF .....	3-21
Información general de los ajustes de NBMA de OSPF .....	3-21
Ejemplo de configuración de NBMA de OSPF .....	3-22
Ejemplo de configuración de un ruteador contiguo con posibilidades de ser DR. ....	3-23
Ejemplo de configuración de un ruteador contiguo sin posibilidades de ser un ruteador designado (DR) .....	3-25
Desactivación de OSPF .....	3-26

## Capítulo 4      **Protocolo de gestión de túneles de Ascend ..... 4-1**

Introducción a ATMP .....	4-1
Ajustes de red para ATMP .....	4-2
Necesidad de reiniciar el sistema .....	4-2
Recomendación sobre la dirección IP del sistema .....	4-2
Definición del puerto UDP .....	4-3
Especificación de límites de reintento de túneles .....	4-4
Definición de un límite de MTU .....	4-4
Relación entre la MTU y la compresión de enlaces .....	4-5
Fragmentación causada por túneles ATMP .....	4-5
Transferencia de la tarea de fragmentación a puntos finales de conexión .....	4-5
Cómo forzar la fragmentación para interactuar con clientes anticuados .....	4-6
Clientes móviles con direcciones IP duplicadas .....	4-6
Aislamiento de la red y direcciones IP duplicadas .....	4-6
Direcciones duplicadas que se conectan con la misma red interna .....	4-7
Configuración de la conexión de agente a agente .....	4-7
Configuración de un agente externo .....	4-8
Ajustes del perfil ATMP del agente externo .....	4-8
Ajustes de los perfiles mobile-client .....	4-9
Ajustes de los perfiles Connection .....	4-9
Ajustes de los perfiles RADIUS .....	4-10
Especificación de direcciones de agentes locales y números de puerto .....	4-11
Especificación del nombre de la red interna .....	4-12
Ejemplo de una configuración de agente externo .....	4-12
Definición de la dirección del sistema del agente externo .....	4-13
Configuración del perfil ATMP del agente externo .....	4-13
Configuración de una conexión con un agente local de gateway .....	4-13
Configuración de una conexión con el agente local de ruteador .....	4-14
Configuración de una conexión de cliente móvil con el agente local de gateway .....	4-15
Configuración de una conexión de cliente móvil con el agente local de ruteador .....	4-15
Ejemplo de un agente externo que dispone de un túnel con un conmutador GRF .....	4-16
Configuración de agentes locales .....	4-17
Ajustes del perfil ATMP del agente local .....	4-17
Especificación de un agente local de gateway .....	4-18
Especificación de un agente local de ruteador .....	4-19
Especificación de la contraseña de túnel .....	4-19
Definición de un temporizador de inactividad para túneles que no se utilizan .....	4-19
Ajustes del perfil de gateway de la red interna .....	4-20
Limitación del número máximo de túneles .....	4-21
Activación de RIP en la interfaz con el ruteador local .....	4-21
Ejemplo de una configuración de agente local de gateway .....	4-23

Definición de la dirección del sistema del agente local.....	4-23
Configuración del perfil ATMP del agente local .....	4-23
Configuración de un perfil de gateway para la conexión con la red interna .....	4-24
Configuración de una conexión de cliente móvil con el agente local de gateway .....	4-24
Ejemplo de una configuración de agente local de ruteador .....	4-25
Definición de la dirección del sistema del agente local.....	4-25
Configuración del perfil IP-Interface para la conexión con la red interna .....	4-25
Configuración del perfil ATMP del agente local .....	4-26
Configuración de una conexión de cliente móvil con el agente local de ruteador .....	4-26
Configuración de un agente local y externo.....	4-27
Configuración del perfil ATMP.....	4-27
Ejemplo de una configuración de agente local y externo .....	4-27
Definición de la dirección del sistema.....	4-28
Configuración del perfil ATMP para un agente local y externo .....	4-28
Configuración de un perfil de cliente móvil .....	4-29
Otro ejemplo de una configuración de agente local y externo .....	4-29
Definición de la dirección IP del sistema .....	4-30
Configuración del perfil ATMP para un agente local y externo .....	4-30
Configuración de un perfil para el cliente móvil 3 .....	4-31
Configuración de IPX sobre ATMP.....	4-31
Configuración de los agentes para el ruteo de IPX.....	4-32
Ejemplo de IPX sobre ATMP con un agente local de gateway .....	4-32
Configuración de una conexión IPX de cliente móvil.....	4-33
Ejemplo de una conexión IPX de perfil de gateway .....	4-33
Requisitos del ruteador local IPX .....	4-34
Ejemplo de IPX sobre ATMP con un agente local de ruteador .....	4-35
Configuración de una conexión IPX de cliente móvil.....	4-35
Ejemplo de una configuración de agente local de ruteador IPX .....	4-36

## Capítulo 5 Túneles L2TP, PPTP e IP en IP..... 5-1

Protocolo de túnel de capa 2 (L2TP) .....	5-1
Componentes de un túnel L2TP.....	5-1
Configuración de operaciones L2TP .....	5-2
Configuración de una conexión con el LNS .....	5-3
Configuración de perfiles de cliente móvil L2TP.....	5-3
Ajustes de L2TP en perfiles Connection .....	5-4
Ajustes de L2TP en perfiles RADIUS.....	5-4
Ejemplos de apertura de un túnel después de autenticar previamente la llamada ...	5-5
Ejemplos de apertura de un túnel después de la autenticación por contraseña .....	5-6
Configuración de la autenticación IPSec .....	5-6
Protocolos de seguridad IPSec .....	5-6
Modos de encapsulación IPSec .....	5-7
Aplicación de IPSec a un servidor de túnel o en una conexión TCP .....	5-7
Configuración de un perfil IPSec para AH de IPSec.....	5-9
Configuración de un perfil IPSec para ESP de IPSec .....	5-11
Configuración de opciones de temporizador de L2TP .....	5-14
Configuración de los intentos por lista de L2TP .....	5-15
Configuración de varios puntos finales para sesiones de túnel .....	5-15
Servidor de túnel secundario para túneles L2TP y L2F (perfiles locales).....	5-16
Ejemplo de configuración de un túnel L2TP con dos puntos finales de servidor .	5-16
Configuración de un nombre de sistema L2TP optativo .....	5-18
Reenvío de capa 2 (L2F).....	5-18

Autenticación de túneles L2F .....	5-19
Configuración de operaciones básicas de L2F .....	5-20
Configuración de perfiles de cliente de L2F .....	5-22
Protocolo de túnel punto a punto (PPTP).....	5-24
Componentes de un túnel PPTP.....	5-24
Configuración de operaciones PPTP .....	5-25
Configuración de una conexión con el PNS .....	5-26
Configuración de perfiles de cliente móvil de PPTP.....	5-27
Ajustes de PPTP en perfiles Connection .....	5-27
Ajustes PPTP en perfiles RADIUS .....	5-28
Ejemplos de apertura de un túnel después de autenticar previamente la llamada ..	5-28
Ejemplos de apertura de un túnel después de la autenticación por contraseña .....	5-29
Resumen del conjunto de atributos de túnel .....	5-29
Información general de identificadores y conjuntos de atributos .....	5-30
Protocolos de túnel soportados .....	5-30
Atributos de túnel que se utilizan con identificadores.....	5-31
Ejemplo de reordenación de conjuntos utilizando Tunnel-Preference.....	5-32
Encapsulación IP en IP .....	5-33
Ajustes de un perfil Connection.....	5-33
Ajustes de un perfil RADIUS .....	5-34
Ejemplos de una conexión IP en IP .....	5-34

## Capítulo 6 Ruteadores virtuales ..... 6-1

Configuración de ruteadores virtuales .....	6-1
Repercusión de los ruteadores virtuales en la tabla de ruteo .....	6-2
Repercusión de los ruteadores virtuales en los comandos de red .....	6-2
Limitaciones actuales.....	6-3
Creación de un ruteador virtual.....	6-3
Ajustes de un perfil VRouter .....	6-3
Ejemplo de definición de un ruteador virtual .....	6-4
Visualización de las tablas de interfaces y de ruteo del ruteador virtual.....	6-5
Visualización de las estadísticas del ruteador virtual .....	6-5
Definición de agrupaciones de direcciones para un ruteador virtual.....	6-6
Asignación de interfaces a un ruteador virtual .....	6-7
Ajustes de los perfiles locales.....	6-7
Ajustes de los perfiles RADIUS.....	6-8
Ejemplos de cómo asignar la pertenencia de una interfaz a un ruteador virtual .....	6-8
Visualización de interfaces asignadas en las tablas del ruteador virtual .....	6-9
Definición de rutas estáticas de ruteador virtual.....	6-9
Ajustes de un perfil IP-Route .....	6-10
Ajustes de los perfiles RADIUS.....	6-10
Ejemplos de definición de una ruta para cada ruteador virtual .....	6-10
Visualización de la ruta estática en la tabla del ruteador virtual .....	6-11
Especificación de una ruta entre ruteadores virtuales.....	6-11
Visualización de la ruta entre ruteadores virtuales en la tabla global.....	6-11
Supresión de un ruteador virtual.....	6-12
Configuración de servidores de nombres de dominio de ruteador virtual .....	6-12
Información general sobre los ajustes DNS del ruteador virtual .....	6-12
Ejemplo de una configuración DNS clásica de ruteador virtual.....	6-13
Configuración de ruteadores virtuales para conexiones L2TP .....	6-14
Establecimiento del perfil Connection .....	6-15
Establecimiento del perfil RADIUS .....	6-15

<b>Capítulo 7</b>	<b>Ruteo IPX.....</b>	<b>7-1</b>
	Ruteo IPX en la WAN .....	7-1
	Utilización de SAP IPX por parte de las unidades TAOS .....	7-1
	Utilización de RIP IPX por parte de las unidades TAOS .....	7-1
	Funcionamiento de RIP IPX .....	7-2
	La ruta RIP IPX predeterminada .....	7-2
	Soporte para negociación de IPXWAN .....	7-2
	Ampliaciones de IPX estándar.....	7-3
	Recomendaciones para software de cliente NetWare .....	7-3
	Configuración del perfil IPX-Global .....	7-4
	Definición de una red IPX virtual para clientes de llamada de entrada.....	7-5
	Ejemplo de una configuración IPX-Global .....	7-5
	Configuración de interfaces IPX de LAN.....	7-5
	Información general de los ajustes de IPX de LAN .....	7-5
	Activación del ruteo y la simulación de IPX en la interfaz .....	7-6
	Asignación de un número de red IPX .....	7-6
	Propagación de paquetes Type-20 de IPX en una interfaz de LAN .....	7-7
	Ejemplo de una configuración de IPX-Interface .....	7-7
	Configuración de interfaces IPX de WAN .....	7-7
	Información general de los ajustes de conexiones IPX .....	7-7
	Ajustes de los perfiles Connection .....	7-8
	Ajustes de los perfiles RADIUS.....	7-9
	Especificación del dispositivo remoto como un ruteador o un cliente de llamada de entrada .....	7-9
	Ajuste de Answer-Defaults IPX Peer-Mode.....	7-10
	Control de actualizaciones RIP y SAP al ruteador remoto y desde éste.....	7-10
	Utilización de Dial-Query.....	7-10
	Cuándo debe utilizarse Net-Number y Net-Alias .....	7-10
	Proxy de servidor inicial.....	7-11
	Ejemplos de una conexión con una LAN de Novell.....	7-11
	Ejemplos de una conexión con un cliente de llamada de entrada.....	7-13
	Configuración de rutas IPX estáticas .....	7-13
	Información general de los ajustes de rutas IPX.....	7-14
	Ajustes de los perfiles IPX-Route locales .....	7-14
	Ajustes de los perfiles ipxroute de RADIUS.....	7-15
	Números de zócalo en rutas estáticas .....	7-16
	Ejemplos de una ruta IPX estática .....	7-16
	Definición y aplicación de filtros SAP IPX .....	7-17
	Información general sobre los ajustes de filtros SAP IPX.....	7-17
	Ejemplo de filtrado de un servidor de archivos de la tabla SAP .....	7-18
	Ejemplo de filtrado de servicios NetWare remotos de la tabla SAP .....	7-19
	Ejemplo de aplicación de un filtro SAP a una interfaz de LAN.....	7-19
	Ejemplo de aplicación de un filtro SAP a una interfaz de WAN .....	7-19
<b>Capítulo 8</b>	<b>Ruteo y acceso remoto de AppleTalk .....</b>	<b>8-1</b>
	Introducción .....	8-1
	Configuración del perfil Atalk-Global.....	8-1
	Configuración de interfaces AppleTalk de LAN .....	8-2
	Ejemplo de configuración de un ruteador raíz.....	8-3
	Configuración de un ruteador no raíz .....	8-3
	Configuración de interfaces AppleTalk de WAN.....	8-4

Ajustes del perfil Answer-Defaults.....	8-4
Ajustes de un perfil Connection.....	8-5
Ajustes de un perfil RADIUS .....	8-6
Ejemplos de configuración de una conexión de cliente ARA .....	8-6
Ejemplos de configuración de una conexión telefónica PPP de AppleTalk.....	8-7
Ejemplos de configuración de una conexión con un ruteador AppleTalk .....	8-8
Ejemplos de una conexión de IP sobre AppleTalk .....	8-9

## Capítulo 9 Filtros de paquetes ..... 9-1

Información general sobre filtros .....	9-1
Tipos básicos de filtros .....	9-1
Filtros de datos y de llamada .....	9-2
Funcionamiento de los filtros .....	9-3
Filtros genéricos .....	9-3
Filtros IP .....	9-4
Tipo de filtros de servicio .....	9-4
Filtros IPX .....	9-5
Filtros de ruta.....	9-5
Especificación de la dirección de un filtro.....	9-6
Especificación de una acción de reenvío de un filtro .....	9-7
Definición de filtros genéricos.....	9-7
Ajustes de un perfil Filter local.....	9-7
Ajustes de un perfil RADIUS .....	9-9
Especificación del desplazamiento de los bytes que se deben examinar.....	9-10
Especificación del número de bytes que se deben analizar .....	9-10
Enmascaramiento del valor antes de la comparación .....	9-11
Ejemplo de un filtro de llamada genérico.....	9-12
Definición de filtros IP.....	9-12
Ajustes de un perfil Filter local.....	9-12
Ajustes de un perfil RADIUS .....	9-14
Filtrado por dirección de origen o de destino .....	9-15
Filtrado por números de puerto.....	9-16
Ejemplos de un filtro IP para evitar la suplantación de direcciones locales.....	9-16
Ejemplos de un filtro IP para cuestiones más complejas de seguridad .....	9-18
Definición de filtros de tipo de servicio (TOS).....	9-19
Ajustes de un perfil Filter local.....	9-20
Ajustes de un perfil RADIUS .....	9-22
Ejemplos de definición de un filtro TOS .....	9-24
Definición de filtros IPX.....	9-25
Filtrado por dirección de origen o de destino .....	9-26
Filtrado por número de zócalo .....	9-27
Ejemplo de un filtro IPX de salida.....	9-27
Ejemplo de un filtro IPX de entrada .....	9-27
Definición de filtros de ruta .....	9-28
Ejemplo de un filtro que excluye una ruta.....	9-29
Ejemplo de un filtro que configura la métrica de una ruta .....	9-29
Definición de filtros remotos dinámicos.....	9-30
Limitaciones actuales.....	9-30
Información general sobre los ajustes de un perfil local .....	9-30
Información general sobre los ajustes del perfil de usuario RADIUS.....	9-31
Ejemplos de configuración de un perfil de filtro en RADIUS .....	9-33
Ejemplos de aplicación de filtros remotos.....	9-33



Aplicación de un filtro a una interfaz.....	9-34
Ajustes de los perfiles locales .....	9-34
Ajustes de los perfiles RADIUS .....	9-35
Utilización por parte del sistema de los ajustes del perfil	
Answer-Defaults.....	9-36
Ejemplos de aplicación de un filtro de datos a una interfaz de WAN .....	9-36
Ejemplos de aplicación de un filtro de llamada a una interfaz de WAN.....	9-37
Ejemplos de aplicación de un filtro TOS a una interfaz de WAN.....	9-38
Ejemplos de aplicación de un filtro de ruta a una interfaz IP de WAN o LAN .....	9-39
Ejemplo de aplicación de un filtro a una interfaz de LAN .....	9-39
<b>Capítulo 10      Fax IP .....</b>	<b>10-1</b>
Fax IP de almacenamiento y reenvío .....	10-1
Faxes IP de entrada y de salida .....	10-1
Parámetros del sistema para el uso del fax-módem IP .....	10-2
Asignación de ancho de banda para el uso habitual del fax IP.....	10-3
Configuración de un perfil Call-Route normal.....	10-4
Especificación del número máximo de llamadas de salida paralelas .....	10-4
Configuración de la unidad TAOS para el fax IP .....	10-5
Ejemplo de una configuración de fax IP para faxes de entrada.....	10-6
Ejemplo de una configuración de fax IP para faxes de salida .....	10-8
Códigos de colgar fax y códigos de causa de la desconexión .....	10-9
Contabilidad de llamadas de fax IP .....	10-9
Cambios SNMP para el funcionamiento del fax IP.....	10-10
Soporte RADIUS para el funcionamiento del fax IP.....	10-11
Soporte Syslog para el funcionamiento del fax IP.....	10-12
Soporte de remarcador en la tarjeta MultiDSP para fax de	
almacenamiento y reenvío.....	10-13
<b>Capítulo 11      Redes de transacciones de corta duración .....</b>	<b>11-1</b>
Información general sobre las redes de transacciones de corta duración .....	11-1
Perfiles Transaction-Server.....	11-2
Configuración de los ajustes de servidor de transacciones.....	11-3
Ejemplo de configuración de un servidor de transacciones.....	11-5
Conexiones de llamada de entrada para clientes de transacciones .....	11-5
Ajustes del perfil Answer-Defaults.....	11-5
Configuración de conexiones HDLC-NRM .....	11-6
Información general sobre los ajustes de HDLC-NRM .....	11-6
Ejemplo de una configuración típica de cliente HDLC-NRM .....	11-7
Configuración de conexiones Visa-II .....	11-8
Información general sobre los ajustes de Visa-II .....	11-8
Ejemplo de una configuración típica de terminal Visa-II.....	11-9
Prevención de retardos de ajuste para llamadas de transacciones por módem.....	11-9
<b>Apéndice A      Métodos de autenticación.....</b>	<b>A-1</b>
Introducción .....	A-1
Autenticación de contraseña para sesiones de protocolo entramado .....	A-1
Autenticación de inicios de sesión en el servidor de terminales.....	A-2
Autenticación de contraseña por tarjeta de testigo .....	A-2
Autenticación previa mediante información de llamada .....	A-2

Utilización de la devolución de llamada como refuerzo de la seguridad .....	A-2
Gestión de contraseñas RADIUS .....	A-2
Contraseñas RADIUS reservadas .....	A-3
Caducidad de la contraseña.....	A-3
El perfil de usuario DEFAULT .....	A-5
Secretos compartidos e intercambios seguros .....	A-5
Autenticación de sesiones de protocolo entramado .....	A-6
Especificación de un protocolo de autenticación obligatorio para llamadas de entrada	A-6
Especificación de un protocolo de autenticación mediante RADIUS .....	A-7
Funcionamiento de PAP .....	A-8
Funcionamiento de CHAP y MS-CHAP .....	A-9
Funcionamiento de la autenticación CHAP bidireccional .....	A-9
Configuración de la autenticación CHAP bidireccional en una unidad TAOS....	A-10
Configuración de la autenticación CHAP bidireccional en RADIUS .....	A-15
Petición de un protocolo para utilizarlo en las llamadas de salida .....	A-20
Ajustes de los perfiles Connection .....	A-20
Ajustes de los perfiles RADIUS .....	A-21
Ejemplos de solicitud de autenticación CHAP para una llamada de salida .....	A-21
Autenticación de inicios de sesión de usuario .....	A-22
Secuencias de comandos de inicio de sesión Expect-Send.....	A-22
Modo de seguridad del servidor de terminales .....	A-23
Personalización de la secuencia de conexión .....	A-24
Especificación de la cabecera y los indicadores .....	A-24
Cuándo debe utilizarse el tercer indicador .....	A-25
Autenticación por tarjeta de testigo .....	A-26
Seguridad ampliada con tarjetas de testigo .....	A-26
Método sencillo de autenticación de llamadas por tarjeta de testigo.....	A-27
Autenticación de conexiones de tarjeta de testigo desde unidades TAOS .....	A-28
Configuración de una unidad TAOS como un NAS .....	A-28
Especificación del tipo de servicio por conexión .....	A-29
Modo de visualización y respuesta del usuario de llamada de entrada a los desafíos .....	A-29
Configuración de perfiles RADIUS para la autenticación por tarjeta de testigo..	A-30
Utilización de la autenticación ACE para usuarios de la red.....	A-34
Autenticación de túnel .....	A-34
Autenticación de túneles ATMP.....	A-34
Autenticación de túneles L2TP.....	A-35
Autenticación previa (CLID o DNIS) .....	A-36
Configuración de una unidad TAOS para que extraiga y utilice información de una llamada .....	A-37
Especificación del elemento causante de una desconexión (sólo RADIUS).....	A-38
Configuración de perfiles para la autenticación CLID o DNIS .....	A-38
Ajustes de los perfiles Connection .....	A-39
Ajustes de los perfiles RADIUS .....	A-39
Ejemplo de utilización del ID de emisor como elemento de verificación (sólo RADIUS).....	A-39
Ejemplo de utilización del nombre de usuario para la autenticación DNIS de primer nivel.....	A-40
Ejemplos en los que es preferible el CLID .....	A-40
Ejemplos en los que es preferible el DNIS .....	A-41
Ejemplos en los que el CLID es obligatorio .....	A-42
Ejemplos en los que el DNIS es obligatorio .....	A-43

Devolución de llamada.....	A-44
Características de la devolución de llamada .....	A-45
Información general sobre la configuración de la devolución de llamada .....	A-46
Configuración de la devolución de llamada CLID o DNIS.....	A-46
Configuración de parámetros globales .....	A-47
Configuración del perfil Connection local .....	A-47
Configuración del perfil Connection externo .....	A-47
Configuración de la espera de devolución de llamada .....	A-48
Configuración de la devolución de llamada Ascend .....	A-49
Configuración de parámetros globales .....	A-50
Configuración del perfil Connection local .....	A-50
Configuración del perfil Connection externo .....	A-50
Configuración de una devolución de llamada CBCP .....	A-52
Configuración de parámetros globales .....	A-52
Configuración del perfil Connection local .....	A-53
Configuración del perfil Connection externo .....	A-53
Ejemplos de configuración de una devolución de llamada tras la autenticación CLID .....	A-54
Ejemplos de configuración de una devolución de llamada tras la autenticación .	A-55

## **Apéndice B      Opciones de autorización ..... B-1**

Introducción .....	B-1
Autorización de un servicio de conexión de modo inmediato .....	B-2
Utilización del perfil Terminal-Server.....	B-3
Utilización de perfiles Connection .....	B-4
Uso de perfiles RADIUS .....	B-4
Autorización del acceso en modo de menú.....	B-4
Ajustes del perfil Terminal-Server .....	B-5
Ajustes de un perfil initial-banner RADIUS.....	B-5
Ejemplos de creación de un menú de hosts .....	B-6
Creación de un menú personalizado de comandos (sólo RADIUS).....	B-7
Ejemplo ampliado de modo de menú y RADIUS.....	B-9
Autorización de conexiones en modo de terminal .....	B-10
Conexiones TCP, Rlogin o Telnet en modo de terminal .....	B-11
Autorización para utilizar los comandos .....	B-11
Configuración del rango de puertos de origen Rlogin.....	B-12
Definición de ajustes predeterminados para sesiones Telnet .....	B-12
Sesiones PPP y SLIP en modo de terminal.....	B-13
Autorización para utilizar los comandos .....	B-14
Definición de ajustes predeterminados para sesiones PPP .....	B-14
Definición de ajustes predeterminados para sesiones SLIP .....	B-15
Autorización a los usuarios para el acceso a la interfaz del servidor de terminales .....	B-16
Autorización del acceso a la gestión SNMP .....	B-16
Definición de cadenas de comunidad .....	B-17
Configuración y aplicación de la seguridad de dirección .....	B-17

## **Índice alfabético..... Índice-1**



# Figuras

Figura 1-1	Servidor RADIUS en una interfaz de LAN .....	1-6
Figura 1-2	Conexión PPP síncrona.....	1-15
Figura 1-3	Conexión PPP asíncrona.....	1-16
Figura 1-4	Conexión de protocolo multienlace (MP).....	1-18
Figura 1-5	Ponderación de muestras de utilización de la línea .....	1-20
Figura 1-6	Conexión de protocolo multienlace Plus (MP+).....	1-23
Figura 1-7	Conexión TCP-Clear a un host local .....	1-29
Figura 1-8	Modo de túnel IPsec para TCP-Clear entre gateways.....	1-30
Figura 1-9	Modo de transporte IPsec para TCP-Clear con host de marcación.....	1-31
Figura 1-10	Conexión permanente .....	1-36
Figura 1-11	Conexión utilizando ancho de banda permanente y conmutado.....	1-38
Figura 1-12	Conexión PPP de llamadas de salida .....	1-46
Figura 2-1	Máscara de subred predeterminada para direcciones IP de clase C.....	2-4
Figura 2-2	Conexión IP de ruteador a ruteador .....	2-18
Figura 2-3	Host de llamada de entrada que requiere una dirección IP estática (una ruta de host) .....	2-19
Figura 2-4	Conexión de interfaz numerada .....	2-20
Figura 2-5	Conexiones IP-Direct.....	2-21
Figura 2-6	Ruta predeterminada hacia un ruteador IP local .....	2-29
Figura 2-7	Ruta predeterminada en una interfaz DLCI de relé de trama .....	2-30
Figura 2-8	Ruta estática hacia una subred remota .....	2-31
Figura 2-9	Redirección de puerto hacia un servidor HTTP.....	2-58
Figura 2-10	Host de llamada de entrada que solicita una dirección IP .....	2-75
Figura 2-11	Unidad TAOS que envía tráfico de difusión múltiple a clientes LAN y WAN.....	2-82
Figura 2-12	Ruteador MBONE en una interfaz LAN .....	2-86
Figura 2-13	Ruteador MBONE en una interfaz WAN .....	2-87
Figura 2-14	Interfaz LAN de cliente de difusión múltiple .....	2-90
Figura 2-15	Interfaces WAN de cliente de difusión múltiple.....	2-90
Figura 3-1	Ruteador designado (DR) y ruteador designado de reserva (BDR) OSPF.....	3-5
Figura 3-2	Costes OSPF para diferentes tipos de enlace .....	3-6
Figura 3-3	División de un sistema autónomo (AS) OSPF en áreas.....	3-7
Figura 3-4	Topología OSPF de ejemplo.....	3-8
Figura 3-5	OSPF en una interfaz de LAN .....	3-13
Figura 3-6	OSPF en una interfaz de WAN.....	3-14
Figura 3-7	Inclusión de rutas ASE en el entorno OSPF.....	3-15
Figura 3-8	Red multiacceso de no difusión (NBMA) de OSPF.....	3-23
Figura 4-1	Túnel ATMP de un ISP a una red interna corporativa.....	4-1
Figura 4-2	Direcciones IP del sistema y rutas entre agentes ATMP .....	4-3
Figura 4-3	MTU de ruta en un segmento Ethernet .....	4-4
Figura 4-4	Agente externo que da soporte a direcciones IP de cliente duplicadas.....	4-7
Figura 4-5	Túnel de agente externo con dos agentes locales.....	4-13
Figura 4-6	Túnel de agente externo con un conmutador GRF .....	4-16

Figura 4-7	Funcionamiento de un agente local de gateway .....	4-18
Figura 4-8	Funcionamiento de un agente local de ruteador .....	4-19
Figura 4-9	Instalación ATMP tolerante a errores .....	4-22
Figura 4-10	Agente local de gateway con línea arrendada hacia la red interna .....	4-23
Figura 4-11	Agente local de ruteador en la red interna .....	4-25
Figura 4-12	Unidad TAOS actuando como agente local y agente externo .....	4-27
Figura 4-13	Configuración para que un cliente móvil eluda la conexión con el agente externo .....	4-29
Figura 4-14	Conexiones de ruteo de IPX para IPX sobre ATMP .....	4-31
Figura 4-15	IPX sobre ATMP con un agente local de gateway .....	4-32
Figura 4-16	IPX sobre ATMP con un agente local de ruteador .....	4-35
Figura 5-1	Túnel L2TP .....	5-1
Figura 5-2	Configuración de un túnel L2TP seguro de IPSec .....	5-9
Figura 5-3	Puntos finales primario y secundario del túnel L2TP .....	5-17
Figura 5-4	Túnel L2F .....	5-19
Figura 5-5	Túnel PPTP .....	5-25
Figura 5-6	Túnel IP en IP .....	5-34
Figura 6-1	Ruteo IP virtual .....	6-1
Figura 6-2	Túneles L2TP contruidos en ruteadores virtuales separados .....	6-14
Figura 7-1	Conexión IPX con servidores NetWare en ambos lados .....	7-11
Figura 7-2	Cliente NetWare de llamada de entrada.....	7-13
Figura 8-1	Conexión telefónica de un cliente ARA .....	8-7
Figura 8-2	Conexión de AppleTalk utilizando un marcador PPP .....	8-7
Figura 8-3	Conexión del ruteo AppleTalk.....	8-8
Figura 8-4	Conexión ARA que encapsula paquetes IP en DDP.....	8-10
Figura 9-1	Los filtros de datos eliminan o reenvían determinados paquetes .....	9-2
Figura 9-2	Los filtros de llamada evitan que determinados paquetes reinicien el temporizador .....	9-3
Figura 10-1	Fax IP de entrada de una máquina de fax a Internet.....	10-1
Figura 10-2	Fax IP de salida de Internet a la máquina de fax .....	10-2
Figura 10-3	Recepción y reenvío de faxes IP de entrada .....	10-6
Figura 10-4	Envío de un fax IP de salida a una máquina de fax .....	10-8
Figura 11-1	Ejemplo de configuración de SDTN.....	11-1
Figura 11-2	Servidores de transacciones con conexiones Ethernet redundantes .....	11-5

## Tablas

Tabla 2-1	Clases de direcciones IP y número de bits de red.....	2-4
Tabla 2-2	Máscaras de subred decimales y longitudes de los prefijos.....	2-5
Tabla 3-1	Bases de datos de estado de los enlaces para la topología OSPF de la Figura 3-4.....	3-8
Tabla 3-2	Árbol de trayectorias más cortas y tabla de ruteo resultante para el ruteador 1	3-9
Tabla 3-3	Árbol de trayectorias más cortas y tabla de ruteo resultante para el ruteador 2	3-9
Tabla 3-4	Árbol de trayectorias más cortas y tabla de ruteo resultante para el ruteador 3 .....	3-10
Tabla 5-1	Protocolos de túnel y conjuntos de atributos con identificadores.....	5-31
Tabla 7-1	Ampliaciones de IPX de TAOS.....	7-3
Tabla 8-1	Ajustes de TCP/IP para Macintosh en conexiones PPP .....	8-9
Tabla 8-2	Ajustes de TCP/IP para Macintosh en conexiones ARA.....	8-10





# Acerca de esta guía

## Contenido de esta guía

En esta guía se describe cómo configurar una unidad APX 8000™, MAXTNT® o DSLTNT™ para su conexión a la red. Se da por sentado que ya ha instalado la unidad TAOS, ha instalado las tarjetas de ranura y ha preparado y comprobado las líneas. Si no ha realizado estas tareas, consulte la guía de instalación del hardware que se adjunta con la unidad y la publicación *Guía de configuración de la interfaz física de APX 8000/MAX TNT/DSLNT*.



**Nota:** En este manual se describen todas las funciones de las unidades APX 8000, MAX TNT y DSLTNT que operan con la versión 8.0.2 o posterior del sistema operativo True Access™ Operating System (TAOS). Es posible que algunas funciones no estén disponibles en versiones anteriores o instalaciones personalizadas del software.

En lo sucesivo se hará referencia al producto como *unidad TAOS*.



**Advertencia:** Antes de instalar la unidad TAOS, lea las instrucciones de seguridad descritas en la *Guía de seguridad y cumplimiento de normativas de redes de acceso*. Para obtener información específica para la unidad, consulte el apéndice “Especificaciones eléctricas, ambientales y físicas de seguridad”, que encontrará en la guía de instalación del hardware de la unidad.




## Lo que debería saber

Si bien esta guía intenta proporcionar un marco conceptual que permita a un administrador que no sea experto en una tecnología de red en particular configurar la unidad TAOS con precisión, no se empieza ninguna cuestión de gestión de redes desde cero. A continuación se indican las áreas generales en las que resulta útil poseer algunos conocimientos previos al configurar las funciones correspondientes de la red:

- Conexiones de llamada de entrada (tanto sesiones de protocolo entramado como inicios de sesión de usuario)
- Gestión y contabilidad de los costes de conexión
- Módems
- Relé de trama
- Ruteo IP
- Ruteo OSPF (si procede)
- Difusión múltiple (si procede)
- Ruteo multiprotocolo (si procede)
- Estructura y formatos de paquetes (para definir filtros)
- Seguridad de redes

## Convenciones utilizadas en la documentación

A continuación se muestran los caracteres especiales y las convenciones tipográficas que se han utilizado en este manual:

Convención	Significado
Texto monoespaciado	Representa el texto que aparece o podría aparecer en la pantalla de la computadora.
<b>Texto monoespaciado en negrita</b>	Representa los caracteres que deben escribirse exactamente como aparecen, a no ser que los caracteres estén también en <i>cursiva</i> (consulte el apartado siguiente, <i>Cursiva</i> ). Si puede escribir los caracteres pero no se le indica específicamente que lo haga, no aparecerán en negrita.
<i>Cursiva</i>	Representa información de variables. No introduzca las palabras propiamente dichas en el comando, sino la información que representan. En el texto normal, la cursiva se utiliza para los títulos de publicaciones, para algunos términos que también podrían aparecer entre comillas o para enfatizar una idea determinada.
[ ]	Los corchetes indican un argumento optativo que se puede agregar a un comando. Para incluir un argumento de este tipo, escriba sólo la información que aparece entre los corchetes. No escriba los corchetes a menos que aparezcan en negrita.
	Sirve para separar las opciones de comandos que son mutuamente excluyentes entre sí.
>	Indica el siguiente nivel de la ruta hacia un parámetro o un elemento de menú. El elemento que aparece tras el corchete angular es una de las opciones que aparecen al seleccionar el parámetro que precede a dicho corchete.
Tecla1-Tecla2	Representa una combinación de teclas. Para introducir una combinación de teclas, pulse la primera tecla y manténgala pulsada mientras pulsa las otras teclas de la combinación. Suelte todas las teclas al mismo tiempo. (Por ejemplo, Ctrl-H significa que debe mantener pulsada la tecla Control y después pulsar la tecla H.)
Pulsar Intro	Significa que debe pulsar la tecla Intro, Retorno o la equivalente en la computadora que esté utilizando.
<b>Nota:</b>	Introduce información adicional importante.
 <b>Precaución:</b>	Le advierte de que, si no sigue el procedimiento recomendado, podría perder información o dañar el equipo.
 <b>Advertencia:</b>	Le advierte del riesgo de sufrir lesiones físicas si no toma las medidas de seguridad apropiadas.
 <b>Advertencia:</b>	Le advierte del peligro de descargas eléctricas.

## Documentación

La documentación de APX 8000/MAX TNT/DSLNTNT consta de los manuales siguientes.

- **Leer en primer lugar:**
  - *Guía de seguridad y cumplimiento de normativas de redes de acceso*  
Contiene instrucciones de seguridad importantes e información sobre el cumplimiento de normativas específicas de los países que debe leer antes de instalar una unidad TAOS.
  - *Guía de la interfaz de línea de comandos de TAOS*  
En este manual se presenta el entorno de línea de comandos de TAOS y se indica cómo utilizar la interfaz de línea de comandos de una manera eficiente. Se describen las combinaciones de teclas y se ofrece una introducción a los comandos, niveles de seguridad, estructura de perfiles y tipos de parámetro.
- **Instalación y configuración básica:**
  - *Guía de instalación del hardware APX 8000*  
Le enseña a instalar el hardware APX 8000 y describe las especificaciones técnicas de APX 8000.
  - *Guía de instalación del hardware MAX TNT/DSLNTNT*  
En este manual se indica cómo instalar el hardware MAX TNT y DSLNTNT, y se describen las especificaciones técnicas para estas unidades.
  - *Guía de configuración de la interfaz física de APX 8000/MAX TNT/DSLNTNT*  
En este manual se indica cómo configurar las tarjetas instaladas en una unidad TAOS y los atributos de línea para funciones como entramado, señalización y uso de canales. También se describe la manera en que se rutean las llamadas mediante el sistema y se proporciona información sobre la configuración de la unidad en un entorno Sistema de señalización número 7 (SS7). En este manual se describe la redundancia del controlador del módulo para la unidad APX 8000.
- **Configuración:**
  - *Guía de configuración ATM de APX 8000/MAX TNT/DSLNTNT*  
En este manual se describe la configuración de operaciones de Modo de transferencia asincrónico (ATM) en una unidad TAOS. Se describe la configuración de los atributos de las capas físicas y la creación de interfaces ATM para circuitos virtuales permanentes (PVC) y circuitos virtuales conmutados (SVC). Este manual contiene información sobre los circuitos ATM direct y ATM-relé de trama.
  - *Guía de configuración de relé de trama para APX 8000/MAX TNT/DSLNTNT*  
En este manual se describe la configuración de las operaciones de relé de trama en una unidad TAOS. Se describe la configuración y las limitaciones para las capas físicas, así como la creación de las interfaces para circuitos virtuales permanentes (PVC) y circuitos virtuales conmutados (SVC). Contiene información sobre el relé de trama de multienlaces (MFR) y la gestión de enlaces, así como los circuitos de relé de trama y circuitos Frame Relay direct.
  - *Guía de configuración, ruteo y túnel para APX 8000/MAX TNT/DSLNTNT*  
En este manual se indica cómo configurar el ruteo de LAN y WAN para conexiones de marcación analógica y digital en una unidad TAOS. Contiene información sobre el ruteo IP, ruteo OSPF (Emplear la trayectoria más corta primero), ruteo IGMP (Protocolo de gestión de grupo Internet), ruteadores multiprotocolo, ruteadores virtuales y protocolos de túnel.

- *MultiVoice™ for MAX TNT/DSLNT Configuration Guide (Guía de configuración de MultiVoice™ para MAX TNT/DSLNT)*  
En este manual se indica cómo configurar la aplicación MultiVoice para ejecutarla en una unidad MAX TNT o DSLNT en entornos con configuración Sistema de señalización número 7 (SS7) y H.323 Voz sobre IP (VoIP).
- **RADIUS: RADIUS Guide and Reference (Guía y referencia de RADIUS para TAOS)**  
En este manual se describe cómo configurar una unidad TAOS para que utilice un servidor RADIUS (Servicio de usuario de marcación con autenticación remota) y contiene una referencia completa de los atributos de RADIUS.
- **Administración y resolución de problemas: Guía de administración de APX 8000/MAX TNT/DSLNT**  
En este manual se describe cómo administrar una unidad TAOS, incluidas la supervisión del sistema y las tarjetas, la resolución de problemas de la unidad y la configuración de ésta para utilizar el protocolo SNMP (Protocolo de gestión de red simple).
- **Referencia:**
  - *APX 8000/MAX TNT/DSLNT Reference (Referencia de APX 8000/MAX TNT/DSLNT)*  
Referencia en orden alfabético de todos los comandos, perfiles y parámetros soportados por las unidades TAOS.
  - *TAOS Glossary (Glosario de TAOS)*  
Define la terminología utilizada en la documentación de las unidades TAOS.

# Conexiones WAN

# 1

Introducción a las conexiones WAN .....	1-1
Perfiles generales del sistema. ....	1-3
Perfiles de autenticación locales y externos. ....	1-7
Configuración de conexiones de marcación conmutadas .....	1-12
Configuración de conexiones permanentes y permanentes MP+ .....	1-33
Configuración de conexiones de salida .....	1-42

## ***Introducción a las conexiones WAN***

Pueden establecerse conexiones WAN realizando llamadas de salida o de entrada en la unidad TAOS. Un usuario remoto o un ruteador de acceso inicia las conexiones de entrada, mientras que la llamada de salida la inicia la propia unidad TAOS (normalmente para el ruteo de paquetes) o un usuario realizando una llamada de salida a través de uno de los módems digitales del sistema.

El extremo distante de una conexión WAN determina si el enlace es síncrono o asíncrono. Por ejemplo, un ruteador de acceso remoto, como una unidad Pipeline®, utiliza un enlace síncrono, mientras que un módem analógico requiere un enlace asíncrono.

Un enlace síncrono utiliza la codificación HDLC y se conecta a un ruteador de acceso para un enlace de red a red. La llamada se rutea como una llamada digital a un canal HDLC en la unidad TAOS y, a continuación, al software del ruteador. Las conexiones síncronas utilizan un protocolo de encapsulación, como el protocolo de punto a punto (PPP) o el relé de trama, para entregar paquetes de un dispositivo a otro. Las conexiones síncronas pueden ser multicanal.

Un enlace asíncrono utiliza el tipo de comunicaciones serie que proporciona un puerto de comunicaciones de PC y se inicia habitualmente mediante un módem de acceso telefónico o un adaptador de terminal (TA) V.120 para una conexión de host a red o de host a host. Una llamada asíncrona iniciada por un módem se rutea generalmente como una llamada de voz a un módem digital en la unidad TAOS y, a continuación, al software del servidor de terminales. Otros tipos de llamadas asíncronas pueden rutearse a un canal HDLC y, seguidamente, al software del servidor de terminales o directamente a un host local.

## Tipos de protocolos de encapsulación

Los protocolos de encapsulación permiten la entrega de paquetes de un dispositivo a otro mediante la WAN. La unidad TAOS reconoce los tipos de encapsulación siguientes:

- Protocolo punto a punto (PPP)
- Protocolo multienlace (MP)
- Protocolo multienlace Plus (MP+ o MPP)
- TCP sin encapsular (TCP-Clear o TCP-Raw)
- V.120
- X.75
- AppleTalk Remote Access (ARA)
- Relé de trama, circuito de relé de trama y circuito ATM-relé de trama

### *PPP, MP y MP+*

Una llamada PPP utiliza un único canal. Una llamada MP utiliza un número estático de varios canales y puede utilizarse para comunicarse con cualquier dispositivo que cumpla los requisitos de MP. Una llamada MP+ puede agregar los canales necesarios dinámicamente y sólo puede establecerse entre unidades TAOS. Si configura MP+ y el dispositivo remoto no ofrece soporte, la unidad TAOS intentará establecer una conexión MP. Si el dispositivo remoto no da soporte a MP, la unidad TAOS establece una conexión PPP de un único canal.

### *Otros protocolos de encapsulación*

La encapsulación V.120 se maneja de forma clara y requiere una configuración mínima (si desea obtener información detallada, consulte el apartado “Perfil Answer-Defaults” en la página 1-3).

El ruteo AppleTalk y las conexiones ARA se describen en el Capítulo 8, “Ruteo y acceso remoto de AppleTalk”.

El relé de trama, los circuitos de relé de trama y los circuitos ATM-relé de trama se describen en la publicación *Guía de configuración de relé de trama para APX 8000/MAX TNT/DSLNT*. Para obtener una descripción de una conexión ATM, consulte la publicación *Guía de configuración ATM de APX 8000/MAX TNT/DSLNT*.

## Cómo responde y autentica llamadas de entrada el sistema

Cuando la unidad TAOS recibe una llamada de entrada en una de sus líneas (por ejemplo, una línea T1), evalúa la llamada basándose en los ajustes del perfil Answer-Defaults. Si la llamada satisface las condiciones de dicho perfil, la unidad TAOS responde a la llamada, la rutea a la tarjeta de host apropiada (por ejemplo, un módem o un canal HDLC) y busca un perfil Connection o un perfil externo equivalente que coincida con los parámetros de la llamada.

Si encuentra un perfil local o externo para el emisor, la unidad TAOS inicia el proceso de autenticación. Si no encuentra un perfil que coincida y el perfil Answer-Defaults requiere un perfil para todos los emisores (el valor predeterminado), la unidad TAOS cancela la llamada.

## Cómo inicia el sistema las llamadas de salida

Cuando la unidad TAOS recibe un paquete de salida con destino a una ubicación remota, busca un perfil Connection o un perfil externo equivalente que coincida con la dirección de destino del paquete. Si encuentra un perfil que coincide, activa la conexión. Este proceso se describe con más detalle en los capítulos de esta guía dedicados al ruteo.

**Nota:** Para permitir que la unidad TAOS active la conexión de acuerdo con el ruteo del paquete, el perfil debe especificar parámetros de salida y el sistema debe disponer de una ruta que le permita encontrar el perfil. Para obtener información detallada, consulte “Configuración de conexiones de salida” en la página 1-42.

Además, la unidad TAOS puede permitir a los usuarios acceder a sus módems de 56 K para iniciar sesiones de llamada de salida. Esta configuración se describe en el apartado “Conexiones de llamada de salida por módem” en la página 1-47.

## Cómo establece y supervisa sesiones el sistema

Después de autenticar una llamada, la unidad TAOS crea y mantiene una sesión con el emisor. Los datos de la llamada pueden reenviarse al software del ruteador de la unidad TAOS (en el caso de una sesión de protocolo entramado), al software del servidor de terminales (para un inicio de sesión interactivo) o a un host especificado, en función de la naturaleza de la llamada.

La unidad TAOS utiliza ajustes del perfil del emisor para supervisar y, si es necesario, dar por finalizada la sesión. Por ejemplo, podría utilizar los ajustes Idle-Timer y Call-Filter para terminar la sesión después de un tiempo determinado de inactividad. Para obtener más información, consulte el apartado “Especificación de límites de tiempo de sesión” en la página 1-8.

## Perfiles generales del sistema

Además de un perfil específico de la conexión, que especifica ajustes de configuración y el nombre y la contraseña que se utilizarán en la secuencia de autenticación, una conexión WAN también se ve afectada por los perfiles Answer-Defaults, Terminal-Server y External-Auth. Los parámetros de estos perfiles tienen aplicación en todo el sistema.

### Perfil Answer-Defaults

El perfil Answer-Defaults define valores iniciales que afectan a todas las llamadas de entrada, por tanto deben comprobarse los valores de Answer-Defaults para asegurarse de que están establecidos correctamente para el entorno del usuario.

Los valores de Answer-Defaults se aplican *antes* de que la unidad TAOS rutee la llamada a una tarjeta de host para su procesamiento y antes de que localice el perfil del emisor. Si el perfil del emisor contiene un parámetro similar con un valor diferente, la unidad TAOS utiliza el valor específico de la conexión y no el valor de Answer-Defaults para crear la sesión.

De manera predeterminada, el perfil Answer-Defaults permite todos los tipos de encapsulación y ruteo, y los parámetros básicos de configuración de llamada utilizan los ajustes del mínimo común denominador. Esto es conveniente en muchos entornos, pero es recomendable cambiar

los ajustes para definir con precisión los criterios de aceptación de las llamadas o para limitar la cantidad de ancho de banda a la que pueden acceder las llamadas PPP multienlace.

### *Ajustes de RADIUS predeterminados*

Si el parámetro Use-Answer-For-All-Defaults se establece en Yes (el valor predeterminado), el sistema crea un perfil inicial predeterminado para las llamadas autenticadas con RADIUS utilizando los ajustes del perfil Answer-Defaults. El sistema recupera de RADIUS el perfil configurado del emisor y utiliza los pares atributo-valor del perfil. Los atributos no especificados en el perfil toman sus valores de los ajustes de Answer-Defaults.

Si se establece Use-Answer-For-All-Defaults en No y un perfil RADIUS no devuelve determinados valores explícitos, la unidad TAOS utiliza en su lugar los valores predeterminados de fábrica para los atributos de RADIUS.

### *Petición de la autenticación en llamadas PPP*

Los siguientes parámetros de Answer-Default (que aparecen con los valores predeterminados) están relacionados con la autenticación:

```
[in ANSWER-DEFAULTS]
profiles-required = yes
clid-auth-mode = ignore

[in ANSWER-DEFAULTS:ppp-answer]
receive-auth-mode = no-ppp-auth
```

De manera predeterminada, no se necesita autenticación de CLID (ID de línea de llamada), DNIS (Servicio de información de número de marcación) ni PPP para las llamadas de entrada. La mayoría de sitios cambian el valor predeterminado de Receive-Auth-Mode, como se muestra en el ejemplo siguiente, para garantizar la autenticación de una llamada PPP antes de establecer una sesión:

```
admin> read answer
ANSWER-DEFAULTS read

admin> set ppp receive-auth = any-ppp-auth

admin> write
ANSWER-DEFAULTS written
```

Al establecer Any-PPP-Auth como el método de autenticación PPP, la unidad TAOS acepta las llamadas PPP de entrada que dan soporte a cualquiera de los métodos de autenticación, pero elimina las conexiones que no ofrezcan ningún protocolo de autenticación durante la negociación LCP. Para obtener información detallada acerca de la autenticación PPP, CLID y DNIS, consulte el Apéndice A, “Métodos de autenticación”.

### *Ajustes de V.120*

Los adaptadores de terminal V.120 (también conocidos como módems ISDN) son dispositivos asíncronos que utilizan la encapsulación ITU-T V.120. Después de que un sistema procese la encapsulación V.120 de la llamada, reenvía la llamada al servidor de terminales. A



continuación se muestran los parámetros de Answer-Defaults relacionados con las conexiones V.120. Los ajustes muestran los valores predeterminados.

```
[in ANSWER-DEFAULTS:v120-answer]
enabled = yes
frame-length = 256
```

De manera predeterminada, el sistema puede responder a llamadas V.120. Frame-Length especifica los tamaños máximos de trama de transmisión y recepción V.120. El valor debe corresponder a los ajustes del software TA. Para que el funcionamiento de V.120 sea compatible con una unidad TAOS, utilice los ajustes de adaptador de terminal siguientes (consulte el manual del dispositivo V.120 para obtener información sobre cómo introducirlos).

- Tamaño máximo de trama de transmisión V.120: 260 bytes.
- Tamaño máximo de trama de recepción V.120: 260 bytes.
- ID de enlace lógico (LLI): 256.
- Módulo: 128.
- Velocidad de canal de la línea: seleccione 56 K si la unidad TAOS acepta llamadas del dispositivo V.120 en una línea T1 o si no está seguro de disponer de una velocidad de canal de 64 Kbps de extremo a extremo.
- Realización de llamadas: la unidad TAOS puede recibir llamadas V.120, pero no puede realizarlas.

El conjunto de comandos siguiente configura las llamadas V.120 con un tamaño máximo de trama de 260 bytes:

```
admin> read answer
ANSWER-DEFAULTS read

admin> set v120 frame-length = 260

admin> write
ANSWER-DEFAULTS written
```

**Nota:** Si el software de marcación del usuario da soporte a la conversión de asíncrono a síncrono, el perfil Connection puede establecerse para la autenticación PAP o CHAP y el usuario puede acceder al servidor de terminales con un inicio de sesión PPP automático. Para conocer los ajustes de autenticación recomendados de las conexiones que utilicen adaptadores de terminal, consulte el Apéndice A, “Métodos de autenticación”.

## Perfil Terminal-Server

El software del servidor de terminales de la unidad TAOS recibe llamadas asíncronas después de ser procesadas por un módem digital. Estas llamadas las efectúa normalmente un módem o TA V.120. Si el emisor no envía paquetes PPP inmediatamente, el servidor de terminales inicia una secuencia de inicio de sesión.

En una llamada PPP asíncrona, el servidor de terminales reenvía la llamada al software del ruteador al detectar un paquete PPP. Para obtener información acerca de la configuración de llamadas PPP asíncronas, consulte el apartado “Ejemplos de una conexión PPP asíncrona” en la página 1-15.

Para un inicio de sesión, cada usuario debe tener un perfil Connection (o perfil externo) que especifique el nombre y la contraseña que se utilizarán en la secuencia de inicio de sesión del servidor de terminales. Además, un perfil Terminal-Server global define el modo en que estas

llamadas se autentican y adónde se dirigen las llamadas tras la autenticación. Para obtener información acerca de estas cuestiones, consulte el Apéndice A, “Métodos de autenticación”.

Debe activar el software de servidor de terminales si la unidad TAOS debe gestionar llamadas asíncronas. A continuación se muestra el parámetro correspondiente con su valor predeterminado:

```
[in TERMINAL-SERVER]
enabled = no
```

El conjunto de comandos siguiente activa el software del servidor de terminales:

```
admin> read terminal-server
TERMINAL-SERVER read

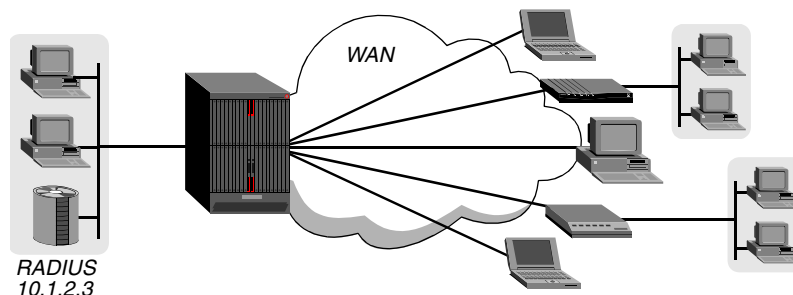
admin> set enabled = yes

admin> write
TERMINAL-SERVER written
```

## Perfil External-Auth

Para la autenticación y la contabilidad externas, la unidad TAOS da soporte a RADIUS, TACACS y TACACS+. En la Figura 1-1, la unidad TAOS responde a llamadas de entrada y reenvía peticiones de autenticación a un servidor RADIUS en una interfaz de LAN:

*Figura 1-1. Servidor RADIUS en una interfaz de LAN*



Los comandos siguientes configuran la unidad TAOS para que acceda al servidor de autenticación RADIUS en 10.1.2.3 en el puerto UDP 5000 utilizando el secreto compartido taospw:

```
admin> read external-auth
EXTERNAL-AUTH read

admin> set auth-type = radius

admin> set rad-auth-client auth-server-1 = 10.1.2.3

admin> set rad-auth-client auth-port = 5000

admin> set auth-key = taospw

admin> write
EXTERNAL-AUTH written
```

Los comandos siguientes configuran una unidad TAOS para acceder al servidor de contabilidad RADIUS en 10.1.2.3 en el puerto UDP 512 utilizando el secreto compartido taospass:

```
admin> read external-auth
EXTERNAL-AUTH read

admin> set acct-type = radius

admin> set rad-acct-client acct-server-1 = 10.1.2.3

admin> set rad-acct-client acct-port = 512

admin> set rad-acct-client acct-key = taospass

admin> write external-auth
EXTERNAL-AUTH written
```

## ***Perfiles de autenticación locales y externos***

Puede definir conexiones WAN localmente en perfiles Connection o en un servidor RADIUS en los perfiles de usuario. En los ejemplos de esta guía se muestran ambos métodos de configuración.

### **Utilización de perfiles Connection**

Un perfil Connection contiene toda la información específica de la conexión, incluidos los ajustes de autenticación, los valores de compresión, las especificaciones de filtros y las opciones de telecomunicaciones. Para crear un perfil Connection nuevo, utilice el comando siguiente:

```
admin> new connection
CONNECTION/" " read
```

### **Utilización compartida de perfiles para cada usuario**

Puede activar perfiles compartidos para cada conexión aunque no estén permitidos en el sistema. En las versiones anteriores del software, esta función sólo estaba disponible en perfiles RADIUS mediante el atributo Ascend-Shared-Profile-Enable. A continuación se muestra el parámetro pertinente con su ajuste predeterminado:

```
[in CONNECTION/" "]
shared-prof = no
```

Parámetro	Descripción
Shared-Prof	Activa y desactiva varios emisores para que compartan el perfil Connection, siempre que no se produzcan conflictos de dirección IP. Con el ajuste predeterminado <code>no</code> , el ajuste del parámetro Shared-Prof en el perfil IP-Global permite los perfiles compartidos en el sistema o los impide.

Si el parámetro Shared-Prof se establece en `yes` en el perfil IP-Global, el ajuste Shared-Prof de un perfil Connection no tiene ningún efecto. Sin embargo, si el parámetro Shared-Prof se establece en `no` en el perfil IP-Global y en `yes` en un perfil Connection, tiene preferencia el ajuste del perfil Connection. Por ejemplo, con los ajustes siguientes, varios emisores pueden llamar y autenticar un perfil Connection denominado `shared-1`:

```
admin> get ip-global shared-prof
[in IP-GLOBAL:shared-prof]
shared-prof = no

admin> read connection shared-1
CONNECTION/shared-1 read

admin> set shared-prof = yes

admin> set ip-options ip-routing-enabled = no

admin> write
CONNECTION/shared-1 written
```

## Utilización de RADIUS

Puede utilizar RADIUS para autenticar externamente las llamadas a las que responde la unidad TAOS. La autenticación externa centraliza la gestión de conexiones WAN y concentra los perfiles de usuario en un único archivo de texto. La utilización de RADIUS también permite la autenticación por tarjeta de testigo para redes seguras o la autenticación mediante una base de datos de contraseñas UNIX.

Los perfiles RADIUS constan de las tres partes siguientes:

```
User-Name  Check-Items
          Reply-Items
```

User-Name debe estar justificado a la izquierda. Normalmente es el nombre del emisor (o dispositivo llamador), pero puede ser también un número de teléfono (para la autenticación CLID o DNIS), una cadena especial que indique un perfil de pseudousuario o la cadena DEFAULT (para el perfil de usuario predeterminado).

Check-Items debe estar en la misma línea que User-Name y debe estar separado de éste por espacios en blanco (espacio o tabulación). Check-Items incluye cero o más pares atributo-valor que deben coincidir con los atributos presentes en el paquete Access-Request para la autenticación del usuario. En Check-Items se incluye habitualmente la contraseña para la entrada.

Reply-Items debe estar sangrado y separado de User-Name y Check-Items en una nueva línea. Si Reply-Items no está sangrado, se interpreta como User-Name de una nueva entrada. Reply-Items incluye cero o más pares atributo-valor que se devuelven en mensajes Access-Accept para autorizar servicios para el usuario.

## Especificación de límites de tiempo de sesión

Una vez que la unidad TAOS ha respondido a una llamada y ha establecido una sesión WAN, utiliza ajustes de un perfil Connection o RADIUS para aplicar filtros o cortafuegos a la corriente de datos de la sesión y cerrar una sesión si permanece inactiva durante un periodo de tiempo especificado.

### *Ajustes del límite de tiempo en un perfil Connection*

A continuación se presentan los parámetros pertinentes para especificar límites de tiempo de sesión en un perfil Connection. Los ajustes muestran los valores predeterminados.

```
[in CONNECTION/"":session-options]
call-filter = ""
data-filter = ""
filter-persistence = no
idle-timer = 120
ts-idle-mode = no-idle
ts-idle-timer = 120
max-call-duration = 0
```

Parámetro	Especifica
Call-Filter o Data-Filter	Nombre del filtro o cortafuegos que debe aplicarse a la conexión. Si desea obtener información detallada, consulte el Capítulo 9, “Filtros de paquetes”.
Filter-Persistence	Activa y desactiva la persistencia del filtro en cambios de estado de la conexión.
Idle-Timer	Número de segundos que puede permanecer inactiva una sesión de red de paquetes antes de que se cancele. El valor predeterminado es 120.
TS-Idle-Mode	Dirección en la que se supervisa el tráfico activo durante una sesión (Input-Only, Input-Output o None).
TS-Idle-Timer	Número de segundos que un inicio de sesión puede permanecer inactivo antes de cancelarse. El valor predeterminado es 120.
Max-Call-Duration	En sesiones de un único canal, número máximo de minutos que una llamada puede permanecer conectada. En sesiones MP+, número máximo de minutos que una llamada puede permanecer conectada dentro de la sesión. Cada llamada del agrupamiento tiene una duración limitada, pero la sesión puede durar indefinidamente si las llamadas cambian de estado.

### *Ajustes del límite de tiempo en un perfil RADIUS*

RADIUS utiliza los pares atributo-valor siguientes para establecer límites de tiempo de sesión:

Atributo	Valor
Filter-ID (11)	Nombre de un perfil Filter local que define un filtro de datos. La próxima vez que una unidad TAOS acceda al perfil de usuario RADIUS en el que aparece este atributo, el filtro de datos al que se hace referencia se aplicará a la conexión. Si desea obtener información detallada, consulte el Capítulo 9, “Filtros de paquetes”.

<b>Atributo</b>	<b>Valor</b>
Idle-Timeout (28)	Número máximo de segundos consecutivos de tiempo inactivo permitido al usuario antes de que se termine la sesión o el indicador. Este atributo RADIUS estándar es muy similar al atributo definido por el proveedor Ascend-Idle-Limit (244) y la unidad TAOS da soporte a la utilización de atributos definidos en documentos RFC. Los atributos definidos por el proveedor Ascend se desestimarán con el tiempo en favor de atributos definidos en los documentos RFC.
Session-Timeout (27)	Número máximo de segundos de servicio que debe proporcionarse al usuario antes de que termine la sesión o el indicador. Este atributo RADIUS estándar es muy similar al atributo definido por el proveedor Ascend-Maximum-Time (194) y la unidad TAOS da soporte a la utilización de atributos definidos en documentos RFC. Los atributos definidos por el proveedor Ascend se desestimarán con el tiempo en favor de atributos definidos en los documentos RFC.
Ascend-TS-Idle-Mode (170)	Dirección en la que se supervisa el tráfico activo durante una sesión (TS-Idle-Input, TS-Idle-Input-Output o TS-Idle-None).
Ascend-TS-Idle-Limit (169)	Número de segundos que un inicio de sesión puede permanecer inactivo antes de cancelarse (120 de forma predeterminada).
Ascend-Maximum-Call-Duration (125)	En sesiones de un único canal, número máximo de minutos que una llamada puede permanecer conectada. En sesiones MP+, número máximo de minutos que una llamada puede permanecer conectada dentro de la sesión. Cada llamada del agrupamiento tiene una duración limitada, pero la sesión puede durar indefinidamente si las llamadas cambian de estado.

### *Ejemplos de definición de límites de tiempo*

El conjunto de comandos siguiente establece el temporizador de inactividad en 60 segundos y especifica que sólo los caracteres de entrada pueden restaurar el temporizador. Limita, asimismo, la duración de cualquier sesión a 2 horas.

```
admin> read connection smith
CONNECTION/smith read

admin> set active = yes

admin> set encaps = tcp-raw

admin> set ppp rcv-password = xyzzy

admin> set tcp host = 10.10.10.1

admin> set session ts-idle-mode = input-only

admin> set session ts-idle-timer = 60

admin> set session max-call = 120

admin> write
CONNECTION/smith written
```

A continuación se muestran los ajustes equivalentes en un perfil RADIUS:

```
smith Password = "xyzyz"
  Service-Type = Login-User,
  Login-Service = Telnet,
  Login-IP-Host = 10.10.10.1,
  Ascend-TS-Idle-Mode = TS-Idle-Input,
  Ascend-TS-Idle-Limit = 60,
  Ascend-Maximum-Call-Duration = 120
```

## Utilización de la contabilidad de sesiones

Tanto RADIUS como TACACS+ permiten a los administradores realizar un seguimiento de las estadísticas de conexión, generalmente para fines de facturación. Para obtener información detallada acerca de los atributos de contabilidad de sesiones, consulte la publicación *APX 8000/MAX TNT/DSLNT Reference (Referencia de APX 8000/MAX TNT/DSLNT)*.

## Especificación de velocidades de recepción y transmisión de datos en RADIUS

El atributo Ascend-Data-Rate especifica la velocidad de recepción de la conexión, en bits por segundo. El atributo Ascend-Xmit-Rate especifica la velocidad de transmisión de la conexión. Los atributos Ascend-Data-Rate y Ascend-Xmit-Rate de RADIUS forman parte de un paquete Access Request y puede utilizarse para proporcionar información de resolución de problemas al usuario.

La información que contienen estos atributos solamente se envía si no se realiza la autenticación con CLID o DNIS. RADIUS utiliza los pares atributo-valor siguientes para establecer velocidades de recepción de datos y velocidades de transmisión de datos:

Atributo	Valor
Ascend-Data-Rate (197)	<p>Especifica la velocidad de recepción de la conexión en bits por segundo. Este atributo aparece en paquetes Accounting-Request para proporcionar información de resolución de problemas al usuario.</p> <p>La unidad TAOS incluye Ascend-Data-Rate en un paquete Accounting-Request cuando se dan las dos condiciones siguientes:</p> <ul style="list-style-type: none"><li>• La sesión ha finalizado o no se ha podido realizar la autenticación porque Acct-Status-Type se ha establecido en Stop.</li><li>• El parámetro Auth-Type no está establecido en RADIUS/LOGOUT.</li></ul>

Atributo	Valor
Ascend-Xmit-Rate (255)	<p>Especifica la velocidad de los datos transmitidos en la conexión, en bits por segundo. En llamadas ISDN, Ascend-Xmit-Rate especifica la velocidad de transmisión de datos. En llamadas analógicas, especifica la velocidad en baudios del módem en el momento de realizar la conexión inicial.</p> <p>Ascend-Xmit-Rate no aparece en un perfil de usuario. El valor predeterminado es 0 (cero). Este atributo aparece en paquetes Accounting-Request para proporcionar información de resolución de problemas al usuario.</p> <p>La unidad TAOS envía el atributo Ascend-Xmit-Rate en paquetes Accounting-Request al final de una sesión si se dan las dos condiciones siguientes (independientemente de si la unidad autentica o no la conexión):</p> <ul style="list-style-type: none"><li>• El paquete Accounting-Request tiene Acct-Status-Type establecido en Stop.</li><li>• El parámetro Auth-Type se ha establecido en un valor que no es RADIUS/LOGOUT.</li></ul>

## Configuración de conexiones de marcación conmutadas

Una conexión de marcación conmutada es una conexión WAN temporal activada por un dispositivo remoto que llama a una unidad TAOS. Es el tipo de conexión WAN más habitual y puede configurarse en un perfil Connection local o en RADIUS. Los subapartados siguientes proporcionan ejemplos de ambos tipos de configuración.

**Nota:** Para obtener información detallada acerca de conexiones que utilicen relé de trama, consulte la publicación *Guía de configuración de relé de trama para APX 8000/MAX TNT/DSLNT*.

## Conexiones PPP de un único canal

Una marcación PPP de un único canal puede iniciarse mediante un dispositivo asíncrono, como un módem analógico, o un dispositivo de red síncrono, como una unidad Pipeline. Para conexiones que requieran más de 56 K de ancho de banda, consulte el apartado “Conexiones de protocolo multienlace (MP)” en la página 1-16 o el apartado “Conexiones del protocolo multienlace Plus (MP+)” en la página 1-19.

### Ajustes de un perfil Connection

Para configurar una conexión de marcación PPP de un único canal en un perfil Connection, utilice los parámetros siguientes (que aparecen con los valores predeterminados):

```
[in CONNECTION/""]
station* = ""
encapsulation-protocol = mpp
```



```
[in CONNECTION/"":ppp-options]
recv-password = ""
link-compression = stac
mru = 1524
lqm = no
lqm-minimum-period = 600
lqm-maximum-period = 600
```

<b>Parámetro</b>	<b>Especifica</b>
Station	Nombre del emisor. El valor distingue entre mayúsculas y minúsculas, y debe coincidir exactamente con el nombre que el dispositivo remoto tiene durante la autenticación.
Encapsulation-Protocol	Protocolo de encapsulación. Se establece en PPP para el protocolo punto a punto de un único canal.
Recv-Password	Contraseña que se espera del emisor.
Link-Compression	Método de compresión de enlaces que debe utilizarse. Para obtener información detallada, consulte “Métodos de compresión de enlaces” en la página 1-14.
MRU	Número máximo de bytes que puede recibir la unidad TAOS en un único paquete (de 1 a 1524, el valor predeterminado es 1524).
LQM	Activa y desactiva el protocolo LQM (Supervisión de calidad del enlace).
LQM-Minimum-Period LQM-Maximum-Period	Período mínimo y máximo para generar paquetes Link-Quality-Report.

### *Ajustes de un perfil RADIUS*

RADIUS utiliza los pares atributo-valor siguientes para conexiones PPP:

<b>Atributo</b>	<b>Valor</b>
Password (2)	Contraseña que se espera del emisor en una conexión de marcación.
Service-Type (6)	Tipo de servicios que puede utilizar el enlace. Se establece en Framed para conexiones PPP de marcación que no utilicen un inicio de sesión del servidor de terminales o en Login para conexiones PPP asíncronas. Si no se especifica, el tipo de servicio no presenta restricciones.
Framed-Protocol (7)	Protocolo de encapsulación. Se establece en PPP (1) para permitir que un usuario realice una marcación con entramado PPP o sin entramado y, a continuación, cambie a entramado PPP.
Framed-MTU (12)	Número máximo de bytes que la unidad TAOS puede enviar en un único paquete (de 1 a 1524, el valor predeterminado es 1524).
Ascend-Link-Compression (233)	Método de compresión de enlaces que debe utilizarse. Para obtener información detallada, consulte “Métodos de compresión de enlaces” en la página 1-14.

#### Autenticación de la contraseña

Si desea obtener información detallada acerca de la autenticación de la contraseña en conexiones PPP, MP y MP+, consulte el Apéndice A, “Métodos de autenticación”.

#### Métodos de compresión de enlaces

El ajuste de compresión de enlaces de un perfil Connection o RADIUS especifica el método de compresión que debe utilizarse para los paquetes encapsulados con PPP que se envían y se reciben en la conexión. Durante la fase de negociación de la conexión, los dos extremos deben acordar utilizar el método especificado. La unidad TAOS da soporte a los tipos de compresión de enlaces PPP siguientes:

- La compresión Stac utiliza una versión modificada del borrador 0 del protocolo CCP, que antecede al documento RFC 1974. El equipo Ascend anterior da soporte a este método de compresión. No se recomienda utilizar este método con conexiones IPX. En un perfil Connection, el ajuste es Stac. En un perfil RADIUS, es Link-Comp-Stac (1).
- La compresión Stac-9 utiliza el borrador 9 del protocolo de compresión Stac LZS, que se describe en el documento RFC 1974. La mayoría de los dispositivos, especialmente el equipo más reciente, utiliza este método de compresión. En un perfil Connection, el ajuste es Stac-9. En un perfil RADIUS, es Link-Comp-Stac-Draft-9 (2).
- La compresión MS-Stac (Microsoft/Stac) es el método que utiliza Windows 95. Utilice este método en conexiones con clientes Windows 95. En un perfil Connection, el ajuste es MS-Stac. En un perfil RADIUS, es Link-Comp-MS-Stac (3).

#### Supervisión de la calidad del enlace

La supervisión de calidad del enlace (LQM) es el proceso de supervisión de la pérdida de datos en un enlace punto a punto (consulte el documento RFC 1989, *PPP Link Quality Monitoring*). Al activar LQM en un perfil Connection, la unidad TAOS realiza recuentos del número de paquetes transmitidos y recibidos de forma satisfactoria y periódicamente transmite esta información al dispositivo del extremo distante en un paquete Link-Quality-Report. El conjunto de comandos siguiente activa LQM para una conexión utilizando el período predeterminado de seis segundos para generar paquetes Link-Quality-Report:

```
admin> read conn test
CONNECTION/test read

admin> set ppp lqm = yes

admin> write
CONNECTION/test written
```

Las conexiones permanentes que utilizan la encapsulación PPP y la supervisión de calidad del enlace (LQM) incluyen soporte de número mágico para detectar enlaces en bucle y otras anomalías de capa en el enlace de datos. Cuando el sistema detecta anomalías, desconecta el enlace.

Si LQM está activado, el sistema selecciona un número al azar y negocia dicho número con el dispositivo del extremo distante durante la negociación LCP del enlace. Si el dispositivo del extremo distante no negocia números mágicos, el campo del número mágico en los paquetes transmitidos se establece en cero. Si el número se negocia de modo satisfactorio, el campo del número mágico local se establece en el número aleatorio seleccionado. El comando WANDisplay en una tarjeta HDLC muestra información acerca de las negociaciones del

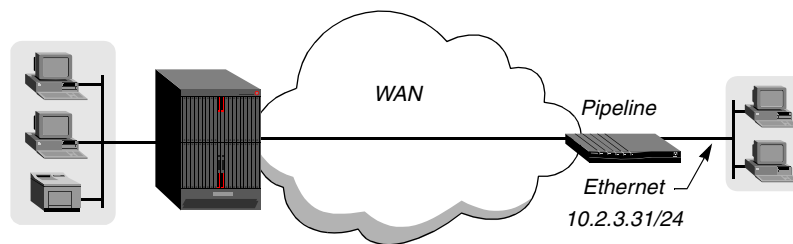
número mágico LQM y los informes LQM periódicos muestran los números mágicos remotos y locales asignados.

La unidad TAOS inspecciona el campo del número mágico en los paquetes recibidos y procesa un paquete normalmente si el campo es igual a cero o al número mágico exclusivo de su homólogo. Si el campo del número mágico es igual al número mágico local, lo que denota un enlace en bucle, la unidad termina el enlace.

### *Ejemplos de una conexión PPP síncrona*

En la Figura 1-2 el emisor es una unidad Pipeline con la dirección IP 10.2.3.31/24.

*Figura 1-2. Conexión PPP síncrona*



Los comandos siguientes crean el perfil Connection del emisor:

```
admin> new connection phani
CONNECTION/phani read

admin> set active = yes

admin> set encapsulation-protocol = ppp

admin> set ip remote-address = 10.2.3.31/24

admin> set ppp recv-password = localpw

admin> write
CONNECTION/phani written
```

A continuación se muestra un perfil RADIUS:

```
phani Password = "localpw"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Framed-IP-Address = 10.2.3.31,
    Framed-IP-Netmask = 255.255.255.0
```

Si desea obtener información detallada acerca de cómo permitir que la unidad TAOS rutee paquetes a la unidad Pipeline realizando la marcación a ese destino, consulte el apartado “Configuración de conexiones de salida” en la página 1-42.

### *Ejemplos de una conexión PPP asíncrona*

Las conexiones asíncronas se autentican primero mediante el software del servidor de terminales, de modo que debe activar el servidor de terminales para que permita estas conexiones. Para obtener información detallada, consulte el apartado “Perfil Terminal-Server” en la página 1-5. Si desea obtener información sobre la autenticación del servidor de terminales, consulte el Apéndice A, “Métodos de autenticación”.

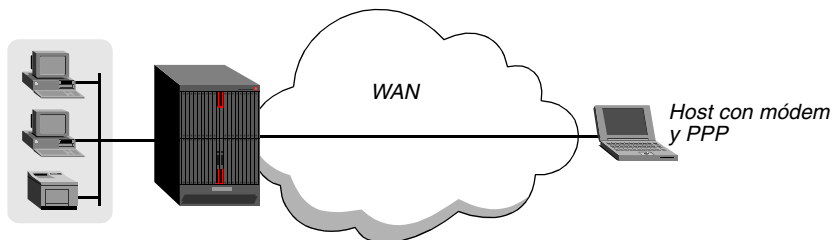
## Conexiones WAN

### Configuración de conexiones de marcación conmutadas

---

En la Figura 1-3 el dispositivo que realiza la llamada es un módem, de modo que la conexión es asíncrona.

Figura 1-3. Conexión PPP asíncrona



Los comandos siguientes crean el perfil Connection del emisor:

```
admin> new connection carlos
CONNECTION/carlos read

admin> set active = yes

admin> set encapsulation-protocol = ppp

admin> set ip remote-address = 10.2.3.78/32

admin> set ppp recv-password = localpw

admin> write
CONNECTION/carlos written
```

A continuación se muestra un perfil RADIUS:

```
carlos Password = "localpw"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Framed-IP-Address = 10.2.3.78,
    Framed-IP-Netmask = 255.255.255.255
```

## Conexiones de protocolo multienlace (MP)

El protocolo multienlace (MP) utiliza la encapsulación definida en el documento RFC 1990. MP permite que el emisor utilice un número de canales estático. Los dos extremos de la conexión deben dar soporte a la encapsulación MP.

Los ajustes de PPP de los perfiles Answer-Defaults y Connection también se aplican a las conexiones MP. Si configura una conexión MP y la unidad TAOS no puede negociar la conexión de forma satisfactoria, se establece una conexión PPP de un único canal (si desea obtener información adicional, consulte el apartado “Configuración de conexiones de salida” en la página 1-42).

**Nota:** Para conseguir un rendimiento óptimo, los dos extremos de la conexión deben establecer el parámetro Base-Channel-Count en el mismo valor.

### Ajustes de un perfil Connection

A continuación se muestran los parámetros relacionados con conexiones MP de marcación. Los ajustes muestran los valores predeterminados.

```
[in CONNECTION/""]
encapsulation-protocol = mpp
```

```
[in CONNECTION/"":mp-options
base-channel-count = 1
minimum-channels = 1
maximum-channels = 2
```

Parámetro	Especifica
Encapsulation-Protocol	Protocolo de encapsulación. Se establece en MP para conexiones de protocolo multienlace.
Base-Channel-Count	Número base de canales que se utilizará en una conexión PPP multienlace. Cuando se recibe una llamada, la unidad TAOS autentica los primeros canales (base) de la llamada y, a continuación, determina los valores mínimo y máximo.
Minimum-Channels	Número mínimo de canales disponibles en una conexión PPP multienlace. En la versión actual del software, el valor puede aplicarse a conexiones MP+, pero no a conexiones MP.
Maximum-Channels	Número máximo de canales disponibles en una conexión PPP multienlace. En la versión actual del software, el valor puede aplicarse a conexiones MP+, pero no a conexiones MP.

### Ajustes de un perfil RADIUS

RADIUS utiliza los siguientes pares atributo-valor para las conexiones MP de marcación:

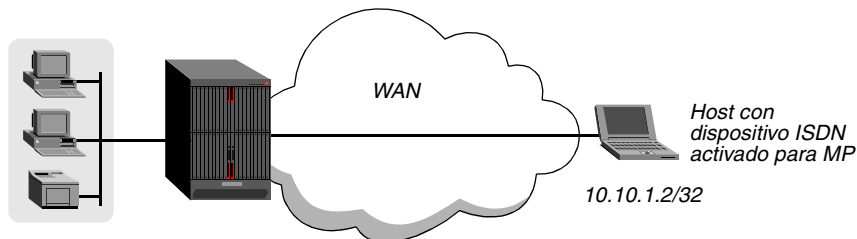
Atributo	Valor
Framed-Protocol (7)	Protocolo de encapsulación. MP (262) indica protocolo multienlace.
Ascend-Base-Channel-Count (172)	Número base de canales que se utilizará en una conexión PPP multienlace. Cuando se recibe una llamada, la unidad TAOS autentica los primeros canales (base) de la llamada y, a continuación, determina los valores mínimo y máximo.
Ascend-Minimum-Channels (173)	Número mínimo de canales disponibles en una conexión PPP multienlace. En la versión actual del software, el valor puede aplicarse a conexiones MP+, pero no a conexiones MP.
Ascend-Maximum-Channels (235)	Número máximo de canales disponibles en una conexión PPP multienlace. En la versión actual del software, el valor puede aplicarse a conexiones MP+, pero no a conexiones MP.

**Nota:** Si en un perfil RADIUS no se especifica Ascend-Maximum-Channels, el valor predeterminado 1 evita que el cliente establezca una llamada multicanal.

#### Ejemplos de una conexión MP

En la conexión MP que se muestra en la Figura 1-4 se han asignado dos canales.

Figura 1-4. Conexión de protocolo multienlace (MP)



A continuación se muestran los comandos introducidos para configurar un perfil local y las respuestas del sistema:

```
admin> new connection kory
CONNECTION/kory read
admin> set active = yes
admin> set encapsulation-protocol = mp
admin> set ip remote-address = 10.10.1.2/32
admin> set ppp recv-password = localpw
admin> set mp base-channel-count = 2
admin> write
CONNECTION/kory written
```

A continuación se muestra un perfil RADIUS equivalente:

```
kory Password = "localpw"
  Service-Type = Framed-User,
  Framed-Protocol = MP,
  Framed-IP-Address = 10.10.1.2,
  Framed-IP-Netmask = 255.255.255.255,
  Ascend-Base-Channel-Count = 2,
  Ascend-Maximum-Channels = 2
```

#### Vinculación de llamadas analógicas mediante MP

MP también opera en tarjetas de módem para enlazar varios canales para llamadas analógicas. Esta característica permite a un cliente con dos módems conectarse a la unidad TAOS a una velocidad que sea el resultado de la suma de las velocidades de ambas conexiones. Por ejemplo, en un sistema Windows NT 4.0 con dos módems de 56 K y con DUN (*Dial Up Networking*, Acceso telefónico a redes) configurado para utilizar varias líneas, pueden definirse ambos módems para que realicen una marcación a una unidad TAOS.

**Nota:** Algunos módems y paquetes de software de cliente presentan problemas de compatibilidad con la vinculación de canales por MP.

Para permitir la vinculación de llamadas analógicas por MP, un administrador de APX 8000 debe especificar una conexión MP estándar. Por ejemplo:

```
admin> new connection baskar
CONNECTION/baskar read
```

```

admin> set active = yes

admin> set encapsulation-protocol = mp

admin> set ip remote-address = 10.10.1.2/29

admin> set ppp rcv-password = localpw

admin> set mp base-channel-count = 2

admin> write
CONNECTION/baskar written

```

O en un perfil RADIUS:

```

baskar Password = "localpw"
  Service-Type = Framed-User,
  Framed-Protocol = MP,
  Framed-IP-Address = 10.10.1.2,
  Framed-IP-Netmask = 255.255.255.248,
  Ascend-Base-Channel-Count = 2

```

La primera llamada del módem de 56 K negocia la conexión MP y la segunda llamada del módem se encuentra agrupada con la primera. La unidad TAOS reconoce un único usuario MP con una conexión de 128 Kbps.

## Conexiones del protocolo multienlace Plus (MP+)

El protocolo multienlace Plus (MP+) utiliza la encapsulación PPP con extensiones TAOS, como se describe en el documento RFC 1934. MP+ permite que una unidad TAOS supervise el tráfico en una conexión con otra unidad TAOS y agregue o quite ancho de banda a petición. Los criterios para agregar o eliminar ancho de banda forman parte de las extensiones TAOS y sólo reciben soporte de equipos Lucent.

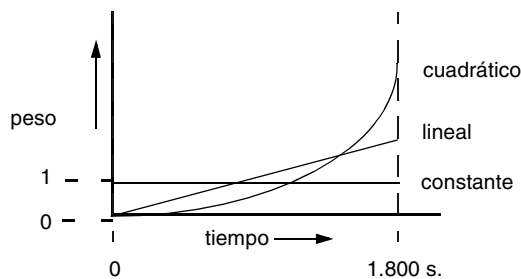
En conexiones MP+, el extremo que realiza la primera llamada realiza las llamadas posteriores para agregar ancho de banda. Si un usuario remoto o un ruteador de acceso realiza la marcación, se efectúan también todas las llamadas para agregar canales. Si la unidad TAOS inicia la primera llamada, se efectúan todas las llamadas para agregar canales.

Los ajustes de PPP y MP de los perfiles Answer-Defaults y Connection también se aplican a las conexiones MP+. Para especificar los canales base de una conexión MP+, debe configurar el subperfil MP-Options (como se describe en “Conexiones de protocolo multienlace (MP)” en la página 1-16).

### *Cómo agregan ancho de banda las unidades TAOS*

La asignación dinámica de ancho de banda (DBA) permite que una unidad TAOS agregue ancho de banda a petición estableciendo conexiones adicionales y multiplexado inverso en la llamada. La DBA utiliza uno de los varios algoritmos de ponderación posibles para determinar cuándo agregar o quitar ancho de banda. El algoritmo de ponderación predeterminado (cuadrático) proporciona más peso a las muestras de utilización recientes que a las muestras anteriores, con lo que la ponderación aumenta a un ritmo cuadrático. Lineal permite que la ponderación aumente a un ritmo lineal y Constante proporciona el mismo peso a todas las muestras de utilización. En la Figura 1-5 se muestra una representación gráfica de los tres algoritmos.

Figura 1-5. Ponderación de muestras de utilización de la línea



Si desea obtener información acerca de la configuración de números de adición por canal que permitan que una unidad TAOS agregue ancho de banda a petición, consulte la publicación *Guía de configuración de la interfaz física de APX 8000/MAX TNT/DSLNT*. Puede agregar un canal cada vez o, si la unidad TAOS está configurada para la marcación paralela, varios a la vez. Si desea configurar la unidad para la marcación paralela, establezca el parámetro Parallel-Dialing en el perfil System. Por ejemplo, en el comando siguiente se muestra que Parallel-Dialing se ha establecido en 2 (el valor predeterminado), lo que permite dos llamadas de salida al mismo tiempo:

```
admin> get system parallel
parallel-dialing = 2
```

Una unidad TAOS puede rechazar la petición de adición de ancho de banda si no hay más canales disponibles en uno o los dos extremos, o si la red está congestionada. En alguna de estas condiciones, los dos extremos entran en el modo de bloqueo de adición de ancho de banda, en el que ningún extremo puede solicitar ancho de banda. La restricción local evita que los dos extremos continúen intentando sin éxito agregar nuevos canales. La unidad TAOS y la unidad TAOS del otro extremo de la conexión eliminan automáticamente la restricción de bloqueo cuando cambia la condición que ha causado el bloqueo. Generalmente los cambios son resultado de la adición de una nueva línea de servicio conmutado, la reconfiguración del perfil de la línea o un tiempo de espera excedido por congestión del servicio conmutado. Una vez que se elimina el bloqueo, los dos extremos pueden agregar ancho de banda.

### *Picos en la utilización media de la línea (ALU)*

Los valores de Seconds-History, Add-Persistence y Sub-Persistence deben suavizar los picos en la utilización de ancho de banda que duran menos tiempo que lo que se tarda en agregar capacidad. En líneas T1, la unidad TAOS puede agregar ancho de banda en menos de diez segundos. En líneas ISDN, la unidad puede agregar ancho de banda en menos de cinco segundos.

### *Tarifas de la compañía de telecomunicaciones*

Cuando la unidad TAOS agrega ancho de banda, normalmente se aplica una tarifa mínima de utilización, después de la cual la facturación se realiza en función del tiempo. El valor Sub-Persistence debe ser al menos igual a la tarifa de duración mínima más uno o dos incrementos de tiempo de facturación. Habitualmente la facturación se realiza para el siguiente múltiplo de seis segundos, con una tarifa mínima en los primeros treinta segundos.

Agregar o quitar canales demasiado rápido (con menos de 10-20 segundos de diferencia) provoca demasiadas llamadas de corta duración, en cada una de las cuales se cobra la tarifa



mínima de la compañía portadora. Asimismo, agregar o quitar canales demasiado rápido puede afectar a la eficacia del enlace, puesto que los dispositivos en ambos extremos tienen que volver a transmitir datos cuando cambia la velocidad del enlace.

### *Ajustes de un perfil Connection*

A continuación se muestran los parámetros del perfil Connection relacionados con conexiones MP+ de marcación. Los ajustes muestran los valores predeterminados.

```
[in CONNECTION/""]
encapsulation-protocol = mpp

[in CONNECTION/"":mpp-options]
aux-send-password = ""
dynamic-algorithm = quadratic
bandwidth-monitor-direction = transmit
increment-channel-count = 1
decrement-channel-count = 1
seconds-history = 15
add-persistence = 5
sub-persistence = 10
target-utilization = 70
```

Parámetro	Especifica
Encapsulation-Protocol	Protocolo de encapsulación. MP+ (el valor predeterminado) especifica el protocolo multienlace Plus. El extremo distante debe ser una unidad TAOS.
Aux-Send-Password	Contraseña que envía la unidad TAOS al agregar canales a una llamada MP+ que utiliza la autenticación PAP-Token-CHAP. Para obtener información detallada, consulte “Autenticación por tarjeta de testigo” en la página A-26.
Dynamic-Algorithm	Algoritmo para calcular la utilización media de la línea (ALU) en un número determinado de segundos (Seconds-History). Para obtener información detallada, consulte “Cómo agregan ancho de banda las unidades TAOS” en la página 1-19.
Bandwidth-Monitor-Direction	Dirección en la que se aplican los criterios, es decir, si los criterios para agregar o eliminar enlaces se aplican al tráfico que se recibe en el enlace, al que se transmite en el enlace o en ambas direcciones. Si los dos extremos del enlace tienen Bandwidth-Monitor-Direction establecido en None, DBA está desactivada.
Increment-Channel-Count	Número de canales que puede agregar la unidad TAOS a la vez; depende del valor del parámetro Parallel-Dialing en el perfil System.
Decrement-Channel-Count	Número de canales que puede quitar la unidad TAOS a la vez, eliminando primero los canales más nuevos.
Seconds-History	Número de segundos que se utilizará como base para calcular la utilización media de la línea (ALU).
Add-Persistence	Número de segundos durante los que la ALU debe permanecer por encima del umbral Target-Utilization antes de que la unidad TAOS agregue ancho de banda.

## Conexiones WAN

### Configuración de conexiones de marcación conmutadas

---

Parámetro	Especifica
Sub-Persistence	Número de segundos durante los que la ALU debe permanecer por debajo del umbral Target-Utilization antes de que la unidad quite ancho de banda.
Target-Utilization	Porcentaje de utilización de la línea (el valor predeterminado es 70 %) que se utilizará como umbral a la hora de determinar si debe agregarse o quitarse ancho de banda.

### Ajustes de un perfil RADIUS

Un perfil de usuario RADIUS puede especificar los atributos siguientes para configurar opciones PPP de conexión MP+ de marcación, además de los atributos PPP que se describen en el apartado “Conexiones PPP de un único canal” en la página 1-12 y los parámetros MP que se describen en el apartado “Conexiones de protocolo multienlace (MP)” en la página 1-16:

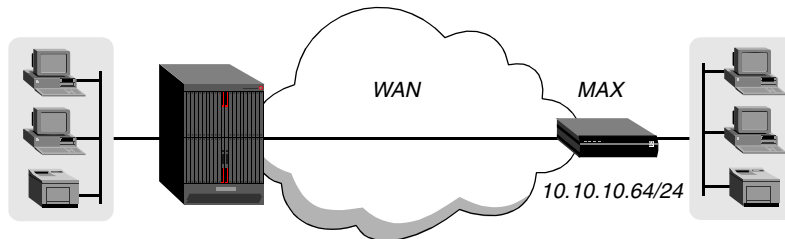
Atributo	Valor
Framed-Protocol (7)	Protocolo de encapsulación. MPP (256) indica una conexión MP+ con otra unidad TAOS.
Ascend-History-Weight-Type (239)	Algoritmo para calcular la utilización media de la línea (ALU) en un número determinado de segundos. Para obtener información detallada, consulte “Cómo agregan ancho de banda las unidades TAOS” en la página 1-19.
Ascend-DBA-Monitor (171)	Criterios para agregar o quitar ancho de banda de la conexión. Puede especificar DBA-Transmit (0), DBA-Transmit-Recv (1) o DBA-None (3). Si los dos extremos del enlace tienen Bandwidth-Monitor-Direction establecido en None, DBA está desactivada.
Ascend-Inc-Channel-Count (236)	Número de canales que puede agregar la unidad TAOS a la vez; depende del valor del parámetro Parallel-Dialing en el perfil System.
Ascend-Dec-Channel-Count (237)	Número de canales que puede quitar la unidad TAOS a la vez, eliminando primero los canales más nuevos.
Ascend-Seconds-Of-History (238)	Número de segundos que se utilizará como base para calcular la utilización media de la línea (ALU).
Ascend-Add-Seconds (240)	Número de segundos durante los que la ALU debe permanecer por encima del umbral Target-Utilization antes de que la unidad TAOS agregue ancho de banda.
Ascend-Remove-Seconds (241)	Número de segundos durante los que la ALU debe permanecer por debajo del umbral Target-Utilization antes de que la unidad quite ancho de banda.
Ascend-Target-Util (234)	Porcentaje de utilización de la línea (el valor predeterminado es 70 %) que se utilizará como umbral a la hora de determinar si debe agregarse o quitarse ancho de banda.
Ascend-Maximum-Channels (235)	Número máximo de canales disponibles en una conexión PPP multienlace. En la versión actual del software, el valor puede aplicarse a conexiones MP+, pero no a conexiones MP.

**Nota:** Si en un perfil RADIUS no se especifica Ascend-Maximum-Channels, el valor predeterminado 1 evita que el cliente establezca una llamada multicanal.

### *Ejemplos de una configuración MP+*

En la Figura 1-6 las dos unidades TAOS especifican la encapsulación MP+.

*Figura 1-6. Conexión de protocolo multienlace Plus (MP+)*



Los comandos siguientes crean un perfil Connection para la unidad MAX™ del extremo distante:

```
admin> new connection max-1
CONNECTION/max-1 read

admin> set active = yes

admin> set encapsulation-protocol = mpp

admin> set ip remote-address = 10.10.10.64/24

admin> set ppp rcv-password = localpw

admin> set mp base-channel-count = 2

admin> set mpp bandwidth-monitor-direction = transmit-rcv

admin> set mpp seconds-history = 30

admin> set mpp add-persistence = 10

admin> write
CONNECTION/max-1 written
```

A continuación se muestra un perfil RADIUS equivalente:

```
max-1 Password = "localpw"
  Service-Type = Framed-User,
  Framed-Protocol = MPP,
  Framed-IP-Address = 10.10.10.64,
  Framed-IP-Netmask = 255.255.255.0,
  Ascend-Base-Channel-Count = 2,
  Ascend-Maximum-Channels = 2,
  Ascend-DBA-Monitor = DBA-Transmit-Recv,
  Ascend-Seconds-Of-History = 30,
  Ascend-Add-Seconds = 10
```

**Nota:** En el perfil RADIUS debe especificarse Ascend-Maximum-Channels, o el valor predeterminado 1 evitará que el cliente establezca una llamada multicanal.

## Protocolo de control de asignación de ancho de banda (BACP)

La unidad TAOS da soporte a BACP para las conexiones de protocolo multienlace PPP (MP). MP se describe en el documento RFC 1990. BACP se describe en el documento RFC 2125. BACP proporciona una asignación dinámica de ancho de banda basada en un umbral de utilización y utilizando criterios muy similares a los que usa la característica de ancho de banda a petición del protocolo multienlace Plus (MP+). BACP puede utilizarse con enlaces digitales o analógicos.

Para que la asignación dinámica de ancho de banda funcione en una conexión MP, los dos extremos de la conexión deben dar soporte a BACP. Los parámetros siguientes (que se muestran con ajustes de ejemplo) activan BACP:

```
[in ANSWER-DEFAULTS:mp-answer]
bacp-enable = yes

[in CONNECTION/"":mp-options]
bacp-enable = yes
```

Parámetro	Especifica
BACP-Enable	Activa y desactiva BACP para conexiones MP. De manera predeterminada BACP está desactivado. En el perfil Answer-Defaults, el ajuste <code>yes</code> permite al sistema aceptar una llamada MP que solicite gestión BACP del ancho de banda. En un perfil Connection, el ajuste <code>yes</code> permite que una conexión específica utilice la gestión BACP del ancho de banda.

BACP comparte los parámetros que utiliza MP+ para especificar criterios para agregar o quitar ancho de banda. A continuación se muestran los parámetros pertinentes, con los ajustes predeterminados:

```
[in CONNECTION/"":mpp-options]
dynamic-algorithm = quadratic
bandwidth-monitor-direction = transmit
increment-channel-count = 1
decrement-channel-count = 1
seconds-history = 15
add-persistence = 5
sub-persistence = 10
target-utilization = 70
```

En la publicación *APX 8000/MAX TNT/DSLNT Reference (Referencia de APX 8000/MAX TNT/DSLNT)* se proporciona más información acerca de cada parámetro. A continuación se muestra un ejemplo de configuración del sistema para activar BACP y configurar una conexión MP que utiliza BACP:

```
admin> read answer
ANSWER-DEFAULTS read

admin> set mp-answer bacp-enable = yes

admin> write
ANSWER-DEFAULTS written

admin> read CONNECTION mp-test
CONNECTION/mp-test read

admin> set encapsulation-protocol = mp
```

```

admin> set mp-options bacp-enable = yes
admin> set mp-options maximum-channels = 4
admin> set mpp-options bandwidth-monitor-direction = transmit-recv
admin> set mpp-options seconds-history = 30
admin> set mpp-options add-persistence = 10
admin> write
CONNECTION/mp-test written

```

## Conexiones TCP-Clear

La unidad TAOS no procesa la encapsulación de paquetes para conexiones TCP-Clear. Estas conexiones utilizan a menudo un método de encapsulación propietario o una encapsulación realizada por una aplicación que se ejecuta por encima de TCP. La unidad TAOS redirige de inmediato los datos de la conexión a un host especificado, en el que se supone que se producirá el proceso de la encapsulación.

Puede configurar TCP-Clear para una conexión específica, como se describe en este apartado. También puede activarlo globalmente en el perfil Terminal-Server utilizando el servicio TCP en *modo inmediato*, como se describe en el apartado “Autorización de un servicio de conexión de modo inmediato” en la página B-2.

### *Mejoras de rendimiento para llamadas TCP-Clear (sólo perfiles locales)*

Las sesiones de marcación TCP-Clear que no requieren proceso V.120 pueden almacenarse en el búfer y transmitirse como paquetes TCP en lugar de como corrientes de datos continuas, con lo que aumenta el rendimiento. Además, a menos que sea necesario el proceso V.120, los datos de WAN de TCP-Clear se envían directamente a la interfaz HDLC en lugar de al subsistema del servidor de terminales. El sistema no reúne estadísticas de sesión para llamadas TCP-Clear que utilizan estas mejoras del rendimiento. Si una sesión requiere el proceso V.120, el servidor de terminales procesa la llamada.

### *Ajustes de un perfil Connection*

A continuación se muestran los parámetros del perfil Connection relacionados con conexiones TCP-Clear de entrada. Los ajustes muestran los valores predeterminados.

```

[in CONNECTION/""]
encapsulation-protocol = tcp-raw

[in CONNECTION/"":ppp-options]
recv-password = localpw

[in CONNECTION/"":tcp-clear-options]
host = ""
port = 0
host1 = ""
port1 = 0
host2 = ""
port2 = 0
host3 = ""
port3 = 0
detect-end-of-packet = no
end-of-packet-pattern = ""

```

## Conexiones WAN

### Configuración de conexiones de marcación conmutadas

---

```
flush-length = 256  
flush-time = 20
```

Parámetro	Especifica
Encapsulation-Protocol	Protocolo de encapsulación. Debe establecerse en TCP-Raw para una conexión TCP-Clear.
Recv-Password	Contraseña que se espera del emisor.
Host o Host/V	Nombres DNS o direcciones IP de un máximo de cuatro hosts. Si la conexión TCP con la primera combinación especificada de host/puerto falla mientras se está estableciendo la sesión TCP-Clear, el sistema intentará conectarse al siguiente host especificado y así sucesivamente. Si fallan todos los intentos de conexión, la sesión termina y la unidad TAOS devuelve un error de conexión TCP al cliente que realiza la marcación.
Port o Port/V	Puerto TCP de destino en el host especificado. Un número de puerto cero (el valor predeterminado) significa cualquier puerto.
Detect-End-of-Packet	Activa y desactiva el almacenamiento en el búfer de los datos de entrada. Con el ajuste Yes, la unidad TAOS empieza a almacenar en el búfer los datos de entrada en el momento en que se autentica la sesión de marcación. Continúa almacenando en el búfer hasta que recibe el parámetro End-of-Packet-Pattern especificado o hasta que alcanza el tiempo de espera especificado (Flush-Time) o la longitud máxima del paquete (Flush-Length), la condición que se produzca primero. Si Detect-End-of-Packet se establece en No (el valor predeterminado), no se aplica ninguno de los parámetros relacionados.
End-of-Packet-Pattern	Patrón de caracteres que señala el final de un paquete. Cuando la unidad TAOS encuentra este patrón en los datos del búfer, inmediatamente vacía el búfer grabando todos los datos, incluido el patrón, en TCP. Observe que los datos se graban antes de que se produzca una coincidencia si se supera el tiempo de espera especificado (Flush-Time) o la longitud máxima del paquete (Flush-Length).
Flush-Length	Número máximo de bytes que se almacenará en el búfer. Los valores válidos se encuentran entre 1 y 8192. El valor predeterminado es 256. Tenga en cuenta que almacenar grandes paquetes en el búfer consume más recursos del sistema. Si el sistema ha almacenado en el búfer el número de bytes especificado sin encontrar End-of-Packet-Pattern, vacía el búfer grabando los datos en TCP.
Flush-Time	Temporizador en milisegundos. Los valores válidos se encuentran entre 1 y 1000. El temporizador empieza la cuenta atrás a partir de la recepción del primer byte de datos del búfer. Si el número de milisegundos especificado transcurre sin encontrar End-of-Packet-Pattern, el sistema vacía el búfer grabando los datos en TCP.

El patrón de caracteres que especifique como valor del parámetro End-of-Packet-Pattern puede tener una longitud máxima de 64 caracteres. Puede contener tanto caracteres ASCII como datos binarios. Para especificar un valor binario, utilice la barra inversa (\) como mecanismo de escape. Para insertar una barra inversa literal en el patrón, introduzca dos caracteres de barra inversa (\\) como escape.

Para insertar un número octal de uno a tres dígitos, introduzca el valor colocando delante una barra inversa como escape. Para evitar confusiones entre los caracteres literales ASCII entre 0 y 7 y un valor octal, puede rellenar el valor octal con ceros. Por ejemplo, el patrón siguiente representa un retorno de carro (octal 15):

```
\015
```

Para insertar en el patrón un número hexadecimal de uno o dos dígitos, introduzca \x delante del número. Por ejemplo, el patrón siguiente representa un retorno de carro (hex 0D):

```
\x0D
```

Las siguientes son otras secuencias de escape:

Secuencia de escape	Descripción	Valor
\a	Alarma	7
\b	Retroceso	8
\f	Salto de página	12
\n	Línea nueva	10
\r	Retorno de carro	13
\t	Tabulación	9
\v	Tabulación vertical	11
\\	Barra inversa	92
\'	Apóstrofe	44
\"	Comillas dobles	34
\?	Comodín	Coincide con cualquier carácter

### *Ajustes de un perfil RADIUS*

Un perfil RADIUS puede incluir un máximo de cuatro ajustes del atributo Login-IP-Host y cuatro ajustes del atributo Login-TCP-Port. Una unidad TAOS valida el número de estos ajustes en el paquete Access-Accept que devuelve RADIUS. Si encuentra más de cuatro, la unidad registra un error en la salida de depuración RADIF y procesa sólo los cuatro primeros.

Mientras se establece la sesión TCP-Clear, si falla la conexión TCP con la primera combinación host/puerto especificada, la unidad intenta conectarse al siguiente host especificado y así sucesivamente. Si fallan todos los intentos de conexión, la sesión termina y la unidad TAOS devuelve un error de conexión TCP al cliente que realiza la marcación.

A continuación se muestran los atributos del perfil RADIUS relacionados con TCP-Clear:

Atributo	Valor
Login-Service (15)	Tipo de servicio de inicio de sesión permitido al emisor. Debe establecerse en TCP-Clear (2). Para eliminar mensajes de estado en función de cada usuario mientras se establece la sesión, establezca TCP-Clear-Quiet (256).
Login-IP-Host (14)	Dirección IP de un host de inicio de sesión TCP.
Login-TCP-Port (16)	Puerto TCP de destino en el host de inicio de sesión especificado (un número entero del 1 al 65535). El valor predeterminado es 23.
Service-Type (6)	Tipo de servicio que puede utilizar el enlace. Especifique Framed (Entramado) o Unframed (No entramado).

### Ejemplos de conexiones TCP-Clear

El conjunto de comandos siguiente especifica una conexión TCP-Clear con un host denominado Sparky en el puerto TCP 23 o un host denominado Boom en el puerto TCP 125:

```
admin> new conn tcpapp1
CONNECTION/tcpapp1 read
admin> set active = yes
admin> set encaps = tcp-raw
admin> set ppp recv-password = localpw
admin> set tcp host = 10.10.10.1
admin> set tcp port = 23
admin> set tcp host1 = 10.10.10.2
admin> set tcp port1 = 125
admin> write
CONNECTION/tcpapp1 written
```

A continuación se muestra un perfil RADIUS equivalente:

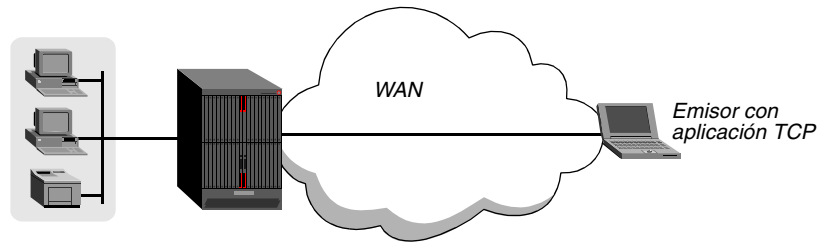
```
tcpapp1 Password = "localpw"
  Service-Type = Login-User,
  Login-Service = TCP-Clear,
  Login-IP-Host = 10.10.10.1,
  Login-TCP-Port = 23,
  Login-IP-Host = 10.10.10.2,
  Login-TCP-Port = 125
```

### Ejemplo de TCP-Clear con almacenamiento de paquetes en el búfer (sólo perfiles locales)

En la Figura 1-7 un emisor que realiza una llamada de entrada a la unidad TAOS ejecuta una aplicación que utiliza un método de encapsulación que debe descodificar un host local. La unidad TAOS envía la corriente de datos desde la llamada de entrada directamente al host.



*Figura 1-7. Conexión TCP-Clear a un host local*



Los comandos siguientes configuran una conexión TCP-Clear con un host denominado Sparky en el puerto TCP 23 y la unidad TAOS almacena en el búfer los paquetes antes de transmitirlos. End-of-Packet-Pattern tiene tres números hexadecimales.

```
admin> read connection tcpapp2
CONNECTION/tcpapp2 read

admin> set active = yes

admin> set encaps = tcp-raw

admin> set ppp recv-password = remotepw

admin> set tcp host 1 = sparky

admin> set tcp port 1 = 23

admin> set tcp detect-end-of-packet = yes

admin> set tcp end-of-packet-pattern = \xfe\xfd\xfe

admin> set tcp flush-length = 16

admin> write
CONNECTION/tcpapp2 written
```

## Aplicación de un perfil IPsec a una sesión TCP-Clear

Los perfiles RADIUS utilizan el par atributo-valor siguiente para aplicar un perfil IPsec a una sesión TCP-Clear. Si desea obtener información acerca de IPsec y la creación de perfiles IPsec, consulte el apartado “Configuración de la autenticación IPsec” en la página 5-6.

Atributo	Valor
Ascend-IPSEC-Profile (73)	Nombre de un perfil IPsec que describe las transformaciones y puntos finales IPsec que deben utilizarse para esta conexión (un valor de tipo cadena).

Para utilizar los pares atributo-valor en el perfil que especifica el atributo Ascend-IPSEC-Profile, el servidor RADIUS debe dar soporte a atributos específicos del proveedor (VSA) y la unidad TAOS debe estar configurada en modo de compatibilidad VSA. A continuación se muestran los ajustes pertinentes:

```
[in EXTERNAL-AUTH]
auth-type = radius

[in EXTERNAL-AUTH:rad-auth-client]
auth-radius-compatible = vendor-specific
```

Si desea obtener información detallada acerca de estos ajustes, consulte la publicación *APX 8000/MAX TNT/DSLNT Reference (Referencia de APX 8000/MAX TNT/DSLNT)*. Si desea obtener información detallada acerca de la configuración de conexiones TCP-Clear, consulte el apartado “Conexiones TCP-Clear” en la página 1-25.

### Modo de túnel y modo de transporte

La unidad TAOS da soporte al modo de transporte IPSec y al modo de túnel IPSec para las conexiones TCP-Clear entre gateways.

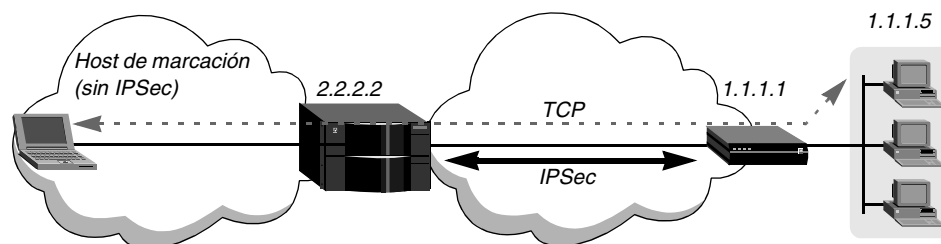
El *modo de túnel* es necesario para conexiones entre un host que no realiza proceso IPSec y un gateway de seguridad. En el modo de túnel, los paquetes IP se encapsulan en una cabecera IP externa que especifica el destino del proceso IPSec (encapsulación IP en IP).

El *modo de transporte* opera entre dos hosts. El modo de transporte proporciona servicios de seguridad para protocolos de capa superior, que pueden incluir partes seleccionadas de la cabecera IP y otras opciones seleccionadas.

En la Figura 1-8 los puntos finales IPSec son una unidad TAOS y una unidad Pipeline 220. El punto final TCP es un host TCP que realiza la marcación a la unidad TAOS. Puesto que los puntos finales IPSec son diferentes del punto final TCP, el perfil IPSec de esta conexión debe especificar el modo de túnel, como se describe en “Modos de encapsulación IPSec” en la página 5-7. Por ejemplo:

```
admin> get ipsec securegw encap-mode
[In IPSEC/securegw:encap-mode]
encap-mode = tunnel
```

Figura 1-8. Modo de túnel IPSec para TCP-Clear entre gateways



El siguiente perfil RADIUS de ejemplo permite que el host que realiza la marcación establezca una sesión TCP-Clear segura con un host de inicio de sesión en 1.1.1.5:

```
tcpapp-user Password = "localpw"
  Service-Type = Login,
  Login-Service = TCP-Clear,
  Login-Host = 1.1.1.5,
  Login-TCP-Port = 23,
  Ascend-IPSEC-Profile = securegw
```

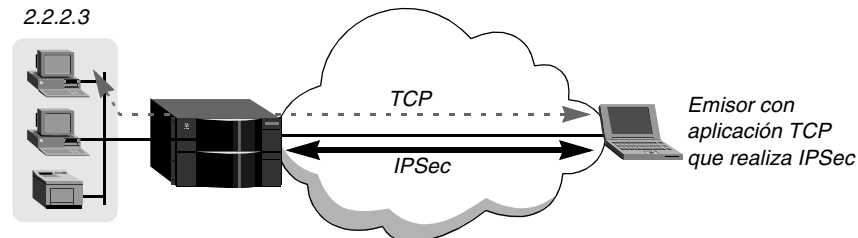
La unidad TAOS aplica un perfil IPSec denominado *securegw* a la corriente de datos de la sesión. Pipeline 220 debe tener la configuración IPSec correspondiente y los dos puntos finales IPSec requieren perfiles Connection o RADIUS para el enlace que hay entre ellos.

En la Figura 1-9 el host que realiza la marcación ejecuta una aplicación TCP capaz de realizar la encapsulación y la eliminación de la encapsulación IPSec. En este caso, los puntos finales

IPSec y el punto final TCP-Clear son los mismos, por lo que el perfil IPSec para esta conexión especifica el modo de transporte. Por ejemplo:

```
admin> get ipsec dialin encap-mode
[In IPSEC/dialin:encap-mode]
encap-mode = transport
```

*Figura 1-9. Modo de transporte IPSec para TCP-Clear con host de marcación*



El perfil de ejemplo siguiente permite que el usuario que realiza la marcación utilice un perfil IPSec denominado `dialin` para establecer una conexión TCP-Clear segura con un host de inicio de sesión en 2.2.2.3.

```
dialin-user Password = "my-password"
  Service-Type = Login,
  Login-Service = TCP-Clear,
  Login-Host = 2.2.2.3,
  Login-TCP-Port = 23,
  Ascend-IPSEC-Profile = dialin
```

### *Ejemplo de una configuración ESP de IPSec para TCP-Clear*

En el ejemplo siguiente un administrador crea un perfil IPSec aplicando ESP de IPSec a los paquetes enviados por túnel a un gateway IPSec de seguridad y desde éste en la dirección IP 2.2.2.2:

```
admin> new ipsec securegw-1
IPSEC/securegw-1 read
admin> set active = yes
admin> set encap-mode = tunnel
admin> set tunnel-address = 2.2.2.2
```

En el conjunto de comandos siguiente, la configuración de envío de la unidad TAOS debe coincidir con los parámetros correspondientes en la configuración de recepción IPSec del gateway de seguridad del extremo distante, y viceversa:

```
admin> set send-esp active = yes
admin> set send-esp spi = 26990
admin> set send-esp version = 2
admin> set send-esp esp-type = des-cbc
admin> set send-esp key = 61083D2A76D57ABC
admin> set send-esp esp-version = 2
admin> set recv-esp active = yes
admin> set recv-esp spi = 26990
admin> set recv-esp version = 2
```

## Conexiones WAN

### Configuración de conexiones de marcación conmutadas

---

```
admin> set recv-esp esp-type = des-cbc
admin> set recv-esp key = 61083D2A76D57ABC
admin> set recv-esp esp-version = 2
admin> write
IPSEC/securegw-1 written
```

A continuación se muestran perfiles RADIUS de ejemplo que hacen referencia al perfil IPsec:

```
tcpapp1 Password = "secret-1"
    Service-Type = Login,
    Login-Service = TCP-Clear,
    Login-Host = 10.10.10.1,
    Login-TCP-Port = 23,
    Login-Host = 10.10.10.2,
    Login-TCP-Port = 125,
    Ascend-IPSEC-Profile = securegw-1

tcpapp2 Password = "secret-2"
    Service-Type = Login,
    Login-Service = TCP-Clear,
    Login-Host = 10.10.10.1,
    Login-TCP-Port = 23,
    Login-Host = 10.10.10.2,
    Login-TCP-Port = 125,
    Ascend-IPSEC-Profile = securegw-1

tcpapp3 Password = "secret-3"
    Service-Type = Login,
    Login-Service = TCP-Clear,
    Login-Host = 10.10.10.1,
    Login-TCP-Port = 23,
    Login-Host = 10.10.10.2,
    Login-TCP-Port = 125,
    Ascend-IPSEC-Profile = securegw-1
```

## Conexiones X.75

Los parámetros siguientes (que aparecen con los valores predeterminados) permiten el acceso de marcación al servidor de terminales desde adaptadores ISDN que utilizan el protocolo X.75. Los ajustes del perfil Answer-Defaults se aplican a las conexiones autenticadas mediante RADIUS.

```
[in ANSWER-DEFAULTS:x75-answer]
enabled = yes
k-frames-outstanding = 7
n2-retransmissions = 10
t1-retran-timer = 1000
frame-length = 1024

[in CONNECTION/":x75-options]
k-frames-outstanding = 7
n2-retransmissions = 10
```

```
t1-retran-timer = 1000
frame-length = 1024
```

Parámetro	Especifica
Enabled	Activa y desactiva X.75 en todo el sistema para las llamadas de entrada. X.75 está activado de manera predeterminada.
K-Frames-Outstanding	Número máximo de paquetes de datos que pueden estar en circulación en una conexión X.75 antes de que sea necesario el acuse de recibo. El rango válido se encuentra entre 2 y 7. El valor predeterminado es 7.
N2-Retransmissions	Límite de reintentos, que es el número máximo de veces que la unidad TAOS puede enviar una trama en una conexión X.75 antes de que alcance su límite el temporizador de retransmisiones T1. El rango válido se encuentra entre 2 y 10 (el valor predeterminado es 10). Dentro de este rango, un valor mayor aumenta la probabilidad de una transferencia correcta de los datos y un valor inferior permite la detección más rápida de una situación de error.
T1-Retran-Timer	Número máximo de ciclos de reloj que debe esperar el transmisor para obtener un acuse de recibo antes de iniciar un procedimiento de recuperación. El rango válido se encuentra entre 500 y 2000. El valor predeterminado es 1000 (1 segundo).
Frame-Length	Tamaño máximo de trama para el enlace. El valor predeterminado es 1024 bytes. La tarjeta HDLC puede dar soporte a un tamaño máximo de trama de 1532 bytes. La tarjeta Hybrid Access puede dar soporte a un máximo de 2048 bytes. En conexiones X.75 el valor máximo es de 2048 bytes.

Puede encontrar especificaciones técnicas completas para X.75 en la serie *CCITT Blue Book Recommendation X*, 1988. A continuación se muestra un ejemplo de configuración de un perfil Connection para X.75 cuando hay una tarjeta HDLC-2 instalada:

```
admin> new conn x75-user
CONNECTION/x75-user read

admin> set active = yes

admin> set ppp rcv-password = passwd

admin> set x75-options frame-length = 1532

admin> write
CONNECTION/x75-user written
```

## Configuración de conexiones permanentes y permanentes MP+

Una conexión permanente es un enlace permanente que siempre está activo y que dura el tiempo que existe la conexión física. Si se reinicia la unidad o el conmutador central, o si el enlace se desactiva, la unidad TAOS intenta restaurar el enlace a intervalos de diez segundos. Si la unidad TAOS o la unidad remota está apagada, el enlace vuelve a activarse cuando el dispositivo vuelve a arrancar.

Una línea no canalizada (como una WAN serie) puede utilizarse enteramente para una conexión permanente. En una línea ISDN, una conexión permanente utiliza uno o más canales que se han configurado para su utilización permanente y a los que se ha asignado un número de grupo. Todos los canales de un grupo se concentran en una unidad de ancho de banda indivisible y dedicada para la conexión que la utiliza. No es posible que más de una conexión comparta el mismo grupo de canales. Si se asigna más de un grupo a una conexión permanente, la suma de los canales en los diferentes grupos forma una unidad de ancho de banda agregada e indivisible.

## Conexiones permanentes

La mayoría de las conexiones permanentes utilizan los mismos ajustes que una conexión conmutada. Si se reinicia la unidad TAOS o el dispositivo del extremo distante, debe volverse a establecer la conexión permanente, generalmente con negociaciones similares a aquellas necesarias para establecer una conexión conmutada. En los subapartados siguientes se describen únicamente los parámetros exclusivos de las conexiones permanentes.

### Ajustes de un perfil Connection

Los parámetros siguientes del perfil Connection son pertinentes en una conexión permanente:

```
[in CONNECTION/""]
dial-number = ""

[in CONNECTION/"":session-options]
backup = ""

[in CONNECTION/"":telco-options]
answer-originate = ans-and-orig
call-type = off
nailed-groups = 0
```

Parámetro	Especifica
Dial-Number	Número que debe marcarse para esta conexión.
Backup	Nombre de un perfil que se utilizará si la conexión permanente se desactiva. Consulte el apartado “Interfaces de reserva para conexiones permanentes” en la página 1-39.
Answer-Originate	Activa y desactiva la emisión de la llamada para establecer la conexión permanente.
Call-Type	Tipo de llamada. Debe establecerse en FT1 para una conexión permanente.
Nailed-Groups	Números de grupo de los canales para la conexión. Puede especificar varios grupos separando los números con comas, en cuyo caso el ancho de banda será una suma de todos los grupos especificados. El ancho de banda permanente no puede compartirse con otras conexiones.

## *Ajustes de un perfil RADIUS*

Los pares atributo-valor de RADIUS siguientes son pertinentes en las conexiones permanentes:

<b>Atributo</b>	<b>Valor</b>
Ascend-Dial-Number (227)	Número que debe marcarse para esta conexión.
Ascend-Backup (176)	Nombre de un perfil que se utilizará si la conexión permanente se desactiva. Consulte el apartado “Interfaces de reserva para conexiones permanentes” en la página 1-39.
Ascend-Call-Type (177)	Tipo de llamada. Debe establecerse en Nailed (1) para una conexión permanente.
Ascend-Group (178)	Números de grupo de los canales dedicados a esta conexión. Puede especificar varios grupos separando los números con comas, en cuyo caso el ancho de banda de la conexión será una suma de todos los grupos especificados. El ancho de banda permanente no puede compartirse con otras conexiones.

Después de crear o modificar un perfil permanente en RADIUS, debe volver a cargar la información del servidor RADIUS. Con el comando siguiente se solicita una recarga de todos los perfiles permanentes (conexiones permanentes) del servidor RADIUS:

```
admin> refresh -n
```

En la versión actual del software, puede determinar el modo en que se gestionan las conexiones permanentes después de especificar Refresh -n. A continuación se muestra el parámetro correspondiente con el valor predeterminado:

```
[in SYSTEM]  
perm-conn-upd-mode = all
```

<b>Parámetro</b>	<b>Especifica</b>
Perm-Conn-Upd-Mode	Método para recargar conexiones permanentes: restablecer todas las conexiones permanentes después de especificar Refresh o restablecer sólo las conexiones permanentes cambiadas. Con el valor All (el valor predeterminado), el sistema se comporta como en versiones anteriores del software: todas las conexiones permanentes existentes se desactivan y, a continuación, se activan (junto con las conexiones nuevas) después de la actualización. Este ajuste provoca la interrupción del servicio cada vez que se actualiza o se agrega un perfil permanente. Con el valor Changed, sólo se crean conexiones nuevas y sólo se restablecen aquellas conexiones con valores de atributos modificados.

## Conexiones WAN

### Configuración de conexiones permanentes y permanentes MP+

---

A continuación se muestra un ejemplo de especificación del comando Refresh -n para que sólo descargue los perfiles cambiados:

```
admin> read system
SYSTEM read

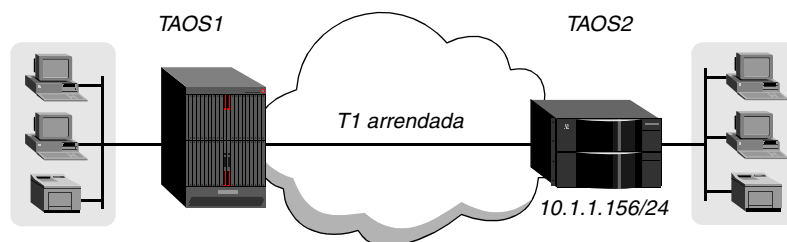
admin> set perm-conn-upd-mode = changed

admin> write
SYSTEM written
```

### Ejemplos de una conexión permanente

En la Figura 1-10 la unidad TAOS y la unidad MAX TNT™ se comunican mediante una línea T1 arrendada con todos los canales asignados al grupo 11.

Figura 1-10. Conexión permanente



El conjunto de comandos siguiente, en la unidad TAOS denominada TAOS1, configura un perfil local para la conexión permanente con TAOS2:

```
admin> new connection TAOS2
CONNECTION/TAOS2 read

admin> set active = yes

admin> set encapsulation-protocol = ppp

admin> set dial-number = 1212

admin> set ip remote-address = 10.1.2.156/24

admin> set ppp send-auth = chap-ppp-auth

admin> set ppp send-password = remotepw

admin> set telco answer-originate = originate-only

admin> set telco call-type = ft1

admin> set telco nailed-groups = 11

admin> write
CONNECTION/TAOS2 written
```

A continuación se muestra un perfil RADIUS equivalente:

```
permconn-TAOS1-1 Password = "ascend", Service-Type = Outbound-User
  User-Name = "TAOS2",
  Framed-Protocol = PPP,
  Framed-IP-Address = 10.1.2.156,
  Framed-IP-Netmask = 255.255.255.0,
  Ascend-Route-IP = Route-IP-Yes,
  Ascend-Call-Type = Nailed,
  Ascend-Group = "11",
  Ascend-Send-Auth = Send-Auth-CHAP,
```



```
Ascend-Send-Secret = "remotepw" ,  
Ascend-Dial-Number = "1212"
```

## Conexiones permanentes MP+

Una conexión que utiliza la encapsulación MP+ puede especificar un determinado número de canales permanentes como conexión básica y, a continuación, agregar los canales conmutados que sea necesario utilizando los algoritmos de DBA. Para obtener información detallada acerca de DBA, consulte el apartado “Conexiones del protocolo multienlace Plus (MP+)” en la página 1-19.

Una conexión *FT1-MPP* empieza como una conexión permanente, pero puede utilizar canales conmutados para aumentar el ancho de banda como sea necesario o para proporcionar una reserva si los canales permanentes se desactivan. El número máximo de canales para la conexión FT1-MPP es Maximum-Channel-Count para la conexión o el número de canales permanentes en el grupo especificado, el valor que sea mayor de los dos.

Los canales básicos de una conexión FT1-MPP son permanentes. Cuando un canal permanente está desactivado temporalmente, la unidad TAOS realiza sondeos continuamente mientras intenta restablecer la conexión. Si llega un paquete de salida mientras la conexión permanente está todavía desactivada, la unidad sustituye el canal permanente por un canal conmutado, aunque la llamada esté en línea con más del número mínimo de canales.

### Ajustes de un perfil Connection

Además de los parámetros MP+ que se describen en el apartado “Conexiones del protocolo multienlace Plus (MP+)” en la página 1-19, los parámetros siguientes son aplicables a una conexión FT1-MPP:

```
[in CONNECTION/"":telco-options]  
answer-originate = ans-and-orig  
call-type = off  
nailed-groups = 0  
ft1-caller = no
```

Parámetro	Especifica
Answer-Originate	Activa y desactiva la emisión de la llamada para establecer la conexión permanente. La combinación de los parámetros Answer-Originate y FT1-Caller especifica que la unidad TAOS es el emisor designado para la parte conmutada de la conexión.
Call-Type	Tipo de llamada. Debe establecerse en FT1-MPP para una conexión MP+.
Nailed-Groups	Números de grupo de los canales dedicados para la parte permanente de la conexión.
FT1-Caller	Activa y desactiva la emisión de la parte conmutada de la conexión. Puesto que se agrega ancho de banda según los cálculos realizados en ambos extremos de la conexión, sólo un extremo de la conexión puede emitir llamadas para FT1-MPP.

### *Ajustes de un perfil RADIUS*

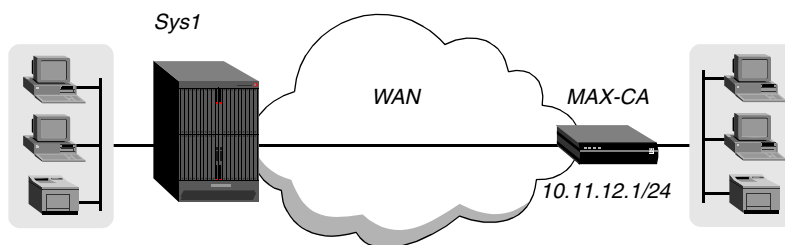
Además de los atributos MPP que se describen en el apartado “Conexiones del protocolo multienlace Plus (MP+)” en la página 1-19, RADIUS utiliza los pares atributo-valor siguientes para conexiones permanentes MP+:

Atributo	Valor
Ascend-Call-Type (177)	Tipo de llamada. Debe establecerse en Nailed/Mpp (2) para una conexión MP+.
Ascend-Group (178)	Números de grupo de los canales dedicados para la parte permanente de la conexión.
Ascend-FT1-Caller (175)	Activa y desactiva la emisión de la parte conmutada de la conexión. Especifique FT1-No (0) para esperar a que el extremo remoto inicie la llamada o FT1-Yes (1) para que la unidad TAOS realice la marcación para agregar canales. Sólo un extremo de la conexión puede ser el emisor FT1.

### *Ejemplos de una conexión permanente MP+*

En la Figura 1-11 la unidad TAOS establece una conexión permanente MP+ con una unidad Pipeline 25 mediante la WAN.

*Figura 1-11. Conexión utilizando ancho de banda permanente y conmutado*



Para que la conexión permanente MP+ utilice canales permanentes en los grupos 1 y 3, el perfil local debería configurarse de la manera siguiente:

```
admin> new connection MAX-CA
CONNECTION/MAX-CA read
admin> set active = yes
admin> set encapsulation-protocol = mpp
admin> set dial-number = 1212
admin> set ip remote-address = 10.11.12.1/24
admin> set ppp send-auth = chap-ppp-auth
admin> set ppp send-password = remotepw
admin> set mpp bandwidth-monitor-direction = transmit-recv
admin> set telco answer-originate = originate-only
admin> set telco ft1-caller = yes
admin> set telco call-type = ft1-mpp
admin> set telco nailed-groups = 1,3
```

```
admin> write
CONNECTION/MAX-CA written
```

**Nota:** Si modifica el perfil Connection para una conexión FT1-MP+ (ft1-mpp), la mayoría de los cambios se activará solamente después de desactivar la llamada y posteriormente activarla, dado que la conexión es principalmente permanente. Sin embargo, si agrega un número de grupo al ajuste del parámetro Nailed-Groups y graba el perfil modificado, los canales adicionales pasan a estar disponibles de forma inmediata.

A continuación se muestra un perfil RADIUS permanente equivalente:

```
permconn-sys1-1 Password = "ascend", Service-Type = Outbound-User
  User-Name = "MAX-CA",
  Framed-Protocol = MPP,
  Framed-IP-Address = 10.11.12.1,
  Framed-IP-Netmask = 255.255.255.0,
  Ascend-Route-IP = Route-IP-Yes,
  Ascend-Send-Auth = Send-Auth-CHAP,
  Ascend-Send-Secret = "remotepw",
  Ascend-Call-Type = Nailed/Mpp,
  Ascend-Group = "1,3",
  Ascend-FT1-Caller = FT1-Yes,
  Ascend-DBA-Monitor = DBA-Transmit-Recv,
  Ascend-Dial-Number = "1212"
```

## Interfaces de reserva para conexiones permanentes

El término *reserva* hace referencia a un conjunto de posibilidades de las que dispone el sistema para establecer y utilizar una conexión alternativa temporal con un destino cuando la conexión primaria no está disponible. Una conexión de reserva sustituye la conexión primaria, que debe ser una conexión permanente. La interfaz de reserva puede ser permanente o conmutada.

Cuando la unidad TAOS detecta que la interfaz primaria ha dejado de estar disponible, pone la interfaz primaria en un estado de reserva activa. No se eliminan las rutas de la interfaz primaria, sino que se desvía el tráfico de la interfaz primaria a la interfaz de reserva. Cuando la unidad detecta que la interfaz primaria está de nuevo disponible, desvía el tráfico a la interfaz primaria. Si la interfaz de reserva es una conexión conmutada, la unidad la desactiva.

Uno de los efectos secundarios de la interfaz de reserva de la capa del enlace de datos es que las rutas de una interfaz permanente nunca se desactivan cuando la interfaz permanente especifica una interfaz de reserva.

Puede especificar una interfaz de reserva para una conexión permanente en perfiles Connection o en RADIUS locales. No se da soporte a interfaces de reserva anidadas. El perfil de una interfaz de reserva no puede especificar otra interfaz de reserva. El perfil de una interfaz de reserva no hereda atributos, como filtros o cortafuegos, del perfil de la conexión permanente primaria.

#### Ajustes de un perfil Connection

El parámetro siguiente asigna una interfaz de reserva en el perfil Connection de la interfaz permanente primaria. Se muestra el valor predeterminado.

```
[in CONNECTION/" ":session-options]
backup = ""
```

Parámetro	Especifica
Backup	Nombre de un perfil Connection para la interfaz de reserva. Se especifica en el perfil de la interfaz permanente primaria.

#### Ajustes de un perfil RADIUS

En RADIUS un perfil Permconn es un perfil de pseudousuario cuya primera línea tiene el formato siguiente:

```
permconn-name-N Password="ascend", Service-Type = Outbound-User
```

El argumento *name* es el nombre de sistema de la unidad TAOS (especificado con el parámetro Name en el perfil System) y *N* es un número de una serie secuencial que empieza por 1. Asegúrese de que no faltan números en las series que especifica *N*. Si existe un espacio vacío en la secuencia de números, la unidad TAOS deja de recuperar los perfiles cuando encuentra dicho espacio.

Puede establecerse el atributo siguiente para especificar una interfaz de reserva para un perfil Permconn de pseudousuario:

Atributo	Valor
Ascend-Backup (176)	Nombre del perfil para la interfaz de reserva.

#### Ejemplos de una interfaz de reserva conmutada

En los perfiles de ejemplo siguientes, la interfaz primaria es una conexión permanente MP+ definida en un perfil denominado `nailed` y la interfaz de reserva es una conexión conmutada PPP definida en un perfil denominado `p7`. En este ejemplo, la dirección IP remota de las conexiones primaria y de reserva es la misma. Si desea ver otro ejemplo de interfaces de reserva que utilizan direcciones IP diferentes en las conexiones primaria y de reserva, ambas permanentes, consulte la publicación *Guía de configuración de relé de trama para APX 8000/MAX TNT/DSLNT*.

El conjunto de comandos siguiente define las interfaces primaria y de reserva en perfiles Connection locales:

```
admin> new conn nailed
CONNECTION/nailed read
admin> set active = yes
admin> set encaps = ppp
admin> set ppp send-auth-mode = pap-ppp-auth
admin> set ppp send-password = ascend
```

```

admin> set ppp rcv-password = ascend
admin> set telco ft1-caller = yes
admin> set telco nailed-groups = 111
admin> set ip remote-address = 10.168.7.9/24
admin> set session backup = p7
admin> write
CONNECTION/nailed written

admin> new conn p7
CONNECTION/p7 read

admin> set active = yes
admin> set encaps = mpp
admin> set dial-number = 55050
admin> set ppp send-auth-mode = pap-ppp-auth
admin> set ppp send-password = ascend
admin> set ppp rcv-password = ascend
admin> set ip remote-address = 10.168.7.9/24
admin> write
CONNECTION/pvc written

```

A continuación se muestran perfiles RADIUS:

```

permconn-taos1-1 Password = "ascend", Service-Type = Outbound-User
    User-Name = "nailed",
    Framed-IP-Address = 10.168.7.9,
    Framed-IP-Netmask = 255.255.255.0,
    Ascend-Route-IP = Route-IP-Yes,
    Ascend-Call-Type = Nailed,
    Ascend-Group = "111",
    Ascend-Send-Auth = Send-Auth-PAP,
    Ascend-Send-Secret = "ascend",
    Ascend-Backup = "p7"

route-taos-1 Password = "ascend", Service-Type = Outbound-User
    Framed-Route = "10.168.7.0/24 10.168.7.9 7 n p7"

p7 Password = "ascend", Service-Type = Outbound-User
    User-Name = "p7",
    Framed-Protocol = MPP,
    Ascend-Dial-Number = "55050",
    Framed-IP-Address = 10.168.7.9,
    Framed-IP-Netmask = 255.255.255.0,
    Ascend-Route-IP = Route-IP-Yes,
    Ascend-Send-Auth = Send-Auth-PAP,
    Ascend-Send-Passwd = "ascend",
    Ascend-Data-Svc = Switched-56K

```

## Conexiones WAN

### Configuración de conexiones de salida

---

Cuando la unidad TAOS activa la conexión permanente, en la tabla de ruteo se incluyen entradas como las siguientes:

```
...
10.1.7.0/24    10.1.7.9    wan44    rGT    60    1    0    543
10.1.7.0/24    10.1.7.9    wan44    *SG    120    7    0    681
10.1.7.9/32    10.1.7.9    wan44    rT     60    1    0    543
10.1.7.9/32    10.1.7.9    wan44    *S     120    7    2    681
...
```

Si la conexión permanente deja de estar disponible, se activa la conexión conmutada. En este caso, puesto que la dirección IP remota de las interfaces primaria y de reserva es la misma, no se produce ningún cambio en la tabla de ruteo (no se agregan ni se eliminan rutas).

El comando `Ifmgr` muestra la interfaz primaria en el estado de reserva activa (que se indica mediante un signo positivo), como se muestra en la siguiente salida de ejemplo:

```
bif slot sif u m p ifname      host-name  remote-addr  local-addr
-----
033 1:03 001 *   mp wan33      p7         10.1.7.9/32  11.1.6.234/32
044 1:17 000 +   p  wan44      nailed     10.1.7.9/32  11.1.6.234/32
```

Observe que `nailed` aparece con un signo positivo (+) para indicar que se encuentra en estado de reserva activa (que funciona con una conexión de reserva). Cuando la conexión permanente se activa de nuevo, la conexión conmutada se desactiva. En este momento, la salida del comando `Ifmgr` muestra la interfaz primaria en estado activo y la conexión de reserva en estado inactivo. Por ejemplo:

```
bif slot sif u m p ifname      host-name  remote-addr  local-addr
-----
033 1:17 000 -   mp wan33      p7         10.1.7.9/32  11.1.6.234/32
044 1:03 002 *   p  wan44      nailed     10.1.7.9/32  11.1.6.234/32
```

## Configuración de conexiones de salida

Generalmente la unidad TAOS inicia conexiones de salida de acuerdo con el ruteo de paquetes. Cuando recibe un paquete para reenviarlo a través de una interfaz de WAN y la conexión WAN no está activa, busca una ruta en la tabla de ruteo y realiza la marcación a la conexión de acuerdo con la entrada de ruteo. Si el perfil de la conexión no se encuentra en el sistema local, la ruta de la red remota debe especificar un perfil de llamada de salida, como se muestra en los ejemplos de RADIUS siguientes. El sistema puede buscar perfiles locales utilizando únicamente la dirección IP.

Otro tipo de llamada de salida se produce cuando se permite a los usuarios acceder a los módems digitales de la unidad TAOS para realizar la llamada de salida. Si desea obtener información detallada acerca de la capacidad de la llamada de salida de los módems, consulte el apartado “Conexiones de llamada de salida por módem” en la página 1-47.

## Acerca de los perfiles RADIUS de llamadas de salida

El nombre del perfil de llamadas de salida puede ser cualquier nombre que convenga (distinto al nombre utilizado para el perfil de llamadas de entrada), aunque el convenio especifica que debe utilizarse el nombre de llamada de entrada seguido de -out. A continuación se muestran dos perfiles de ejemplo de llamadas de entrada y de salida correspondientes:

```
joel Password = "localpw", Service-Type = Framed-User
    Framed-Protocol = PPP,
    Framed-IP-Address = 10.2.3.31,
    Framed-IP-Netmask = 255.255.255.0,
    Ascend-Link-Compression = Link-Comp-Stac

route-taos-1 Password = "ascend", Service-Type = Outbound-User
    Framed-Route = "10.2.3.0/24 10.2.3.31 1 n joel-out"

joel-out Password = "localpw", Service-Type = Outbound-User
    User-Name = "joel",
    Framed-Protocol = PPP,
    Framed-IP-Address = 10.2.3.31,
    Framed-IP-Netmask = 255.255.255.0,
    Ascend-Link-Compression = Link-Comp-Stac,
    Ascend-Dial-Number = "1212",
    Ascend-Send-Auth = Send-Auth-PAP,
    Ascend-Send-Secret = "remotepw"
```

En todos los perfiles RADIUS de llamadas de entrada se incluyen como mínimo un nombre de usuario y una contraseña. Cuando la unidad TAOS desea realizar una llamada de salida, utiliza el nombre y una contraseña conocida para recuperar el perfil de llamada de salida. Para eliminar la posibilidad de que alguien utilice la contraseña conocida y un perfil de llamada de salida para obtener acceso a la red, todos los perfiles de llamada de salida deben tener Service-Type establecido en Outbound-User. Este par atributo-valor impide que alguien utilice el perfil para la autenticación de entrada.

El atributo User-Name del perfil de llamadas de salida debe especificar el nombre del perfil de llamadas de entrada para evitar conflictos entre llamadas de entrada y de salida simultáneas para el mismo usuario. Se recomienda este procedimiento para evitar posibles problemas.

## Temporizador de llamadas de salida que se puede configurar

La unidad TAOS utiliza un temporizador de 20 segundos para establecer una llamada de salida. Si el extremo remoto no se conecta en este tiempo, el intento de llamada de salida fallará. Sin embargo, puede establecer el temporizador de llamadas de salida para proporcionar una mayor flexibilidad en llamadas internacionales. A continuación se muestra el parámetro pertinente con su ajuste predeterminado:

```
[in SYSTEM]
max-dialout-time = 20
```

Max-Dialout-Time especifica el número máximo de segundos durante el que el sistema espera un paquete Call Setup Complete del extremo remoto cuando realiza una llamada de salida. Los valores válidos se encuentran entre 0 y 255. El valor predeterminado es 20 segundos. Si el parámetro se establece en cero, la unidad TAOS utiliza el valor predeterminado interno de 20 segundos. En el ejemplo siguiente el temporizador de llamadas de salida se establece en 60 segundos:

```
admin> read system
SYSTEM read

admin> set max-dialout-time = 60

admin> write
SYSTEM written
```

**Nota:** El ajuste Max-Dialout-Time no influye en el tiempo de espera del módem para la detección de la portadora. Los módems poseen un temporizador interno que realiza una cuenta desde la llamada de salida hasta el establecimiento de la portadora con el módem remoto (incluida la preparación), cuyo valor predeterminado es de 45 segundos en los módems Rockwell.

## Perfiles de llamada de salida PPP y PPP multicanal

Es posible que algunos emisores no requieran la capacidad de realizar llamadas de salida en un perfil PPP, MP o MP+. La razón principal para proporcionar capacidad de realizar llamadas de salida es permitir que la unidad TAOS active la conexión para reenviar paquetes.

### Ajustes de un perfil Connection

Los parámetros siguientes del perfil Connection, que aparecen con los ajustes predeterminados, activan la llamada de salida en un perfil PPP o PPP multicanal:

```
[in CONNECTION/""]
dial-number = ""

[in CONNECTION/"":ppp-options]
send-auth -mode = no-ppp-auth
send-password = ""

[in CONNECTION/"":ip-options]
remote-address = 0.0.0.0/0
```

Parámetro	Especifica
Dial-Number	Número que debe marcarse para esta conexión.
Send-Auth-Mode	Protocolo de autenticación que se solicita cuando la unidad TAOS inicia la conexión. Consulte el apartado “Autenticación de la contraseña” en la página 1-14.
Send-Password	Contraseña que se envía al dispositivo remoto cuando la unidad TAOS inicia la conexión.
Remote-Address	Dirección IP del dispositivo remoto. La unidad TAOS activa la conexión para rutear paquetes de acuerdo con esta dirección.



## *Ajustes de un perfil RADIUS*

Si desea obtener información al respecto, consulte el apartado “Acerca de los perfiles RADIUS de llamadas de salida” en la página 1-43. Un perfil de usuario RADIUS puede incluir los pares atributo-valor siguientes para configurar una conexión PPP de llamadas de salida:

<b>Atributo</b>	<b>Valor</b>
Service-Type (6)	Tipo de servicio. Debe establecerse en Outbound-User en los perfiles de llamada de salida para evitar posibles problemas de seguridad.
User-Name (1)	Nombre del dispositivo remoto. En los perfiles de llamada de salida, especifique el nombre asignado al perfil de llamadas de entrada correspondiente para evitar conflictos si se producen conexiones de salida y entrada simultáneamente.
Ascend-Dial-Number (227)	Número que debe marcarse para esta conexión (un valor de tipo cadena).
Ascend-Send-Auth (231)	Protocolo de autenticación que debe utilizarse para una conexión de salida. Consulte el apartado “Autenticación de la contraseña” siguiente.
Ascend-Send-Secret (232)	Contraseña que se envía al dispositivo remoto cuando la unidad TAOS inicia la conexión. Si el perfil utiliza el atributo Ascend-Send-Passwd (232) para especificar la contraseña, el daemon RADIUS no realiza ningún cifrado antes de enviar la contraseña a NAS mediante la red. Para obtener más información, consulte el apartado “Secretos compartidos e intercambios seguros” en la página A-5.
Ascend-Remote-Addr (154)	Dirección IP del dispositivo remoto. La unidad TAOS activa la conexión para rutear paquetes de acuerdo con esta dirección.

## *Autenticación de la contraseña*

La autenticación PPP para llamadas de salida utiliza el ajuste del parámetro Send-Auth-Mode en un perfil local o el atributo Ascend-Send-Auth en un perfil RADIUS para determinar el protocolo que debe solicitarse del extremo distante. Puede especificar los protocolos siguientes:

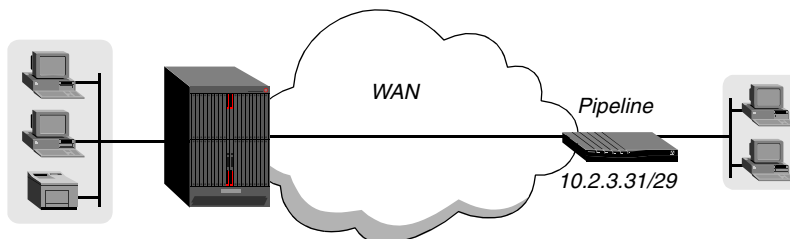
- Ninguno (la unidad TAOS no requiere la utilización de un protocolo concreto). Éste es el valor predeterminado, que se especifica como No-PPP-Auth en un perfil local o Send-Auth-None(0) en un perfil RADIUS.
- Protocolo de autenticación de contraseñas (PAP). La unidad TAOS requiere PAP, pero utiliza CHAP si el extremo distante así lo requiere. En un perfil local el ajuste es PAP-PPP-Auth. En un perfil RADIUS es Send-Auth-PAP (1).
- Protocolo de autenticación de establecimiento de enlace con desafío (CHAP). La unidad TAOS requiere la utilización de CHAP. En un perfil local el ajuste es CHAP-PPP-Auth. En un perfil RADIUS el ajuste es Send-Auth-CHAP (2).
- La extensión de Microsoft CHAP, utilizada en Windows NT/LAN Manager (MS-CHAP). En un perfil local el ajuste es MS-CHAP-PPP-Auth. En un perfil RADIUS el ajuste es Send-Auth-MS-CHAP (3).

Si desea obtener información detallada acerca de la autenticación de la contraseña en conexiones PPP, MP y MP+, consulte el Apéndice A, “Métodos de autenticación”.

### Ejemplos de una conexión PPP de llamadas de salida

En la Figura 1-12 el dispositivo del extremo distante es una unidad Pipeline con la dirección IP 10.2.3.31/29.

Figura 1-12. Conexión PPP de llamadas de salida



Los comandos siguientes crean un perfil que permite al sistema responder a llamadas de entrada o iniciar llamadas de salida hacia el extremo distante:

```
admin> new connection phani
CONNECTION/phani read

admin> set active = yes

admin> set encapsulation-protocol = ppp

admin> set dial-number = 1212

admin> set ip remote-address = 10.2.3.31/29

admin> set ppp send-auth-mode = chap-ppp-auth

admin> set ppp send-password = remotepw

admin> set ppp rcv-password = localpw

admin> write
CONNECTION/phani written
```

A continuación se muestran perfiles RADIUS equivalentes:

```
phani Password = "localpw"
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Framed-IP-Address = 10.2.3.31,
  Framed-IP-Netmask = 255.255.255.248

route-taos-1 Password = "ascend", Service-Type = Outbound-User
  Framed-Route = "10.2.3.0/29 10.2.3.31 1 n phani-out"

phani-out Password = "localpw", Service-Type = Outbound-User
  User-Name = "phani",
  Ascend-Dial-Number = "1212",
  Framed-Protocol = PPP,
  Framed-IP-Address = 10.2.3.31,
  Framed-IP-Netmask = 255.255.255.248,
  Ascend-Send-Auth = Send-Auth-PAP,
  Ascend-Send-Secret = "remotepw"
```

## Conexiones de llamada de salida por módem

Si se ha activado Direct-Access del módem en el perfil Terminal-Server, los usuarios pueden realizar llamadas de salida mediante los módems digitales de la unidad TAOS. El servicio Direct-Access utiliza el protocolo Telnet, en lugar de una conexión TCP de bajo nivel, para comunicarse con procesos cliente. Por lo tanto, cualquier proceso cliente que vaya a utilizar este servicio para transmitir o recibir datos binarios debe, como mínimo, generar una secuencia de escape para los caracteres IAC (0xFF), tratar los caracteres IAC entrantes en las secuencias de escape y descartar las opciones de Telnet entrantes. Para obtener una descripción del protocolo Telnet y saber en qué grado difiere de una conexión TCP de bajo nivel, consulte los documentos RFC 854 y 855.

### *Necesidad de reiniciar el sistema*

Después de configurar el sistema para que espere conexiones de llamadas de salida por módem en un puerto especificado, debe reiniciar el sistema para activar la característica.

### *Activación de Direct-Access del módem*

Puede activar el acceso directo para los módems de 56 K estableciendo los parámetros siguientes (que aparecen con los valores predeterminados):

```
[in TERMINAL-SERVER:dialout-configuration]
enabled = no
direct-access = no
port-for-direct-access = 5000
password-for-direct-access = ""
security-for-direct-access = none
```

**Nota:** Para activar el acceso de los módems, debe establecer los parámetros Enabled y Direct-Access en Yes en el perfil Terminal-Server.

Parámetro	Especifica
Enabled	Activa y desactiva cualquier tipo de llamada de salida por módem. Con el ajuste No, no se aplica ninguno de los demás parámetros en el subperfil Dialout-Configuration.
Direct-Access	Activa y desactiva la característica Direct-Access de las llamadas de salida. Con el ajuste Yes, los usuarios pueden iniciar una sesión Telnet con un puerto determinado de la unidad TAOS para obtener de inmediato servicio de llamada de salida. El número de puerto configurado como Port-for-Direct-Access indica a la unidad TAOS que todas las sesiones Telnet con ese puerto solicitan acceso a un módem. Con el ajuste No, no se aplican los parámetros restantes en el subperfil Dialout-Configuration.
Port-for-Direct-Access	Número de puerto TCP que debe utilizarse para un servicio de llamada de salida inmediato. Debe establecerse en un número entero entre 5000 (el valor predeterminado) y 32767 si se ha activado Direct-Access.
Password-for-Direct-Access	Contraseña (de 64 caracteres como máximo) que se utiliza para la autenticación de modo Global. Si Security-for-Direct-Access no se establece en Global, este parámetro se pasa por alto.

Parámetro	Especifica
Security-for-Direct-Access	<p>Seguridad por contraseña para Direct-Access. None (el valor predeterminado) significa que no es necesaria ninguna contraseña para acceder a los módems.</p> <p>Si este parámetro se establece en Global, una única contraseña global protege la utilización del módem. El parámetro Password-for-Direct-Access debe especificar la contraseña global. Cuando un usuario inicia una sesión Telnet con el puerto especificado, el sistema solicita el parámetro Password-for-Direct-Access asignado.</p> <p>Si el ajuste es User, un usuario debe tener un perfil de llamadas de salida que permita de forma específica las llamadas de salida por módem. En este caso, es necesario Recv-Password de PPP en el perfil del usuario para acceder a los módems de la unidad.</p>

### *Ejemplo de Direct-Access utilizando una contraseña global*

Los comandos siguientes definen las llamadas de salida Direct-Access en el puerto TCP 5028 con el ajuste de seguridad Global:

```
admin> read terminal-server
TERMINAL-SERVER read

admin> list dialout-configuration
enabled = no
direct-access = no
port-for-direct-access = 5000
password-for-direct-access = ""
security-for-direct-access = none

admin> set enabled = yes

admin> set direct-access = yes

admin> set port = 5028

admin> set password = pizza

admin> set security = global

admin> write
TERMINAL-SERVER written
```

Con esta configuración, un usuario realiza una llamada de salida en un módem de la manera que sigue:

- 1 Inicie una sesión Telnet en la unidad TAOS, especificando el número de puerto de Direct-Access en la línea de comandos. Por ejemplo:  
**telnet taos01 5028**
- 2 Cuando se solicite una contraseña, introduzca el valor de Password-for-Direct-Access.  
Password: **pizza**
- 3 Utilice los comandos AT estándar de Rockwell para realizar llamadas de salida en el módem, del mismo modo que utilizaría un módem conectado directamente al equipo. Por ejemplo:  
**ATDT 555-1212**

- 4 Para terminar la sesión con el módem, finalice la sesión Telnet.

### *Conexiones de llamadas de salida por módem que requieren perfiles*

Si establece Security-for-Direct-Access en User, un usuario debe tener un perfil de llamadas de salida que permita específicamente la llamada de salida por módem. En este caso, el ajuste Send-Password en el perfil del usuario protege la utilización del módem. Por ejemplo, si utiliza los ajustes siguientes:

```
[in TERMINAL-SERVER:dialout-configuration]
password-for-direct-access = ""
security-for-direct-access = user
```

Cuando un usuario inicia una sesión Telnet para Direct-Access, el sistema solicita un nombre de usuario y compara la entrada del usuario con un perfil Connection (o un perfil RADIUS). A continuación, autentica la sesión de llamadas de salida con la contraseña utilizando la contraseña del perfil.

### *Ajustes del perfil Connection*

A continuación se muestran los parámetros del perfil Connection relacionados con llamadas de salida Direct Access (aparecen con los valores predeterminados):

```
[in CONNECTION/":ppp-options]
recv-password = ""

[in CONNECTION/":telco-options]
dialout-allowed = no
```

Parámetro	Especifica
Recv-Password	Contraseña del usuario. El sistema solicita esta contraseña antes de permitir al usuario acceder a los módems.
Dialout-Allowed	Si el nombre de usuario y la contraseña coinciden, el sistema comprueba el ajuste Dialout-Allowed. Si el ajuste es Yes, el sistema proporciona acceso a uno de sus módems.

### *Ajustes del perfil RADIUS*

A continuación se muestran los atributos del perfil RADIUS relacionados con llamadas de salida Direct Access:

Atributo	Utilización para una llamada de salida Direct-Access
Password (2)	Contraseña del usuario. El sistema solicita esta contraseña antes de permitir al usuario acceder a los módems.
Ascend-Dialout-Allowed (131)	Si el nombre de usuario y la contraseña coinciden, el sistema comprueba este atributo. Si el ajuste es Dialout-Allowed (1), el sistema proporciona acceso a uno de sus módems.

### *Ejemplos de Direct-Access con seguridad de usuario*

Los comandos siguientes configuran llamadas de salida Direct-Access en el puerto TCP 5000 con el ajuste de seguridad User:

```
admin> read terminal-server
TERMINAL-SERVER read

admin> set dialout enabled = yes

admin> set dialout direct-access = yes

admin> set dialout security = user

admin> write
TERMINAL-SERVER written
```

El conjunto de comandos siguiente configura un perfil Connection para llamadas de salida:

```
admin> new connection kevin
CONNECTION/kevin read

admin> set ppp rcv-password = kpassword

admin> set telco dialout-allowed = yes

admin write
CONNECTION/kevin written
```

A continuación se muestra un perfil RADIUS equivalente:

```
kevin Password = "kpassword"
    Service-Type = Framed-User,
    Framed-Protocol = MPP,
    Ascend-Dialout-Allowed = Dialout-Allowed
```

Con esta configuración, el usuario llamado Kevin realiza una llamada de salida en un módem de la siguiente manera:

- 1 Especifica el número de puerto Direct-Access en la línea de comandos Telnet. Por ejemplo:  
**telnet taos01 5000**
- 2 Introduce el nombre de usuario en el indicador del sistema:  
User: **kevin**
- 3 Introduce la contraseña en el indicador del sistema:  
Password: **kpassword**
- 4 Utiliza los comandos estándar AT de Rockwell para realizar llamadas de salida en el módem, del mismo modo que utilizaría un módem conectado directamente a una estación de trabajo. Por ejemplo:  
**ATDT 555-1212**
- 5 Para terminar la sesión con el módem, finaliza la sesión Telnet.

Información general sobre el ruteo .....	2-1
Configuración de interfaces IP LAN .....	2-6
Configuración de interfaces IP WAN .....	2-12
Configuración de rutas IP estáticas .....	2-25
Definición de políticas de ruteo TCP/IP .....	2-39
Configuración de DNS .....	2-57
Configuración y utilización de agrupaciones de direcciones .....	2-68
Configuración del envío de difusión múltiple .....	2-80

## ***Información general sobre el ruteo***

Cuando se enciende o reinicia la unidad TAOS, ésta crea una tabla de ruteo IP que contiene todas las rutas que conoce, incluidas las siguientes:

- Rutas de interfaces IP activas locales (perfiles IP-Interface configurados)
- Rutas de conexiones IP WAN activas (conexiones conmutadas o permanentes que están activadas)
- Rutas de conexiones IP WAN conmutadas inactivas (perfiles Connection configurados)
- Rutas definidas en perfiles IP-Route o perfiles de ruta RADIUS

Si se han activado protocolos de ruteo dinámico en una o más interfaces, la unidad TAOS agrega rutas que obtiene de paquetes de actualización de ruteo. Además, realiza una actualización continua de la tabla de ruteo mediante la adición de rutas de enlaces que se vuelven activos y la eliminación de rutas de conexiones inactivas. Si una conexión permanente se desactiva, la unidad TAOS elimina la ruta de la tabla de ruteo.

## **Rutas e interfaces**

Una ruta IP especifica una dirección de destino, un gateway a la red y una interfaz que conduce al gateway. También puede especificar la métrica y otros valores asociados a la ruta.

Una ruta definida en un perfil es una *ruta estática*. Una *ruta dinámica* se obtiene a partir de las actualizaciones de RIP (Protocolo de información de ruteo) u OSPF (Emplear la trayectoria más corta primero) enviadas por otros ruteadores. Las actualizaciones dinámicas proporcionan acceso a muchas más rutas de las configuradas realmente en la unidad TAOS y se actualizan

automáticamente a medida que las rutas cambian. Sin embargo, producen una actividad de ruteo adicional, por lo que están desactivadas de manera predeterminada.

Una *interfaz* es un punto de entrada al sistema o de salida del sistema. Por ejemplo, una interfaz local es un puerto Ethernet y una interfaz WAN es una conexión permanente o conmutada. Una *interfaz IP* es la dirección IP lógica que permite enviar y recibir datos IP.

### Visualización de la tabla de ruteo

Para ver la tabla de ruteo, utilice el comando Netstat. Por ejemplo:

```
admin> netstat -r
```

Destination	Gateway	IF	Flg	Pref	Met	Use	Age
0.0.0.0/0	10.32.8.1	ie0	SGP	60	1	31460	1986
0.0.0.0/0	20.1.1.8	wan9	*SGP	60	8	0	0
10.4.5.0/24	10.4.5.6	wan12	SG	120	7	0	1978086
10.4.5.6/32	10.4.5.6	wan12	S	120	7	1	1978086
10.56.1.0/24	-	ie0-1	C	0	0	0	4504466
10.56.1.1/32	-	local	CP	0	0	0	4504466
127.0.0.0/8	-	bh0	CP	0	0	0	450446
127.0.0.1/32	-	local	CP	0	0	0	4504466
127.0.0.2/32	-	rj0	CP	0	0	0	4504466
10.32.8.0/24	-	ie0	C	0	0	7820	4504466
10.32.8.0/24	10.32.8.21	wan11	*SG	120	7	0	1978086
10.32.8.21/32	10.32.8.21	wan11	S	120	7	1	1978086
10.32.8.25/32	-	local	CP	0	0	47039	4504466
224.0.0.0/4	-	mcast	CP	0	0	0	4504466
224.0.0.1/32	-	local	CP	0	0	0	4504466
224.0.0.2/32	-	local	CP	0	0	0	4504466
224.0.0.5/32	-	local	CP	0	0	3158	4504466
224.0.0.6/32	-	local	CP	0	0	0	4504466
224.0.0.9/32	-	local	CP	0	0	14194	4504466
255.255.255.255/32	-	ie0	CP	0	0	0	4504466

Para cada ruta de la tabla, los campos Destination y Gateway muestran la dirección de destino y la dirección del ruteador del siguiente salto utilizado para llegar a dicho destino. La dirección de destino cero es la ruta predeterminada. Si el sistema no encuentra una ruta para el destino de un paquete, en lugar de descartar el paquete, lo envía a la ruta predeterminada. Observe que el sistema utiliza la ruta más específica (la que tiene un prefijo más largo) que coincida con un destino determinado. Las rutas directas no muestran una dirección de gateway.

Un asterisco (\*) en la columna Flg indica una ruta oculta; es decir, que no está incluida en las actualizaciones de ruteo que envía la unidad TAOS y no se utiliza para enviar paquetes. Las rutas ocultas se utilizan únicamente para la visualización.

El campo IF muestra el nombre de la interfaz a través de la cual se enviará un paquete dirigido al destino correspondiente a la entrada de la tabla. La ruta hacia el nombre de interfaz mcast encapsula el emisor de difusión múltiple para todo el espacio de direcciones de clase D. Para obtener más información, consulte “Configuración del envío de difusión múltiple” en la página 2-80.

Las rutas a la máquina local muestran el nombre de interfaz local. Los paquetes para las interfaces 224.0.0.1 y 224.0.0.2 pueden ser de difusión múltiple y pueden recibirse como paquetes de difusión múltiple normales, pero durante la recepción de un paquete de este tipo, el



ruteador no lo envía a otro dispositivo de capa de enlace. De hecho, estos paquetes tienen una MTU de 1.

OSPF utiliza 224.0.0.5 y 224.0.0.6 para las comunicaciones entre ruteadores (en lugar de utilizar difusiones generales, como hace RIP).

### *Visualización de la tabla de interfaces*

Para visualizar la tabla de interfaces, utilice la opción `-i` en la línea del comando `Netstat`:

```
admin> netstat -i
```

Name	MTU	Net/Dest	Address	Ipkts	Ierr	Opkts	Oerr
ie0	1500	10.32.8.0/24	10.32.8.25	1018339	1	622450	1
ie0-1	1500	10.56.1.0/24	10.56.1.1	0	0	0	0
lo0	1500	127.0.0.1/32	127.0.0.1	26622	0	26622	0
rj0	1500	127.0.0.2/32	127.0.0.2	0	0	0	0
bh0	1500	127.0.0.3/32	127.0.0.3	1	0	1	0
wanabe	1500	127.0.0.3/32	127.0.0.3	0	0	0	0
local	65535	127.0.0.1/32	127.0.0.1	233371	0	233371	0
mcast	65535	224.0.0.0/4	224.0.0.0	0	0	0	0
tunnel8	1500	10.32.8.0/24	10.32.8.25	0	0	0	0
vr0_main	1500	10.32.8.25/32	10.32.8.25	0	0	0	0
sip0	65535	-	-	0	0	0	0
wan11	1500	10.32.8.21	10.32.8.25	0	0	0	0
wan12	1500	10.4.5.6	10.32.8.25	0	0	0	0
wan13	1500	-	-	0	0	0	0
wan14	1500	-	-	0	0	0	0
ie1-15-1	1500	-	-	0	0	0	0
ie1-15-2	1500	-	-	0	0	0	0
ie1-15-3	1500	-	-	0	0	0	0
ie1-15-4	1500	-	-	0	0	0	0
ie1-15-1-1	1500	-	-	0	0	0	0
ie1-15-1-2	1500	-	-	0	0	0	0
ie1-15-1-3	1500	-	-	0	0	0	0

Las entradas denominadas `ie0` o `ieN-N-N[-N]` representan interfaces Ethernet. `N-N-N-N` representa el número de módulo, el número de ranura, el número de elemento y el número de elemento lógico de la interfaz. Si el número de elemento lógico es cero (la interfaz física), no aparece en el nombre de la interfaz. La misma secuencia de números forma la dirección utilizada para indexar el perfil IP-Interface. Por ejemplo, el perfil predeterminado para 1-4-1 se indexa del modo siguiente:

```
IP-INTERFACE { { 1 4 1 } 0 }
```

Cuando el número de elemento lógico *no* es cero, sí que aparece en el nombre de la interfaz. De nuevo, la secuencia de números es idéntica al índice del perfil. Por ejemplo, un perfil IP-Interface con el índice siguiente:

```
IP-INTERFACE { { 1 4 1 } 3 }
```

tiene el nombre de interfaz siguiente:

```
ie1-4-1-3
```

Los otros nombres de la tabla de interfaces, y su significado, son:

- La interfaz `lo0` (*loopback*) es la prueba de bucle local.

- Las interfaces `rj0` (*reject*) y `bh0` (*blackhole*) se utilizan en la función Pool-Summary.
- La interfaz `wanabe` es un perfil RADIUS de llamadas de salida inactivo.
- La interfaz `local` es la máquina local.
- La interfaz `mcast` es la interfaz de difusión múltiple, que representa el emisor de difusión múltiple para todo el espacio de direcciones de clase D. Para obtener más información, consulte “Configuración del envío de difusión múltiple” en la página 2-80.
- La interfaz `tunnel` es una pseudointerfaz que se utiliza sólo cuando la unidad TAOS está configurada como agente local de ruteador ATMP. En esta configuración la unidad TAOS crea una ruta para cada cliente móvil registrado. Independientemente del número de túneles que pueda finalizar el agente local, siempre hay una sola interfaz `tunnel` (el número que termina el nombre de interfaz `tunnel` es un número interno que puede variar de una versión de software a la siguiente).
- La interfaz `vr0_main` representa el propio ruteador. Para obtener información detallada, consulte el apartado “Configuración de ruteadores virtuales” en la página 6-1.
- La interfaz `sip0` es una interfaz IP lógica. Para obtener información detallada, consulte el apartado “Definición de una dirección IP de origen del sistema” en la página 2-39.
- Las interfaces WAN numeradas (`wanN`) son conexiones WAN que se introducen en la tabla de interfaces a medida que se vuelven activas.

## Sintaxis de las direcciones IP

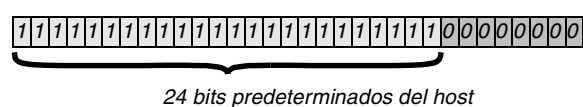
Una unidad TAOS utiliza el formato decimal con puntos (no hexadecimal) para las direcciones IP. Si no se especifica ninguna máscara de subred, la unidad adopta una máscara predeterminada basada en la clase de dirección. En la Tabla 2-1 se muestran las clases de direcciones y el número de bits de red de la máscara predeterminada para cada clase.

Tabla 2-1. Clases de direcciones IP y número de bits de red

Clase	Rango de direcciones	Bits de red predeterminados
Clase A	0.0.0.0–127.255.255.255	8
Clase B	128.0.0.0–191.255.255.255	16
Clase C	192.0.0.0–223.255.255.255	24

Por ejemplo, una dirección de clase C, como puede ser 198.5.248.40, tiene 24 bits de red, lo que deja 8 bits para la parte del host de la dirección. Si no se especifica ninguna máscara de subred para una dirección de clase C, la unidad TAOS adopta la máscara predeterminada de 24 bits, como se muestra en la Figura 2-1.

Figura 2-1. Máscara de subred predeterminada para direcciones IP de clase C



Una dirección de subred incluye una longitud de prefijo que especifica el número de bits de red de la dirección. Por ejemplo, en la siguiente dirección se especifica una subred de 29 bits:

ip-address = 198.5.248.40/29

En esta dirección, 29 bits de la dirección se utilizan para especificar la red. Los 3 bits restantes se utilizan para especificar hosts exclusivos de la subred. Gracias a los 3 bits que se utilizan para especificar hosts en una subred de 29 bits, se pueden obtener hasta 8 combinaciones diferentes de bits. De esas 8 direcciones de host posibles, dos están reservadas:

- 000 — Reservada para la red (dirección base)
- 001
- 010
- 100
- 110
- 101
- 011
- 111 — Reservada para la dirección de difusión general de la subred

**Nota:** Tenga cuidado con las subredes cero (subredes con la misma dirección base que una red de clase A, B o C). Las primeras implantaciones de TCP/IP no las permitían. Por ejemplo, la subred 192.32.8.0/30 no estaba permitida porque tenía la misma dirección base que la red de clase C 192.32.8.0/24, mientras que la subred 192.32.8.4/30 sí que estaba permitida. Las implantaciones más actuales de TCP/IP sí que admiten las subredes cero y la implantación de RIP por parte de unidad TAOS trata estas subredes igual que cualquier otra red. No obstante, es importante que maneje las subredes cero de manera coherente en toda la red. De lo contrario, se producirán problemas de ruteo.

En la Tabla 2-2 se muestran las máscaras de subred y las longitudes de los prefijos para un número de red de clase C.

*Tabla 2-2. Máscaras de subred decimales y longitudes de los prefijos*

Máscara de subred	Número de direcciones de host	Longitud de prefijo
255.255.255.0	254 de host + 1 de difusión, 1 de red base	/24
255.255.255.128	126 de host + 1 de difusión, 1 de red base	/25
255.255.255.192	62 de host + 1 de difusión, 1 de red base	/26
255.255.255.224	30 de host + 1 de difusión, 1 de red base	/27
255.255.255.240	14 de host + 1 de difusión, 1 de red base	/28
255.255.255.248	6 de host + 1 de difusión, 1 de red base	/29
255.255.255.252	2 de host + 1 de difusión, 1 de red base	/30
255.255.255.254	máscara no válida (sin hosts)	/31
255.255.255.255	1 host (una ruta de host)	/32

La dirección de difusión general de una subred tiene la parte del host de la dirección IP establecida en todo unos. La dirección de red (o dirección base) representa a la propia red

porque la parte del host de la dirección IP está constituida por todo ceros. Por ejemplo, si la configuración de unidad TAOS asigna la dirección siguiente a un ruteador remoto:

198.5.248.120/29

La red Ethernet conectada a ese ruteador dispone del siguiente rango de direcciones:

198.5.248.120 — 198.5.248.127

Una ruta de host es una dirección IP especial con una longitud de prefijo de /32. Por ejemplo:

198.5.248.40/32

Las rutas de host conducen a un host individual en lugar de a un ruteador o una subred.

## **Configuración de interfaces IP LAN**

Una interfaz IP LAN es un puerto Ethernet configurado para IP. Una unidad TAOS crea un perfil IP-Interface para un puerto Ethernet cuando detecta por primera vez la presencia del puerto. Por ejemplo, a continuación se muestran los perfiles IP-Interface predeterminados para el controlador del módulo y una tarjeta Ethernet-2 instalada en la ranura 12:

```
admin> dir ip-interface
 6  09/14/1999  10:13:24  { { any-shelf any-slot 0 } 0 }
 8  09/14/1999  10:13:24  { { shelf-1 left-controller 1 } 0 }
19  09/14/1999  10:14:02  { { shelf-1 right-controller 1 } 0 }
 8  09/14/1999  11:36:32  { { shelf-1 slot-12 2 } 0 }
 8  09/14/1999  11:36:32  { { shelf-1 slot-12 3 } 0 }
 8  09/14/1999  11:36:32  { { shelf-1 slot-12 4 } 0 }
64  09/14/1999  11:53:12  { { shelf-1 slot-12 1 } 0 }
```

El perfil para el primer puerto Ethernet de una tarjeta en el módulo 1, ranura 12, utiliza el índice siguiente:

```
{ { 1 12 1 } 0 }
```

Este índice consiste en una dirección física y un número de elemento lógico con el formato siguiente:

```
{ { shelf-num slot-num item-num } logical-item-num }
```

El elemento lógico hace referencia a una interfaz lógica específica. Su valor es cero excepto cuando se han configurado varias interfaces (virtuales) en el puerto físico. Para obtener información detallada, consulte el apartado “Ejemplo de definición de interfaces LAN virtuales” en la página 2-9.

## **Información general sobre los ajustes de una interfaz LAN**

A continuación se muestran los parámetros de un perfil IP-Interface, con los ajustes predeterminados:

```
[in IP-INTERFACE/{ { any-shelf any-slot 0 } 0 } ]
interface-address* = { { any-shelf any-slot 0 } 0 }
ip-address = 0.0.0.0/0
proxy-mode = Off
rip-mode = routing-off
route-filter = ""
```

```
rip2-use-multicast = yes
ospf = { no 0.0.0.0 normal 10 40 5 simple ***** 0 1 16777215 type-1+
multicast-allowed = no
multicast-rate-limit = 100
multicast-group-leave-delay = 0
directed-broadcast-allowed = yes
vrouter = ""
management-only = no
```

Parámetro	Especifica
Interface-Address	Dirección del módulo de la interfaz Ethernet o, si el número de elemento no es cero, dirección de la interfaz virtual.
IP-Address	Dirección IP de la interfaz LAN.
Proxy-Mode	Activa y desactiva respuestas ARP de proxy para dispositivos de llamada de entrada que tienen direcciones locales asignadas.
RIP-Mode	Activa y desactiva las actualizaciones de RIP en la interfaz. De manera predeterminada, RIP está desactivado en las interfaces LAN.
Route-Filter	Filtro para paquetes de actualización de RIP. Si desea obtener información detallada, consulte el Capítulo 9, “Filtros de paquetes”.
RIP2-Use-Multicast	Activa y desactiva la utilización de la dirección de difusión múltiple (224.0.0.9), en lugar de la dirección de difusión general, para las actualizaciones de RIP. De manera predeterminada, las actualizaciones de RIP utilizan la dirección de difusión múltiple.
OSPF	Opciones de ruteo OSPF. Consulte el apartado “Adición de una unidad TAOS a una red OSPF” en la página 3-10.
Multicast-Allowed	Opción de envío de difusión múltiple. Consulte el apartado “Configuración del envío de difusión múltiple” en la página 2-80.
Multicast-Rate-Limit	Opción de envío de difusión múltiple. Consulte el apartado “Configuración del envío de difusión múltiple” en la página 2-80.
Multicast-Group-Leave-Delay	Opción de envío de difusión múltiple. Consulte el apartado “Configuración del envío de difusión múltiple” en la página 2-80.
Directed-Broadcast-Allowed	Activa y desactiva el envío de tráfico de difusión general dirigido en la interfaz y su red.
VRouter	Nombre de un ruteador virtual. Consulte el apartado “Asignación de interfaces a un ruteador virtual” en la página 6-7.
Management-Only-Interface	Activa y desactiva la opción de sólo gestión en la interfaz IP.

## Ejemplo de configuración de una interfaz IP LAN

Los comandos siguientes establecen la dirección IP del puerto Ethernet situado más a la izquierda del controlador de módulo:

```
admin> dir ip-interface
      6  09/14/1999  10:13:24  { { any-shelf any-slot 0 } 0 }
```

```

      8  09/14/1999  10:13:24  { { shelf-1 left-controller 1 } 0 }
     19  09/14/1999  10:14:02  { { shelf-1 right-controller 1 } 0 }
admin> read ip-interface { { 1 41 1 } 0}
IP-INTERFACE/{ { shelf-1 left-controller 1 } 0 } read
admin> set ip-address = 10.1.2.65/24
admin> write
IP-INTERFACE/{ { shelf-1 left-controller 1 } 0 } written

```

En este ejemplo, la unidad TAOS reside en la subred 10.1.2. Para que se pueda comunicar con routers de otras subredes locales, bien debe tener una configuración de ruta estática hacia otro router de su propia subred, o bien debe activar RIP. Para ver un ejemplo de la configuración de una ruta hacia un router local, consulte “Ejemplos de configuración de rutas predeterminadas” en la página 2-29.

Después de asignar una dirección IP, puede verificar si la unidad TAOS es un host IP válido en ese segmento de red ejecutando Ping para otro host, como se muestra en el ejemplo siguiente:

```

admin> ping 10.65.212.19
PING 10.65.212.19: 56 Data bytes
64 bytes from 10.65.212.19: icmp_seq=0 ttl=255 time=0 ms
64 bytes from 10.65.212.19: icmp_seq=3 ttl=255 time=0 ms
^C
--- 10.65.212.19: Ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms

```

### *Activación de ARP de proxy*

Si activa ARP de proxy, los hosts de la red local pueden realizar peticiones ARP en los hosts o subredes que residen en la WAN, pero que tienen una dirección IP en la red local. La unidad TAOS responde a las peticiones ARP y, a continuación, rutea los paquetes para dichas conexiones en la WAN.

Puede activar Proxy-Mode estableciéndolo en Active (responder sólo para conexiones WAN activas), Inactive (responder sólo para conexiones WAN inactivas) o Always (responder para todas las direcciones de la agrupación, incluidas las de conexiones inactivas). Si la unidad TAOS está configurada para que responda a peticiones ARP para conexiones inactivas, ésta activa la conexión WAN necesaria.

Los comandos siguientes configuran ambas interfaces LAN del controlador del módulo en una unidad TAOS para responder como servidores proxy a peticiones ARP de conexiones WAN activas:

```

admin> read ip-interface { { 1 41 1 } 0}
IP-INTERFACE/{ { shelf-1 left-controller 1 } 0 } read
admin> set proxy-mode = active
admin> write
IP-INTERFACE/{ { shelf-1 left-controller 1 } 0 } written
admin> read ip-interface { { 1 42 1 } 0}
IP-INTERFACE/{ { shelf-1 right-controller 1 } 0 } read
admin> set proxy-mode = active
admin> write
IP-INTERFACE/{ { shelf-1 right-controller 1 } 0 } written

```

En este caso, si se produce el cese y relevo del controlador, el sistema puede continuar respondiendo a peticiones ARP.

## *Activación de RIP*

De manera predeterminada, RIP está desactivado, de modo que una unidad TAOS no envía su tabla de ruteo ni recibe información de ruteo de otros ruteadores de la interfaz. Por lo tanto, los hosts locales de otras subredes no pueden acceder a hosts remotos sin configuraciones de ruta estática y los hosts de llamada de entrada no tienen acceso a otras rutas mantenidas localmente.

Puede activar RIP para recibir actualizaciones de tablas de ruteo, enviarlas o ambas cosas. La recepción de actualizaciones de otros ruteadores hace aumentar el tamaño de la tabla de ruteo de la unidad TAOS. En este caso, la tabla proporciona acceso a más redes, pero las búsquedas de rutas no son tan rápidas. El envío de actualizaciones propaga información sobre redes remotas a ruteadores locales.

**Nota:** No se recomienda ejecutar RIP-v2 y RIP-v1 en la misma red de forma que los ruteadores reciban anuncios los unos de los otros. RIP-v1 realiza una estimación aproximada de las máscaras de subred, mientras que RIP-v2 las trata de forma explícita. Si se ejecutan las dos versiones en la misma red, se puede hacer que las estimaciones de RIP-v1 anulen la información precisa sobre la subred obtenida a través de RIP-v2.

Los comandos siguientes configuran una unidad TAOS para que reciba actualizaciones de RIP-v2 en la dirección de difusión múltiple:

```
admin> read ip-interface { { 1 41 1 } 0 }
IP-INTERFACE/{ { shelf-1 left-controller 1 } 0 } read
admin> set rip-mode = routing-recv-v2
admin> write
IP-INTERFACE/{ { shelf-1 left-controller 1 } 0 } written
admin> read ip-interface { { 1 42 1 } 0 }
IP-INTERFACE/{ { shelf-1 right-controller 1 } 0 } read
admin> set rip-mode = routing-recv-v2
admin> write
IP-INTERFACE/{ { shelf-1 right-controller 1 } 0 } written
```

## **Ejemplo de definición de interfaces LAN virtuales**

Puede configurar hasta 16 perfiles IP-Interface para cada tarjeta Ethernet como un todo global, con una dirección IP especificada para cada uno de ellos. El sistema crea el perfil predeterminado para una interfaz y le asigna el número de elemento lógico cero. Para configurar otra dirección IP en una interfaz LAN, debe crear un perfil IP-Interface con un número de elemento lógico que no sea cero en su dirección de interfaz. Por ejemplo, los comandos siguientes crean una interfaz virtual para un puerto Ethernet instalado en el módulo 1, ranura 12:

```
admin> new ip-int { {1 12 1 } 1 }
IP-INTERFACE/{ { shelf-1 slot-12 1 } 1 } read
admin> set ip-addr = 10.9.1.212/24
admin> write
IP-INTERFACE/{ { shelf-1 slot-12 1 } 1 } written
```

No es necesario que los números de elemento lógico sean consecutivos, pero sí que deben ser exclusivos. Las restricciones siguientes se aplican a interfaces LAN virtuales:

- El perfil IP-Interface predeterminado (con el número de elemento lógico cero) debe tener una dirección IP configurada, ya que de lo contrario no funcionará ninguno de los demás perfiles IP-Interface del mismo puerto. Si suprime el perfil predeterminado, no espere que las demás configuraciones funcionen.
- Si Proxy-Mode está activo en cualquiera de los perfiles IP-Interface para un puerto Ethernet determinado, estará activo para todas las peticiones ARP que lleguen al puerto físico.
- Puede activarse OSPF en cualquiera de las interfaces IP de un puerto, pero no en más de una interfaz del mismo puerto. Esta restricción está en conformidad con el documento RFC 1583.

## Ejemplo de definición de la interfaz software

Una unidad TAOS admite una interfaz IP software, que es una interfaz interna que nunca se desactiva. Por lo tanto, siempre que una de las interfaces IP de la unidad esté activa, se podrá acceder a la dirección de la interfaz software.

**Nota:** No utilice la dirección IP de una interfaz LAN física para la dirección de interfaz software.

El perfil IP-Interface con índice cero está reservado para la interfaz software. Si se ha activado RIP, la unidad anuncia la dirección de la interfaz como si fuera una ruta de host (con una longitud de prefijo de 32 bits) mediante la interfaz de prueba de bucle. Si no se ha activado RIP, los ruteadores que se encuentren a un salto de distancia de la unidad deben disponer de una ruta estática que conduzca a la dirección de interfaz software.

Los comandos siguientes establecen la dirección IP de la interfaz software en 1.1.1.128/24:

```
admin> read ip-interface { 0 0 0 }
IP-INTERFACE/{ { any-shelf any-slot 0 } 0 } read

admin> set ip-addr = 1.1.1.128/24

admin> write
IP-INTERFACE/{ { any-shelf any-slot 0 } 0 } written
```

Si desea crear una dirección independiente de la interfaz para un VRouter, cree un nuevo perfil IP-Interface con un valor de elemento lógico mayor que cero. Por ejemplo:

```
admin> new ip-interface
IP-INTERFACE/{ { any-shelf any-slot 0 } 0 } read

admin> set interface-address = { { 0 0 0 } 1 }
(New index value; will save profile as IP-INTERFACE/{ { any-shelf any-
slot 0 } 1 }.)

admin> set ip-addr = 10.10.1.1

admin> write
IP-INTERFACE/{ { any-shelf any-slot 0 } 1 } written
```

La unidad TAOS agrega la dirección de software a su tabla de interfaces con el nombre sip#, donde # es el número de elemento lógico procedente del índice del perfil IP-Interface. Para



obtener información detallada acerca de los ruteadores virtuales, consulte “Asignación de interfaces a un ruteador virtual” en la página 6-7.

Si se han activado las actualizaciones de ruteo (RIP u OSPF), una unidad TAOS anunciará la dirección de interfaz como una ruta de host con una máscara de /32 mediante la interfaz de prueba de bucle. Si no se han activado RIP ni OSPF, los ruteadores que se encuentren a un salto de distancia de la unidad TAOS deberán disponer de una ruta estática a la dirección de software. Para verificar si los demás hosts de la red tienen una ruta a la dirección de software, ejecute Ping o Traceroute desde los otros hosts. Por ejemplo:

```
host1% ping 11.168.7.100
PING 11.168.7.100 (11.168.7.100): 56 Data bytes
64 bytes from 11.168.7.100: icmp_seq=0 ttl=255 time=0 ms
64 bytes from 11.168.7.100: icmp_seq=7 ttl=255 time=0 ms
^C
--- 11.168.7.100 Ping statistics ---
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

## Ejemplo de desactivación de difusiones generales dirigidas

Los ataques de denegación de servicio, conocidos en inglés como ataques “*smurf*”, suelen utilizar paquetes de petición de eco ICMP con una dirección de origen falsa y paquetes dirigidos a direcciones IP de difusión general. Estos ataques van dirigidos a mermar el rendimiento de la red, posiblemente hasta el punto de dejarla inutilizable.

Para evitar la utilización del ruteador TAOS como intermediario en este tipo de ataque lanzado desde otra red, debe desactivar para el ruteador TAOS el envío de las difusiones generales dirigidas que recibe de otra red. En el ejemplo siguiente se muestra cómo desactivar difusiones generales dirigidas que no se generan localmente. Todas las interfaces IP del sistema deben desactivar esta función de forma explícita. Los comandos del ejemplo configuran tanto las interfaces del controlador del módulo (de modo que las difusiones generales sigan desactivadas en caso de producirse el cese y relevo del controlador) como las interfaces IP de una tarjeta Ethernet de cuatro puertos en el módulo 1, ranura 12.

```
admin> read ip-int { { 1 41 1 } 0 }
IP-INTERFACE/{ { shelf-1 left-controller 1 } 0 } read

admin> set directed-broadcast-allowed = no

admin> write
IP-INTERFACE/{ { shelf-1 left-controller 1 } 0 } written

admin> read ip-int { { 1 42 1 } 0 }
IP-INTERFACE/{ { shelf-1 right-controller 1 } 0 } read

admin> set directed-broadcast-allowed = no

admin> write
IP-INTERFACE/{ { shelf-1 right-controller 1 } 0 } written

admin> read ip-int { { 1 12 1 } 0 }
IP-INTERFACE/{ { shelf-1 slot-12 1 } 0 } read

admin> set directed-broadcast-allowed = no

admin> write
IP-INTERFACE/{ { shelf-1 slot-12 1 } 0 } written
```

```
admin> read ip-int {{1 12 2} 0}
IP-INTERFACE/{ { shelf-1 slot-12 2 } 0 } read

admin> set directed-broadcast-allowed = no

admin> write
IP-INTERFACE/{ { shelf-1 slot-12 2 } 0 } written

admin> read ip-int {{1 12 3} 0}
IP-INTERFACE/{ { shelf-1 slot-12 3 } 0 } read

admin> set directed-broadcast-allowed = no

admin> write
IP-INTERFACE/{ { shelf-1 slot-12 3 } 0 } written

admin> read ip-int {{1 12 4} 0}
IP-INTERFACE/{ { shelf-1 slot-12 4 } 0 } read

admin> set directed-broadcast-allowed = no

admin> write
IP-INTERFACE/{ { shelf-1 slot-12 4 } 0 } written
```

## **Ejemplo de definición de una interfaz de sólo gestión**

*De sólo gestión* significa que el tráfico de entrada de la interfaz termina en el propio sistema. No se reenvía el tráfico a ninguna otra interfaz. Además, únicamente el tráfico generado por el sistema se reenvía a la interfaz de sólo gestión. El tráfico generado externamente se descarta en la interfaz. Si se establece el parámetro Management-Only en Yes, se aplican estas condiciones en el puerto.

Los comandos siguientes especifican que un puerto de una tarjeta instalada es una interfaz de sólo gestión:

```
admin> read ip-int {{ 1 12 1 } 0}
IP-INTERFACE/{ { shelf-1 slot-12 1 } 0 } read

admin> set management-only = yes

admin> write
IP-INTERFACE/{ { shelf-1 slot-12 1 } 0 } written
```

El comando `Ifmgr -d` muestra un campo Management Only para reflejar el estado del puerto.

## **Configuración de interfaces IP WAN**

Una interfaz IP WAN es una conexión permanente o conmutada configurada para IP. Una unidad TAOS crea una interfaz de ruteo para perfiles Connection locales (si no utilizan direcciones de la agrupación) cuando el sistema arranca. Para las interfaces que utilizan direcciones de la agrupación o que están definidas en perfiles de usuario RADIUS, la unidad crea una interfaz de ruteo al activarse una sesión.

## **Información general sobre los ajustes de una interfaz WAN**

Las interfaces IP WAN se configuran en perfiles Connection o RADIUS. Como mínimo, cada perfil especifica la dirección IP del dispositivo de extremo distante o una agrupación a partir de

la cual el sistema asigna una dirección. También puede establecer diversos parámetros de servicio y ruteo.

### *Ajustes de los perfiles Connection*

A continuación se muestran las opciones IP (que aparecen con los ajustes predeterminados) de un perfil Connection:

```
[in CONNECTION/"":ip-options]
ip-routing-enabled = yes
vj-header-prediction = yes
remote-address = 0.0.0.0/0
local-address = 0.0.0.0/0
routing-metric = 1
preference = 60
down-preference = 120
private-route = no
multicast-allowed = no
address-pool = 0
ip-direct = 0.0.0.0
rip = routing-off
route-filter = ""
source-ip-check = no
ospf-options = { no 0.0.0.0 normal 30 120 5 simple ***** 10 1000 +
multicast-rate-limit = 100
multicast-group-leave-delay = 0
client-dns-primary-addr = 0.0.0.0
client-dns-secondary-addr = 0.0.0.0
client-dns-addr-assign = yes
client-default-gateway = 0.0.0.0

[in CONNECTION/"":ip-options:tos-options]
active = no
precedence = 000
type-of-service = normal
apply-to = input
```

Parámetro	Especifica
IP-Routing-Enabled	Activa y desactiva el ruteo IP de la interfaz. De manera predeterminada, el ruteo IP está activo.
VJ-Header-Prediction	Activa y desactiva la predicción Van Jacobsen para paquetes TCP en las llamadas de entrada mediante protocolos de encapsulación que admiten la compresión Van Jacobsen. El ajuste predeterminado es Yes.
Remote-Address	Dirección IP del dispositivo llamador, en que puede incluirse una especificación de subred. Si en la dirección no se incluye una máscara de subred, el ruteador adopta la máscara de subred predeterminada en función de la clase de dirección.
Local-Address	Dirección IP asignada al lado local de una conexión de interfaz numerada. Si desea obtener información detallada, consulte “Ejemplos de una conexión de interfaz numerada” en la página 2-20.

<b>Parámetro</b>	<b>Especifica</b>
Routing-Metric	Métrica RIP para la ruta especificada (un número del 1 al 15, donde 1 es el ajuste predeterminado). Si los valores de preferencia son iguales, cuanto más alta sea la métrica, menos probabilidades habrá de que la unidad TAOS utilice esta ruta.
Preference	Valor de preferencia para la ruta. Los valores validos se encuentran entre 0 y 255. Para obtener más información, consulte el apartado “Definición de preferencias de ruta estática” en la página 2-45.
Down-Preference	Valor de preferencia para la ruta cuando la interfaz está inactiva.
Private-Route	Activa y desactiva el anuncio de la ruta cuando el ruteador envía actualizaciones de RIP u OSPF. Con el ajuste Yes, la ruta queda excluida de los paquetes de actualización.
Multicast-Allowed	Consulte el apartado “Configuración del envío de difusión múltiple” en la página 2-80.
Address-Pool	Número de la agrupación de direcciones a partir del cual se obtiene una dirección (consulte “Configuración y utilización de agrupaciones de direcciones” en la página 2-68).
IP-Direct	Dirección IP de un host al que se dirigirán todos los paquetes IP recibidos en el enlace (consulte “Ejemplos de una conexión IP-Direct” en la página 2-21).
RIP	Activa y desactiva las actualizaciones de RIP en la interfaz. De manera predeterminada, RIP está desactivado.
Route-Filter	Filtro para paquetes de actualización de RIP. Si desea obtener información detallada, consulte el Capítulo 9, “Filtros de paquetes”.
Source-IP-Check	Activa y desactiva la protección frente a engaños para la sesión. Con el ajuste Yes, el sistema no acepta paquetes que no se originen en la subred a la que está conectado el dispositivo remoto. El sistema determina la subred durante la negociación IPCP. Si Remote-Address especifica una subred, se aceptarán los paquetes que se originen en dicha subred. Si Remote-Address especifica una máscara de 32 bits, sólo se aceptarán los paquetes procedentes de este host. Los paquetes enviados desde una dirección que no coincida se descartarán.
OSPF-Options	Opciones de ruteo OSPF (consulte el Capítulo 3, “Ruteo OSPF”).
Multicast-Rate-Limit	Opción de envío de difusión múltiple (consulte el apartado “Configuración del envío de difusión múltiple” en la página 2-80).
Multicast-Group-Leave-Delay	Opción de envío de difusión múltiple (consulte el apartado “Configuración del envío de difusión múltiple” en la página 2-80).
Client-DNS-Primary-Addr	Opción de DNS de cliente (consulte el apartado “Utilización del DNS de cliente” en la página 2-63).
Client-DNS-Secondary-Addr	Opción de DNS de cliente (consulte el apartado “Utilización del DNS de cliente” en la página 2-63).
Client-DNS-Addr-Assign	Opción de DNS de cliente (consulte el apartado “Utilización del DNS de cliente” en la página 2-63).

<b>Parámetro</b>	<b>Especifica</b>
Client-Default-Gateway	Ruta predeterminada para el tráfico procedente de esta conexión. Para obtener información detallada, consulte el apartado “Ejemplos de gateways predeterminados de cliente” en la página 2-23.
TOS-Options:Active	Activa y desactiva proxy-QoS y TOS para esta conexión (consulte el apartado “Ejemplos de definición de la política QoS y TOS” en la página 2-24).
TOS-Options:Precedence	Nivel de prioridad de la corriente de datos. Los tres bits más significativos del byte TOS son bits de prioridad utilizados para determinar la prioridad para la puesta en cola por prioridades. Si TOS está activo, puede establecer los bits en uno de los valores siguientes (el bit más significativo en primer lugar): <ul style="list-style-type: none"> <li>• 000: Prioridad normal</li> <li>• 001: Nivel de prioridad 1</li> <li>• 010: Nivel de prioridad 2</li> <li>• 011: Nivel de prioridad 3</li> <li>• 100: Nivel de prioridad 4</li> <li>• 101: Nivel de prioridad 5</li> <li>• 110: Nivel de prioridad 6</li> <li>• 111: Nivel de prioridad 7 (la prioridad más alta)</li> </ul>
TOS-Options:Type-of-Service	Tipo de servicio de la corriente de datos. Los cuatro bits siguientes del byte TOS se utilizan para elegir un enlace en función del tipo de servicio. Si TOS está activo, Type-of-Service puede especificar Normal (servicio normal), Cost (minimizar coste económico), Reliability (maximizar fiabilidad), Throughput (maximizar rendimiento), Latency (minimizar retardo).
TOS-Options:Apply-To	Dirección en la que se ha activado TOS. Con el ajuste Input (el ajuste predeterminado), los bits se establecen en paquetes recibidos en la interfaz. Con el ajuste Output, los bits se establecen únicamente en paquetes de salida. Con el ajuste Both, se etiquetan tanto los paquetes de entrada como los de salida.

## Ajustes de los perfiles RADIUS

Los pares atributo-valor siguientes configuran opciones IP en un perfil RADIUS:

<b>Atributo</b>	<b>Valor</b>
Ascend-Route-IP (228)	Activa y desactiva el ruteo IP de la interfaz. De manera predeterminada, el ruteo IP está activo.
Framed-Compression (13)	Activa y desactiva la predicción Van Jacobsen. Puede especificar Van-Jacobson-TCP-IP para activar la compresión de cabeceras TCP/IP. Si no especifica este valor, RADIUS utiliza la opción predeterminada, que es sin compresión de cabeceras.
Framed-IP-Address (8)	Dirección IP del dispositivo llamador.

<b>Atributo</b>	<b>Valor</b>
Framed-IP-Netmask (9)	Máscara de subred de la dirección del emisor. Si no especifica una máscara de subred, el ruteador adopta la máscara de subred predeterminada en función de la clase de dirección.
Ascend-PPP-Address (253)	Dirección IP asignada al lado local de una conexión de interfaz numerada. Para obtener información detallada, consulte el apartado “Ejemplos de una conexión de interfaz numerada” en la página 2-20.
Ascend-IF-Netmask (153)	Máscara de subred en uso para la interfaz numerada del lado local.
Ascend-Metric (225)	Métrica RIP para la ruta especificada (un número del 1 al 15, donde 7 es el ajuste predeterminado). Si los valores de preferencia son iguales, cuanto más alta sea la métrica, menos probabilidades habrá de que la unidad TAOS utilice esta ruta.
Ascend-Route-Preference (126)	Un valor de preferencia para la ruta. Los valores validos se encuentran entre 0 y 255. El valor 255 impide la utilización de la ruta. Si desea obtener información detallada acerca del establecimiento de preferencias, consulte el apartado “Definición de preferencias de ruta estática” en la página 2-45.
Framed-Route (22)	Definición de ruta estática, que puede utilizarse para convertir un perfil de usuario en una ruta privada. Para obtener información detallada, consulte el apartado “Configuración de rutas IP estáticas” en la página 2-25.
Ascend-Assign-IP-Pool (218)	Número de la agrupación de direcciones a partir del cual se obtiene una dirección. Para obtener más información, consulte el apartado “Configuración y utilización de agrupaciones de direcciones” en la página 2-68.
Ascend-Assign-IP-Global-Pool (146)	Nombre de una agrupación global de direcciones. Para obtener información detallada, consulte el apartado “Agrupaciones RADIUS globales (RADIPAD)” en la página 2-69.
Ascend-IP-Direct (209)	Dirección IP de un host al que se dirigirán todos los paquetes IP recibidos en el enlace. Para obtener información detallada, consulte el apartado “Ejemplos de una conexión IP-Direct” en la página 2-21.
Framed-Routing (10)	Activa y desactiva las actualizaciones de RIP en la interfaz. De manera predeterminada, RIP está desactivado. Los valores válidos son None(0), Broadcast(1), Listen(2), Broadcast-Listen(3), Broadcast-v2(4), Listen-v2(5) y Broadcast-Listen-v2(6).
Ascend-Source-IP-Check (96)	Activa y desactiva la protección frente a engaños para la sesión. El ajuste predeterminado es Source-IP-Check-No (0). Con el ajuste Source-IP-Check-Yes (1), el sistema descarta los paquetes que no se originen en la subred a la que está conectado el dispositivo remoto. El sistema determina la subred durante la negociación IPCP. Si Framed-IP-Netmask especifica una subred, se aceptarán los paquetes que se originen en dicha subred. Si Framed-IP-Netmask especifica una máscara de 32 bits, sólo se aceptarán paquetes de un único host. Los paquetes enviados desde una dirección que no coincida se descartarán.

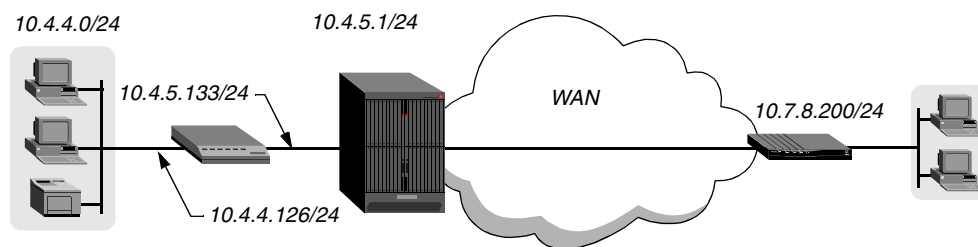
<b>Atributo</b>	<b>Valor</b>
Ascend-Multicast-Client (155)	Opción de envío de difusión múltiple. Para obtener información detallada, consulte el apartado “Configuración del envío de difusión múltiple” en la página 2-80.
Ascend-Multicast-Rate-Limit (152)	Opción de envío de difusión múltiple. Para obtener información detallada, consulte el apartado “Configuración del envío de difusión múltiple” en la página 2-80.
Ascend-Multicast-GLeave-Delay (111)	Opción de envío de difusión múltiple. Para obtener información detallada, consulte el apartado “Configuración del envío de difusión múltiple” en la página 2-80.
Ascend-Client-Primary-DNS (135)	Opción de DNS de cliente. Para obtener información detallada, consulte el apartado “Utilización del DNS de cliente” en la página 2-63.
Ascend-Client-Secondary-DNS (136)	Opción de DNS de cliente. Para obtener información detallada, consulte el apartado “Utilización del DNS de cliente” en la página 2-63.
Ascend-Client-Assign-DNS (137)	Opción de DNS de cliente. Para obtener información detallada, consulte el apartado “Utilización del DNS de cliente” en la página 2-63.
Ascend-Client-Gateway (132)	Ruta predeterminada para el tráfico procedente de esta conexión. Para obtener información detallada, consulte el apartado “Ejemplos de gateways predeterminados de cliente” en la página 2-23.
Ascend-IP-TOS (87)	<p>Tipo de servicio de la corriente de datos. El valor de este atributo establece los cuatro bits siguientes a los tres bits más significativos del byte TOS. Estos cuatro bits se utilizan para elegir un enlace de acuerdo con el tipo de servicio. Especifique uno de los valores siguientes:</p> <ul style="list-style-type: none"><li>• Ascend-IP-TOS IP-TOS-Normal (0): Servicio normal</li><li>• Ascend-IP-TOS IP-TOS-Disabled (1): Desactivar TOS</li><li>• Ascend-IP-TOS IP-TOS-Cost (2): Minimizar coste económico</li><li>• Ascend-IP-TOS IP-TOS-Reliability (4): Maximizar fiabilidad</li><li>• Ascend-IP-TOS IP-TOS-Throughput (8): Maximizar rendimiento</li><li>• Ascend-IP-TOS IP-TOS-Latency (16): Minimizar retardo</li></ul>

Atributo	Valor
Ascend-IP-TOS-Precedence (88)	<p>Nivel de prioridad de la corriente de datos. Los tres bits más significativos del byte TOS son bits de prioridad utilizados para determinar la prioridad para la puesta en cola por prioridades. Si TOS está activo, establezca los bits en uno de los valores siguientes (el bit más significativo en primer lugar):</p> <ul style="list-style-type: none"><li>• IP-TOS-Precedence-Pri-Normal (0): Prioridad normal</li><li>• IP-TOS-Precedence-Pri-One (32): Nivel de prioridad 1</li><li>• IP-TOS-Precedence-Pri-Two (64): Nivel de prioridad 2</li><li>• IP-TOS-Precedence-Pri-Three (96): Nivel de prioridad 3</li><li>• IP-TOS-Precedence-Pri-Four (128): Nivel de prioridad 4</li><li>• IP-TOS-Precedence-Pri-Five (160): Nivel de prioridad 5</li><li>• IP-TOS-Precedence-Pri-Six (192): Nivel de prioridad 6</li><li>• IP-TOS-Precedence-Pri-Seven (224): Nivel de prioridad 7 (la prioridad más alta)</li></ul>
Ascend-IP-TOS-Apply-To (89)	<p>Dirección en la que se ha activado TOS. Con el ajuste IP-TOS-Apply-To-Incoming (1024), que es el ajuste predeterminado, los bits se establecen en paquetes recibidos en la interfaz. Con el ajuste IP-TOS-Apply-To-Outgoing (2048), los bits se establecen únicamente en paquetes de salida. Con el ajuste IP-TOS-Apply-To-Both (3072), se etiquetan tanto los paquetes de entrada como los de salida.</p>

## Ejemplos de una conexión a otro ruteador IP

En la Figura 2-2 se muestra la conexión de la unidad TAOS con una ruteador de extremo distante, como una Pipeline. Puede tratarse, por ejemplo, de una configuración de teletrabajo en la que la Pipeline se encuentra en una sucursal u oficina central.

*Figura 2-2. Conexión IP de ruteador a ruteador*



Los ajustes predeterminados para el subperfil IP-Options permiten el ruteo IP, activan la compresión de cabeceras Van Jacobsen y desactivan RIP. Estos ajustes resultan apropiados para el ejemplo siguiente, que muestra la configuración de un perfil Connection para la unidad Pipeline en la Figura 2-2:

```
admin> read conn pipeline1
CONNECTION/pipeline1 read

admin> set active = yes

admin> set encapsulation-protocol = ppp
```



```
admin> set dial-number = 9-1-333-555-1212
admin> set ppp send-auth-mode = pap-ppp-auth
admin> set ppp send-password = remotepw
admin> set ppp recv-password = localpw
admin> set ip-options remote = 10.7.8.200/24
admin> write
CONNECTION/pipeline1 written
```

A continuación se muestran los perfiles RADIUS equivalentes:

```
pipeline1 Password = "localpw"
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Framed-IP-Address = 10.7.8.200,
  Framed-IP-Netmask = 255.255.255.0

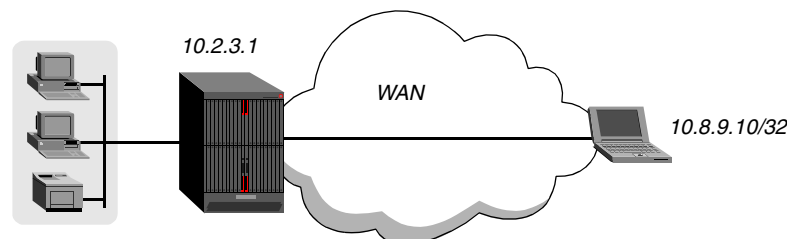
route-taos-1 Password = "ascend", Service-Type = Outbound-User
  Framed-Route = "10.7.8.0/24 10.7.8.200 1 n pipeline1-out"

pipeline1-out Password = "localpw", Service-Type = Outbound-User
  User-Name = "pipeline1",
  Ascend-Dial-Number = "9-1-333-555-1212",
  Framed-Protocol = PPP,
  Framed-IP-Address = 10.7.8.200,
  Framed-IP-Netmask = 255.255.255.0,
  Ascend-Send-Auth = Send-Auth-PAP,
  Ascend-Send-Password = "remotepw"
```

## Ejemplos de una conexión de ruta de host

Una ruta de host se anuncia como una dirección IP con una máscara de subred de 32. Representa un único host en lugar de un ruteador remoto. En la Figura 2-3 se muestra un ejemplo de conexión en la que un host de llamada de entrada con una tarjeta de módem ISDN se conecta a una unidad TAOS.

*Figura 2-3. Host de llamada de entrada que requiere una dirección IP estática (una ruta de host)*



La configuración PPP incluye la dirección del host. Por ejemplo:

```
Username=patti
Accept Assigned IP=N/A (or No)
IP address=10.8.9.10
Netmask=255.255.255.255
Default Gateway=N/A (or None)
Name Server=10.7.7.1
```

```
Domain suffix=abc.com
VAN Jacobsen compression ON
```

Los ajustes predeterminados para el subperfil IP-Options permiten el ruteo IP, activan la compresión de cabeceras Van Jacobsen y desactivan RIP. Estos ajustes resultan apropiados para el ejemplo siguiente, que muestra la configuración del perfil Connection para el host de la Figura 2-3:

```
admin> new conn patti
CONNECTION/patti read

admin> set active = yes

admin> set encapsulation-protocol = ppp

admin> set ppp recv-password = localpw

admin> set ip-options remote = 10.8.9.10/32

admin> write
CONNECTION/patti written
```

A continuación se muestra un perfil RADIUS equivalente:

```
patti Password = "localpw"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Framed-IP-Address = 10.8.9.10,
    Framed-IP-Netmask = 255.255.255.255
```

## Ejemplos de una conexión de interfaz numerada

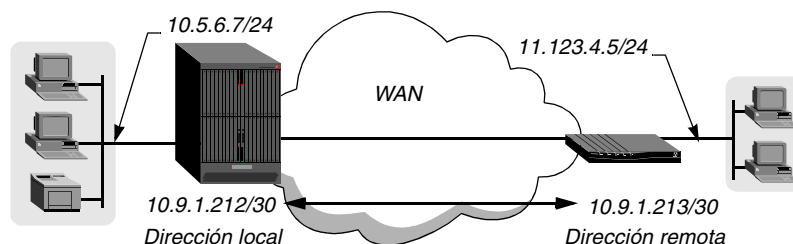
Para una conexión de interfaz numerada, se asigna a cada lado de la conexión una dirección exclusiva aplicable únicamente a la conexión. Esto es obligatorio para algunas aplicaciones, como SNMP.

El valor Local-Address asignado a una interfaz numerada debe ser exclusivo para la conexión y para la red. Puede asignar una dirección IP ficticia o una dirección IP de una de las subredes locales. Una unidad TAOS acepta paquetes IP destinados a la dirección especificada y los trata como si estuvieran destinados al propio sistema. Los paquetes pueden llegar a cualquier interfaz y la interfaz de destino no debe estar necesariamente en estado activo.

**Nota:** No asigne una dirección local que pertenezca a una de las interfaces LAN físicas reales de la unidad TAOS. Esto provocaría problemas de ruteo.

En la Figura 2-4 se muestra una conexión de interfaz numerada. La interfaz Ethernet física real de la unidad TAOS posee la dirección IP 10.5.6.7/24. Las otras dos direcciones representan las direcciones local y remota de la conexión de interfaz numerada.

*Figura 2-4. Conexión de interfaz numerada*



El conjunto de comandos siguiente especifica un perfil Connection para la interfaz numerada:

```
admin> new conn numbered
CONNECTION/numbered read

admin> set active = yes

admin> set encapsulation-protocol = ppp
admin> set ppp rcv-password = localpw
admin> set ip-options remote-address = 10.9.1.213/30
admin> set ip-options local-address = 10.9.1.212/30

admin> write
CONNECTION/numbered written
```

A continuación se muestra un perfil RADIUS equivalente:

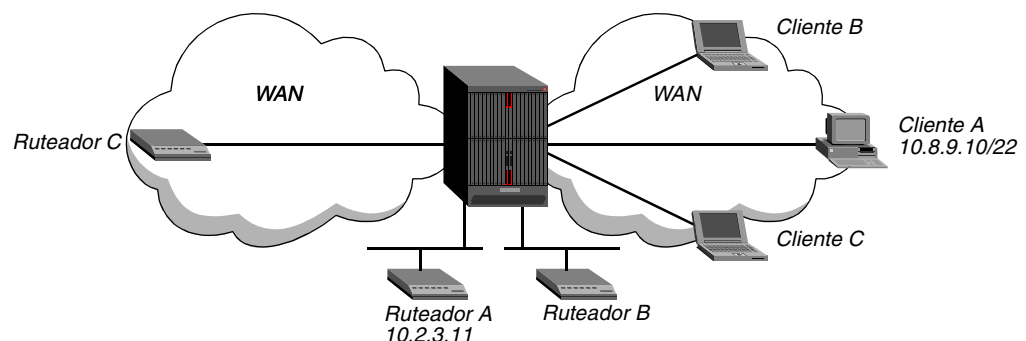
```
numbered Password = "localpw"
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Ascend-Route-IP = Route-IP-Yes,
  Framed-IP-Address = 10.9.1.213,
  Framed-IP-Netmask = 255.255.255.252,
  Ascend-PPP-Addr = 10.9.1.212,
  Ascend-IF-Netmask = 255.255.255.252
```

En este ejemplo, la interfaz tiene asignada una subred de 30 bits, de modo que hay 4 combinaciones de bits disponibles para las asignaciones de host. De las cuatro direcciones de host posibles, la que sea divisible por 4 es la dirección de red o dirección base (la dirección que especifica ceros en los bits de host). Esta dirección se agrega a la tabla de ruteo. Las otras direcciones de host tienen asignada una máscara de subred de /32 y se agregan como rutas de host. Puede suprimir el anuncio de las rutas de host asociadas a una interfaz numerada mediante el parámetro Suppress-Host-Routes, como se describe en “Supresión de anuncios de ruta de host” en la página 2-49.

## Ejemplos de una conexión IP-Direct

Los paquetes recibidos en una conexión IP-Direct eluden las tablas de ruteo y, en cambio, se redirigen a una dirección IP de destino del siguiente salto. Los paquetes de salida se rutean de la forma habitual. Actualmente esta función sólo se lleva a la práctica para las llamadas de datos. En la Figura 2-5 se muestra un ejemplo del flujo de tráfico de IP-Direct.

*Figura 2-5. Conexiones IP-Direct*



En la Figura 2-5, se aplican las condiciones siguientes:

- El perfil del cliente A dirige los paquetes de entrada al router A en una interfaz LAN.
- El perfil del cliente B dirige los paquetes de entrada al router B en una interfaz LAN.
- El perfil del cliente C dirige los paquetes de entrada al router C a través de una conexión conmutada.

Los paquetes de salida destinados a cualquiera de los tres clientes se enrutan de la forma habitual mediante la unidad TAOS, lo que significa que estas conexiones de cliente pueden *recibir* paquetes desde cualquier origen, y no sólo desde la dirección IP a la que se han enviado los paquetes.

El conjunto de comandos siguiente configura un perfil Connection IP-Direct para el cliente A:

```
admin> read conn client-A
CONNECTION/client-A read
admin> set active = yes
admin> set encapsulation-protocol = ppp
admin> set ppp recv-password = localpw
admin> set ip-options remote = 10.8.9.10/22
admin> set ip-options ip-direct = 10.2.3.11
admin> write
CONNECTION/client-A written
```

A continuación se muestra un perfil RADIUS equivalente:

```
client-A Password = "localpw"
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Framed-IP-Address = 10.8.9.10,
  Framed-IP-Netmask = 255.255.252.0,
  Ascend-IP-Direct = 10.2.3.11
```

Las conexiones IP-Direct requieren el tratamiento especial siguiente:

- Si el perfil permite la recepción o la recepción y transmisión de actualizaciones de RIP, todos los paquetes RIP de una conexión de entrada se conservan localmente y se envían a la dirección IP-Direct, de modo que la unidad TAOS puede enviar correctamente los paquetes *destinados* al cliente.
- Las peticiones ARP recibidas de la conexión de entrada se pasan por alto.
- El emisor no puede realizar una operación Telnet con la unidad TAOS, dado que se pasa por la conexión para ir al host IP-Direct.

## **Ejemplos de creación de la ruta hacia una conexión privada**

Una ruta privada aparece en la tabla de ruteo pero está marcada con un indicador que impide a los protocolos de ruteo anunciarla. Los comandos siguientes especifican una ruta privada en un perfil Connection:

```
admin> read conn david
CONNECTION/david read
admin> set ip-options remote = 10.8.9.10/24
```

```
admin> set ip-options private = yes
admin> set ip-options routing-metric = 3
admin> write
CONNECTION/david written
```

A continuación se muestra un perfil RADIUS equivalente:

```
david Password = "localpw"
  Service-Type = Framed-User,
  Framed-Protocol = MPP,
  Framed-IP-Address = 10.8.9.10,
  Framed-IP-Netmask = 255.255.255.0,
  Framed-Route = "10.8.9.10/24 0.0.0.0 3 y"
```

## Ejemplos de gateways predeterminados de cliente

Un gateway predeterminado de cliente es una ruta que reemplaza la ruta predeterminada para una conexión concreta en todo el sistema. Para los paquetes que llegan en la conexión, si la unidad TAOS consulta la tabla de ruteo y no encuentra ninguna coincidencia para el destino de los paquetes (si sólo encuentra la ruta predeterminada del sistema o, de no haber ruta predeterminada, si no encuentra ninguna coincidencia en absoluto), envía los paquetes a la dirección del gateway predeterminado de cliente.

La dirección especificada debe ser un salto siguiente válido, es decir, la unidad TAOS debe poder llegar al ruteador directamente en un salto. Si éste no es el caso, la unidad descarta los paquetes que debería rutear hacia el gateway predeterminado de cliente.

Los paquetes procedentes de otros usuarios o de la red Ethernet se gestionan de la forma habitual. La tabla de ruteo del sistema no se modifica por la utilización de esta función. Los comandos siguientes especifican un gateway predeterminado específico de la conexión:

```
admin> read connection test
CONNECTION/test read

admin> set ip-options client-default-gateway = 17.1.1.1
admin> write
CONNECTION/test written
```

A continuación se muestra un ajuste equivalente de un perfil RADIUS:

```
test Password = "localpw"
  Service-Type = Framed-User,
  Ascend-Client-Gateway = 17.1.1.1
```

## Ejemplos de verificación de la dirección de origen por sesión

Puede configurar interfaces IP WAN para que el sistema verifique la dirección IP de origen de todos los paquetes recibidos y descarte aquellos paquetes cuya dirección no coincida con la negociada para la subred del extremo distante. Este tipo de configuración permite a la unidad TAOS detectar paquetes con direcciones IP de origen falsas y descartarlos.

Si el sistema detecta inicialmente un intento de engaño (una dirección de origen no coincidente), registra un mensaje en el que se incluye el número de puerto en que se ha producido dicho intento. Por ejemplo:

```
[1/4/1/1] Spoofing Attempt:from port 1[MBID 1; 1119855018] [ed-mc1-p75]
```

Los comandos siguientes configuran un perfil Connection para la protección frente a engaños:

```
admin> read connection ed-mc1-p75
CONNECTION/ed-mc1-p75 read

admin> set ip-options source-ip-check = yes

admin> write
CONNECTION/ed-mc1-p75 written
```

A continuación se muestra un ajuste equivalente de un perfil RADIUS:

```
ed-mc1-p75 Password = "localpw"
      Service-Type = Framed-User,
      Ascend-Source-IP-Check = Source-IP-Check-Yes
```

## Ejemplos de definición de la política QoS y TOS

Puede configurar la unidad TAOS para que defina bits de prioridad QoS (Calidad de servicio) y clases de servicio TOS (Tipo de servicio) en nombre de las aplicaciones del cliente. La unidad TAOS no aplica la puesta en cola por prioridades, pero define información que pueden utilizar otros ruteadores para asignar una prioridad a los enlaces y seleccionarlos para corrientes de datos concretas.

Para activar el TOS basado en el servicio o definir la prioridad QoS para el tráfico en una conexión WAN concreta, configure las opciones TOS en un perfil Connection o RADIUS. Estos ajustes hacen que la unidad TAOS establezca bits en el byte TOS de las cabeceras de paquetes IP que se reciben (de manera predeterminada), transmiten o ambos en la interfaz WAN. A continuación, otro ruteador puede interpretar los bits de forma acorde.

También puede especificar la política proxy-QoS y TOS en un filtro TOS, que a continuación puede aplicarse a cualquier número de perfiles Connection o RADIUS. Si a un perfil Connection o RADIUS se le aplican tanto su propia política local como un filtro TOS, prevalece la política definida en el filtro TOS. Por ejemplo, la aplicación de un filtro TOS a una conexión activa con TOS le permite definir un ajuste de prioridad para los paquetes de entrada en una conexión y otro para los paquetes de entrada dirigidos a un destino concreto (el destino en un filtro TOS). Si desea obtener información detallada, consulte el Capítulo 9, “Filtros de paquetes”.

El conjunto de comandos siguiente activa TOS para los paquetes de entrada en una interfaz WAN. Establece la prioridad de los paquetes en 6, lo que significa que otro ruteador que aplique la puesta en cola por prioridades no descartará los paquetes hasta que haya descartado todos los paquetes de prioridad menor. Estos comandos también establecen TOS para que dé preferencia al máximo rendimiento, lo que significa que el ruteador de puesta en cola por prioridades elegirá una conexión con un ancho de banda elevado si hay alguna disponible, aunque tenga un coste superior, tenga mayor latencia o sea menos fiable que otro enlace disponible.

```
admin> read connection jfan-pc
CONNECTION/jfan-pc read
```

```
admin> set ip-options remote-address = 10.168.6.120/24
admin> set ip-options tos active = yes
admin> set ip-options tos precedence = 110
admin> set ip-options tos type = throughput
admin> write
CONNECTION/jfan-pc written
```

A continuación se muestra un perfil RADIUS equivalente:

```
jfan-pc Password = "localpw"
Service-Type = Framed-User,
Framed-IP-Address = 10.168.6.120,
Framed-IP-Netmask = 255.255.255.0,
Ascend-IP-TOS = IP-TOS-Throughput,
Ascend-IP-TOS-Precedence = IP-TOS-Precedence-Pri-Six,
Ascend-IP-TOS-Apply-To = IP-TOS-Apply-To-Incoming
```

## ***Configuración de rutas IP estáticas***

Cualquier perfil que especifique cómo llegar a un dispositivo IP o una subred (como un perfil de usuario IP-Interface, Connection o RADIUS) especificará también una ruta IP estática hacia este destino. Sin embargo, a veces los administradores configuran rutas estáticas de una forma más flexible a fin de ampliar o hacer más precisa la tabla de ruteo.

La ruta predeterminada es una ruta estática especial que actúa como ruta general para los paquetes para los que la unidad TAOS no encuentra una ruta. Si define una ruta predeterminada (con la dirección de destino cero), la unidad TAOS rutea todos los paquetes cuyo destino se desconoce al gateway especificado. Si no se ha definido ninguna ruta predeterminada, la unidad TAOS descarta estos paquetes.

Si las direcciones IP LAN de la unidad incluyen especificaciones de subred, debe crear una ruta estática hacia otro ruteador LAN para que la unidad TAOS pueda llegar a redes locales situadas más allá de sus propias subredes. También puede configurar una ruta estática hacia un ruteador LAN para reducir la actividad de ruteo local de la unidad TAOS.

Otra razón para configurar rutas estáticas es especificar rutas de varios trayectos, que definen distintos trayectos para el mismo destino. Las rutas de varios trayectos, con igual métrica e iguales valores de preferencia, distribuyen el tráfico a un único destino a través de varias interfaces.

**Nota:** La unidad TAOS no admite rutas de llamada de salida de varios trayectos desde RADIUS.

## Información general sobre los ajustes de rutas estáticas

Puede definir rutas estáticas en perfiles IP-Route o RADIUS.

### *Ajustes de los perfiles IP-Route*

A continuación se muestran los parámetros de un perfil IP-Route local (con los ajustes predeterminados):

```
in IP-ROUTE/" " (new)]
name* = " "
dest-address = 0.0.0.0/0
gateway-address = 0.0.0.0
metric = 8
cost = 1
preference = 60
third-party = no
ase-type = type-1
ase-tag = c0:00:00:00
private-route = no
active-route = yes
ase7-adv = N/A
vrouter = " "
inter-vrouter = " "
```

Parámetro	Especifica
Name	Nombre del perfil (de hasta 31 caracteres).
Dest-Address	Dirección IP de destino, en la que puede incluirse una especificación de subred. El ajuste predeterminado es 0.0.0.0, que representa una ruta predeterminada.
Gateway-Address	Dirección IP de un ruteador que se utiliza para llegar al destino especificado.
Metric	Métrica RIP para la ruta especificada (un número del 1 al 15, donde 8 es el ajuste predeterminado). Si los valores de preferencia son iguales, cuanto más alta sea la métrica, menos probabilidades habrá de que la unidad TAOS utilice esta ruta.
Cost	Opción de OSPF (consulte “Configuración de información de ruta estática OSPF” en la página 3-18).
Preference	Valor de preferencia de la ruta. Para obtener información detallada, consulte el apartado “Definición de preferencias de ruta estática” en la página 2-45.
Third-Party	Opción de OSPF. Para obtener información detallada, consulte el apartado “Configuración de información de ruta estática OSPF” en la página 3-18.
ASE-Type	Opción de OSPF. Para obtener información detallada, consulte el apartado “Configuración de información de ruta estática OSPF” en la página 3-18.
ASE-Tag	Opción de OSPF. Para obtener información detallada, consulte el apartado “Configuración de información de ruta estática OSPF” en la página 3-18.



Parámetro	Especifica
Private-Route	Activa y desactiva el anuncio de la ruta cuando el ruteador envía actualizaciones de RIP u OSPF. Con el ajuste Yes, la ruta queda excluida de los paquetes de actualización.
Active-Route	Activa y desactiva la introducción de la ruta en la tabla de ruteo (establecer el parámetro en el valor No es una manera útil de hacer que una ruta esté inactiva temporalmente, de modo que pueda restituirla posteriormente).
ASE7-Adv	Opción de OSPF. Para obtener información detallada, consulte el apartado “Configuración de información de ruta estática OSPF” en la página 3-18.
VRouter	Opción de ruteador virtual. Para obtener información detallada, consulte el apartado “Definición de rutas estáticas de ruteador virtual” en la página 6-9.
Inter-VRouter	Opción de ruteador virtual. Para obtener información detallada, consulte el apartado “Definición de rutas estáticas de ruteador virtual” en la página 6-9.

### Ajustes de un perfil de ruta RADIUS

Un perfil de ruta es un perfil de pseudousuario cuya primera línea presenta el formato siguiente:

```
route-name-N Password = "ascend", Service-Type = Outbound-User
```

El argumento *name* es el nombre de sistema de la unidad TAOS (especificado por el parámetro Name en el perfil System) y *N* es un número de una serie secuencial que empieza por 1. Asegúrese de que no faltan números en la serie que especifica *N*. Si existe un espacio vacío en la secuencia de números, la unidad TAOS deja de recuperar los perfiles cuando encuentra dicho espacio.

Para especificar rutas a las que puede llamar más de un sistema, elimine el argumento name. En este caso, la primera palabra del perfil de pseudousuario es *route-N*.

Cada perfil de pseudousuario especifica una o varias rutas con el atributo Framed-Route (22). El protocolo RADIUS limita el número de definiciones Framed-Route en un único perfil de ruta. El límite varía con el contenido exacto de las rutas. Sin embargo, el valor máximo recomendado es de 25 definiciones Framed-Route por perfil.

El valor del atributo Framed-Route utiliza la sintaxis siguiente:

```
"dest-addr gateway-addr metric [private]
[profile] [preference] [VRouter] "
```

Elemento de sintaxis	Especifica
<i>dest-addr</i>	Dirección IP de destino, en la que puede incluirse una especificación de subred. El ajuste predeterminado es 0.0.0.0, que representa una ruta predeterminada.
<i>gateway-addr</i>	Dirección IP del ruteador del siguiente salto para llegar al destino especificado.

Elemento de sintaxis	Especifica
<i>metric</i>	Métrica RIP para la ruta especificada (un número del 1 al 15, donde 8 es el ajuste predeterminado). Si los valores de preferencia son iguales, cuanto más alta sea la métrica, menos probabilidades habrá de que la unidad TAOS utilice esta ruta.
<i>private</i>	Activa y desactiva el anuncio de la ruta cuando el ruteador envía actualizaciones de RIP u OSPF. El ajuste Yes convierte la ruta en privada, con lo que se excluye de los paquetes de actualización.
<i>profile</i>	Nombre del perfil de usuario de llamada de salida para la ruta. El valor predeterminado es nulo.
<i>preference</i>	Valor de preferencia de la ruta. Para obtener información detallada, consulte el apartado “Definición de preferencias de ruta estática” en la página 2-45.
<i>VRouter</i>	Opción de ruteador virtual. Para obtener información detallada, consulte el apartado “Definición de rutas estáticas de ruteador virtual” en la página 6-9.

### *Ajustes de ruta en un perfil de usuario RADIUS*

También puede incluir el atributo Framed-Route (22) en un perfil de usuario RADIUS para definir una ruta estática. Para obtener información detallada acerca de la utilización de Framed-Route, consulte “Ajustes de un perfil de ruta RADIUS” en la página 2-27.

En un perfil de usuario puede especificar la dirección cero como dirección de gateway. En este contexto, la dirección 0.0.0.0 es una entrada comodín que la unidad TAOS reemplaza por la dirección IP del emisor. Cuando RADIUS autentica el emisor y envía a la unidad TAOS un mensaje Access-Accept con el valor 0.0.0.0 para la dirección del ruteador, la unidad TAOS actualiza sus tablas de ruteo con el valor Framed-Route, pero sustituye la dirección IP del emisor por la dirección del ruteador. Este ajuste resulta útil si la unidad TAOS asigna una dirección IP procedente de una agrupación de direcciones y RADIUS no tiene acceso a la dirección IP del emisor.

Si una definición Framed-Route en un perfil de usuario duplica una ruta definida en el perfil IP-Route o la tabla de ruteo de la unidad TAOS, la definición del perfil de usuario tiene preferencia mientras la conexión esté activa. Por ejemplo, supongamos que una ruta estática hacia la red 10.10.10.10 está definida en un perfil IP-Route local con una métrica de 10. Un perfil de usuario RADIUS define una ruta estática hacia 10.10.10.10 con una métrica de 7. Mientras la ruta del usuario RADIUS no está en uso, la tabla de ruteo indica que la ruta tiene una métrica de 10. Cuando la ruta está en uso, la tabla de ruteo de la unidad TAOS indica que la ruta tiene una métrica de 7, con una *r* en la columna de indicadores para indicar que la ruta procede de RADIUS. Es más, la ruta con una métrica de 10 permanece en la tabla de ruteo con un asterisco (\*) en la columna de indicadores, lo que indica que se trata de una ruta oculta.

### *Rutas estáticas privadas específicas de la conexión (sólo RADIUS)*

El par atributo-valor siguiente configura opciones IP en un perfil RADIUS:

Atributo	Valor
Ascend-Private-Route (104)	Ruta privada entramada conocida únicamente en el perfil en el que está especificada. El valor es una dirección de destino y una dirección de ruteador del siguiente salto (en este orden). Para obtener información detallada, consulte el apartado “Ejemplos de rutas estáticas privadas” en la página 2-38.

## Ejemplos de configuración de rutas predeterminadas

Una ruta con la dirección de destino cero es una ruta predeterminada. Si el sistema no encuentra una ruta para el destino de un paquete, en lugar de descartar dicho paquete, lo envía a una ruta predeterminada. Si no hay ninguna ruta predeterminada en la tabla de ruteo, la unidad TAOS descarta todos los paquetes para los que no encuentre una ruta.

La unidad TAOS crea un perfil IP-Route denominado `default`, pero el perfil no será válido hasta que se especifique una dirección de gateway, de modo que la ruta no estará activa hasta que asigne una dirección y active la ruta. Por ejemplo:

```
admin> read ip-route default
IP-ROUTE/default read

admin> set gateway-address = 10.10.10.10

admin> set active-route = yes

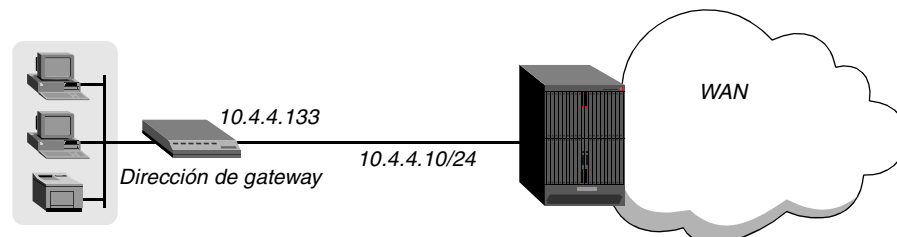
admin> write
IP-ROUTE/default written
```

Puede crear una ruta predeterminada modificando el perfil `default` o creando uno o más perfiles IP-Route que especifiquen un destino cero y una dirección de gateway válida.

### *Ejemplos de una ruta predeterminada basada en LAN*

En la Figura 2-6 se muestra un ruteador que reside en la misma subred que una de las interfaces IP locales de la unidad TAOS.

*Figura 2-6. Ruta predeterminada hacia un ruteador IP local*



Dado que la unidad TAOS reside en una subred, debe ser informada sobre los otros ruteadores de red troncal que pueden rutear más allá de la subred. En este ejemplo, la unidad TAOS reduce parte de la actividad de ruteo utilizando una ruta predeterminada al ruteador LAN. Los comandos siguientes definen una ruta predeterminada hacia el ruteador local:

```
admin> new ip-route lanroute-1
IP-ROUTE/lanroute-1 read
admin> set gateway-address = 10.4.4.133
admin> write
IP-ROUTE/lanroute-1 written
```

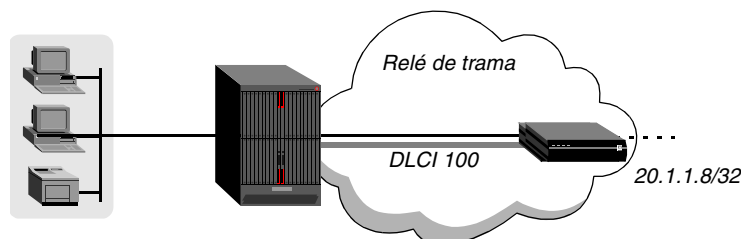
A continuación se muestra una ruta RADIUS predeterminada equivalente:

```
route-taos-1 Password = "ascend", Service-Type = Outbound-User
Framed-Route = "0.0.0.0 10.4.4.133"
```

### *Ejemplos de una ruta predeterminada en un enlace WAN*

En la Figura 2-7 se muestra un ruteador que reside en una interfaz DLCI de relé de trama. Si el enlace WAN hacia esta ruta predeterminada se desconecta por el motivo que sea, la unidad TAOS elimina esta ruta de la tabla de ruteo.

*Figura 2-7. Ruta predeterminada en una interfaz DLCI de relé de trama*



En este ejemplo, los ajustes de relé de trama siguientes definen el enlace de datos:

```
[in FRAME-RELAY/fr1]
fr-name* = fr1
active = yes
nailed-up-group = 1
link-mgmt = ansi-t1.617d
link-type = dte
```

Y el perfil Connection siguiente define la interfaz DLCI:

```
[in CONNECTION/pvc1]
station* = pvc1
active = yes
encapsulation-protocol = frame-relay
ip-options = { yes yes 20.1.1.8/32 0.0.0.0/0 1 60 120 no no 0 0.0.0.0+
telco-options = { ans-and-orig no ft1 1 no no 56k-clear 0 "" "" no no+
fr-options = { fr1 16 "" no "" 16 }
```

Los comandos siguientes definen una ruta predeterminada hacia el dispositivo remoto:

```
admin> new ip-route dlci
IP-ROUTE/dlci read
admin> set gateway-address = 20.1.1.8
```

```
admin> set private-route = yes  
  
admin> write  
IP-ROUTE/dlci written
```

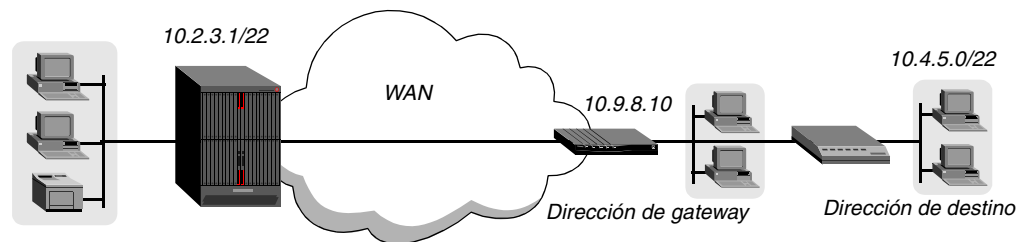
A continuación se muestra una ruta RADIUS predeterminada equivalente:

```
route-taos-1 Password = "ascend", Service-Type = Outbound-User  
Framed-Route = "0.0.0.0 20.1.1.8 y"
```

## Ejemplos de configuración de una ruta hacia una subred remota

Si RIP y OSPF están desactivados en una interfaz IP, el ruteador no puede llegar a otros ruteadores de la misma interfaz a menos que posea una ruta estática. Por ejemplo, si un perfil Connection especifica la dirección de destino de un host de una subred remota, pero los paquetes deben rutearse a través de un dispositivo intermediario para llegar a dicho host (y no está activo ni RIP ni OSPF), debe configurar una ruta estática que especifique el dispositivo intermediario como gateway. En la Figura 2-8 se muestra un ejemplo.

*Figura 2-8. Ruta estática hacia una subred remota*



Los comandos siguientes configuran una ruta estática hacia todos los hosts de la subred remota:

```
admin> new ip-route subnet  
IP-ROUTE/subnet read  
  
admin> set dest = 10.4.5.0/22  
  
admin> set gateway = 10.9.8.10  
  
admin> write  
IP-ROUTE/subnet written
```

A continuación se muestra un perfil RADIUS que incorpora la ruta predeterminada y una ruta a la subred remota:

```
route-taos-1 Password = "ascend", Service-Type = Outbound-User  
Framed-Route = "10.4.5.0/22 10.9.8.10"
```

## Ejemplos de configuración de una ruta de varios trayectos

Las rutas estáticas de varios trayectos distribuyen el tráfico a un destino a través del ancho de banda agregado de varias interfaces. Una ruta de varios trayectos requiere que las diferentes rutas estáticas tengan la misma dirección de destino y la misma máscara de subred, pero direcciones de gateway distintas. Además, deben tener la misma métrica de ruta o el mismo

coste OSPF y la misma preferencia de ruta. De lo contrario, se utilizaría exclusivamente la ruta con los valores más bajos para estos ajustes.

**Nota:** Las rutas predeterminadas también pueden ser de varios trayectos. Si más de una ruta tiene el destino 0.0.0.0, la unidad TAOS crea rutas predeterminadas de varios trayectos.

A continuación se muestra un ejemplo en el que el administrador configura una ruta de varios trayectos hacia la red 10.76.109.0/24:

```
admin> new ip-route bdvnet-1
IP-ROUTE/bdvnet-1 read

admin> set dest = 10.76.109.0/24
admin> set gateway = 11.65.212.1
admin> set metric = 2

admin> write
IP-ROUTE/bdvnet-1 written

admin> new ip-route bdvnet-2
IP-ROUTE/bdvnet-2 read

admin> set dest = 10.76.109.0/24
admin> set gateway = 11.65.210.1
admin> set metric = 2

admin> write
IP-ROUTE/bdvnet-2 written
```

Las rutas de varios trayectos aparecen en la tabla de ruteo con el indicador M. Por ejemplo:

```
admin> netstat -rn

Destination      Gateway          IF    Flg    Pref  Met Use  Age
...
10.76.109.0/24  11.65.212.1     ie1-12-2 SGM    100    2   20  7772
10.76.109.0/24  11.65.210.1     ie1-12-3 SGM    100    2   24  7772
```

**Nota:** La unidad TAOS no admite rutas de llamada de salida de varios trayectos desde RADIUS. Si un perfil RADIUS define rutas de llamada de salida de varios trayectos, como la siguiente:

```
route-taos-1 Password = "ascend", Service-Type = Outbound-User
  Framed-Route = "10.1.0.0/16 10.7.7.7 4 n one-out",
  Framed-Route = "10.1.0.0/16 10.7.7.8 4 n two-out"
```

la unidad TAOS agrega a su tabla de ruteo únicamente la última ruta de llamada de salida que lee (en este ejemplo, la ruta denominada two-out).

## ***Configuración de tablas de ruteo privado***

En versiones anteriores del software, se podían definir rutas privadas mediante la utilización del atributo Ascend-Private-Route (104) únicamente con un perfil de usuario RADIUS. En la versión actual del software, también puede utilizar este atributo en perfiles de pseudousuario de ruta privada, a los que posteriormente pueden asociarse varios perfiles RADIUS, Connection, o ambos. Estas tablas de ruteo privado definidas de forma externa se guardan en la caché localmente durante un intervalo sujeto a configuración. El comando PrtCache visualiza

estadísticas acerca de cada perfil RADIUS de ruta privado guardado en la caché y le permite eliminar perfiles de la caché.

También puede definir tablas de ruteo privado de forma local en el perfil Private-Route-Table. Posteriormente, varios perfiles RADIUS, Connection o ambos podrán asociarse a estos perfiles.

## Información general sobre los ajustes de un perfil local

Para configurar tablas de ruteo privado, debe establecer los parámetros siguientes (que aparecen con los ajustes predeterminados):

```
[in PRIVATE-ROUTE-TABLE/""]
name* = ""

[in PRIVATE-ROUTE-TABLE/":route-description-list [1]]
enabled = no
dest-address = 0.0.0.0/0
netmask = 0.0.0.0
gateway-address = 0.0.0.0
metric = 0

[in CONNECTION/":ip-options]
private-route-table = ""
private-route-profile-required = no

[in ANSWER-DEFAULTS:ip-answer]
private-route-profile-required = no

[in IP-GLOBAL]
default-prt-cache-time = 1440
```

Parámetro	Especifica
Name	Nombre del perfil, de un máximo de 23 caracteres. Este nombre se utiliza para asociar un perfil RADIUS o Connection a las rutas privadas definidas.
Enabled	Activa y desactiva la ruta específica para su utilización en la tabla de ruteo privado. Una tabla puede contener hasta 24 rutas.
Dest-Address	Dirección IP de destino, que puede incluir una especificación de subred. Este ajuste actúa del mismo modo que su equivalente en un perfil IP-Route. Para obtener información detallada al respecto, consulte la publicación <i>APX 8000/MAX TNT/DSLNT Reference</i> (Referencia de APX 8000/MAX TNT/DSLNT).
Netmask	Máscara de red de la dirección IP de destino, que se establece de forma automática cuando se especifica una longitud de prefijo como parte de la dirección IP.
Gateway-Address	Dirección IP de un router que se utiliza para llegar al destino especificado. Este ajuste actúa del mismo modo que su equivalente en un perfil IP-Route. Para obtener información detallada al respecto, consulte la publicación <i>APX 8000/MAX TNT/DSLNT Reference</i> (Referencia de APX 8000/MAX TNT/DSLNT).

<b>Parámetro</b>	<b>Especifica</b>
Metric	Métrica RIP para la ruta especificada (un número del 1 al 15, donde el 8 es el valor predeterminado). Este ajuste actúa del mismo modo que su equivalente en un perfil IP-Route. Para obtener información detallada al respecto, consulte la publicación <i>APX 8000/MAX TNT/DSLNT Reference (Referencia de APX 8000/MAX TNT/DSLNT)</i> .
Private-Route-Table	Nombre de un perfil Private-Route-Table asociado a la conexión. El nombre puede ser el de un perfil local o el de un perfil de pseudousuario de ruta privada en RADIUS. Sin embargo, si un perfil Connection local no utiliza la autenticación, no puede hacer referencia a un perfil RADIUS de ruta privada.
Private-Route-Profile-Required	Define si el acceso a la tabla de ruteo privado es obligatorio para la sesión. Con el valor predeterminado <code>no</code> , el sistema establece la sesión aunque no se encuentre la tabla de ruteo privado asociada. Si el parámetro tiene el valor <code>yes</code> , el sistema desconecta la llamada si no se encuentra la tabla de ruteo privado especificada. Este parámetro no se aplica si el perfil no hace referencia a una tabla de ruteo privado por su nombre.  En el perfil Answer-Defaults, este parámetro se utiliza para perfiles de usuario RADIUS que hacen referencia a una tabla de ruteo privado y no especifican un valor para Ascend-Private-Route-Required (55).
Default-Prt-Cache-Time	Número de minutos durante los que se deben guardar en la caché los perfiles RADIUS de ruta privada que no incluyan ningún valor para Ascend-Cache-Time (57). El valor predeterminado es 1440 (24 horas). Al alcanzar su límite el temporizador de la caché, los perfiles guardados en la caché se eliminan de la memoria del sistema. La próxima vez que se precise una ruta privada, el sistema recuperará el perfil de RADIUS y lo almacenará de nuevo en la caché. Si se guarda un perfil en la caché, aumenta el rendimiento de las búsquedas de ruta, aunque a expensas de ocupar algo de la memoria del sistema. Si este parámetro tiene el valor 0 (cero), el temporizador predeterminado está desactivado, de modo que únicamente se guardarán en la caché los perfiles RADIUS que especifiquen un tiempo de permanencia en caché.

## **Información general sobre los atributos RADIUS para hacer referencia a una tabla de ruteo privado**

Los perfiles de usuario RADIUS pueden hacer referencia a perfiles de ruta privada si se especifican los atributos específicos del proveedor (VSA) siguientes:

<b>Atributo</b>	<b>Especifica</b>
Ascend-Private-Route-Table-ID (54)	Nombre de un perfil RADIUS de ruta privada asociado a la conexión.



Atributo	Especifica
Ascend-Private-Route-Required (55)	Define si el acceso a la tabla de ruteo privado es obligatorio para la sesión. Con el valor predeterminado Required-No (0), el sistema establece la sesión aunque no se encuentre la tabla de ruteo privado asociada. Si el atributo tiene el valor Required-Yes (1), el sistema desconecta la llamada si no se encuentra la tabla de ruteo privado especificada. Este atributo no se aplica si el perfil no hace referencia a una tabla de ruteo privado por su nombre. Si no se ha especificado ningún valor para este atributo, se utiliza el definido para el parámetro Private-Route-Profile-Required en el perfil Answer-Defaults.

## Información general sobre los atributos RADIUS para definir una tabla de ruteo privado

En RADIUS, las tablas de ruteo privado se definen en un perfil de pseudousuario. Un perfil de ruta privada es un perfil de pseudousuario cuyas dos primeras líneas tienen el formato siguiente:

```
nombre-perfil Password = "ascend" Service-Type = Outbound
```

El valor *nombre-perfil* es el nombre asignado al perfil. Las definiciones del perfil Private-route pueden incluir los atributos específicos del proveedor siguientes:

Atributo	Especifica
Ascend-Private-Route (104)	Dirección de destino y dirección del ruteador del siguiente salto para una ruta privada. Cada perfil de ruta privada especifica una o varias rutas privadas con este atributo, lo cual se describe con más detalle en la publicación <i>Guía y referencia de TAOS RADIUS</i> .
Ascend-Cache-Refresh (56)	Define si el temporizador para las rutas en caché de este perfil debe reiniciarse cada vez que se active una nueva sesión que haga referencia al perfil de pseudousuario. Con el valor Refresh-No (0), no se reinicia el temporizador. Con el valor Refresh-Yes (1), se reinicia el temporizador de la caché cada vez que se activa una sesión que hace referencia al perfil.
Ascend-Cache-Time (57)	Número de minutos durante los que se debe guardar el perfil en la caché. Al alcanzar su límite el temporizador de la caché para un perfil RADIUS, el perfil se elimina de la memoria del sistema. La próxima vez que se necesite, el sistema lo recuperará de RADIUS y lo almacenará de nuevo en la caché. Si se guarda un perfil en la caché, aumenta el rendimiento de las búsquedas de ruta, aunque a expensas de ocupar algo de la memoria del sistema. El tiempo en caché mínimo posible es 0 minutos, con lo que el sistema recupera el perfil en la tabla para cada búsqueda de ruta. Este valor no suele ser recomendable. Si no se ha especificado ningún valor para este atributo, se utiliza el definido para el parámetro Default-Prt-Cache-Time en el perfil IP-Global.

Para utilizar estos atributos, el servidor RADIUS debe permitir atributos específicos del proveedor (VSA) y la unidad TAOS debe estar configurada en el modo de compatibilidad con VSA. A continuación se muestran los ajustes pertinentes:

```
[in EXTERNAL-AUTH]
auth-type = radius

[in EXTERNAL-AUTH:rad-auth-client]
auth-radius-compat = vendor-specific
```

Para obtener información detallada acerca de estos ajustes, consulte la publicación *APX 8000/MAX TNT/DSLNT Reference (Referencia de APX 8000/MAX TNT/DSLNT)*.

## Ejemplos de configuración de una tabla de ruteo privado

Puede configurar tablas de ruteo privado localmente o en RADIUS. Por ejemplo, los comandos siguientes definen una tabla de ruteo privado denominada *check*:

```
admin> new private-route-table check
PRIVATE-ROUTE-TABLE/check read

admin> list route-description-list 1
[in PRIVATE-ROUTE-TABLE/check:route-description-list[1] (new)]
enabled = no
dest-address = 0.0.0.0/0
netmask = 0.0.0.0
gateway-address = 0.0.0.0
metric = 0

admin> set enabled = yes

admin> set dest-address = 1.1.1.1/24

admin> set gateway-address = 2.2.2.2

admin> set metric = 2

admin> list
[in PRIVATE-ROUTE-TABLE/check:route-description-list[1]]
enabled = yes
dest-address = 1.1.1.1/24
netmask = 255.255.255.0
gateway-address = 2.2.2.2
metric = 2

admin> list .. 2
[in PRIVATE-ROUTE-TABLE/check:route-description-list[1]]
enabled = no
dest-address = 0.0.0.0/0
netmask = 0.0.0.0
gateway-address = 0.0.0.0
metric = 0

admin> set enabled = yes

admin> set dest-address = 3.3.3.3/28

admin> set gateway-address = 2.2.2.2

admin> set metric = 3

admin> write
PRIVATE-ROUTE-TABLE/check written
```

A continuación se muestra un perfil RADIUS de ruta privada equivalente:

```
check Password = "ascend", Service-Type = Outbound
  Ascend-Cache-Time = 3,
  Ascend-Cache-Refresh = Refresh-Yes,
  Ascend-Private-Route = "1.1.1.1/24 2.2.2.2 2",
  Ascend-Private-Route = "3.3.3.3/28 2.2.2.2 3"
```

Los comandos siguientes configuran el tiempo de permanencia en caché predeterminado para perfiles RADIUS de ruta privada:

```
admin> read ip-global
IP-GLOBAL read

admin> set default-prt-cache-time = 180

admin> write
IP-GLOBAL written
```

A continuación se muestra un ejemplo de perfil RADIUS de ruta privada que utiliza el valor predeterminado en lugar de especificar un valor para Ascend-Cache-Time (57):

```
my-routes Password = "ascend"
  Service-Type = Outbound,
  Ascend-Private-Route = "1.1.1.1/24 2.2.2.2",
  Ascend-Private-Route = "3.3.3.3/28 2.2.2.2"
```

## Ejemplos de utilización de tablas de ruteo privado

Los comandos siguientes modifican un perfil Connection de forma que la sesión tenga acceso a las rutas de la tabla de ruteo privado y que el sistema desconecte la llamada si no se encuentra la tabla de ruteo privado:

```
admin> read connection p50-v2
CONNECTION/p50-v2 read

admin> set ip-options private-route-table = check

admin> set ip-options private-route-profile-required = yes

admin> write
CONNECTION/p50-v2 written
```

El perfil RADIUS siguiente hace referencia a la misma tabla de ruteo privado y tiene los mismos requisitos. Este perfil también especifica cómo se guardan en la caché las rutas para esta conexión.

```
p50-v2 Password = "my-password"
  Service-Type = Framed,
  Framed-Protocol = PPP,
  Framed-IP-Address = 10.1.1.1,
  Framed-IP-Netmask = 255.0.0.0,
  Ascend-Private-Route-Table-ID = "check",
  Ascend-Private-Route-Required = Required-Yes
```

Los comandos siguientes configuran el sistema para que rechace las llamadas de entrada si el perfil de usuario RADIUS especifica una tabla de ruteo privado que no se encuentra:

```
admin> read answer-defaults
ANSWER-DEFAULTS read

admin> set ip-answer private-route-profile-required = yes
```

```
admin> write
ANSWER-DEFAULTS written
```

A continuación se muestra un ejemplo de perfil RADIUS que utiliza el valor predeterminado en lugar de especificar un valor para Ascend-Private-Route-Required (55):

```
p50-v2 Password = "my-password"
Service-Type = Framed,
Framed-Protocol = PPP,
Framed-IP-Address = 10.1.1.1,
Framed-IP-Netmask = 255.0.0.0,
Ascend-Private-Route-Table-ID = "check"
```

## Ejemplos de rutas estáticas privadas

Un perfil de usuario RADIUS puede especificar una lista de rutas privadas asociadas a la conexión (no existe una función equivalente en los perfiles Connection locales).

Las rutas privadas definidas por el atributo Ascend-Private-Route en un perfil de usuario afectan únicamente a los paquetes recibidos de la conexión. Estas rutas no se agregan a la tabla de ruteo global. Si no se encuentra un destino en la lista de rutas privadas y no hay ninguna ruta privada predeterminada, se consulta la tabla de ruteo global para tomar una decisión sobre el ruteo de los paquetes. En caso contrario, sólo se consulta la tabla de ruteo privado.

A continuación se muestra un ejemplo de un perfil de usuario que crea tres rutas privadas asociadas al usuario:

```
pipe50 Password = "ascend" User-Service = Framed
Framed-Protocol = PPP,
Framed-IP-Address = 10.1.1.1,
Framed-IP-Netmask = 255.0.0.0,
Ascend-Private-Route = "170.1.0.0/16 10.10.10.1"
Ascend-Private-Route = "200.1.1.1/32 10.10.10.2"
Ascend-Private-Route = "20.1.0.0/16 10.10.10.3"
Ascend-Private-Route = "0.0.0.0/0 10.10.10.4"
```

Con este perfil, la tabla de ruteo privado para la conexión contiene las rutas siguientes, la última de las cuales es la ruta predeterminada:

Dest/Mask	Gateway
170.1.0.0/16	10.10.10.1
200.1.1.1/32	10.10.10.2
20.1.0.0/16	10.10.10.3
0.0.0.0/0	10.10.10.4

**Nota:** El perfil de usuario también puede especificar un valor para el atributo Ascend-Client-Gateway, pero este valor *no* modificará una ruta privada predeterminada especificada por el atributo Ascend-Private-Route.

Si la dirección del ruteador del siguiente salto especificada por un atributo Ascend-Private-Route es la dirección cero (0.0.0.0), se efectúa una búsqueda de esta ruta en la tabla de ruteo global, con lo que se proporciona un mecanismo para ir a la tabla global para rutas privadas específicas. Por ejemplo, con las rutas privadas definidas en el perfil de usuario RADIUS siguiente:

```
pipe50 Password = "ascend" User-Service = Framed
Framed-Protocol = PPP,
```

```
Framed-IP-Address = 10.1.1.1,  
Framed-IP-Netmask = 255.0.0.0,  
Ascend-Private-Route = "170.1.0.0/16 10.10.10.1 1"  
Ascend-Private-Route = "200.1.1.1/32 10.10.10.2"  
Ascend-Private-Route = "20.1.0.0/16 0.0.0.0 1"  
Ascend-Private-Route = "0.0.0.0/0 10.10.10.4 1"
```

La tabla de ruteo privado para esta conexión contiene las rutas siguientes:

Dest/Mask	Gateway
170.1.0.0/16	10.10.10.1
200.1.1.1/32	10.10.10.2
20.1.0.0/16	0.0.0.0
0.0.0.0/0	10.10.10.4

Con esta tabla de ruteo privado, una búsqueda de ruta para la red 20.1.0.0/16 pasa a la tabla de ruteo global.

## ***Definición de políticas de ruteo TCP/IP***

El ruteador TAOS posee muchos ajustes de configuración que repercuten en su funcionamiento. Los ajustes que determinan sus políticas de ruteo son la seguridad, opciones RIP, opciones de caché de ruta IP y otras opciones. Estos ajustes sólo están disponibles en el perfil IP-Global. No tienen un equivalente en RADIUS.

**Nota:** También puede configurar la unidad TAOS para que defina bits de prioridad QoS y clases de servicio TOS en nombre de las aplicaciones del cliente. Estos ajustes podrán ser utilizados posteriormente por otros ruteadores para asignar una prioridad a los enlaces y seleccionarlos para corrientes de datos concretas. Estas políticas se definen en interfaces WAN. Para obtener información detallada, consulte el apartado “Ejemplos de definición de la política QoS y TOS” en la página 2-24.

## **Definición de una dirección IP de origen del sistema**

La dirección IP de sistema es la dirección de origen que se utiliza para todos los paquetes generados por el sistema. Por ejemplo, esta dirección se utiliza para peticiones RADIUS, peticiones de túnel ATMP o un comando Telnet, Traceroute o Ping originado en la unidad. Debe ser la dirección real de una de las interfaces IP LAN de la unidad o la dirección independiente de la interfaz que se describe en “Ejemplo de definición de la interfaz software” en la página 2-10.

A continuación se muestra el parámetro utilizado para especificar una dirección de sistema:

```
[in IP-GLOBAL]  
system-ip-addr = 0.0.0.0
```

Con la dirección predeterminada cero, la unidad TAOS utiliza la dirección IP asignada a la interfaz Ethernet del controlador del módulo como dirección de origen para los paquetes que genera. Una razón para establecer una dirección de sistema que no sea la dirección predeterminada es que de este modo se simplifica el control de accesos. Por ejemplo, la mayoría de los servidores RADIUS mantienen una base de datos de clientes RAS conocidos y sus claves de autenticación. Si no se especifica una dirección de sistema, la base de datos

RADIUS deberá incluir una lista completa de todas las direcciones de interfaz del sistema. Si se especifica una dirección de sistema, se utiliza para todos los paquetes de petición RADIUS.

Otra razón para establecer una dirección de sistema es garantizar que los paquetes enviados desde un agente local ATMP a agentes externos tengan una dirección de origen única estándar. Se recomienda una dirección de sistema para agentes locales ATMP que tengan varias interfaces en la nube IP que las separe de los agentes externos, a fin de evitar que se produzcan problemas de comunicación si una ruta cambia dentro de la nube IP. Para obtener información detallada, consulte el apartado “Recomendación sobre la dirección IP del sistema” en la página 4-2.

A continuación se muestra un ejemplo de configuración del parámetro System-IP-Addr con una dirección asignada a un puerto en una tarjeta de ranura:

```
admin> dir ip-interface
      6  09/14/1999  10:13:24  { { any-shelf any-slot 0 } 0 }
      8  09/14/1999  10:13:24  { { shelf-1 left-controller 1 } 0 }
     19  09/14/1999  10:14:02  { { shelf-1 right-controller 1 } 0 }
      8  09/14/1999  11:36:32  { { shelf-1 slot-12 2 } 0 }
      8  09/14/1999  11:36:32  { { shelf-1 slot-12 3 } 0 }
      8  09/14/1999  11:36:32  { { shelf-1 slot-12 4 } 0 }
      8  09/14/1999  11:36:59  { { shelf-1 slot-12 5 } 0 }
     64  09/14/1999  11:53:12  { { shelf-1 slot-12 1 } 0 }

admin> get ip-int { { 1 12 1 } 0 } ip-address
ip-address = 10.2.3.4

admin> read ip-global
IP-GLOBAL read

admin> set system-ip-addr = 10.2.3.4

admin> write
IP-GLOBAL written
```

## Definición de políticas de seguridad del ruteador

Los parámetros siguientes (que aparecen con los ajustes predeterminados) afectan a la seguridad del ruteador:

```
[in IP-GLOBAL]
must-accept-address-assign = no
shared-prof = no
telnet-password = ""
user-profile = ""
```

Parámetro	Especifica
Must-Accept-Address-Assign	Activa y desactiva el rechazo de una dirección IP asignada por un emisor de entrada durante la negociación PPP.
Shared-Prof	Activa y desactiva los perfiles compartidos. Sólo se recomienda compartir perfiles en las redes de baja seguridad.
Telnet-Password	Contraseña necesaria para el acceso Telnet a la unidad TAOS.
User-Profile	Nombre de un perfil User predeterminado para sesiones Telnet.

## *Requisito de aceptación de asignación dinámica de direcciones*

Durante la negociación PPP, puede ser que una estación que realice una llamada rechace una dirección IP ofrecida por el ruteador y que presente la propia dirección IP del emisor. Por razones de seguridad, muchos entornos establecen Must-Accept-Address-Assign con el valor Yes para garantizar que la unidad TAOS finalice la llamada, como se muestra en el ejemplo siguiente:

```
admin> read ip-global
IP-GLOBAL read

admin> set must-accept-address-assign = yes

admin> write
IP-GLOBAL written
```

Para que se produzca la asignación de direcciones, la unidad TAOS debe poseer una dirección disponible para la asignación, el perfil Answer-Defaults debe permitir la asignación dinámica, el perfil del emisor debe especificar la asignación dinámica y el software de llamada de entrada PPP del emisor debe estar configurado para obtener la dirección IP de forma dinámica. Para obtener información detallada, consulte el apartado “Ejemplos de asignación de una dirección desde una agrupación” en la página 2-74.

## *Perfiles compartidos*

En situaciones de baja seguridad, varios emisores pueden compartir un nombre y una contraseña para acceder a la red local. Si no necesita la seguridad agregada de garantizar que cada conexión sea autenticada con su propia contraseña, puede establecer el parámetro Shared-Prof de la forma siguiente:

```
admin> read ip-global
IP-GLOBAL read

admin> set shared-prof = yes

admin> write
IP-GLOBAL written
```

Si activa los perfiles compartidos, el perfil no debe tener como resultado una dirección IP compartida (dos emisores en ubicaciones distintas que comparten la misma dirección). El perfil no debe asignar ninguna dirección IP o debe asignar una de forma dinámica. Si el perfil compartido utiliza la asignación dinámica de direcciones, cada llamada es una conexión diferente que comparte el mismo nombre y la misma contraseña, pero a cada emisor se le asigna una dirección IP distinta de forma dinámica. Para obtener información detallada acerca de la asignación dinámica de direcciones IP, consulte “Ejemplos de asignación de una dirección desde una agrupación” en la página 2-74.

También puede activar perfiles compartidos para cada conexión aunque estos ya no estén permitidos para todo el sistema. Esta función también está disponible en perfiles RADIUS a través del atributo Ascend-Shared-Profile-Enable. Utilice el parámetro siguiente (que aparece con el ajuste predeterminado) para activar o desactivar perfiles compartidos para cada usuario:

```
[in CONNECTION/""]
shared-prof = no
```

<b>Parámetro</b>	<b>Especifica</b>
Shared-Prof	Activa y desactiva varios emisores para que compartan el perfil Connection, siempre que no se produzcan conflictos de dirección IP. Con el ajuste predeterminado establecido en <b>no</b> , el ajuste del parámetro Shared-Prof en el perfil IP-Global permite o impide los perfiles compartidos en el sistema.

Si el perfil IP-Global establece Shared-Prof en **yes**, el ajuste Shared-Prof en un perfil Connection no tiene ningún efecto. Sin embargo, si el perfil IP-Global establece Shared-Prof en **no** y un perfil Connection establece el valor en **yes**, tiene preferencia el ajuste de un perfil Connection. Por ejemplo, con los ajustes siguientes, varios emisores pueden llamar y autenticar un perfil Connection denominado **shared-1**:

```
admin> get ip-global shared-prof
[in IP-GLOBAL:shared-prof]
shared-prof = no

admin> read connection shared-1
CONNECTION/shared-1 read

admin> set shared-prof = yes

admin> set ip-options ip-routing-enabled = no

admin> write
CONNECTION/shared-1 written
```

### *Especificación de un perfil User predeterminado para el acceso Telnet*

RADIUS utiliza el par atributo-valor siguiente para especificar un perfil User predeterminado para el acceso Telnet autenticado por RADIUS a la unidad TAOS:

<b>Atributo</b>	<b>Especifica</b>
Ascend-Telnet-Profile (91)	Nombre de un perfil User de la unidad TAOS que se va a utilizar para autenticar inicios de sesión Telnet.

Cuando un usuario intenta ejecutar Telnet en la interfaz de la unidad TAOS, el sistema busca en primer lugar un perfil User que coincida con el nombre y la contraseña de inicio de sesión proporcionados por el usuario. Si no lo encuentra, el sistema utiliza el servidor especificado en el perfil External-Auth para encontrar un perfil de usuario RADIUS. Si el servidor RADIUS devuelve un perfil que incluya el atributo Ascend-Telnet-Profile, el sistema utiliza el perfil User especificado para autenticar y establecer los permisos para la sesión. Sólo es posible utilizar perfiles RADIUS que especifiquen un valor para este atributo para autenticar un inicio de sesión Telnet en la interfaz de la unidad TAOS. A continuación se muestra un ejemplo de perfil RADIUS que permite el acceso Telnet a la unidad TAOS con permisos de administrador:

```
admin Password = "secret-pw"
    Service-Type = Framed-User,
    Ascend-Telnet-Profile = admin
```



## *Restricción del acceso Telnet al sistema*

Un usuario puede iniciar una sesión Telnet en la línea de comandos de la unidad TAOS desde una estación de trabajo local o desde una conexión WAN. En ambos casos, la unidad TAOS autentica la sesión mediante un perfil User, el cual define un nivel de permiso para el usuario que se conecta. Para obtener información detallada acerca de los perfiles User, consulte la publicación *APX 8000/MAX TNT/DSLNT Reference (Referencia de APX 8000/MAX TNT/DSLNT)*.

Además de la contraseña necesaria para un perfil User, puede especificar que Telnet requiera su propia autenticación de contraseña, lo que tiene lugar antes de la autenticación del perfil User.

Los comandos del ejemplo siguiente establecen el parámetro Telnet-Password y especifican el perfil Default User para inicios de sesión Telnet. El perfil Default autoriza unos permisos mínimos y no requiere contraseña.

```
admin> read ip-global
IP-GLOBAL read

admin> set telnet-password = !234#@

admin> set user-profile = default

admin> write
IP-GLOBAL written
```

Cuando los usuarios ejecutan Telnet al sistema, disponen de tres intentos, cada uno de ellos con un límite de 60 segundos, para introducir la contraseña Telnet correcta. Si los tres intentos fallan, la conexión agota el tiempo de espera. Si se especifica la contraseña Telnet correcta, la unidad TAOS solicita de nuevo un nombre de usuario y una contraseña para autenticar un perfil User. En el ejemplo siguiente un usuario inicia una sesión Telnet para una unidad TAOS denominada TAOS01, para la que se ha especificado una contraseña Telnet.

```
% telnet taos01
<taos01> Enter Password:

Trying 10.1.2.3 ...
Connected to taos01.abc.com.
Escape character is '^]'.
User:
```

Una vez introducida la contraseña Telnet correcta, el sistema solicita al usuario un nombre de usuario y una contraseña para autenticar un perfil User.

## **Definición de políticas de ruteo general del sistema**

Los parámetros siguientes (que aparecen con los ajustes predeterminados) especifican políticas de ruteo general del sistema:

```
[in IP-GLOBAL]
ignore-icmp-redirects = no
icmp-reply-directed-bcast = no
```

```
drop-source-routed-ip-packets = no
static-pref = 100
```

Parámetro	Especifica
Ignore-ICMP-Redirects	Activa y desactiva el proceso de paquetes de redireccionamiento ICMP.
ICMP-Reply-Directed-Bcast	Activa y desactiva la respuesta como host a peticiones de eco ICMP de difusión general dirigida.
Drop-Source-Routed-IP-Packets	Activa y desactiva el envío de paquetes IP que tienen activa la opción de ruta de origen.
Static-Pref	Preferencia predeterminada asignada a las rutas IP estáticas.

### *Cómo pasar por alto paquetes ICMP*

Los paquetes de redireccionamiento ICMP pueden falsificarse y utilizarse para cambiar la forma que tiene un dispositivo de rutear paquetes. Por razones de seguridad, muchos entornos optan por pasar por alto los redireccionamientos ICMP.

Las peticiones de eco ICMP a la dirección de difusión general se han utilizado en ataques de denegación de servicio. Para evitar la utilización del ruteador TAOS en un ataque de denegación de servicio cuando un atacante comprometa a otro ruteador de la misma red Ethernet que la unidad TAOS, puede impedir que la unidad TAOS responda a peticiones de eco ICMP de difusión general dirigida enviadas a la dirección IP de difusión general.

Los comandos siguientes configuran la unidad para que pase por alto ambos tipos de paquetes ICMP. De manera predeterminada, la unidad no responde a peticiones de eco ICMP enviadas a la dirección de difusión general.

```
admin> read ip-global
IP-GLOBAL read

admin> set ignore-icmp-redirects = yes

admin> write
IP-GLOBAL written
```

### *Descarte de paquetes de ruteados en origen*

El ajuste predeterminado para el parámetro Drop-Source-Routed-IP-Packets es No, que hace que el ruteador envíe todos los paquetes ruteados en origen de la forma descrita en el documento RFC1812, *Requirements For Routers*. Si el parámetro está establecido en Yes, el ruteador descarta todos los paquetes que tienen una ruta de origen de tipo Loose o Strict entre sus opciones IP. El conjunto de comandos siguiente hace que el ruteador descarte los paquetes ruteados en origen:

```
admin> read ip-global
IP-GLOBAL read

admin> set drop-source-routed-ip-packets = yes

admin> write
IP-GLOBAL written
```

### *Definición de preferencias de ruta estática*

Dado que la métrica RIP y la métrica OSPF son incompatibles, la unidad TAOS admite preferencias de ruta, que proporcionan un modo de ponderar las rutas que tiene preferencia sobre la métrica de rutas. Al seleccionar una ruta, el ruteador compara en primer lugar los valores de preferencia y elige el número más bajo. Si los valores de preferencia son iguales, el ruteador compara los valores de métrica y utiliza la ruta con una métrica más baja. A continuación se muestran las preferencias predeterminadas para distintos tipos de ruta:

- 0 (cero): Rutas conectadas
- 10: Rutas OSPF
- 30: Rutas obtenidas a partir de redireccionamientos ICMP
- 100: Rutas obtenidas a partir de RIP
- 100: Rutas estáticas

Si el valor de preferencia de una ruta dinámica es menor que el de la ruta estática, la ruta dinámica puede ocultar (sobrescribir temporalmente) una ruta estática de la misma red. Sin embargo, las rutas dinámicas envejecen y, si no se reciben actualizaciones, finalmente caducan. En ese caso, la ruta estática oculta reaparece en la tabla de ruteo. De manera predeterminada, las rutas estáticas y las rutas RIP tienen el mismo valor de preferencia, a fin de poder ponderarlas de forma igual. Los redireccionamientos ICMP tienen preferencia sobre los dos tipos de ruta anteriores y OSPF tiene preferencia sobre todos.

El comando siguiente disminuye el valor de preferencia de las rutas estáticas e indica al ruteador que utilice dichas rutas en primer lugar, si las hay:

```
admin> read ip-global
IP-GLOBAL read

admin> set static-pref = 50

admin> write
IP-GLOBAL written
```

## **Definición de opciones de protocolo de ruteo**

Los parámetros siguientes (que aparecen con los ajustes predeterminados) definen el tratamiento de las actualizaciones de protocolo de ruteo por parte de la unidad TAOS :

```
[in IP-GLOBAL]
rip-policy = Poison-Rvrs
summarize-rip-routes = no
rip-trigger = yes
rip-pref = 100
dialout-poison = no
rip-queue-depth = 0
ignore-def-route = yes
suppress-host-routes = no
ospf-pref = 10
ospf-ase-pref = 150
rip-tag = c8:00:00:00
rip-ase-type = 1
```

```
[in IP-GLOBAL:ospf-global]  
as-boundary-router = yes
```

Parámetro	Especifica
RIP-Policy	Política para enviar paquetes de actualización que incluyen rutas recibidas en la misma interfaz.
Summarize-RIP-Routes	Activa y desactiva el resumen de la información de la subred en actualizaciones de RIP-v1. Este ajuste no tiene ningún efecto en actualizaciones de RIP-v2.
RIP-Trigger	Activa y desactiva el accionamiento de RIP. Con el ajuste Yes (el ajuste predeterminado), las actualizaciones de RIP incluyen únicamente las rutas modificadas.
RIP-Pref	Ajuste de preferencia para las rutas obtenidas a partir de RIP.
Dialout-Poison	Activa y desactiva el anuncio de rutas de llamada de salida cuando no hay líneas troncales disponibles. La desactivación del anuncio (el ajuste Yes) permite que una unidad redundante asuma el control.
Ignore-Def-Route	Activa y desactiva la exclusión de rutas predeterminadas anunciadas de la tabla de ruteo.
RIP-Queue-Depth	Número máximo de paquetes RIP que se retienen para el proceso. Los valores válidos van del 0 al 1024. El ajuste predeterminado (0) implica que la unidad TAOS no descartará ningún paquete RIP, independientemente del origen del paquete.
Suppress-Host-Routes	Activa y desactiva la supresión de rutas de host para interfaces con una máscara de subred de menos de 32 bits.
OSPF-Pref	Opción de OSPF (consulte “Configuración de opciones de ruta” en la página 3-16).
OSPF-ASE-Pref	Opción de OSPF (consulte “Configuración de opciones de ruta” en la página 3-16).
RIP-Tag	Opción de OSPF (consulte “Configuración de opciones de ruta” en la página 3-16).
RIP-ASE-Type	Opción de OSPF (consulte “Configuración de opciones de ruta” en la página 3-16).
AS-Boundary-Router	Opción de OSPF (consulte “Configuración de opciones de ruta” en la página 3-16).

### *Política RIP para propagar las actualizaciones de vuelta a la subred de origen*

Puede especificar una política de horizonte dividido o de veto de rutas inverso para los paquetes de actualización de salida que incluyen rutas recibidas en la misma interfaz en la que se envía la actualización. *Horizonte dividido* significa que el ruteador no propaga rutas de vuelta a la subred desde la que se han recibido. *Veto de rutas inverso* significa que el ruteador propaga rutas de vuelta a la subred desde la que se han recibido, pero con una métrica de 16 (métrica infinita).

El conjunto de comandos siguiente especifica la política de horizonte dividido:

```
admin> read ip-global
IP-GLOBAL read

admin> set rip-policy = split

admin> write
IP-GLOBAL written
```

### *Activación de RIP*

La activación de RIP permite al ruteador etiquetar rutas que se han actualizado en la tabla de ruteo y enviar actualizaciones en las se incluyen únicamente las rutas modificadas. El resultado es una reducción de la actividad de proceso para el ruteador TAOS y sus nodos vecinos.

Con el valor predeterminado (Yes), el ruteador etiqueta los cambios de la tabla de ruteo y en la próxima actualización sólo selecciona las rutas etiquetadas. Los cambios se producen cuando una llamada llega o se desconecta, cuando RIP u OSPF obtiene una ruta de otro ruteador o cuando el administrador modifica un perfil relativo a una ruta. El ruteador realiza una difusión general de las actualizaciones de cinco a ocho segundos después de la detección del primer cambio en la tabla de ruteo. El retardo ayuda a evitar que se produzcan actualizaciones constantes durante los períodos de mayor tráfico.

Si RIP-Trigger está establecido en No, el ruteador envía actualizaciones de la tabla completa cada 20-40 segundos. Para evitar que los ruteadores RIP de una red se sincronicen y envíen actualizaciones de gran tamaño al unísono, se ha dejado de realizar una difusión general de la actualización de tabla completa a intervalos fijos de 30 segundos.

### *Definición de los valores de preferencia para rutas obtenidas de actualizaciones de RIP*

Para ver una introducción sobre las preferencias de ruta, consulte “Definición de preferencias de ruta estática” en la página 2-45. El comando siguiente aumenta el valor de preferencia de rutas obtenidas de actualizaciones de RIP e indica al ruteador que sólo utilice dichas rutas si no existe ninguna otra ruta con el mismo destino:

```
admin> read ip-global
IP-GLOBAL read

admin> set rip-pref = 150

admin> write
IP-GLOBAL written
```

### *Veto de rutas para forzar el uso de una unidad TAOS redundante*

Si tiene otra unidad TAOS que actúa como reserva de la unidad TAOS en una configuración redundante en la misma red, puede establecer el parámetro Dialout-Poison para dejar que la unidad redundante asuma el control cuando sea necesario. Si establece el parámetro en Yes, y por cualquier motivo las líneas troncales de la unidad TAOS experimentan una situación de alarma, la unidad TAOS deja de anunciar rutas IP que utilizan servicios de marcación. Con el ajuste No, la unidad continúa anunciando las rutas de llamada de salida, con lo que se impide que la unidad redundante asuma el control de la actividad de ruteo. Defina el parámetro del modo siguiente si desea que la unidad TAOS permita asumir el control a una unidad redundante.

```
admin> read ip-global
IP-GLOBAL read

admin> set dialout-poison = yes

admin> write
IP-GLOBAL written
```

### *Limitación del tamaño de las colas de paquetes UDP*

Cuando el ruteador está muy ocupado y recibe un flujo de paquetes UDP procedentes de peticiones SNMP o actualizaciones de RIP, una acumulación de paquetes a la espera de ser procesados puede crear un retardo en el ruteo suficiente para provocar problemas esporádicos con los paquetes dependientes del tiempo, como paquetes de gestión de relé de trama o de negociación LCP.

Para evitar este tipo de problemas, el proceso UDP se ejecuta con una prioridad menor que el proceso de paquetes ruteados. En un sistema muy ocupado con el ruteo de paquetes, podría significar que el proceso UDP está atrasado y que se está creando una acumulación de paquetes UDP. El parámetro RIP-Queue-Depth del perfil IP-Global y el parámetro Queue-Depth del perfil SNMP especifican el tamaño máximo de esta acumulación de paquetes.

Si establece uno de estos parámetros para especificar una profundidad de cola, es más probable que la unidad TAOS descarte los paquetes UDP cuando esté ocupada ruteando paquetes. Sin embargo, con los paquetes ruteados dependientes del tiempo los retardos son menos probables y la memoria del sistema se utiliza de una forma más eficaz.

En el ejemplo siguiente, el administrador establece ambas profundidades de cola en 50. Se retendrán para el proceso 50 paquetes de cada tipo y, si llegan paquetes adicionales de cualquiera de los dos tipos cuando la cola esté llena, se descartarán.

```
admin> read ip-global
IP-GLOBAL read

admin> set rip-queue-depth = 50

admin> write
IP-GLOBAL written

admin> read snmp
SNMP read

admin> set queue-depth = 50

admin> write
SNMP written
```

La salida del comando Netstat muestra la profundidad de cola de varios puertos UDP, así como el total de paquetes recibidos y descartados en cada puerto. En el recuento total de paquetes recibidos se incluyen los paquetes descartados. En el ejemplo siguiente, la profundidad de cola SNMP se ha establecido en 32:

```
admin> netstat udp
udp:
Socket  Local Port  InQLen  InQMax  InQDrops  Total Rx
0       1023      0       1       0         0
1       route    0       50      0         509
2       echo     0       32      0         0
3       ntp      0       32      0         0
4       1022     0       128     0         0
5       SNMP    32      32     5837     20849
```

### *Cómo pasar por alto rutas predeterminadas al actualizar la tabla de ruteo*

El parámetro Ignore-Def-Route evita que las actualizaciones de ruteo modifiquen la ruta predeterminada en la tabla de ruteo. Se trata de la configuración recomendada. El conjunto de comandos siguiente protege la ruta predeterminada frente a actualizaciones de RIP:

```
admin> read ip-global
IP-GLOBAL read

admin> set ignore-def-route = yes

admin> write
IP-GLOBAL written
```

### *Supresión de anuncios de ruta de host*

Si establece el parámetro Suppress-Host-Routes en Yes, se eliminan rutas de acuerdo con las reglas siguientes:

- Si en un perfil Connection se incluye una máscara de subred de menos de 32 bits en el ajuste Remote-Address, se eliminan las rutas de host para la interfaz mientras se negocia la sesión y, una vez establecida la sesión, sólo se anuncian las rutas de red para la interfaz.
- Si en un perfil Connection se incluye una máscara de subred de 32 bits en el ajuste Remote-Address, las rutas de host para la interfaz no se eliminan (las direcciones de la agrupación también tienen una máscara de 32 bits, de modo que no se eliminan).

El conjunto de comandos siguiente configura el ruteador para que elimine las rutas de host para conexiones que especifiquen una máscara de subred de menos de 32 bits:

```
admin> read ip-global
IP-GLOBAL read

admin> set suppress-host-routes = yes

admin> write
IP-GLOBAL written
```

## **Definición de opciones de caché de ruta IP y puerto IP**

Los parámetros siguientes (que aparecen con los ajustes predeterminados) definen la forma en que el sistema maneja el almacenamiento de rutas en la caché y el ruteo dentro del módulo y entre módulos:

```
[in IP-GLOBAL]
iproute-cache-enable = yes
iproute-cache-size = 0
ipport-cache-enable = yes
```

Parámetro	Especifica
IProute-Cache-Enable	Activa y desactiva la caché de ruta. Si debe controlar la utilización de memoria para una tarjeta, puede restringir el tamaño de la caché o desactivar la caché de ruta. <i>La opción que se recomienda es dejar las cachés de ruta activas con su tamaño predeterminado.</i>
IProute-Cache-Size	Tamaño de la caché de ruta interna. El ajuste predeterminado (0) no establece ningún límite para el tamaño de la caché. Si establece un número más alto, éste indica el número de entradas en la caché. Por lo general, no se requiere ningún límite.
IPPort-Cache-Enable	Activa y desactiva el envío de paquetes IP de tarjeta a tarjeta en función del puerto y la dirección IP de destino del paquete. Con el ajuste No, los paquetes destinados a la unidad TAOS se rutean desde la tarjeta de ranura receptora hasta la tarjeta de ranura de destino a través del controlador del módulo, en lugar de enviarse directamente desde la tarjeta de ranura receptora.

### *Cachés de ruta*

La tabla de ruteo global, que se mantiene en el controlador del módulo, se utiliza para rutear paquetes internamente hacia la interfaz correcta. Para reducir parte de la actividad de ruteo y mejorar el rendimiento, la unidad TAOS utiliza cachés de ruta en cada tarjeta de ranura. Las cachés de ruta funcionan del modo siguiente:

- Cuando una tarjeta de módem o HDLC recibe un paquete IP, lo envía al controlador del módulo, que lo rutea hacia la ranura adecuada, como una tarjeta Ethernet.
- Cuando el controlador del módulo rutea el paquete, registra una entrada de caché que se descarga en la caché de ruta de cada tarjeta de ranura.
- Si la tarjeta de módem o HDLC recibe otro paquete IP con la misma dirección de destino, comprueba su caché de ruta y envía el paquete directamente a la ranura adecuada, sin implicar al controlador del módulo.

El controlador del módulo conserva la tarea de gestionar los protocolos de ruteo, la tabla de ruteo global y las propias cachés de ruta. Pero cada tarjeta de ranura puede examinar una caché IP de pequeñas dimensiones y rutear paquetes hacia una interfaz de destino sin implicar al controlador del módulo. Si una tarjeta de ranura recibe un paquete IP para el que no dispone de ninguna entrada de caché, lo envía al controlador del módulo, el cual lo rutea y registra una entrada de caché en todas las tarjetas de ranura.

### *Cachés de puerto*

Al igual que las cachés de ruta IP, las cachés de puerto reducen la carga de trabajo del controlador del módulo permitiendo que las tarjetas de ranura gestionen sus propias tareas. Mientras que las cachés de ruta permiten a las tarjetas buscar una interfaz de destino para el tráfico de salida, las cachés de puerto permiten a las tarjetas rutear el tráfico dirigido a la propia unidad TAOS, pero con una capa de protocolo superior (por ejemplo, el tráfico en una sesión TCP-Clear).



En una sesión TCP-Clear, por ejemplo, se establece una conexión TCP entre una tarjeta de ranura de host, como una tarjeta de módem, y un host local al que se puede acceder mediante uno de los puertos Ethernet de la unidad TAOS. La tarjeta de módem crea paquetes TCP que contienen corrientes de datos del cliente y los envía al servidor. El almacenamiento de rutas IP en la caché permite a la tarjeta de módem enviar los paquetes TCP directamente a la tarjeta Ethernet sin tener que pasar por el controlador del módulo. Sin embargo, cuando el host local devuelve paquetes al cliente de llamada de entrada, no hay caché de ruta IP, dado que el paquete está destinado a la propia unidad TAOS. De modo que los paquetes se entregan al ruteador, que los envía a la tarjeta de módem mediante el número de puerto de destino.

Si el parámetro IP-Port-Cache-Enable está establecido en Yes (el valor predeterminado), la tarjeta de ranura que recibe los paquetes destinados a la unidad TAOS (por ejemplo, una tarjeta Ethernet) los rutea directamente a la tarjeta de ranura de destino (como la tarjeta de módem), en lugar de enviarlos a través del controlador del módulo.

## Activación de opciones de protocolo

Los parámetros siguientes (que aparecen con los ajustes predeterminados) configuran opciones de protocolo TCP/IP:

```
[in IP-GLOBAL]
bootp-enabled = no
rarp-enabled = no
udp-cksum = yes
tcp-timeout = 0
finger = no

[in IP-GLOBAL:bootp-relay]
active = no

[in IP-GLOBAL:bootp-relay:bootp-servers]
bootp-servers[1] = 0.0.0.0
bootp-servers[2] = 0.0.0.0

[in IP-GLOBAL:sntp-info]
enabled = no
gmt-offset = utc+0000
host = [0.0.0.0 0.0.0.0 0.0.0.0]

[in IP-GLOBAL:sntp-info:host]
host[1] = 0.0.0.0
host[2] = 0.0.0.0
host[3] = 0.0.0.0
```

Parámetro	Especifica
BOOTP-Enabled	Activa y desactiva la consulta de un servidor BOOTP.
RARP-Enabled	Activa y desactiva la obtención de las direcciones IP del sistema a partir de un servidor RARP.
UDP-Cksum	Activa y desactiva las sumas de comprobación UDP.
TCP-Timeout	Intervalo para los reintentos TCP. Los valores válidos son de 0 a 200 segundos.

<b>Parámetro</b>	<b>Especifica</b>
Finger	Activa y desactiva la respuesta a consultas Finger remotas. Si Finger está establecido en No (el valor predeterminado), la unidad TAOS rechaza las consultas procedentes de clientes Finger y envía un mensaje en el que indica que se ha denegado la lista de usuarios en línea Finger.
BOOTP-Relay:Active	Activa y desactiva el relé BOOTP.
BOOTP-Relay:BOOTP-Servers[1]	Dirección IP de hasta dos servidores BOOTP. Sólo es necesaria una dirección.
BOOTP-Relay:BOOTP-Servers[2]	
SNTP-Info:Enabled	Activa y desactiva el protocolo SNTP.
SNTP-Info:GMT-Offset	Zona horaria actual expresada como diferencia respecto a la UTC (Hora universal coordinada). UTC se encuentra en la misma zona horaria que GMT (Hora media de Greenwich).
SNTP-Info:Host[1]	Direcciones IP de hasta tres servidores SNTP. Sólo es necesaria una dirección.
SNTP-Info:Host[2]	
SNTP-Info:Host[3]	

### *Activación del protocolo Boot y Reverse-ARP*

El protocolo Boot (BOOTP) es un protocolo basado en UDP/IP que permite a un host obtener su configuración de forma dinámica a partir de un servidor BOOTP. Reverse-ARP (RARP) permite a un host obtener su dirección a partir de un servidor RARP. Los comandos siguientes activan BOOTP y RARP:

```
admin> read ip-global
IP-GLOBAL read

admin> set bootp-enabled = yes

admin> set rarp-enabled = yes

admin> write
IP-GLOBAL written
```

### *Activación de sumas de comprobación UDP*

Si la integridad de los datos es prioritaria en la red y las comprobaciones de redundancia son importantes, puede activar las sumas de comprobación UDP para generar una suma de comprobación cada vez que se transmite un paquete UDP. Los paquetes UDP se transmiten para consultas y respuestas relativas a ATMP, SYSLOG, DNS, ECHOSERV, RADIUS, TACACS, RIP, SNTP y TFTP.

Los comandos siguientes activan sumas de comprobación UDP para paquetes transmitidos:

```
admin> read ip-global
IP-GLOBAL read

admin> set udp-cksum = yes

admin> write
IP-GLOBAL written
```

## *Definición de un tiempo de espera TCP*

El parámetro TCP-Timeout ajusta el temporizador de reintentos TCP. Con el ajuste predeterminado (0), el sistema realiza un número fijo de reintentos a intervalos crecientes que ascienden hasta unos 170 segundos en total. Hay otros límites del sistema que interrumpen los reintentos TCP después de unos 170 segundos, aunque el parámetro tenga un número más alto. Si establece TCP-Timeout con un valor distinto de cero, dicho valor especifica el número de segundos durante los que persisten los reintentos TCP. Una vez transcurridos los minutos especificados, los reintentos cesan y la conexión se considera perdida.

TCP-Timeout se aplica a todas las conexiones TCP iniciadas desde la unidad TAOS, incluidas Telnet, Rlogin, TCP-Clear y la porción TCP de las consultas DNS. Este parámetro se aplica tanto a las conexiones TCP establecidas como a los intentos iniciales de conectarse. Una situación en la que debería ajustar el temporizador de reintentos TCP sería, por ejemplo, cuando un usuario emplea software de cliente para introducir un nombre de host en una sesión de servidor de terminales y DNS devuelve una lista de direcciones IP para el host. Si la primera dirección resulta inaccesible y el tiempo de espera en cada intento es largo, el software de cliente a menudo agota el tiempo de espera antes de encontrar una dirección correcta.

Los comandos siguientes establecen el tiempo de espera en 50 segundos:

```
admin> read ip-global
IP-GLOBAL read

admin> set tcp-timeout = 50

admin> write
IP-GLOBAL written
```

El ajuste óptimo para el parámetro TCP-Timeout depende de las características de los hosts (servidor) de destino TCP y, por lo tanto, deben basarse en la experiencia. Por ejemplo, si todos los destinos se encuentran en una LAN subordinados al mismo control administrativo que la unidad TAOS y tienen un tráfico ligero, puede ser razonable un tiempo de espera corto (unos pocos segundos), ya que un host que no responda dentro de dicho intervalo probablemente estará desconectado. Por el contrario, si el entorno incluye servidores con tiempos de latencia de red prolongados (por ejemplo, los conectados en la WAN), si el tráfico es intenso en la red o el ruteador, o si las características de los hosts remotos no son del todo conocidas, resulta apropiado un tiempo de espera más largo. Los valores de 30 a 60 segundos son habituales en las implementaciones TCP UNIX.

## *Activación de respuestas a consultas Finger*

Si Finger (descrito en el documento RFC 1288) está activo en el perfil IP-Global, la unidad TAOS puede devolver información de usuario a una consulta Finger remota. Los comandos siguientes permiten a la unidad TAOS aceptar consultas Finger y devolver a un cliente remoto los detalles solicitados sobre las sesiones activas:

```
admin> read ip-global
IP-GLOBAL read

admin> set finger = yes

admin> write
IP-GLOBAL written
```

Si el parámetro Finger está establecido en Yes, un cliente (por ejemplo, un cliente UNIX) puede solicitar información sobre sesiones para el sistema denominado TAOS1 introduciendo el comando siguiente:

```
# finger @taos1
```

Este comando visualiza la información con un formato estrecho (80 caracteres de ancho). El cliente puede solicitar la información con formato ancho utilizando el comando con la opción -l. Por ejemplo, el comando siguiente:

```
# finger -l @taos1
```

muestra con un formato ancho (140 caracteres de ancho) información sobre sesiones para el sistema denominado TAOS1. El cliente puede, asimismo, solicitar los detalles de todas las sesiones o de una sola sesión. Por ejemplo, el comando siguiente solicita información sobre un solo usuario llamado Gavin:

```
# finger gavin@taos1
```

No se da soporte al servicio de envío Finger. Utiliza el formato de nombre de host siguiente:

```
@host1@host2
```

Un cliente remoto que utilice el formato de petición de envío recibirá el mensaje siguiente:

```
Finger forwarding service denied.
```

### *Activación de BOOTP-Relay*

Si un host que solicita una dirección no reside en la misma red IP que un servidor BOOTP, se necesita un sistema intermediario para que transfiera los mensajes entre el cliente y el servidor. El host intermediario es un agente retransmisor BOOTP.

Los comandos siguientes activan la función de retransmisión BOOTP y especifican la dirección de un servidor BOOTP:

```
admin> read ip-global
IP-GLOBAL read

admin> list bootp-relay
[in IP-GLOBAL:bootp-relay]
active = no
bootp-servers = [ 0.0.0.0 0.0.0.0 ]

admin> set active = yes

admin> set bootp-servers 1 = 10.178.10.125

admin> write
IP-GLOBAL written
```

Si se ha especificado más de un servidor, la unidad TAOS utiliza el primer servidor hasta que deja de estar disponible. Una vez que la unidad empieza a utilizar el segundo servidor, continúa utilizándolo hasta que deja de estar disponible, momento en el que la unidad pasa a utilizar de nuevo el primer servidor.

## *Utilización de SNTP para ajustar y mantener la hora del sistema*

La unidad TAOS puede utilizar el SNTP (Protocolo de hora de red simple), descrito en el documento RFC 1305, para ajustar y mantener la hora del sistema mediante la comunicación con un servidor SNTP.

La zona horaria del sistema se expresa como diferencia respecto a la UTC (Hora universal coordinada). UTC se encuentra en la misma zona horaria que GMT (Hora media de Greenwich). La diferencia especifica las horas y los minutos respecto a UTC mediante un reloj de 24 horas. Dado que algunas zonas horarias, como Terranova, no poseen un límite horario par, la diferencia incluye cuatro dígitos y precisa incrementos de media hora.

Por ejemplo, en Terranova es 1,5 horas más temprano que la hora UTC, de modo que la diferencia es UTC-0130. En San Francisco, donde es 8 horas más temprano que la hora UTC, la diferencia es UTC -0800. En Fráncfort, donde es una hora más tarde que la hora UTC, la diferencia es UTC +0100.

Los comandos del ejemplo siguiente especifican la zona horaria para San Francisco y la dirección de un servidor SNTP:

```
admin> read ip-global
IP-GLOBAL read

admin> list sntp-info
enabled = no
gmt-offset = utc+0000
host = [0.0.0.0 0.0.0.0 0.0.0.0]

admin> set enabled = yes
admin> set gmt = utc-0800
admin> set host 1 = 10.2.3.4
admin> write
IP-GLOBAL written
```

La unidad TAOS siempre se comunica con la primera dirección a menos que ésta sea inaccesible. En ese caso, la unidad intenta comunicarse con la segunda dirección y sólo lo intenta con la tercera si las otras dos son inaccesibles.

## **Configuración de una redirección de puerto**

La redirección de puerto permite configurar un perfil Connection o RADIUS que redirija determinados tipos de paquete a un servidor especificado. Por ejemplo, puede redirigir tráfico HTTP (Protocolo de transferencia de hipertexto) a un servidor de caché de Web de una red local. Sin embargo, la redirección de puerto no está limitada al tráfico HTTP. Puede utilizar esta función para redirigir cualquier paquete TCP o UDP en función de la información del puerto y el protocolo.

### *Información general sobre los ajustes del perfil Connection*

Para configurar la redirección de puerto en un perfil Connection, establezca los parámetros siguientes (que aparecen con los ajustes predeterminados):

```
[in CONNECTION/"":port-redirect-options]
protocol = none
```

```
port-number = 0
redirect-address = 0.0.0.0
```

<b>Parámetro</b>	<b>Especifica</b>
Protocol	Tipo de protocolo. Los ajustes válidos son none (el ajuste predeterminado, que desactiva la redirección de puerto), udp y tcp. El ajuste especificado, junto con el ajuste de Port-Number, define un tipo de paquete. Por ejemplo, tcp con 21 representa tráfico FTP y tcp con 23 representa tráfico Telnet. Para el tráfico HTTP, establezca el parámetro en tcp.
Port-Number	Número de puerto que se debe comparar con el puerto de destino de un paquete. Por lo general, los números de puerto TCP y UDP se asignan a servicios. Por ejemplo, el tráfico HTTP utiliza el puerto TCP 80. Para obtener una lista de los números de puerto asignados, consulte el documento RFC 1700, <i>Assigned Numbers</i> .
Redirect-Address	Dirección IP a la que se redirigen los paquetes que coinciden con los valores especificados.

### *Información general sobre los ajustes de RADIUS*

RADIUS utiliza los pares atributo-valor siguientes para la redirección de puerto:

<b>Atributo</b>	<b>Especifica</b>
Ascend-Port-Redir-Protocol (82)	Tipo de protocolo. Los valores válidos son Ascend-Proto-TCP (6) y Ascend-Proto-UDP (17). El valor especificado, junto con el valor de Ascend-Port-Redir-Portnum, define un tipo de paquete. Por ejemplo, Ascend-Proto-TCP con 21 representa tráfico FTP y Ascend-Proto-TCP con 23 representa tráfico Telnet. Para el tráfico HTTP, especifique Ascend-Proto-TCP (6).
Ascend-Port-Redir-Portnum (83)	Número de puerto que se debe comparar con el puerto de destino de un paquete. Por lo general, los números de puerto TCP y UDP se asignan a servicios. Por ejemplo, el tráfico HTTP utiliza el puerto TCP 80. Para obtener una lista de los números de puerto asignados, consulte el documento RFC 1700, <i>Assigned Numbers</i> .
Ascend-Port-Redir-Server (84)	Dirección IP a la que se redirigen los paquetes que coinciden con los valores especificados.

Para utilizar estos atributos, el servidor RADIUS debe permitir atributos específicos del proveedor (VSA) y la unidad TAOS debe estar configurada en el modo de compatibilidad con VSA. A continuación se muestran los ajustes pertinentes:

```
[in EXTERNAL-AUTH]
auth-type = radius

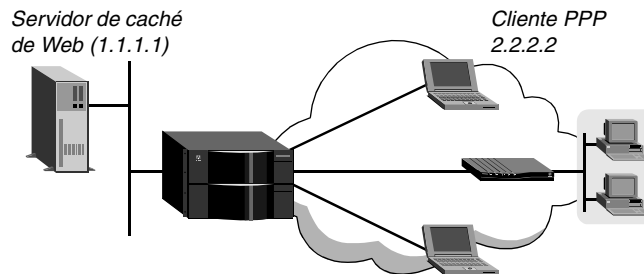
[in EXTERNAL-AUTH:rad-auth-client]
auth-radius-compatible = vendor-specific
```

Si desea obtener información detallada acerca de estos ajustes, consulte la publicación *APX 8000/MAX TNT/DSLNT Reference (Referencia de APX 8000/MAX TNT/DSLNT)*.

### *Ejemplo de configuración de una redirección de puerto*

En este ejemplo, la unidad TAOS redirige las peticiones de explorador de un cliente PPP hacia un servidor de caché de Web en 1.1.1.1. El servidor de caché de Web puede responder directamente si se encuentra una entrada de caché; pero si no se encuentra ninguna, envía la petición de explorador a su destino original. La configuración de ejemplo se muestra en la Figura 2-9.

*Figura 2-9. Redirección de puerto hacia un servidor HTTP*



Los comandos siguientes configuran un perfil local para el cliente PPP de forma que redirija el tráfico HTTP al servidor que se encuentra en 1.1.1.1:

```
admin> new connection atcp50
CONNECTION/atcp50 read
admin> set active = yes
admin> set ip-options remote-address = 2.2.2.2/32
admin> set ppp-options recv-password = test
admin> set port-redirect-options protocol = tcp
admin> set port-redirect-options port-number = 80
admin> set port-redirect-options redirect-address = 1.1.1.1
admin> write
CONNECTION/atcp50 written
```

A continuación se muestra un perfil RADIUS equivalente:

```
atcp50 Password = "test"
  Service-Type = Framed,
  Framed-Protocol = MPP,
  Framed-IP-Address = 2.2.2.2,
  Framed-IP-Netmask = 255.255.255.255,
  Ascend-Port-Redir-Protocol = Ascend-Proto-TCP,
  Ascend-Port-Redir-Portnum = 80,
  Ascend-Port-Redir-Server = 1.1.1.1
```

## **Configuración de DNS**

DNS (Sistema de nombres de dominio) es un servicio TCP/IP para la gestión centralizada de la resolución de direcciones. Los proveedores de servicios pueden realizar el mantenimiento de varios servidores DNS, cada uno de los cuales puede estar dedicado a un cliente o ubicación determinados. En ese caso, puede ser importante por razones de seguridad garantizar que esas conexiones se dirijan siempre al servicio DNS correcto. Con un acceso DNS por conexión, un

proveedor de servicios puede dirigir usuarios específicos hacia los servidores DNS apropiados para sus servicios o ubicaciones.

En la unidad TAOS la configuración DNS incluye ajustes para activar búsquedas DNS locales y dar soporte a la lista DNS, ajustes para una tabla DNS local mantenida en la RAM y, finalmente, DNS de cliente para redirigir conexiones hacia un servicio DNS concreto.

## Configuración de búsquedas DNS y la lista DNS

A continuación se muestran los parámetros (con los ajustes predeterminados) para configurar DNS de forma que permita búsquedas y dé soporte a la lista DNS:

```
[in IP-GLOBAL]
domain-name = ""
dns-primary-server = 0.0.0.0
dns-secondary-server = 0.0.0.0
netbios-primary-ns = 0.0.0.0
netbios-secondary-ns = 0.0.0.0
dns-list-attempt = no
dns-list-size = 6
sec-domain-name = ""
```

Parámetro	Especifica
Domain-Name	Número de dominio primario que se debe utilizar para las búsquedas DNS. La unidad TAOS agrega este nombre de dominio a los nombres de host al realizar búsquedas.
DNS-Primary-Server	Dirección del servidor DNS local primario que se debe utilizar para las búsquedas.
DNS-Secondary-Server	Dirección del servidor DNS local secundario que se debe utilizar para las búsquedas. Sólo se utiliza si no se encuentra el servidor primario.
NetBIOS-Primary-NS NetBIOS-Secondary-NS	Direcciones de un servidor NetBIOS primario y secundario.
DNS-List-Attempt	Activa y desactiva la lista DNS.
DNS-List-Size	Número máximo de hosts que puede haber en una lista DNS, hasta 35.
Sec-Domain-Name	Número de dominio secundario que se debe utilizar para las búsquedas DNS si no se encuentra el nombre de host en el dominio primario.

### *Especificación de nombres de dominio para las búsquedas*

La unidad TAOS, cuando recibe un nombre de host que debe buscar, intenta varias combinaciones, incluida la adición del nombre de dominio especificado en el perfil IP-Global. Los comandos siguientes especifican un nombre de dominio primario y secundario para las búsquedas DNS:

```
admin> read ip-global
IP-GLOBAL read
admin> set domain-name = abc.com
```



```
admin> set sec-domain-name = eng.abc.com  
  
admin> write  
IP-GLOBAL written
```

Si una búsqueda falla con el primer nombre de dominio, el ruteador lo intenta de nuevo con el nombre de dominio secundario.

### *Especificación de direcciones de servidor DNS local*

Para permitir que la unidad TAOS busque direcciones mediante DNS, especifique direcciones de servidor DNS como se muestra en el ejemplo siguiente:

```
admin> read ip-global  
IP-GLOBAL read  
  
admin> set dns-pri = 10.2.3.56  
  
admin> set dns-sec = 10.2.3.107  
  
admin> write  
IP-GLOBAL written
```

Si el servidor primario no está disponible, la unidad TAOS intenta realizar una búsqueda en el servidor secundario. Para ejecutar una búsqueda de forma manual, utilice el comando Nslookup. Por ejemplo:

```
admin> nslookup techpubs  
Resolving host techpubs  
IP address for host techpubs is 10.6.212.19.
```

Los servidores DNS locales proporcionan información acerca de la red local y en ocasiones, por razones de seguridad, están aislados de los emisores de entrada. Para obtener información detallada, consulte el apartado “Utilización del DNS de cliente” en la página 2-63.

### *Soporte a la lista DNS*

Algunos servidores DNS dan soporte a una función de lista que les permite devolver varias direcciones para un nombre de host en respuesta a una consulta DNS. Sin embargo, en las respuestas no se incluye información acerca de la disponibilidad de los hosts de la lista. Por lo general, los usuarios intentan acceder a la primera dirección de la lista. Si un host no está disponible, el usuario debe intentarlo con el siguiente, y así sucesivamente.

Si un usuario de llamada de entrada utiliza la lista DNS para una conexión inmediata (por ejemplo, una conexión Telnet inmediata con un host local) y el primer intento falla, la conexión física se interrumpe. Para evitar esta desconexión y la reconexión posterior antes de intentar acceder al próximo host de la lista, active la función de lista DNS. En el ejemplo siguiente se muestra cómo activar la lista DNS con un máximo de 14 host contenidos en ella:

```
admin> read ip-global  
IP-GLOBAL read  
  
admin> set dns-list-attempt = yes  
  
admin> set dns-list-size = 14  
  
admin> write  
IP-GLOBAL written
```

Si desea obtener información al respecto, consulte “Utilización de la función Auto-Update” en la página 2-62.

## Configuración de una tabla DNS local

La unidad TAOS puede mantener en la RAM una tabla DNS de hasta ocho nombres de host y sus direcciones IP. Sólo consulta la tabla de la RAM para la resolución de direcciones si fallan las peticiones al servidor DNS. La tabla local actúa como salvaguarda para asegurar que la unidad TAOS pueda resolver el conjunto local de nombres DNS incluso si todos los servidores DNS devienen inaccesibles o se desactivan.

La tabla DNS local se propaga a la RAM desde un subperfil DNS-Local-Table configurado en el perfil IP-Global. Al encenderse, el sistema copia valores del perfil en la tabla de la RAM. Si más adelante el usuario modifica el subperfil DNS-Local-Table, los cambios se propagan a la tabla de la RAM cuando se graba el perfil.

La tabla DNS de la RAM tiene espacio para un máximo de 35 direcciones IP por entrada Host-Name (35 es el ajuste máximo para DNS-List-Size). El subperfil DNS-Local-Table permite una única dirección IP por nombre de host. Si desea obtener información al respecto, consulte “Utilización de la función Auto-Update” en la página 2-62.

Para configurar la tabla DNS local, configure los parámetros siguientes (que aparecen con los ajustes predeterminados) en el perfil IP-Global:

```
[in IP-GLOBAL:dns-local-table]
enabled = no
auto-update = no

[in IP-GLOBAL:dns-local-table:table-config]
table-config [1] = { "" 0.0.0.0 }
table-config [2] = { "" 0.0.0.0 }
table-config [3] = { "" 0.0.0.0 }
table-config [4] = { "" 0.0.0.0 }
table-config [5] = { "" 0.0.0.0 }
table-config [6] = { "" 0.0.0.0 }
table-config [7] = { "" 0.0.0.0 }
table-config [8] = { "" 0.0.0.0 }

[in IP-GLOBAL:dns-local-table:table-config[1]]
host-name = ""
ip-address = 0.0.0.0
```

<b>Parámetro de tabla DNS local</b>	<b>Especifica</b>
---	-------------------

Enabled	
---------	--

	Si la tabla DNS local de la RAM estará disponible en caso de fallar las consultas DNS. Con el ajuste No (el ajuste predeterminado), si una consulta DNS agota el tiempo de espera, la petición falla. Con el ajuste Yes, la unidad TAOS intenta resolver la consulta analizando la tabla DNS de la RAM. Si el nombre de host de la consulta DNS posee una entrada en la tabla de la RAM, el sistema devuelve las direcciones IP correspondientes al solicitante.
--	--

<b>Parámetro de tabla DNS local</b>	<b>Especifica</b>
Auto-Update	Si las consultas DNS ordinarias realizadas correctamente actualizan la tabla DNS local. Para obtener información detallada acerca de Auto-Update, consulte “Utilización de la función Auto-Update” en la página 2-62.
Table-Config[1-8]	Matriz de un máximo de ocho nombres de host y direcciones IP para la inclusión en la tabla DNS local.
Table-Config Host-Name	Nombre de host, que debe ser exclusivo dentro de la tabla y debe cumplir los requisitos descritos en “Coincidencia de nombres de host” en la página 2-61.
Table-Config IP-Address	Dirección IP válida para el ajuste Host-Name o la dirección cero. Si Auto-Update está activo e IP-Address especifica la dirección predeterminada cero, las consultas DNS realizadas correctamente crearán gradualmente la tabla local.

### *Coincidencia de nombres de host*

Un nombre de host de la tabla DNS local debe empezar por un carácter alfabético y debe tener menos de 256 caracteres. Los puntos de cola no se tienen en cuenta en la comparación.

El nombre puede ser un nombre de host o un nombre de dominio totalmente cualificado. Si en el nombre no se incluye un nombre de dominio y se han especificado uno o más ajustes Domain-Name, el sistema agrega el nombre de dominio especificado al buscar el nombre de host. Por ejemplo, si se han introducido los ajustes que se muestran en “Especificación de nombres de dominio para las búsquedas” en la página 2-58, una consulta DNS del nombre de host `wheelers` da como resultado una búsqueda de los siguientes nombres de dominio totalmente cualificados:

```
wheelers.eng.abc.com
wheelers.abc.com
```

### *Definición de la tabla local*

A continuación se muestra un ejemplo de configuración de una tabla local que especifica tres hosts:

```
admin> read ip-global
IP-GLOBAL read

admin> list dns-local
enabled = no
auto-update = no
table-config = [ { " 0.0.0.0 } { " 0.0.0.0 } { " 0.0.0.0 } { "
0.0.0.0+

admin> set enabled = yes

admin> list table 1
hostname = "
ip-address = 0.0.0.0

admin> set host = host1.abc.com

admin> set ip = 10.1.2.3
```

```
admin> list ..
table-config[1] = { host1.abc.com 10.1.2.3 }
table-config[2] = { "" 0.0.0.0 }
table-config[3] = { "" 0.0.0.0 }
table-config[4] = { "" 0.0.0.0 }
table-config[5] = { "" 0.0.0.0 }
table-config[6] = { "" 0.0.0.0 }
table-config[7] = { "" 0.0.0.0 }
table-config[8] = { "" 0.0.0.0 }

admin> set 2 host = host2.xyz.

admin> set 2 ip = 11.1.2.3

admin> set 3 host = localhost

admin> set 3 ip = 10.0.0.1

admin> write
IP-GLOBAL written
```

Si especifica una dirección IP sin especificar también un nombre de host, aparecerá un mensaje como el siguiente al grabar el perfil:

```
error: dns-local-table: host-name missing (#3 1.2.3.4)
```

Si introduce un nombre de host que no es válido, aparecerá un mensaje como el siguiente al grabar el perfil:

```
error: dns-local-table: host-name must start with alpha char (#5
11foo)
```

### *Utilización de la función Auto-Update*

Si el parámetro Auto-Update está establecido en No (el ajuste predeterminado), las consultas DNS realizadas correctamente no afectarán al contenido de la tabla local. Con el ajuste Yes, cuando se realice correctamente una consulta DNS normal, el sistema efectuará una búsqueda del nombre de host en la tabla local. Si existe una entrada para el nombre de host, las direcciones IP de la entrada se sustituyen por la respuesta a la consulta. El número de direcciones agregadas a la tabla depende de los ajustes DNS-List-Attempt y DNS-List-Size. Si DNS-List-Attempt está establecido en No, una consulta DNS realizada correctamente devolverá una única dirección para un nombre de host determinado. Esta dirección se almacena en la tabla DNS de la RAM y las 34 direcciones restantes se borran (se establecen en cero).

Si DNS-List-Attempt está establecido en Yes, una consulta DNS realizada correctamente devuelve el número de direcciones encontradas para el host hasta el valor de DNS-List-Size. En la tabla DNS de la RAM, estas direcciones se almacenan y sobrescriben la dirección configurada o las direcciones recuperadas a partir de consultas DNS anteriores. Si la tabla de la RAM contiene más direcciones que las especificadas por DNS-List-Size, las direcciones sobrantes se borran en cada actualización a fin de evitar la acumulación de direcciones caducadas.

**Nota:** Si modifica el subperfil DNS-Local-Table asignando una sola dirección a un host, la nueva dirección configurada se propaga a la tabla de la RAM. La primera dirección de la entrada Host-Name se sobrescribe con la dirección configurada y las direcciones restantes se borran. Si el parámetro Auto-Update está establecido en Yes, la próxima consulta DNS realizada correctamente sobrescribe la dirección configurada y restablece varias direcciones (hasta el ajuste de DNS-List-Size).

En el ejemplo siguiente, un administrador configura ocho nombres de host con direcciones nulas y, a continuación, establece Auto-Update en Yes. Los cambios en DNS-Local-Table se propagarán a la RAM y las consultas DNS realizadas correctamente formarán la tabla local con un máximo de 14 direcciones para cada host.

```
admin> read ip-global
IP-GLOBAL read

admin> set dns-list-attempt = yes

admin> set dns-list-size = 14

admin> list dns-local
enabled = no
auto-update = no
table-config = [ { "" 0.0.0.0 } { "" 0.0.0.0 } { "" 0.0.0.0 } { ""
0.0.0.0+

admin> set enabled = yes

admin> set auto-update = yes

admin> list table
table-config[1] = { "" 0.0.0.0 }
table-config[2] = { "" 0.0.0.0 }
table-config[3] = { "" 0.0.0.0 }
table-config[4] = { "" 0.0.0.0 }
table-config[5] = { "" 0.0.0.0 }
table-config[6] = { "" 0.0.0.0 }
table-config[7] = { "" 0.0.0.0 }
table-config[8] = { "" 0.0.0.0 }

admin> set 1 host = mercury
admin> set 2 host = venus
admin> set 3 host = earth
admin> set 4 host = mars
admin> set 5 host = jupiter
admin> set 6 host = saturn
admin> set 7 host = uranus
admin> set 8 host = neptune

admin> write
IP-GLOBAL written
```

## Utilización del DNS de cliente

El DNS de cliente especifica servidores concretos para clientes de llamada de entrada. Los ISP utilizan un DNS de cliente para dirigir los emisores hacia los servidores pertenecientes a ubicaciones o usuarios concretos, así como para evitar que dichos emisores accedan a la información de host de otros clientes.

Se puede especificar un DNS de cliente para todo el sistema a fin de permitir el acceso de los clientes de llamada de entrada a uno o dos servidores DNS. También se puede configurar para cada conexión, a fin de permitir que cada conexión configurada adecuadamente pueda acceder a uno o dos servidores específicos. En el nivel del sistema, un DNS de cliente también proporciona un mecanismo de salida hacia los servidores locales si no se puede acceder a los servidores de cliente.

Las direcciones configuradas para los servidores DNS de cliente se entregan a las conexiones WAN durante la negociación IPCP.

### *Información general sobre los ajustes de un DNS de cliente*

Puede configurar un DNS de cliente en el nivel del sistema en el perfil IP-Global. En el nivel de la conexión, puede especificar servidores DNS de cliente en perfiles Connection o RADIUS.

#### *Ajustes del perfil IP-Global*

Los parámetros siguientes (que aparecen con los ajustes predeterminados) especifican un DNS de cliente en el nivel del sistema:

```
[in IP-GLOBAL]
client-primary-dns-server = 0.0.0.0
client-secondary-dns-server = 0.0.0.0
allow-as-client-dns-info = true
```

<b>Parámetro</b>	<b>Especifica</b>
Client-DNS-Primary-Server	Dirección de un servidor DNS de cliente para clientes de llamada de entrada.
Client-DNS-Secondary-Server	Dirección de un servidor DNS secundario para clientes de llamada de entrada.
Allow-As-Client-DNS-Info	Activa y desactiva un mecanismo de salida hacia servidores locales si no se encuentran servidores DNS de cliente. Para aislar información de red local, establezca el valor False.

#### *Ajustes de los perfiles Connection*

Los parámetros siguientes (que aparecen con los ajustes predeterminados) especifican un DNS de cliente en el nivel de la conexión:

```
[in CONNECTION/"":ip-options]
client-dns-primary-addr = 0.0.0.0
client-dns-secondary-addr = 0.0.0.0
client-dns-addr-assign = yes
```

<b>Parámetro</b>	<b>Especifica</b>
Client-DNS-Primary-Addr	Dirección de un servidor DNS de cliente para la conexión.
Client-DNS-Secondary-Addr	Dirección de un servidor DNS de cliente secundario para la conexión.
Client-DNS-Addr-Assign	Activa y desactiva un DNS de cliente para la conexión. Con el ajuste Yes (el ajuste predeterminado), el sistema entrega direcciones de servidor DNS de cliente durante la negociación de la conexión. Las direcciones que presenta pueden especificarse en el perfil Connection o IP-Global.

### *Ajustes de un perfil RADIUS*

Los pares atributo-valor siguientes configuran servidores DNS de cliente en perfiles RADIUS:

<b>Atributo</b>	<b>Valor</b>
Ascend-Client-Primary-DNS (135)	Dirección de un servidor DNS de cliente para la conexión.
Ascend-Client-Secondary-DNS (136)	Dirección de un servidor DNS de cliente secundario para la conexión.
Ascend-Client-Assign-DNS (137)	Activa y desactiva un DNS de cliente para la conexión. Con el valor DNS-Assign-Yes (1), el sistema entrega direcciones de servidor DNS de cliente durante la negociación de la conexión. Las direcciones que entrega pueden especificarse en el perfil RADIUS o IP-Global.

### *Ejemplo de configuración de servidores DNS de cliente en el nivel del sistema*

Los comandos siguientes configuran servidores DNS de cliente en el nivel del sistema:

```
admin> read ip-global
IP-GLOBAL read

admin> set client-dns-pri = 10.22.17.56

admin> set client-dns-sec = 10.22.17.107

admin> set allow-as-client-dns-info = false

admin> write
IP-GLOBAL written
```

Sólo se accede al servidor secundario si el primario es inaccesible. Si ninguno de estos dos servidores DNS de cliente está accesible y el perfil del emisor no especifica servidores DNS de cliente, la unidad TAOS *no* permite que el cliente acceda a servidores DNS locales.

### *Ejemplos de configuración de un DNS de cliente en el nivel de la conexión*

Los comandos siguientes identifican dos servidores DNS para esta conexión. Sólo se accede al servidor secundario si el primario es inaccesible.

```
admin> read connection cherry
CONNECTION/cherry read

admin> set ip-options client-dns-primary-addr = 10.2.3.4

admin> set ip-options client-dns-secondary-addr = 10.2.3.56

admin> set ip-options client-dns-addr-assign = yes

admin> write
CONNECTION/cherry written
```

A continuación se muestran los ajustes equivalentes en un perfil RADIUS:

```
cherry Password = "localpw"
  Service-Type = Framed-User,
  Ascend-Client-Primary-DNS = 10.2.3.4,
```

```
Ascend-Client-Secondary-DNS = 10.2.3.56,  
Ascend-Client-Assign-DNS = DNS-Assign-Yes
```

## Configuración de la asignación de WINS de Microsoft

En la versión actual del software, puede especificar un servidor WINS (Servicio de nombres de Internet para Windows) primario y secundario para cada conexión, ya sea en perfiles RADIUS o Connection locales.

En versiones anteriores, la unidad TAOS permitía la configuración para todo el sistema de un servidor WINS NetBIOS primario y secundario a fin de dar soporte a la resolución de nombres WINS por parte de las máquinas conectadas a una red NetBIOS.

**Nota:** Para disponer de esta función, la computadora que efectúa la llamada debe tener activado el DHCP (Protocolo de configuración dinámica de hosts) para WINS en la configuración de la red.

### *Ajustes de un perfil Connection*

A continuación se muestran los parámetros locales (con los ajustes predeterminados) para configurar servidores WINS de cliente:

```
[in CONNECTION/"":ip-options]  
client-wins-primary-addr = 0.0.0.0  
client-wins-secondary-addr = 0.0.0.0  
client-wins-addr-assign = yes
```

Parámetro	Especifica
Client-WINS-Primary-Addr	Dirección de un servidor WINS de cliente para la conexión.
Client-WINS-Secondary-Addr	Dirección de un servidor WINS de cliente secundario para la conexión.
Client-WINS-Addr-Assign	Activa y desactiva un servidor WINS de cliente para la conexión. Con el ajuste Yes (el ajuste predeterminado), el sistema entrega direcciones de servidor WINS de cliente durante la negociación de la conexión.

Para obtener información detallada acerca de estos ajustes, consulte la publicación *Guía y referencia de TAOS RADIUS*. Para obtener información acerca de la especificación de servidores NetBIOS en el perfil IP-Global, consulte “Configuración de búsquedas DNS y la lista DNS” en la página 2-58.

### *Ajustes de un perfil RADIUS*

Los pares atributo-valor siguientes configuran servidores WINS de cliente en perfiles RADIUS:

Atributo RADIUS	Valor
Ascend-Client-Primary-WINS (78)	Dirección de un servidor WINS de cliente para la conexión.



<b>Atributo RADIUS</b>	<b>Valor</b>
Ascend-Client-Secondary-WINS (79)	Dirección de un servidor WINS de cliente secundario para la conexión.
Ascend-Client-Assign-WINS (80)	Activa y desactiva la utilización de servidores WINS de cliente para la conexión. Con el valor WINS-Assign-Yes (1), el sistema proporciona direcciones de servidor WINS de cliente durante la negociación de la conexión.

Para obtener información detallada acerca de estos atributos, consulte la publicación *Guía y referencia de TAOS RADIUS*.

Para utilizar estos atributos, el servidor RADIUS debe permitir atributos específicos del proveedor (VSA) y la unidad TAOS debe estar configurada en el modo de compatibilidad con VSA. A continuación se muestran los ajustes pertinentes:

```
[in EXTERNAL-AUTH]
auth-type = radius

[in EXTERNAL-AUTH:rad-auth-client]
auth-radius-compatible = vendor-specific
```

Para obtener información detallada acerca de estos ajustes, consulte la publicación APX 8000/MAX TNT/DSLNT Reference (*Referencia de APX 8000/MAX TNT/DSLNT*) que se adjunta con la unidad.

### *Ejemplos de configuración de servidores WINS de cliente*

Los comandos siguientes identifican dos servidores WINS para una conexión configurada. Sólo se accede al servidor secundario si el primario es inaccesible.

```
admin> read connection pc-1
CONNECTION/pc-1 read

admin> set ip-options client-wins-primary-addr = 10.2.3.4
admin> set ip-options client-wins-secondary-addr = 10.2.3.56
admin> set ip-options client-wins-addr-assign = yes
admin> write
CONNECTION/pc-1 written
```

A continuación se muestran los ajustes equivalentes en un perfil RADIUS:

```
pc-1 Password = "localpw", Service-Type = Framed
    Framed-Protocol = PPP,
    Framed-IP-Address = 1.1.1.1,
    Framed-IP-Netmask = 255.255.255.0,
    Ascend-Client-Primary-WINS = 10.2.3.4,
    Ascend-Client-Secondary-WINS = 10.2.3.56,
    Ascend-Client-Assign-WINS = WINS-Assign-Yes
```

Una agrupación de direcciones es un intervalo de direcciones contiguas de una subred o red IP local. Las direcciones de la agrupación están disponibles para ser asignadas a los emisores de entrada que solicitan una dirección. Al finalizar la llamada, la dirección se devuelve a la agrupación, donde pasa a estar de nuevo disponible para ser asignada.

Si designa una subred para agrupaciones de direcciones IP, debe asegurarse de que otros hosts IP de la red local conozcan la ruta hacia dicha subred. También debe comprobar que las agrupaciones no se solapan (no contengan direcciones duplicadas).

Si desea obtener información al respecto, consulte el apartado “Definición de agrupaciones de direcciones para un ruteador virtual” en la página 6-6.

Puede definir hasta 128 agrupaciones de direcciones de forma local en el perfil IP-Global. Estas agrupaciones pueden utilizarse para asignar direcciones a emisores autenticados localmente (en perfiles Connection) o mediante RADIUS. Si utiliza la autenticación RADIUS, puede optar por definir agrupaciones de direcciones en RADIUS en lugar de las definidas localmente, o además de éstas. Si tiene instalado el programa RADIPAD, puede utilizarlo para gestionar agrupaciones de direcciones de forma centralizada en un solo servidor RADIUS.

Los parámetros siguientes (que aparecen con los ajustes predeterminados) configuran agrupaciones de direcciones de forma local:

```
[in IP-GLOBAL]
pool-summary = no
pool-ospf-adv-type = type-1
pool-base-address = [ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.+
assign-count = [ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0+
pool-name = [ " " " " " " " " " " " " " " " " " " " " " " " "
```

Parámetro	Específica
Pool-Summary	Activa y desactiva el indicador Pool Summary. Para obtener información detallada, consulte el apartado “Ejemplos de configuración de agrupaciones de direcciones resumidas” en la página 2-72.
Pool-OSPF-Adv-Type	Opción de OSPF. Para obtener información detallada, consulte el apartado “Configuración de opciones de ruta” en la página 3-16.
Pool-Base-Address	Dirección base de una agrupación de direcciones contiguas en una subred o red local.
Assign-Count	Número de direcciones de la agrupación.
Pool-Name	Nombre de agrupación, necesario sólo si se utiliza la autenticación TACACS+. Si no se utiliza la autenticación TACACS+, el nombre se trata como un comentario.

## Ajustes de los perfiles de pseudousuario RADIUS

Puede definir agrupaciones de direcciones en un perfil de pseudousuario `pools` de RADIUS. La primera línea del perfil de pseudousuario `pools` tiene el formato siguiente:

```
pools-name Password = "ascend", Service-Type = Outbound-User
```

El argumento *name* es el nombre de sistema de la unidad TAOS (especificado por el parámetro Name en el perfil System). Las líneas subsiguientes del perfil definen agrupaciones de direcciones IP mediante el atributo Ascend-IP-Pool-Definition (217). El valor del atributo Ascend-IP-Pool-Definition utiliza la sintaxis siguiente:

```
"pool-num base-addr assign-count"
```

Elemento de sintaxis	Descripción
<i>pool-num</i>	Número de agrupación. Si utiliza el mismo número para designar dos agrupaciones, una localmente y la otra en RADIUS, la definición RADIUS tiene prioridad. Por tanto, si ha definido varias agrupaciones en el perfil IP-Global y no desea anularlas, empiece a numerar las agrupaciones con el número siguiente. Por ejemplo, si ha definido 10 agrupaciones en el perfil IP-Global, empiece con el número 11 en RADIUS. En caso contrario, empiece con 1.
<i>base-addr</i>	Dirección base de una agrupación de direcciones contiguas en la subred o red local.
<i>assign-count</i>	Número de direcciones incluidas en la agrupación.

## Agrupaciones RADIUS globales (RADIPAD)

RADIPAD (Daemon de direcciones IP RADIUS) es un programa que funciona junto con la autenticación RADIUS para gestionar agrupaciones de direcciones IP de forma centralizada, de modo que todas las conexiones puedan obtener una dirección de una agrupación global, independientemente de cuál sea el sistema que responda a la llamada.

RADIPAD se ejecuta en un servidor RADIUS de la red. Una unidad TAOS envía una petición de autenticación a RADIUS y, si el perfil de usuario contiene un atributo para asignar una dirección IP de la agrupación global de direcciones, RADIUS envía una petición a RADIPAD para obtener la dirección.

La unidad TAOS no se comunica directamente con RADIPAD, de modo que la utilización de este programa no precisa de configuración adicional. Para configurar RADIPAD, se deben definir las agrupaciones globales de direcciones, especificar qué servidor RADIUS ejecuta RADIPAD y (opcionalmente) especificar qué unidad TAOS puede obtener direcciones a partir de estas agrupaciones. A continuación, puede crear perfiles de usuario RADIUS que obtienen una dirección IP de la agrupación global.

Durante el arranque, Syslog anota las peticiones RADIUS para liberar direcciones IP asignadas por RADIUS. Puede ser que algunas versiones del servidor RADIUS agoten el tiempo de espera de la petición, en cuyo caso aparecerá un mensaje de registro en que se notifica la liberación de las direcciones de la agrupación global.

### *Definición de agrupaciones globales*

Las agrupaciones globales de direcciones se definen en un perfil de pseudousuario `global-pools` en el servidor que ejecuta RADIPAD. La primera línea de un perfil de pseudousuario `global-pools` tiene el formato siguiente:

```
global-pools-name Password = "ascend", Service-Type = Outbound-User
```

El argumento *name* es una designación para todas las clases de usuario. Puede crear varios perfiles de agrupación global para varias clases de usuario. Por ejemplo, puede crear perfiles denominados `Global-Pool-PPP`, `Global-Pool-SLIP`, etc. Las líneas subsiguientes del perfil definen agrupaciones de direcciones IP mediante el atributo `Ascend-IP-Pool-Definition` (217). Éste es el mismo atributo que se describe en “Ajustes de los perfiles de pseudousuario RADIUS” en la página 2-69 y sigue las mismas reglas para las agrupaciones globales. Además, cuando la unidad TAOS asigna una dirección de una agrupación gestionada por el daemon RADIPAD, éste intenta asignar una dirección de las agrupaciones de forma ordenada, por número de agrupación, y selecciona una dirección de la primera agrupación que tenga una dirección IP disponible.

### *Especificación del host RADIPAD*

Cada servidor RADIUS debe especificar el host que ejecuta RADIPAD y (opcionalmente) las unidades TAOS que pueden acceder a las agrupaciones globales. Estos ajustes se definen en un perfil de pseudousuario `radipa-hosts`, que utiliza el formato siguiente en la primera línea del perfil:

```
radipa-hosts Password = "ascend", Service-Type = Outbound-User
```

Las líneas subsiguientes del perfil utilizan los pares atributo-valor siguientes para definir qué unidades TAOS pueden asignar direcciones de las agrupaciones gestionadas por RADIPAD:

<b>Atributo</b>	<b>Valor</b>
Ascend-Assign-IP-Client (144)	Dirección de una unidad TAOS a la que se permite acceder a las agrupaciones globales de direcciones gestionadas por RADIPAD. Puede especificar varios casos de este atributo. Si no se ha especificado ninguna dirección de cliente, todas las unidades que aparecen en el archivo de clientes RADIUS podrán acceder a las agrupaciones RADIPAD.
Ascend-Assign-IP-Server (145)	Dirección del servidor que ejecuta RADIPAD. Sólo puede aparecer un caso de este atributo en el perfil y debe especificar la dirección IP correcta.

Por ejemplo:

```
radipa-hosts Password = "ascend", Service-Type = Outbound-User
  Ascend-Assign-IP-Server = 10.31.4.34,
  Ascend-Assign-IP-Client = 10.31.4.10,
  Ascend-Assign-IP-Client = 10.31.4.11
```

Sólo puede especificar un servidor RADIPAD, pero puede incluir varios clientes. El perfil de ejemplo indica que dos unidades TAOS (10.31.4.10 y 10.31.4.11) pueden acceder a las agrupaciones RADIPAD como clientes.

## Ejemplos de configuración de agrupaciones de direcciones

En el caso de una agrupación no resumida, cada dirección asignada se anuncia como su propia ruta de host. Una agrupación de este tipo puede iniciarse en cualquier dirección base. Las direcciones no aceptan un componente de máscara de subred, ya que siempre se anuncian como rutas de host.

Los comandos siguientes definen tres agrupaciones de direcciones, cada una de ellas con 50 direcciones. La agrupación 1 contiene de la 10.2.3.4 a la 10.2.3.54. La agrupación 2 contiene de la 11.5.7.51 a la 11.5.7.101. La agrupación 3 contiene de la 12.7.112.15 a la 12.7.112.65.

```
admin> read ip-global
IP-GLOBAL read

admin> set pool-base-address 1 = 10.2.3.4
admin> set pool-base-address 2 = 11.5.7.51
admin> set pool-base-address 3 = 12.7.112.15
admin> set assign-count 1 = 50
admin> set assign-count 2 = 50
admin> set assign-count 3 = 50

admin> write
IP-GLOBAL written
```

A continuación se muestra un perfil `pools` de RADIUS equivalente (para su uso con un único servidor RADIUS):

```
pools-taos01 Password = "ascend", Service-Type = Outbound-User
  Ascend-IP-Pool-Definition = "1 10.2.3.4 50",
  Ascend-IP-Pool-Definition = "2 11.5.7.51 50",
  Ascend-IP-Pool-Definition = "3 12.7.112.15 50"
```

A continuación se muestra una definición de agrupaciones globales equivalente (para su uso con RADIPAD):

```
global-pool-ppp Password = "ascend", Service-Type = Outbound-User
  Ascend-IP-Pool-Definition = "1 10.2.3.4 50",
  Ascend-IP-Pool-Definition = "2 11.5.7.51 50",
  Ascend-IP-Pool-Definition = "3 12.7.112.15 50"
```

Aunque algún software de cliente presupone una máscara de subred predeterminada de 255.255.255.0 para las interfaces PPP, puede definir agrupaciones en subredes con un ancho superior a /24. Por ejemplo, los comandos siguientes definen una agrupación de direcciones en una subred de /23:

```
admin> read ip-global
IP-GLOBAL read

admin> set pool-base-address 1 = 10.55.178.1
admin> set assign-count 1 = 510

admin> write
IP-GLOBAL written
```

Esta definición de agrupación da como resultado 10.55.178.0/23 (una máscara de subred de 255.255.254.0). A continuación se muestran definiciones RADIUS equivalentes:

```
pools-taos01 Password = "ascend", Service-Type = Outbound-User
Ascend-IP-Pool-Definition = "1 10.55.178.1 510"

global-pool-ppp Password = "ascend", Service-Type = Outbound-User
Ascend-IP-Pool-Definition = "1 10.55.178.1 510"
```

**Nota:** Si define agrupaciones de direcciones con más de 254 direcciones, tenga en cuenta que el sistema asigna las direcciones de límite de clase (x.y.z.0 y x.y.z.255) como direcciones válidas de emisor. De acuerdo con CIDR, está permitido porque la agrupación no es una red de /24. Sin embargo, algunos sistemas de cliente, como Windows, no toleran bien las direcciones de límite de clase. Por ejemplo, como Windows presupone una red de /24, realiza una difusión general de NetBIOS a través del servicio de nombres IP hacia la dirección .255, lo que podría colapsar una conexión a la que se ha asignado la dirección de host .255.

Para evitar que el software de cliente utilice una dirección de host para difusiones generales, debe aplicar de forma explícita un filtro que impida al sistema utilizar las direcciones de límite de clase. Por ejemplo, si utiliza la autenticación RADIUS, puede aplicar un filtro de datos, en el perfil Answer-Defaults, que descarte los paquetes procedentes de cualquier origen destinados a las direcciones de la agrupación x.y.z.0 o x.y.z.255.

## Ejemplos de configuración de agrupaciones de direcciones resumidas

La función Pool-Summary reduce la actividad de ruteo asociada a las agrupaciones de direcciones. En lugar de anunciar cada dirección asignada de una agrupación como ruta de host, la unidad TAOS elimina los anuncios de ruta de host y, en su lugar, anuncia una ruta estática a la propia agrupación.

Para utilizar agrupaciones resumidas localmente o en RADIUS, debe establecer el indicador Pool-Summary en Yes en el perfil IP-Global. Si Pool-Summary está establecido en Yes, todas las agrupaciones deben definirse con alineación de red.

### *Activación del indicador Pool-Summary*

Los comandos siguientes activan el indicador Pool-Summary:

```
admin> read ip-global
IP-GLOBAL read

admin> set pool-summary = yes

admin> write
IP-GLOBAL written
```

### *Definición de agrupaciones con alineación de red*

A continuación se indican las reglas para las agrupaciones de direcciones con alineación de red:

- El número especificado de direcciones de la agrupación debe ser dos números menos que el número total de direcciones de la agrupación (suma 2 al valor Assign-Count para obtener el número total de direcciones en la subred y calcule la máscara para la subred de acuerdo con este total).  
 $assign-count + 2 = \text{número de hosts de subred}$
- La dirección base especificada de la agrupación debe ser la primera dirección de host (reste 1 al valor Pool-Base-Address para obtener la dirección base de la subred).

*pool-base-address - 1* = dirección de subred con alineación de red

Los comandos siguientes activan el indicador Pool-Summary y definen una agrupación con alineación de red:

```
admin> read ip-global
IP-GLOBAL read

admin> set pool-summary = yes

admin> set assign-count 1 = 62

admin> set pool-base-address 1 = 10.12.253.1

admin> write
IP-GLOBAL written
```

En las configuraciones de ejemplo anteriores, el parámetro Assign-Count está establecido en 62. Si suma 2 a este valor, obtendrá 64. La máscara de subred para 64 direcciones es 255.255.255.192 (256-64 = 192). La longitud del prefijo para una máscara 255.255.255.192 es /26.

El parámetro Pool-Base-Address está establecido en 10.12.253.1. Si resta 1 a este valor, obtendrá 10.12.253.0, que es una dirección base con alineación de red válida para la máscara de subred 255.255.255.192. Observe que 10.12.253.64, 10.12.253.128 y 10.12.253.192 son también direcciones cero válidas para la misma máscara. La subred de agrupación de direcciones resultante es 10.12.253.0/26.

A continuación se muestra un perfil pools de RADIUS equivalente (para su uso con un único servidor RADIUS):

```
pools-taos01 Password = "ascend", Service-Type = Outbound-User
  Ascend-IP-Pool-Definition = "1 10.12.253.1 62"
```

A continuación se muestra una definición de agrupaciones globales equivalente (para su uso con RADIPAD):

```
global-pool-ppp Password = "ascend", Service-Type = Outbound-User
  Ascend-IP-Pool-Definition = "1 10.12.253.1 62"
```

La unidad TAOS aún crea (pero no anuncia) una ruta de host para cada dirección asignada de la agrupación. Las rutas de host tienen prioridad sobre las rutas de subred, por lo que los paquetes cuyo destino coincide con una dirección IP asignada de la agrupación se rutean adecuadamente. Sin embargo, dado que la unidad TAOS anuncia toda la agrupación como una ruta y sólo conoce de forma privada qué direcciones IP de la agrupación están activas, una red remota podría enviar un paquete incorrectamente a la unidad TAOS para una dirección IP inactiva. Si esto ocurre, los paquetes se rutean hacia la interfaz Reject (rj0) (127.0.0.2). Los paquetes ruteados hacia la interfaz Reject se devuelven al remitente con un mensaje ICMP unreachable (ICMP inaccesible).

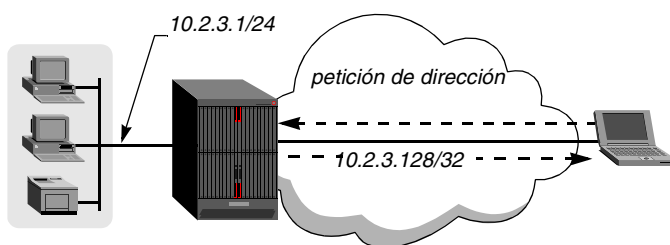
## Ejemplos de asignación de una dirección desde una agrupación

Cuando una llamada de entrada solicita una dirección IP, la unidad TAOS asigna una dirección a partir de una agrupación de direcciones. Un host solicita una dirección si su software de cliente tiene unos ajustes como los siguientes:

```
Username=victor
Accept Assigned IP=Yes
IP address=Dynamic (or Assigned or N/A)
Netmask=255.255.255.255 (or None or N/A)
Default Gateway=None or N/A
Name Server=10.2.3.55
Domain suffix=abc.com
Baud rate=38400
Hardware handshaking ON
VAN Jacobsen compression ON
```

En la Figura 2-10 se muestra cómo un host de llamada de entrada solicita una dirección IP y cómo se le asigna una:

*Figura 2-10. Host de llamada de entrada que solicita una dirección IP*



Los comandos siguientes activan la asignación dinámica de direcciones en todo el sistema:

```
admin> read answer
ANSWER-DEFAULTS read

admin> set ip-answer assign = yes

admin> write
ANSWER-DEFAULTS written
```

Para obtener información acerca de cómo garantizar que las conexiones acepten la dirección ofrecida, consulte “Requisito de aceptación de asignación dinámica de direcciones” en la página 2-41.

Los comandos siguientes configuran un perfil para que obtenga una dirección de la primera agrupación que tenga direcciones disponibles:

```
admin> new conn victor
CONNECTION/victor read

admin> set active = yes

admin> set encapsulation-protocol = ppp

admin> set ppp recv-password = localpw

admin> set ip-options address-pool = 0

admin> write
CONNECTION/victor written
```



A continuación se muestra un perfil RADIUS equivalente:

```
victor Password = "localpw"
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Ascend-Assign-IP-Pool = 0
```

A continuación se muestra un perfil RADIUS equivalente que obtiene una dirección de cualquier agrupación global gestionada por el daemon RADIPAD:

```
victor Password = "localpw"
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Ascend-Assign-IP-Pool = 65535
  Ascend-Assign-IP-Global-Pool = "global-pool-ppp"
```

## Encadenamiento de agrupaciones IP

Dado que las direcciones de una agrupación deben ser contiguas, en muchos entornos se han definido un gran número de agrupaciones, cada una de ellas con sólo un rango reducido de direcciones. Por ejemplo, el perfil RADIUS siguiente define seis agrupaciones, cada una de ellas con 10 direcciones:

```
pools-JFAN-TNT Password = "ascend"
  Service-Type = Outbound,
  Ascend-IP-Pool-Definition = "1 11.168.6.10 10",
  Ascend-IP-Pool-Definition = "2 12.168.6.10 10",
  Ascend-IP-Pool-Definition = "3 13.168.6.10 10",
  Ascend-IP-Pool-Definition = "7 17.168.6.10 10",
  Ascend-IP-Pool-Definition = "8 18.168.6.10 10",
  Ascend-IP-Pool-Definition = "9 19.168.6.10 10"
```

En versiones anteriores del software, se podía permitir que un emisor obtuviera una dirección de cualquier agrupación (asignando el número de agrupación 0 en el perfil del emisor) o de una única agrupación especificada, como la agrupación 1. El encadenamiento de agrupaciones IP permite que un emisor pueda obtener una dirección de cualquier agrupación de una cadena.

Si el encadenamiento de agrupaciones IP está activo, las agrupaciones contiguas se tratan como un *espacio de agrupación* con direcciones compartidas. Cuando el sistema asigna una dirección a un usuario final, empieza buscando una dirección disponible en la primera agrupación de la cadena y se detiene al encontrar una o al encontrar una definición de agrupación nula. Por tanto, las agrupaciones de una cadena deben definirse en una secuencia contigua. Por ejemplo, el perfil siguiente contiene dos cadenas de agrupaciones IP (agrupaciones 1, 2, 3 y agrupaciones 7, 8, 9), y cada cadena contiene 30 direcciones:

```
pools-JFAN-TNT Password = "ascend", Service-Type = Outbound
  Ascend-IP-Pool-Chaining = IP-Pool-Chaining-Yes,
  Ascend-IP-Pool-Definition = "1 11.168.6.10 10",
  Ascend-IP-Pool-Definition = "2 12.168.6.10 10",
  Ascend-IP-Pool-Definition = "3 13.168.6.10 10",
  Ascend-IP-Pool-Definition = "7 17.168.6.10 10",
  Ascend-IP-Pool-Definition = "8 18.168.6.10 10",
  Ascend-IP-Pool-Definition = "9 19.168.6.10 10"
```

**Nota:** Para permitir el encadenamiento de agrupaciones IP en perfiles RADIUS, el servidor RADIUS debe admitir atributos específicos del proveedor (VSA) y la unidad TAOS debe estar

Tanto las agrupaciones de direcciones definidas en RADIUS como las agrupaciones definidas localmente en el perfil IP-Global admiten el encadenamiento de agrupaciones IP. Por ejemplo, los ajustes siguientes en el perfil IP-Global activan el encadenamiento de agrupaciones y definen una cadena de agrupaciones (agrupaciones 1 y 2) que contiene 252 direcciones:

```
[in IP-GLOBAL]
pool-chaining = yes
pool-base-address = [ 172.20.31.1 172.20.33.1 0.0.0.0 153.37.21.1 0.0+
assign-count = [ 126 126 0 30 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 +
```

Independientemente de si las cadenas de agrupaciones están definidas localmente o en RADIUS, las direcciones de la agrupación pueden asignarse de forma dinámica sin importar dónde se haya autenticado el perfil del emisor.

A continuación se muestran los parámetros, con los ajustes predeterminados, que son pertinentes para el encadenamiento de agrupaciones IP:

```
[in IP-GLOBAL]
pool-chaining = no
pool-base-address = [ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0+
assign-count = [ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0+

[in CONNECTION/"":ip-options]
address-pool = 0
```

Parámetro	Especifica
Pool-Chaining	Activa y desactiva el encadenamiento de agrupaciones IP. Con el ajuste <code>yes</code> , el sistema trata las agrupaciones de direcciones IP contiguas como un único espacio de agrupación ampliado al buscar una dirección disponible para asignar a un emisor.
Pool-Base-Address	Matriz de un máximo de 128 direcciones IP para utilizarla como primera dirección en una agrupación. Estos valores se utilizan junto con los valores <code>Assign-Count</code> para definir agrupaciones de direcciones localmente. Una cadena de agrupaciones contiene todas las agrupaciones definidas en orden dentro de la matriz, como 1, 2, 3. Para terminar una cadena de agrupaciones, deje un valor nulo en la matriz.
Assign-Count	Matriz de un máximo de 128 números que especifica el número de direcciones en una agrupación que empieza con el correspondiente <code>Pool-Base-Address</code> .

Parámetro	Especifica
Address-Pool	Número de una agrupación de direcciones a partir del cual se obtiene una dirección. Si el encadenamiento de agrupaciones está activo, en un número de agrupación de una cadena se incluyen direcciones de todas las demás agrupaciones de la cadena. Por ejemplo, si las agrupaciones 1, 2 y 3 están en una cadena de agrupaciones, establecer este parámetro en 1 tendrá el mismo efecto que establecerlo en 2 o 3.

### *Ejemplo de una definición de cadena de agrupaciones locales*

Los comandos siguientes definen cinco agrupaciones de direcciones, que forman dos cadenas de agrupaciones. Observe que los números de las agrupaciones (sus índices en las matrices Pool-Base-Address y Assign-Count) son contiguos dentro de la cadena.

```
admin> read ip-global
IP-GLOBAL read

admin> set pool-chaining = yes

admin> set pool-base-address 1 = 10.1.1.1
admin> set pool-base-address 2 = 11.1.1.1
admin> set pool-base-address 3 = 12.1.1.1

admin> set assign-count 1 = 50
admin> set assign-count 2 = 50
admin> set assign-count 3 = 50

admin> set pool-base-address 7 = 13.1.1.1
admin> set pool-base-address 8 = 14.1.1.1
admin> set assign-count 7 = 50
admin> set assign-count 8 = 50

admin> write
IP-GLOBAL written
```

Los comandos siguientes activan la asignación dinámica de direcciones en todo el sistema:

```
admin> read answer
ANSWER-DEFAULTS read

admin> set ip-answer assign = yes

admin> write
ANSWER-DEFAULTS written
```

Los comandos siguientes configuran los perfiles para que obtengan una dirección de la primera cadena de agrupaciones. Cuando los usuarios finales realizan una llamada de entrada, pueden obtener una dirección de 10.1.1.1 a 10.1.1.51, de 11.1.1.1 a 11.1.1.51 o de 12.1.1.1 a 12.1.1.51. Si no hay ninguna dirección disponible dentro de estos rangos, se denegará la conexión.

```
admin> new conn jfan
CONNECTION/jfan read

admin> set active = yes

admin> set encapsulation-protocol = ppp
```

```
admin> set ppp-options rcv-password = localpw
admin> set ip-options address-pool = 2
admin> write
CONNECTION/jfan written
admin> new conn ravi
CONNECTION/ravi read
admin> set active = yes
admin> set encapsulation-protocol = ppp
admin> set ppp-options rcv-password = localpw
admin> set ip-options address-pool = 1
admin> write
CONNECTION/ravi written
```

A continuación se muestran los perfiles RADIUS equivalentes:

```
jfan Password = "localpw"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Ascend-Assign-IP-Pool = 2
ravi Password = "localpw"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Ascend-Assign-IP-Pool = 1
```

## *Encadenamiento de agrupaciones en RADIUS*

Independientemente de si las cadenas de agrupaciones están definidas localmente o en un perfil de pseudousuario de agrupación de RADIUS, las direcciones de la agrupación pueden asignarse de forma dinámica sin importar dónde se haya autenticado el perfil del emisor.

### *Información general sobre los ajustes del perfil RADIUS*

Los servidores RADIUS utilizan los pares atributo-valor siguientes para definir y aplicar cadenas de agrupaciones:

<b>Atributo</b>	<b>Valor</b>
Ascend-IP-Pool-Chaining (85)	Activa y desactiva el encadenamiento de agrupaciones IP en un perfil de pseudousuario que define agrupaciones de direcciones. Si este atributo está establecido en IP-Pool-Chaining-Yes (1), el sistema trata las agrupaciones de direcciones IP contiguas como un único espacio de agrupación ampliado al buscar una dirección disponible para asignársela a un emisor. Con el valor IP-Pool-Chaining-No (0), el sistema trata cada agrupación de direcciones como un espacio separado.  <b>Nota:</b> Si este atributo está especificado en un perfil RADIUS, su valor anula el ajuste Pool-Chaining en el perfil IP-Global.

Atributo	Valor
Ascend-IP-Pool-Definition (217)	<p>Definición de agrupación de direcciones en un perfil de pseudousuario. El valor tiene la sintaxis siguiente:</p> <pre><i>pool-number base-addr assign-count</i></pre> <p>El valor <i>pool-number</i> es un número entero que identifica la agrupación. Una cadena de agrupaciones contiene todas las agrupaciones definidas en orden, como 1, 2, 3. Para terminar una cadena, deje un espacio vacío en la secuencia de valores de <i>pool-number</i>. El valor <i>base-addr</i> es una dirección IP que se debe utilizar como primera dirección de una agrupación y el valor <i>assign-count</i> especifica el número de direcciones de la agrupación.</p>
Ascend-Assign-IP-Pool (218)	<p>Número de la agrupación de direcciones a partir del cual el perfil de usuario RADIUS debe obtener una dirección. Si el encadenamiento de agrupaciones está activo, en un número de agrupación de una cadena se incluyen direcciones de todas las demás agrupaciones de la cadena. Por ejemplo, si las agrupaciones 1, 2 y 3 están en una cadena de agrupaciones, establecer este valor en 1 tendrá el mismo efecto que establecerlo en 2 o 3.</p>

Para utilizar estos atributos, el servidor RADIUS debe permitir atributos específicos del proveedor (VSA) y la unidad TAOS debe estar configurada en el modo de compatibilidad con VSA. A continuación se muestran los ajustes pertinentes:

```
[in EXTERNAL-AUTH]
auth-type = radius

[in EXTERNAL-AUTH:rad-auth-client]
auth-radius-compatible = vendor-specific
```

Si desea obtener información detallada acerca de estos ajustes, consulte la publicación *APX 8000/MAX TNT/DSLNT Reference (Referencia de APX 8000/MAX TNT/DSLNT)*.

### Ejemplo de encadenamiento de agrupaciones en RADIUS

El perfil de pseudousuario siguiente define cinco agrupaciones de direcciones, que forman dos cadenas de agrupaciones. Observe que los números de las agrupaciones son contiguos dentro de una cadena.

```
pools-JFAN-TNT Password = "ascend"
  Service-Type = Outbound,
  Ascend-IP-Pool-Chaining = IP-Pool-Chaining-Yes,
  Ascend-IP-Pool-Definition = "1 10.1.1.1 50",
  Ascend-IP-Pool-Definition = "2 11.1.1.1 50",
  Ascend-IP-Pool-Definition = "3 12.1.1.1 50",
  Ascend-IP-Pool-Definition = "7 13.1.1.1 50",
  Ascend-IP-Pool-Definition = "8 14.1.1.1 50"
```

Los comandos siguientes configuran los perfiles Connection locales para que obtengan una dirección de la primera cadena de agrupaciones. Cuando los usuarios finales realizan una llamada de entrada, pueden obtener una dirección de 13.1.1.1 a 13.1.1.51 o de 14.1.1.1 a

14.1.1.51. Si no hay ninguna dirección disponible dentro de estos rangos, se denegará la conexión.

```
admin> new conn hanif
CONNECTION/hanif read

admin> set active = yes

admin> set encapsulation-protocol = ppp

admin> set ppp-options recv-password = localpw

admin> set ip-options address-pool = 7

admin> write
CONNECTION/hanif written

admin> new conn hasnain
CONNECTION/hasnain read

admin> set active = yes

admin> set encapsulation-protocol = ppp

admin> set ppp-options recv-password = localpw

admin> set ip-options address-pool = 8

admin> write
CONNECTION/hasnain written
```

A continuación se muestran perfiles de usuario RADIUS equivalentes:

```
hanif Password = "localpw"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Ascend-Assign-IP-Pool = 7

hasnain Password = "localpw"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Ascend-Assign-IP-Pool = 8
```

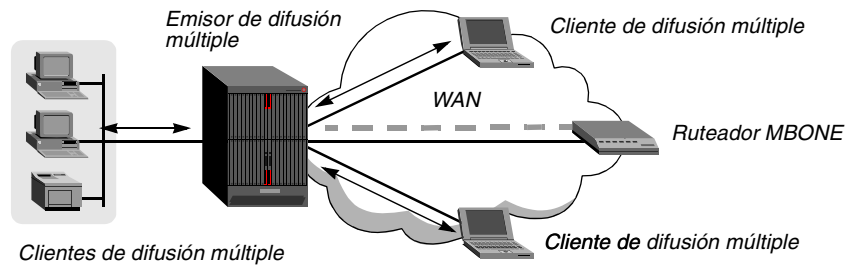
## ***Configuración del envío de difusión múltiple***

La red troncal de difusión múltiple (MBONE) de IP proporciona una comunicación de uno a varios y de varios a varios en lugar de la comunicación punto a punto que utilizan muchos otros tipos de aplicaciones de red. Las transmisiones de audio y vídeo utilizan la red MBONE como una forma rápida y barata de proporcionar la misma información a varios hosts.

Los routers MBONE mantienen grupos de difusión múltiple, en los que los hosts deben registrarse para recibir una transmisión de difusión múltiple. Las funciones del grupo de difusión múltiple se gestionan con el protocolo de gestión de grupo Internet (IGMP). La unidad TAOS envía paquetes IGMP versión 1 o versión 2, incluido IGMP MTRACE (rastreo de difusión múltiple).

En la Figura 2-11 se muestra una unidad TAOS que envía tráfico de difusión múltiple desde un router MBONE a través de la WAN a dos interfaces WAN de cliente de difusión múltiple y una interfaz LAN de cliente de difusión múltiple.

Figura 2-11. Unidad TAOS que envía tráfico de difusión múltiple a clientes LAN y WAN



La interfaz para el ruteador MBONE es la interfaz MBONE. La unidad TAOS puede tener sólo una única interfaz MBONE, que puede ser una interfaz IP LAN o WAN.

Para los ruteadores MBONE, la unidad TAOS es como un cliente de difusión múltiple, ya que responde como un cliente a los paquetes IGMP. Para los clientes de difusión múltiple, la unidad TAOS es como un ruteador MBONE, ya que envía las consultas IGMP a estos clientes, recibe las respuestas y envía tráfico de difusión múltiple.

## Ajustes globales para activar el envío por difusión múltiple

Los parámetros siguientes (que aparecen con los ajustes predeterminados) inician el envío de difusión múltiple en el nivel del sistema:

```
[in IP-GLOBAL]
multicast-forwarding = no
mbone-profile = ""
mbone-lan-interface = { { any-shelf any-slot 0 } 0 }
multicast-hbeat-addr = 0.0.0.0
multicast-hbeat-port = 0
multicast-hbeat-slot-time = 0
multicast-hbeat-number-slot = 0
multicast-hbeat-alarm-threshold = 0
multicast-hbeat-src-addr = 0.0.0.0
multicast-hbeat-src-addr-mask = 0.0.0.0
multicast-member-timeout = 360
```

**Nota:** El control del pulso es opcional. No es obligatorio para el envío de difusión múltiple.

Parámetro	Especifica
Multicast-Forwarding	Activa y desactiva el envío de difusión múltiple en la unidad TAOS. Si cambia el valor a Yes y graba el perfil, el subsistema de difusión múltiple lee los valores en el perfil IP-Global e inicia la función de envío.
MBONE-Profile	Nombre de un perfil Connection local para un ruteador MBONE en una interfaz WAN. Este parámetro y el parámetro MBONE-LAN-Interface se excluyen mutuamente. Para obtener información detallada, consulte el apartado “Configuración de la interfaz MBONE” en la página 2-84.

<b>Parámetro</b>	<b>Especifica</b>
MBONE-LAN-Interface	Dirección de interfaz (módulo, ranura y puerto) para el ruteador MBONE en una interfaz LAN. Este parámetro y el parámetro MBONE-Profile se excluyen mutuamente. Para obtener información detallada, consulte el apartado “Configuración de la interfaz MBONE” en la página 2-84.
Multicast-Hbeat-Addr	Dirección de difusión múltiple que debe controlarse para determinar un nivel mínimo de tráfico (pulso).
Multicast-Hbeat-Port	Número de puerto UDP que debe controlarse. La unidad TAOS únicamente cuenta los paquetes recibidos en este puerto.
Multicast-Hbeat-Slot-Time	Intervalo de sondeo (en segundos) durante el que la unidad TAOS realiza un sondeo del tráfico de difusión múltiple.
Multicast-Hbeat-Number-Slot	Número de veces que debe efectuarse un sondeo para el intervalo especificado antes de comparar el número de paquetes de pulso recibidos en el umbral de alarma.
Multicast-Hbeat-Src-Addr	Dirección IP de origen que debe pasarse por alto. Los paquetes recibidos de esta dirección no se tienen en cuenta para el control del pulso.
Multicast-Hbeat-Src-Addr-Mask	Máscara de subred que debe aplicarse al valor Multicast-Hbeat-Src-Addr antes de compararlo con la dirección de origen de un paquete.
Multicast-Hbeat-Alarm-Threshold	Número de paquetes que representan un tráfico de difusión múltiple normal. Si el número de paquetes controlados es inferior a dicho número, se envía la captura de alarma SNMP.
Multicast-Member-Timeout	Tiempo de espera (en segundos) para las respuestas del cliente a los mensajes de sondeo de difusión múltiple. Si no recibe ninguna respuesta en una interfaz de cliente al transcurrir el número especificado de segundos, la unidad TAOS deja de enviar tráfico de difusión múltiple en la interfaz.

### *Especificación de un tiempo de espera para miembros de un grupo*

El parámetro Multicast-Member-Timeout especifica el tiempo de espera (en segundos) para las respuestas del cliente a mensajes de sondeo de difusión múltiple. Si ningún cliente responde a los mensajes de sondeo en el tiempo especificado para Multicast-Member-Timeout, la unidad TAOS deja de enviar tráfico de difusión múltiple en la interfaz. Los comandos siguientes establecen el tiempo de espera en 60 segundos:

```
admin> read ip-global
IP-GLOBAL read

admin> set multicast-member-timeout = 60

admin> write
IP-GLOBAL written
```



## *Control del pulso del tráfico de difusión múltiple*

El control del pulso es opcional. Permite a los administradores controlar posibles problemas de conectividad de difusión múltiple mediante la realización de sondeos continuos para determinar la existencia de un determinado nivel de tráfico de difusión múltiple y la generación de la siguiente captura de alarma SNMP en caso de interrumpirse el tráfico:

```
Trap type:  TRAP_ENTERPRISE
Code:       TRAP_MULTICAST_TREE_BROKEN (19)
Arguments:
1) Multicast group address being monitored (4 bytes),
2) Source address of last heartbeat packet received (4 bytes)
3) Slot time interval configured in seconds (4 bytes),
4) Number of slots configured (4 bytes).
5) Total number of heartbeat packets received before the unit started
   sending SNMP Alarms (4 bytes).
```

### *Activación del control del pulso*

Para activar el control del pulso de difusión múltiple, debe especificar una frecuencia de sondeo y el umbral por debajo del que se generará la alarma.

Con la siguiente configuración de ejemplo, la unidad TAOS realiza un sondeo 10 veces a intervalos de 10 segundos y, a continuación, compara el recuento total de tráfico con el valor umbral. Si se han recibido menos de 30 paquetes, la unidad genera la alarma SNMP.

```
admin> read ip-global
IP-GLOBAL/ read

admin> set multicast-hbeat-slot-time = 10

admin> set multicast-hbeat-number-slot = 10

admin> set multicast-hbeat-alarm-threshold = 30

admin> write
IP-GLOBAL/ written
```

### *Especificación de los paquetes que se deben controlar*

Para hacer más preciso el control del pulso, puede especificar qué paquetes debe contar el sistema como tráfico de difusión múltiple. Esto puede realizarse de una o varias de las maneras siguientes:

- Especificar una dirección de difusión múltiple concreta para utilizarla para el control.
- Especificar un número de puerto UDP (todos los paquetes recibidos en este puerto se utilizarán para el control).
- Especificar una dirección de origen (los paquetes procedentes de este host no se tendrán en cuenta para el control).
- Especificar una máscara de subred que se debe aplicar a la dirección de origen (los paquetes procedentes de esta subred o red no se tendrán en cuenta para el control).

En el ejemplo siguiente se muestra cómo controlar únicamente los paquetes enviados a la dirección de difusión múltiple 224.1.1.1 y recibidos desde ésta:

```
admin> read ip-global
IP-GLOBAL/ read

admin> set multicast-hbeat-addr = 224.1.1.1

admin> write
IP-GLOBAL/ written
```

La siguiente configuración de ejemplo limita el control a los paquetes enviados a la dirección de difusión múltiple 224.1.1.1 en el puerto UDP 16387 y recibidos desde ésta:

```
admin> read ip-global
IP-GLOBAL/ read

admin> set multicast-hbeat-addr = 224.1.1.1

admin> set multicast-hbeat-port = 16387

admin> write
IP-GLOBAL/ written
```

En el ejemplo siguiente se muestra cómo especificar que los paquetes de difusión múltiple procedentes de la subred 10.1.0.0 no se tengan en cuenta para el control del pulso:

```
admin> read ip-global
IP-GLOBAL/ read

admin> set multicast-hbeat-src-addr = 10.1.2.3

admin> set multicast-hbeat-src-addr-mask = 255.255.0.0

admin> write
IP-GLOBAL/ written
```

## Configuración de la interfaz MBONE

La interfaz MBONE es la interfaz sencilla IP LAN o WAN en la que reside un router MBONE. La interfaz MBONE no admite clientes de difusión múltiple.

Para que una unidad TAOS pueda enviar tráfico a y desde un router MBONE, debe configurar los ajustes de IP-Global y los ajustes apropiados en un perfil IP-Interface o Connection.

### *Información general sobre los ajustes de la interfaz MBONE*

El parámetro siguiente (que aparece con el ajuste predeterminado) se utiliza en la interfaz MBONE:

```
[in IP-INTERFACE/{ { any-shelf any-slot 0 } 0 } ]
multicast-allowed = no

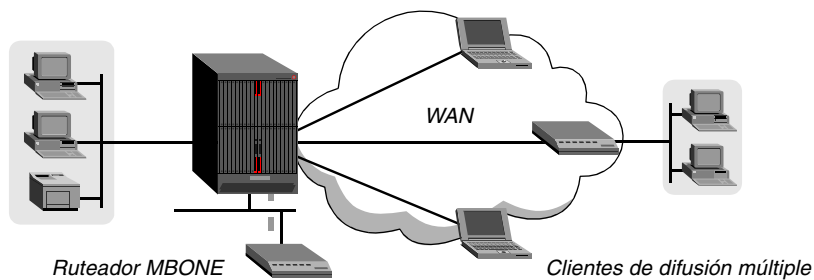
[in CONNECTION/":ip-options]
multicast-allowed = no
```

Parámetro	Especifica
Multicast-Allowed	Activa y desactiva la gestión de peticiones y respuestas IGMP en la interfaz. La unidad TAOS <i>no</i> envía tráfico de difusión múltiple basándose en este ajuste.

### *Ejemplo de un ruteador MBONE local*

En la Figura 2-12 se muestra un ruteador MBONE en una de las interfaces IP LAN del sistema.

*Figura 2-12. Ruteador MBONE en una interfaz LAN*



Los comandos siguientes configuran el puerto Ethernet situado más a la izquierda del controlador del módulo como interfaz MBONE:

```
admin> read ip-global
IP-GLOBAL read

admin> set multicast-forwarding = yes

admin> set mbone-lan-interface = { { 1 41 1 } 0 }

admin> write
IP-GLOBAL written

admin> read ip-interface { { 1 41 1 } 0 }
IP-INTERFACE/{ { shelf-1 left-controller 1 } 0 } read

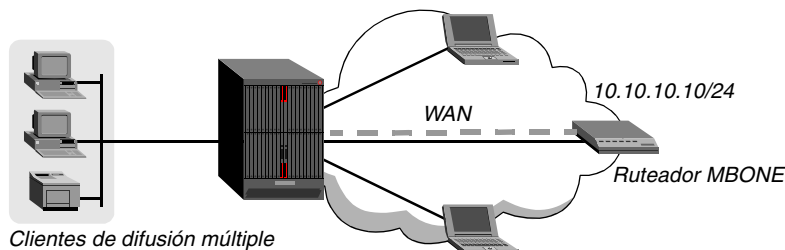
admin> set multicast-allowed = yes

admin> write
IP-INTERFACE/{ { shelf-1 left-controller 1 } 0 } written
```

## Ejemplo de un ruteador MBONE en una interfaz WAN

En la Figura 2-13 se muestra un ruteador MBONE en una interfaz WAN:

Figura 2-13. Ruteador MBONE en una interfaz WAN



Los comandos siguientes configuran una interfaz IP WAN conmutada con el ruteador MBONE:

```
admin> read ip-global
IP-GLOBAL read

admin> set multicast-forwarding = yes
admin> set mbone-profile = multicast-router

admin> write
IP-GLOBAL written

admin> read connection multicast-router
CONNECTION/multicast-router read

admin> set active = yes
admin> set encapsulation-protocol = mp
admin> set ip remote-address = 10.10.10.10/24
admin> set ip multicast-allowed = yes
admin> set ppp recv-password = localpw
admin> set mp base-channel-count = 12

admin> write
CONNECTION/multicast-router written
```

## Configuración de interfaces de cliente de difusión múltiple

La unidad TAOS puede enviar transmisiones de difusión múltiple a cualquier interfaz, excepto la interfaz MBONE. Para comunicarse con clientes de difusión múltiple, que normalmente ejecutan VAT (*Video Audio Tools*) o Windows, la unidad TAOS gestiona las consultas IGMP y las respuestas, y envía la transmisión MBONE que recibe del ruteador MBONE.

### Ajustes de los perfiles IP-Interface y Connection locales

Los parámetros siguientes (que aparecen con los ajustes predeterminados) se utilizan para configurar una interfaz de cliente de difusión múltiple:

```
[in IP-INTERFACE/{ { any-shelf any-slot 0 } 0 } ]
multicast-allowed = no
multicast-rate-limit = 100
multicast-group-leave-delay = 0
```

```
[in CONNECTION /":ip-options]
multicast-allowed = no
multicast-rate-limit = 100
multicast-group-leave-delay = 0
```

Parámetro	Especifica
Multicast-Allowed	Activa y desactiva la gestión de peticiones y respuestas IGMP en la interfaz. La unidad TAOS <i>no</i> envía tráfico de difusión múltiple basándose en este ajuste.
Multicast-Rate-Limit	Velocidad a la que la unidad TAOS acepta paquetes de difusión múltiple de clientes en la interfaz. El ajuste predeterminado (100) desactiva el envío de transmisiones de difusión múltiple. Para obtener información detallada, consulte el apartado “Definición del límite de velocidad de difusión múltiple” en la página 2-88.
Multicast-Group-Leave-Delay	Número de segundos que debe esperar la unidad TAOS antes de enviar un mensaje de abandono de grupo IGMP-v2 desde un cliente de difusión múltiple al ruteador MBONE. Para obtener información detallada, consulte el apartado “Especificación de un retardo para la eliminación de grupos IGMP” en la página 2-88.

### *Ajustes de los perfiles RADIUS*

Pueden especificarse los pares atributo-valor siguientes en perfiles RADIUS para interfaces WAN de cliente de difusión múltiple:

Atributo	Valor
Ascend-Multicast-Client (155)	Activa y desactiva la gestión de peticiones y respuestas IGMP en la interfaz. La unidad TAOS <i>no</i> envía tráfico de difusión IGMP basándose en este valor.
Ascend-Multicast-Rate-Limit (152)	Velocidad a la que la unidad TAOS acepta paquetes de difusión múltiple de clientes en la interfaz. El valor predeterminado (100) desactiva el envío de transmisiones de difusión múltiple. Para obtener información detallada, consulte el apartado “Definición del límite de velocidad de difusión múltiple” en la página 2-88.
Ascend-Multicast-GRP-Leave-Delay (111)	Número de segundos que debe esperar la unidad TAOS antes de enviar un mensaje de abandono de grupo IGMP-v2 desde un cliente de difusión múltiple al ruteador MBONE. Para obtener información detallada, consulte el apartado “Especificación de un retardo para la eliminación de grupos IGMP” en la página 2-88.

### *Definición del límite de velocidad de difusión múltiple*

Multicast-Rate-Limit especifica la velocidad a la que la unidad TAOS acepta paquetes de difusión múltiple de clientes en la interfaz.

**Nota:** De manera predeterminada, Multicast-Rate-Limit tiene el valor 100. Este ajuste desactiva el envío de difusión múltiple en la interfaz (el emisor gestiona los paquetes IGMP, pero no acepta paquetes de clientes ni envía paquetes de difusión múltiple desde el ruteador MBONE). Para permitir el envío de difusión múltiple en la interfaz, debe establecer el parámetro Multicast-Rate-Limit en un número *menor que* 100.

Por ejemplo, si establece Multicast-Rate-Limit en 5, la unidad TAOS acepta un paquete cada cinco segundos procedente de clientes de difusión múltiple en la interfaz. Los paquetes subsiguientes recibidos dentro de la ventana de 5 segundos se descartan.

Además del límite de velocidad de difusión múltiple, la unidad TAOS también permite descartar paquetes por prioridad para aplicaciones de difusión múltiple de datos, voz y audio con un gran ancho de banda. Si la unidad TAOS es un dispositivo receptor con un tráfico muy intenso, descarta los paquetes de acuerdo con una clasificación de prioridades, determinada por los siguientes rangos de puertos UDP:

- El tráfico en los puertos 0–16384 (tráfico sin clasificar) tiene la prioridad más baja (50).
- El tráfico en los puertos 16385–32768 (tráfico de audio) tiene la prioridad más alta (70).
- El tráfico en los puertos 32769–49152 (tráfico de datos multidifusión) tiene una prioridad media (60).
- El tráfico en los puertos 49153–65536 (tráfico de vídeo) tiene una prioridad baja (55).

### *Especificación de un retardo para la eliminación de grupos IGMP*

Multicast-Group-Leave-Delay especifica el número de segundos que espera la unidad TAOS antes de enviar al ruteador MBONE un mensaje de abandono de grupo versión 2 IGMP que recibe en una interfaz de cliente de difusión múltiple. Normalmente, estos mensajes indican que la sesión del grupo IGMP puede eliminarse. Sin embargo, una interfaz de difusión múltiple en la unidad TAOS puede admitir varios clientes, algunos de los cuales pueden establecer varias sesiones de difusión múltiple para grupos idénticos, en cuyo caso un mensaje de abandono de grupo de un cliente individual debe tratarse de una forma especial.

Si Multicast-Group-Leave-Delay está establecido en cero (el valor predeterminado), la unidad TAOS envía el mensaje de abandono de grupo inmediatamente.

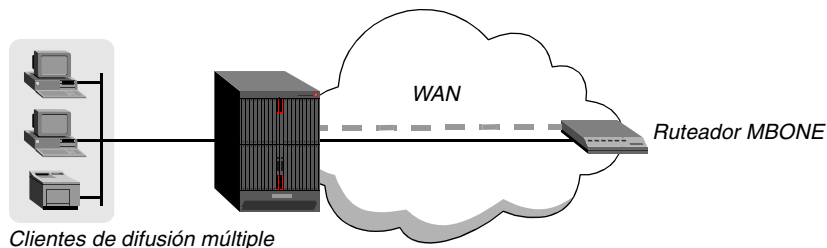
Si establece Multicast-Group-Leave-Delay en un valor que no sea cero, la unidad TAOS no envía inmediatamente un mensaje de abandono de grupo procedente de un cliente en la interfaz. En lugar de ello, envía una consulta para asegurarse de que ningún cliente en la interfaz tiene una sesión de difusión múltiple activa para ese grupo. Si la unidad TAOS recibe una respuesta antes de que transcurra el intervalo Multicast-Group-Leave-Delay, no enviará el mensaje de abandono de grupo. Si la unidad no recibe respuesta, envía el mensaje y borra la sesión del grupo IGMP de sus tablas después del intervalo especificado.

Para que los usuarios puedan establecer varias sesiones de difusión múltiple para grupos idénticos, debe establecer este parámetro con un valor de 10 a 20.

### *Ejemplo de configuración de una interfaz LAN de cliente de difusión múltiple*

En la Figura 2-14 se muestran clientes de difusión múltiple en una interfaz LAN.

*Figura 2-14. Interfaz LAN de cliente de difusión múltiple*



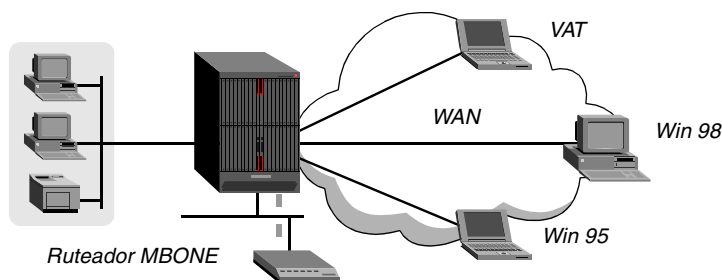
Los comandos siguientes configuran la interfaz IP LAN para que envíe transmisiones de difusión múltiple a clientes de difusión múltiple registrados:

```
admin> read ip-interface { { 1 6 1 } 0 }  
IP-INTERFACE/{ { shelf-1 slot-6 1 } 0 } read  
admin> set multicast-allowed = yes  
admin> set multicast-rate-limit = 5  
admin> set multicast-group-leave-delay = 10  
admin> write  
IP-INTERFACE/{ { shelf-1 slot-6 1 } 0 } written
```

### *Ejemplos de configuración de interfaces WAN de cliente de difusión múltiple*

En la Figura 2-15 se muestran clientes de difusión múltiple en interfaces WAN.

*Figura 2-15. Interfaces WAN de cliente de difusión múltiple*



Los comandos siguientes activan el envío de difusión múltiple para las interfaces WAN de cliente de difusión múltiple en los perfiles Connection denominados VAT-1, W98-1 y W95-1:

```
admin> read connection vat-1  
CONNECTION/vat-1 read  
admin> set ip multicast-allowed = yes  
admin> set ip multicast-rate-limit = 5  
admin> set ip multicast-group-leave-delay = 20  
admin> write  
CONNECTION/vat-1 written  
admin> read connection w98-1  
CONNECTION/w98-1 read
```

## Ruteo IP

### Configuración del envío de difusión múltiple

---

```
admin> set ip multicast-allowed = yes
admin> set ip multicast-rate-limit = 5
admin> set ip multicast-group-leave-delay = 20
admin> write
CONNECTION/w98-1 written
admin> read connection w95-1
CONNECTION/w95-1 read
admin> set ip multicast-allowed = yes
admin> set ip multicast-rate-limit = 5
admin> set ip multicast-group-leave-delay = 20
admin> write
CONNECTION/w95-1 written
```

A continuación se muestran los ajustes equivalentes de perfiles RADIUS:

```
vat-1 Password = "vat1pw"
  Service-Type = Framed-User,
  Ascend-Multicast-Client = Multicast-Yes,
  Ascend-Multicast-GRP-Leave-Delay = 20,
  Ascend-Multicast-Rate-Limit = 5

w98-1 Password = "w98-1pw"
  Service-Type = Framed-User,
  Ascend-Multicast-Client = Multicast-Yes,
  Ascend-Multicast-GRP-Leave-Delay = 20,
  Ascend-Multicast-Rate-Limit = 5

w95-1 Password = "w95-1pw"
  Service-Type = Framed-User,
  Ascend-Multicast-Client = Multicast-Yes,
  Ascend-Multicast-GRP-Leave-Delay = 20,
  Ascend-Multicast-Rate-Limit = 5
```



# Ruteo OSPF

Introducción a OSPF .....	3-1
Adición de una unidad TAOS a una red OSPF .....	3-10
Configuración de opciones de ruta. ....	3-16
Configuración de información de ruta estática OSPF .....	3-18
Soporte multiacceso de no difusión (NBMA) de OSPF .....	3-21
Desactivación de OSPF .....	3-25

## Introducción a OSPF

El protocolo OSPF (*Open Shortest Path First*, Emplear la trayectoria más corta primero) es el protocolo de ruteo por Internet de última generación. El término *Open* del nombre hace referencia a que OSPF se desarrolló en el dominio público como una especificación abierta. *Shortest Path First* hace referencia a un algoritmo que desarrolló Dijkstra en 1978 para crear un árbol con raíz propia de la trayectoria más corta a partir del cual se pudieran derivar tablas de ruteo. Si desea obtener una descripción del algoritmo, consulte el apartado “Algoritmo de ruteo de estado de enlaces” en la página 3-8.

## Limitaciones de RIP resueltas por OSPF

El rápido crecimiento de Internet ha puesto al límite las posibilidades del Protocolo de información de ruteo (RIP), especialmente en las áreas de métrica de distancia-vector, la limitación de 15 saltos y la lenta convergencia debido al exceso de tráfico de ruteo.

### Métrica de distancia-vector

RIP es un protocolo de distancia-vector, que utiliza el número de saltos para seleccionar la ruta más corta a una red de destino. RIP siempre utiliza el número de saltos más bajo, independientemente de la velocidad o la fiabilidad de un enlace.

OSPF es un protocolo de estado de enlaces, lo que significa que OSPF puede tener en cuenta distintas condiciones de los enlaces, como la fiabilidad o la velocidad del enlace, a la hora de determinar la mejor trayectoria a una red de destino.

### *Limitación de 15 saltos*

Con RIP se considera inalcanzable un destino que requiere más de 15 saltos consecutivos y esta restricción limita el tamaño máximo de una red. OSPF no tiene limitaciones de saltos. Puede agregar a la red tantos ruteadores como sea necesario.

### *Exceso de tráfico de ruteo y convergencia lenta*

RIP crea una tabla de ruteo y, a continuación, la propaga a través de la red de ruteadores, salto tras salto. El tiempo que tardan todos los ruteadores en recibir información acerca de un cambio de topología se denomina *convergencia*. Una convergencia lenta puede ser el resultado de bucles y errores de ruteo.

Un ruteador RIP difunde la tabla de ruteo cada 30 segundos. En una red de 15 saltos, la convergencia puede ser de hasta 7,5 minutos. Además, una tabla grande puede requerir varias difusiones por cada actualización, lo que consume una gran cantidad de ancho de banda. OSPF utiliza una base de datos topológica para representar la red y solamente propaga los cambios en la base de datos. Si desea obtener más información acerca de la propagación, consulte el apartado “Intercambio de información de ruteo” en la página 3-4.

## **Implementación TAOS de OSPF**

El objetivo principal de la implementación de OSPF es permitir que la unidad TAOS se comuniquen con otros ruteadores dentro de un único sistema autónomo (AS).

### *Funciones limitadas de ruteador de frontera*

Una unidad TAOS actúa como un ruteador OSPF interno con funciones limitadas de ruteador de frontera.

Actualmente la unidad TAOS no funciona como un gateway IGP, aunque realiza cálculos de ruteador de frontera del sistema autónomo (ASBR) para rutas externas (por ejemplo, enlaces de WAN que no dan soporte a OSPF). La unidad TAOS importa rutas externas a la base de datos OSPF y les coloca el distintivo Externo al sistema autónomo (ASE). Redistribuye estas rutas mediante anuncios ASE de OSPF y propaga sus rutas OSPF a ruteadores de WAN remotos que ejecutan RIP.

### *Autenticación*

La unidad TAOS da soporte a la autenticación por contraseña simple, a la autenticación criptográfica MD5 y a la no autenticación. Para obtener información detallada, consulte “Seguridad” en la página 3-4.

## *Una interfaz IP activa por puerto*

La implantación OSPF de TAOS se ajusta a las especificaciones del documento RFC 1583. No se da soporte a interfaces IP virtuales. Es decir, si se asigna más de una dirección IP al mismo puerto físico, sólo una de las interfaces lógicas pueden tener OSPF activo. Por ejemplo, en la lista siguiente el primer puerto de la tarjeta Ethernet en la ranura 15 (módulo 1, ranura 15, puerto 1) tiene tres interfaces virtuales:

```
admin> dir ip-int
      8  09/14/1998 14:43:14 { { shelf-1 slot-15 2 } 0 }
      8  09/14/1998 14:43:14 { { shelf-1 slot-15 3 } 0 }
      8  09/14/1998 14:43:14 { { shelf-1 slot-15 4 } 0 }
     20  09/14/1998 14:57:48 { { shelf-1 controller 1 } 0 }
     11  09/14/1998 15:24:28 { { shelf-1 slot-15 1 } 0 }
     10  09/14/1998 11:56:47 { { shelf-1 slot-15 1 } 1 }
     10  09/14/1998 11:57:01 { { shelf-1 slot-15 1 } 2 }
     10  09/14/1998 11:57:09 { { shelf-1 slot-15 1 } 3 }
```

OSPF puede activarse en cualquier interfaz IP del puerto, pero no en más de una interfaz del mismo puerto.

## **Comandos de diagnóstico de OSPF**

Los comandos de nivel de diagnóstico de OSPF permiten al administrador visualizar información relacionada con el ruteo OSPF, incluidos los anuncios de estado de enlaces (LSA), la información de ruteador de frontera y las áreas, interfaces, estadísticas y tabla de ruteo de OSPF. Si desea obtener información acerca de la utilización de estos comandos, consulte las publicaciones *APX 8000/MAX TNT/DSLNT Reference (Referencia de APX 8000/MAX TNT/DSLNT)* o *Guía de administración de APX 8000/MAX TNT/DSLNT*.

## **Capturas OSPF**

La unidad TAOS da soporte a las capturas OSPF como se define en el documento RFC 1850, *OSPF Version 2 Management Information Base*. Para generar una captura OSPF cuando se produzca la condición de captura, las capturas OSPF deben estar activas, ya sea en el perfil Trap, ya sea estableciendo el bit correspondiente en el objeto MIB `ospfSetTrap`, que se define en el documento RFC 1850. Debe activarse, asimismo, la captura individual que representa la condición de captura. Si desea obtener información detallada acerca de las capturas OSPF, consulte la publicación *Guía de administración de APX 8000/MAX TNT/DSLNT*.

## **Características de OSPF**

En este apartado se proporciona una breve descripción general del ruteo OSPF que resultará de ayuda para configurar correctamente la unidad TAOS. Si desea obtener información detallada acerca del funcionamiento de OSPF, consulte el documento RFC 1583, *OSPF Version 2*.

Un sistema autónomo (AS) es un grupo de ruteadores OSPF que intercambian información, normalmente bajo el control de una compañía. Un AS puede incluir un gran número de redes, a las que se asigna el mismo número de AS. Toda la información que se intercambia dentro del AS es *interna*.

Los protocolos exteriores se utilizan para intercambiar información de ruteo entre sistemas autónomos. La sigla EGP (Protocolo de gateway externo) hace referencia a estos protocolos. Los ruteadores de frontera pueden utilizar el número de AS para filtrar determinada información de ruteo de EGP. OSPF puede utilizar como información ASE los datos de EGP que han generado y han agregado otros ruteadores de frontera al sistema OSPF, así como las rutas estáticas configuradas localmente o en RADIUS.

## *Seguridad*

Todos los intercambios de protocolos OSPF se autentican. Sólo los ruteadores fiables pueden participar en el ruteo del AS. Pueden utilizarse distintos esquemas de autenticación. De hecho, pueden configurarse diferentes tipos de autenticación para cada área. Si desea obtener una explicación de las áreas, consulte el apartado “Ruteo jerárquico (áreas)” en la página 3-6.

La autenticación proporciona seguridad añadida para los ruteadores que se encuentran en la red. Los ruteadores que no disponen de la contraseña no pueden obtener acceso a la información de ruteo, puesto que un fallo en la autenticación evita que un ruteador forme adyacencias (si desea obtener una explicación sobre las adyacencias, consulte el apartado “Intercambio de información de ruteo” en la página 3-4). Si los dos lados de una conexión no dan soporte al mismo método de autenticación, pueden producirse mensajes de error de los paquetes.

Además de la autenticación simple y la no autenticación, la unidad TAOS da soporte al método de autenticación criptográfica MD5 para OSPF, con lo que cumple con lo especificado en el documento RFC 2328. Si desea obtener información detallada acerca del cifrado MD5, consulte el documento RFC 2328.

## *Soporte para máscaras de subred de longitud variable*

Los ruteadores OSPF manejan máscaras de subred de longitud variable (VLSM). Cada ruta que distribuye OSPF tiene una dirección de destino y una máscara de subred, y dos subredes diferentes de la misma red IP pueden utilizar máscaras de subred de diferente tamaño. Un paquete se rutea a la opción con el mayor número de coincidencias (las más largas o las más específicas). Las rutas de host se consideran subredes cuyas máscaras se componen solamente de unos (0xFFFFFFFF).

**Nota:** Aunque OSPF es muy útil en redes que utilizan VLSM, debe intentar asignar subredes lo más contiguas posible para evitar que todos los ruteadores OSPF realicen un exceso de cálculos de estado de enlaces en la red.

## *Intercambio de información de ruteo*

OSPF almacena la información acerca de la red en una base de datos topológica y propaga únicamente los cambios en la base de datos. Los ruteadores contiguos seleccionados forman relaciones, denominadas *adyacencias*, con el fin de intercambiar información de ruteo. No todos los pares de ruteadores contiguos son adyacentes. Los ruteadores conectados mediante redes punto a punto y los enlaces virtuales siempre son adyacentes. En las redes de multiacceso, todos los ruteadores son adyacentes tanto al ruteador designado como al ruteador designado de reserva.

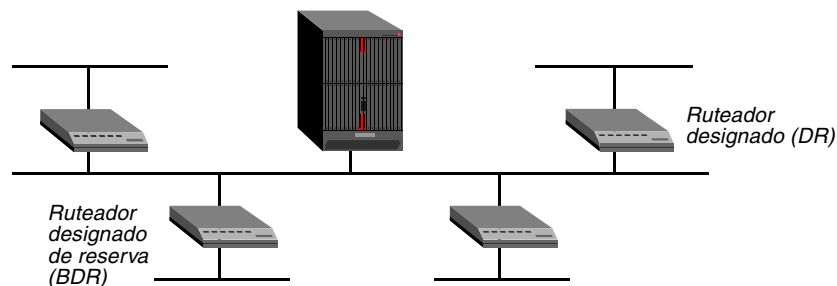
A medida que se establece la adyacencia, los ruteadores contiguos intercambian bases de datos y crean una base de datos coherente y sincronizada común a todos ellos. Cuando un ruteador OSPF detecta un cambio en una de sus interfaces, modifica la base de datos topológica y

realiza una difusión múltiple del cambio a los routers contiguos adyacentes, que a su vez propagan el cambio a sus routers contiguos adyacentes, hasta que todos los routers del área tienen sincronizadas las bases de datos topológicas. Este proceso proporciona una convergencia rápida entre routers.

### *Ruteadores designados y ruteadores designados de reserva*

En la terminología OSPF, una red de difusión es toda aquella red que posee más de dos routers OSPF conectados y que da soporte a la posibilidad de dirigir un único mensaje físico a todos los routers conectados.

*Figura 3-1. Ruteador designado (DR) y ruteador designado de reserva (BDR) OSPF*



Para reducir el número de adyacencias que debe formar cada router, OSPF denomina a uno de los routers el router designado. A medida que los routers empiezan a formar adyacencias, eligen un router designado y, a continuación, todos los routers de la red establecen primariamente adyacencias con el router designado. Esto simplifica el procedimiento de actualización de la tabla de ruteo y reduce el número de registros de estado de enlaces en la base de datos. El router designado desempeña otros papeles importantes y reduce la actividad general de los procedimientos de estado de enlaces de OSPF. Por ejemplo, otros routers envían anuncios LSA únicamente al router designado utilizando la dirección de difusión múltiple de todos los routers designados 224.0.0.6.

Para evitar la dependencia excesiva de la red en el router designado en caso de producirse anomalías, los routers OSPF también eligen un router designado de reserva al mismo tiempo. Los demás routers mantienen adyacencias con el router designado y el de reserva, pero el router de reserva deja el máximo de tareas de proceso posible al router designado. Si el router designado falla, el router de reserva se convierte en el router designado y se elige un nuevo router de reserva.

Puede elegir el router designado en función de la potencia de procesamiento, la velocidad y la memoria del sistema y, a continuación, asignar prioridades a otros routers de la red por si el router de reserva queda inactivo al mismo tiempo.

**Nota:** La unidad TAOS puede funcionar como un router designado (DR) o un router designado de reserva (BDR). Sin embargo, en muchos entornos se elige asignar para estas funciones un router basado en la LAN a fin de que la unidad TAOS se dedique a procesos de la WAN.

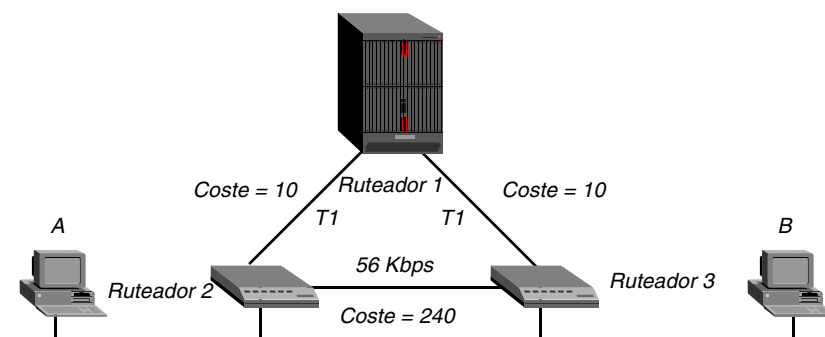
## *Métrica configurable del coste*

Puede asignar un coste a la salida de cada interfaz de router. Cuanto menor sea el coste, mayor será la probabilidad de que se utilice la interfaz para reenviar tráfico de datos. Los costes también se pueden asociar a los datos de ruteo derivados externamente.

El coste de OSPF puede utilizarse para la selección de la trayectoria preferida. Si dos trayectorias con un mismo destino tienen costes idénticos, puede asignar un coste superior a una de las trayectorias para configurarla como trayectoria de reserva, que se utilizará solamente cuando la trayectoria primaria no esté disponible.

En la Figura 3-2 se muestra el modo en que se utilizan los costes para dirigir el tráfico en enlaces de alta velocidad. Por ejemplo, si el router 2 de la Figura 3-2 recibe paquetes con destino al host B, los rutea a través del router 1 por dos enlaces T1 (Coste=20) en lugar de rutearlos por un canal B de 56 Kbps al router 3 (Coste=240).

*Figura 3-2. Costes OSPF para diferentes tipos de enlace*



La unidad TAOS tiene el coste predeterminado 1 para una ruta conectada (Ethernet) y 10 para un enlace de WAN. Si tiene dos trayectorias al mismo destino, se utilizará la que tenga un coste menor, a menos que las preferencias de ruta cambien la ecuación. Si desea obtener información acerca de las preferencias de ruta, consulte el Capítulo 2, “Ruteo IP”. A la hora de asignar costes, debe tener en cuenta el ancho de banda de una conexión. Por ejemplo, para una conexión de un único canal B, el coste sería 24 veces mayor que el de un enlace T1.

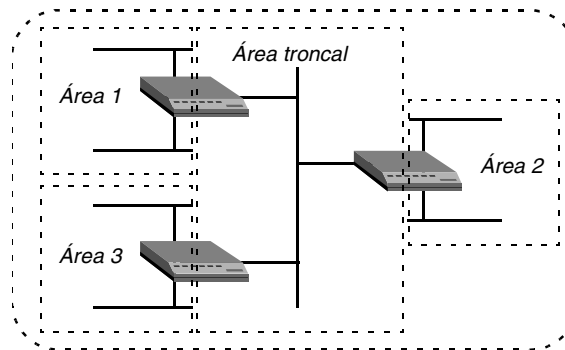
**Nota:** Preste mucha atención cuando asigne costes. Una métrica de coste incorrecta puede causar retardos y la congestión de la red.

## *Ruteo jerárquico (áreas)*

Si una red se hace demasiado grande, el tamaño de la base de datos, el tiempo necesario para el cálculo de rutas y el tráfico de red relacionado serán excesivos. Puede dividir un AS en áreas para proporcionar un ruteo jerárquico, con un área troncal que conecte las demás áreas. El área troncal es especial y siempre tiene el número de área 0.0.0.0. A las demás áreas se les asignan números de área exclusivos dentro del AS.

Cada área actúa como una red propia: toda la información del ruteo específica del área permanece dentro del área y todos los routers del área deben tener una base de datos topológica sincronizada. Para unir las áreas, algunos routers pertenecen al área troncal y a alguna de las demás áreas. Estos routers se denominan routers de frontera de área (ABR). En la Figura 3-3 todos los routers son ABR.

*Figura 3-3. División de un sistema autónomo (AS) OSPF en áreas*



Con los ABR y los límites del área configurados correctamente, las bases de datos de estado de los enlaces son exclusivas de un área. Puede configurar la unidad TAOS para realizar ruteos en tres tipos de área, que difieren en el manejo de las rutas externas. Es decir, las rutas externas del AS (ASE), que originan los ASBR como LSA de tipo 5, se manejan de forma diferente en cada una de las áreas siguientes:

- Normal
- Stub
- NSSA (Not So Stubby Area)

### **Áreas normales**

Un área OSPF normal permite el paso de anuncios LSA de tipo 5 en el área.

### **Áreas stub**

En las áreas conectadas al área troncal únicamente mediante un ABR (es decir, el área tiene un punto de salida), no es necesario mantener información acerca de las rutas externas. Para reducir el coste de ruteo, OSPF da soporte a las áreas stub, en las que una ruta predeterminada resume todas las rutas externas. Un área stub no permite que se propaguen anuncios LSA de tipo 5 en el área o a través de ella; en cambio, depende del ruteo predeterminado a destinos externos.

### **NSSA**

Las NSSA se parecen a las áreas stub en que no reciben ni originan anuncios LSA de tipo 5. Sin embargo, las NSSA dependen únicamente del ruteo predeterminado de las rutas externas. Emplean LSA de tipo 7 para transportar información de ruta ASE en el área. Los anuncios LSA de tipo 7 utilizan un bit de propagación (P) para indicar al ruteador de frontera de NSSA que convierta los anuncios LSA de tipo 7 en LSA de tipo 5, que pueden propagarse a otras áreas.

Cuando la unidad TAOS rutea OSPF en una NSSA, importa rutas ASE definidas en perfiles locales o RADIUS como anuncios LSA de tipo 7. Estos LSA de ASE importados siempre tienen activado el bit P, que indica a los ruteadores de frontera que deben convertirlos en anuncios LSA de tipo 5.

Puede listar los ID de los ruteadores de frontera de NSSA (que realizan la conversión de LSA de tipo 7 a tipo 5) introduciendo el comando OSPF Translators. Por ejemplo:

```
admin> ospf translators
```

```
Area ID      Router ID
0.0.0.1      10.105.0.13
0.0.0.2      12.1.1.1
```

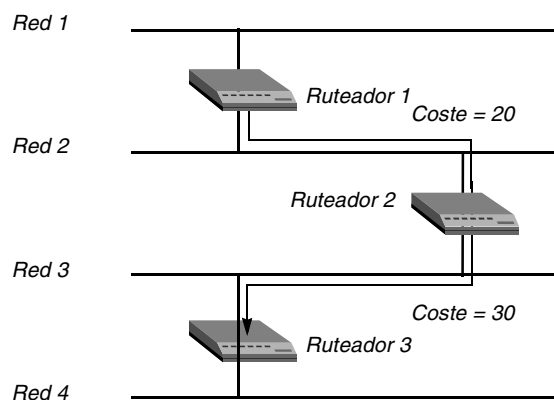
**Nota:** Si desea obtener información detallada acerca de la especificación NSSA, consulte el documento RFC 1587.

### *Algoritmo de ruteo de estado de enlaces*

Los algoritmos de ruteo de estado de enlaces requieren que todos los ruteadores de un dominio mantengan bases de datos topológicas sincronizadas (idénticas) y que las bases de datos describan la topología completa del dominio. Un dominio de un ruteador OSPF puede ser un AS o un área dentro de un AS.

Los ruteadores OSPF crean y actualizan una base de datos de estado de los enlaces a partir de la información que intercambian con otros ruteadores. Las bases de datos de estado de los enlaces se sincronizan entre pares de ruteadores adyacentes (como se describe en el apartado “Intercambio de información de ruteo” en la página 3-4). Además, cada ruteador OSPF utiliza su base de datos de estado de los enlaces para calcular un árbol con raíz propia de las trayectorias más cortas a todos los destinos. La tabla de ruteo se crea a partir de estos árboles de trayectoria más corta que se han calculado. Por ejemplo, observe la topología de la red de la Figura 3-4.

*Figura 3-4. Topología OSPF de ejemplo*



En la Tabla 3-1 se muestra la información pertinente de las bases de datos de estado de los enlaces de los ruteadores.

*Tabla 3-1. Bases de datos de estado de los enlaces para la topología OSPF de la Figura 3-4*

Ruteador 1	Ruteador 2	Ruteador 3
Red 1/Coste 0	Red 2/Coste 0	Red 3/Coste 0
Red 2/Coste 0	Red 3/Coste 0	Red 4/Coste 0



*Tabla 3-1. Bases de datos de estado de los enlaces para la topología OSPF de la Figura 3-4 (continuación)*

Ruteador 1	Ruteador 2	Ruteador 3
Ruteador 2/Coste20	Ruteador 1/Coste 20	Ruteador 2/Coste 30
	Ruteador 3/Coste 30	

Desde la base de datos de estado de los enlaces, cada ruteador crea un árbol de trayectoria más corta con raíz propia y, a continuación, calcula una tabla de ruteo que indica la trayectoria más corta a cada destino en el AS (la tabla también incluye información de ruteo derivada externamente).

Todos los ruteadores calculan una tabla de ruteo de las trayectorias más cortas basándose en la base de datos de estado de los enlaces. Los datos de ruteo derivados externamente se anuncian a través del AS, pero permanecen separados de los datos de estado de los enlaces. Cada ruta externa puede llevar una etiqueta del ruteador que realiza el anuncio, con lo que permite el paso de información adicional entre ruteadores en los límites del AS.

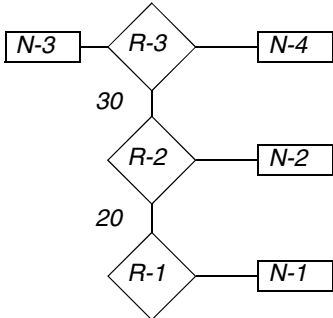
*Tabla 3-2. Árbol de trayectorias más cortas y tabla de ruteo resultante para el ruteador 1*

	Destino	Salto siguiente	Métrica
	Red 1	Directo	0
	Red 2	Directo	0
	Red 3	Ruteador 2	20
	Red 4	Ruteador 2	50

*Tabla 3-3. Árbol de trayectorias más cortas y tabla de ruteo resultante para el ruteador 2*

	Destino	Salto siguiente	Métrica
	Red 1	Ruteador 1	20
	Red 2	Directo	0
	Red 3	Directo	0
	Red 4	Ruteador 2	30

Tabla 3-4. Árbol de trayectorias más cortas y tabla de ruteo resultante para el ruteador 3

	<i>Destino</i>	<i>Salto siguiente</i>	<i>Métrica</i>
	Red 1	Ruteador 2	50
	Red 2	Ruteador 2	30
	Red 3	Directo	0
	Red 4	Directo	0

Adición de una unidad TAOS a una red OSPF

Antes de poder ejecutar OSPF, debe configurarse para el ruteo IP la unidad TAOS, como se describe en el Capítulo 2, “Ruteo IP”.

Información general de los ajustes OSPF de LAN y WAN

Los subperfiles OSPF de los perfiles IP-Interface y Connection (para la configuración de interfaces locales y de WAN, respectivamente) contienen los mismos parámetros. A continuación se muestran los parámetros OSPF, con los ajustes predeterminados:

```
[in IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf]
active = no
area = 0.0.0.0
area-type = normal
hello-interval = 10
dead-interval = 40
priority = 5
authen-type = simple
auth-key = ascend0
md5-auth-key = *****
key-id = 0
cost = 1
down-cost = 16777215
ase-type = type-1
ase-tag = c0:00:00:00
transit-delay = 1
retransmit-interval = 5
non-multicast = no

[in CONNECTION/"/":ip-options:ospf-options]
active = no
area = 0.0.0.0
area-type = normal
hello-interval = 30
dead-interval = 120
priority = 5
authen-type = simple
```

```

auth-key = ascend0
md5-auth-key = *****
key-id = 0
cost = 10
down-cost = 1000
ase-type = type-1
ase-tag = c0:00:00:00
transit-delay = 1
retransmit-interval = 5
non-multicast = no

[in OSPF-VIRTUAL-LINK/0/0/0/0]
md5-authen-key = *****

```

Parámetro	Especifica
Active	Activa y desactiva OSPF en una interfaz.
Area	Número de área en formato decimal con puntos. El número de área predeterminado es 0.0.0.0, que representa el área troncal de OSPF. Observe que los números de área no son direcciones IP, si bien utilizan un formato similar. Si desea obtener una explicación de las áreas, consulte el apartado “Ruteo jerárquico (áreas)” en la página 3-6.
Area-Type	Tipo de área. El valor predeterminado es el tipo de área Normal, en el que las rutas externas se anuncian a través del AS.
Hello-Interval	Número de segundos entre paquetes Hello. El valor predeterminado del parámetro Hello-Interval es 30. Si desea obtener información sobre cómo el ruteador utiliza estos paquetes, consulte el apartado “Intercambio de información de ruteo” en la página 3-4.
Dead-Interval	Número de segundos que esperará el ruteador sin recibir un paquete Hello antes de considerar que el ruteador contiguo está inactivo y registrar un cambio de estado del enlace. Para obtener información detallada, consulte “Intercambio de información de ruteo” en la página 3-4.
Priority	Valor de prioridad que se utiliza para elegir un ruteador designado (DR) y un ruteador designado de reserva (BDR). Un ajuste igual o mayor que 1 coloca la unidad TAOS en la lista de ruteadores DR posibles. Un ajuste de 0 excluye la unidad TAOS de ser DR o BDR. Cuanto mayor sea el valor de prioridad de la unidad TAOS en relación con los demás ruteadores OSPF de la red, más posibilidades tiene de ser BDR o DR. Para obtener información detallada, consulte “Ruteadores designados y ruteadores designados de reserva” en la página 3-5.

## Ruteo OSPF

### Adición de una unidad TAOS a una red OSPF

---

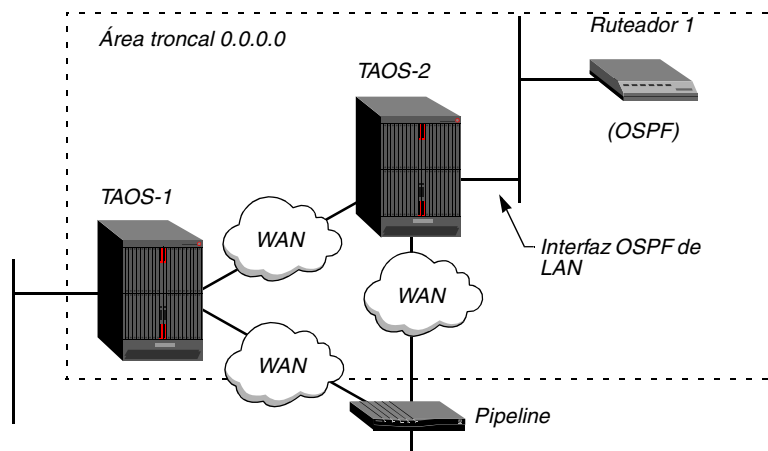
Parámetro	Especifica
Authen-Type	<p>Tipo de autenticación que se debe utilizar para validar los intercambios de paquetes OSPF. Especifique uno de los valores siguientes:</p> <ul style="list-style-type: none"><li>• None: la autenticación no es necesaria.</li><li>• Simple (el valor predeterminado): el ruteador utiliza la contraseña que proporciona el parámetro Auth-Key para validar los intercambios de paquetes OSPF.</li><li>• MD5: el ruteador utiliza el cifrado MD5 y el ID de clave de autenticación que proporciona el parámetro Key-ID para validar los intercambios de paquetes OSPF. Si desea obtener información al respecto, consulte “Seguridad” en la página 3-4.</li></ul>
Auth-Key	<p>Clave secreta para la autenticación de tráfico en el área del ruteador. Si Authen-Type se establece en md5, debe establecer el parámetro MD5-Auth-Key para especificar una clave.</p>
MD5-Auth-Key	<p>Clave secreta que se utilizará en el método de autenticación criptográfica MD5 de 16 caracteres como máximo. El valor predeterminado es <code>ascend0</code>.</p>
MD5-Authen-Key	<p>Clave secreta que se utilizará en el método de autenticación criptográfica MD5 de 16 caracteres como máximo. El valor predeterminado es <code>ascend0</code>. Si Authen-Type se establece en md5, debe proporcionar una clave en el nuevo campo puesto que el ajuste Auth-Key, que se utilizaba anteriormente, ya no será aplicable.</p>
Key-ID	<p>Número entre 0 y 255 que se utiliza para cifrar la clave secreta cuando Authen-Type se establece en MD5.</p>
Cost	<p>Coste del ruteo a la interfaz. Cuanto menor sea el coste asignado a una ruta, mayor será la probabilidad de que se utilice para reenviar tráfico. Para obtener información detallada, consulte “Métrica configurable del coste” en la página 3-6.</p>
Down-Cost	<p>Coste que debe aplicarse a la interfaz cuando está inactiva.</p>
ASE-Type	<p>Tipo de métrica que se aplica a las rutas que se obtienen de RIP. Type-1 expresa la métrica en las mismas unidades que el coste de la interfaz. Type-2 se considera mayor que cualquier trayectoria de estado de enlaces. Este parámetro se aplica a un perfil Connection solamente cuando OSPF <i>no</i> está activo.</p>
ASE-Tag	<p>Número hexadecimal que aparece en utilidades de gestión y que identifica la ruta como externa. También pueden utilizarlo los ruteadores de frontera para filtrar un registro. Está activo en un perfil Connection solamente cuando OSPF <i>no</i> está activo.</p>
Transit-Delay	<p>Número estimado de segundos que se tarda en transmitir un paquete de actualización del estado de los enlaces a través de esta interfaz, teniendo en cuenta los retardos de transmisión y propagación. En una ruta conectada, puede dejar el valor predeterminado 1.</p>

Parámetro	Especifica
Retransmit-Interval	Número de segundos entre las retransmisiones de anuncio de estado de enlaces para adyacencias que pertenecen a esta interfaz. Este valor se utiliza también a la hora de retransmitir paquetes de petición de estado de enlaces y descripción de bases de datos. En una ruta conectada, normalmente debe dejarse el valor predeterminado 5.
Non-Multicast	Activa y desactiva una unidad TAOS para que ejecute OSPF en un enlace de relé de trama con un conmutador GRF®. GRF modela el relé de trama como una red multiacceso de no difusión (NBMA), mientras que la unidad TAOS modela el relé de trama como una red serie (punto a punto). Si Non-Multicast se establece en Yes, todos los paquetes de difusión múltiple se vuelven a correlacionar con una dirección contigua indicada, que permite la formación de adyacencias entre ruteadores contiguos. Este ajuste se pasa por alto en una red de difusión Ethernet. No se recomienda su utilización en interfaces sin numerar. Si se especifica en una interfaz sin numerar, los paquetes se perderán.

## Ejemplo de configuración de una interfaz OSPF de LAN

En la Figura 3-5 se muestran tres ruteadores OSPF en el área troncal de un AS. Puesto que todos los ruteadores OSPF se encuentran en la misma área, las unidades forman adyacencias y sincronizan sus bases de datos. En este ejemplo se muestra cómo configurar la interfaz de LAN de la unidad denominada TAOS-2 de la Figura 3-5.

*Figura 3-5. OSPF en una interfaz de LAN*



Todos los ruteadores OSPF de la Figura 3-5 tienen el protocolo RIP desactivado. La ejecución de RIP y OSPF es innecesaria y desactivar RIP reduce la actividad general del procesador. OSPF puede obtener rutas de interfaces RIP, incorporarlas en la tabla de ruteo, asignarles una métrica externa y etiquetarlas como rutas externas.

Aunque en la documentación RFC no se especifica una limitación del número de rutas del área troncal, debe mantener un número de rutas relativamente reducido, puesto que los cambios que se producen en el área cero se propagan por el AS. Otro modo de configurar las mismas unidades consiste en crear una segunda área (por ejemplo, 0.0.0.1) en uno de los ruteadores

OSPF existentes y agregar la unidad TAOS a dicha área. A continuación puede asignar el mismo nombre de área (0.0.0.1) a todos los ruteadores OSPF que se han alcanzado con la unidad TAOS en el enlace de WAN.

En la Figura 3-5 se muestra un ejemplo de configuración de TAOS-2. Los comandos asignan la dirección IP 10.168.8.17/24 a la interfaz local y configuran el ruteador OSPF en el área troncal:

```
admin> read ip-int {{ 1 12 1 } 0 }  
IP-INTERFACE/{ { shelf-1 slot-12 1 } 0 } read  
  
admin> set ip-address = 10.168.8.17/24  
  
admin> set rip-mode = routing-off  
  
admin> set ignore-def-route = yes  
  
admin> set ospf active = yes  
  
admin> write  
IP-INTERFACE/{ { shelf-1 slot-12 1 } 0 } written
```

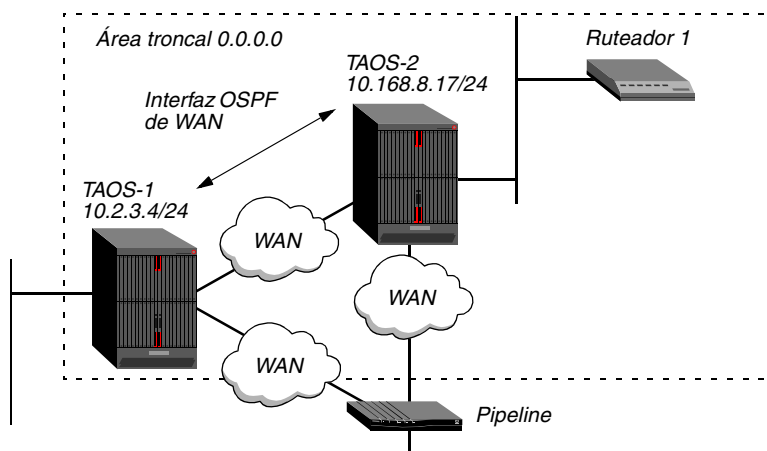
En el ejemplo siguiente se muestra cómo configurar la interfaz IP para la autenticación MD5:

```
admin> read ip-interface { { 1 12 1 } 0 }  
IP-INTERFACE/{ { shelf-1 slot-12 1 } 0 } read  
  
admin> set ospf authen-type = md5  
admin> set ospf md5-auth-key = 12!secret*34key  
admin> write  
IP-INTERFACE/{ { shelf-1 slot-12 1 } 0 } written
```

## Ejemplo de configuración de interfaces OSPF de WAN

En este ejemplo se muestra cómo configurar perfiles Connection en los modelos de la unidad TAOS que se muestran en la Figura 3-6 con el fin de que puedan rutear OSPF por la WAN que los separa. En este ejemplo, la unidad denominada TAOS-1 tiene la dirección IP 10.2.3.4/24 y la unidad denominada TAOS-2 tiene la dirección 10.168.8.17/24.

*Figura 3-6. OSPF en una interfaz de WAN*



Las interfaces de WAN de la unidad TAOS forman redes punto a punto. Es decir, cada enlace une un par de ruteadores. Por lo general, las redes punto a punto no proporcionan ningún servicio de difusión o de difusión múltiple, de modo que todos los anuncios se envían de punto a punto.

Los comandos siguientes configuran el enlace OSPF de WAN en TAOS-1 en la Figura 3-6:

```
admin> read conn taos2link
CONNECTION/taos2link read

admin> set ip-options remote = 10.168.8.17/24

admin> set ip-options rip = routing-off

admin> set ip-options ospf active = yes

admin> write
CONNECTION/taos2link written
```

Los comandos siguientes configuran el enlace OSPF de WAN en TAOS-2 en la Figura 3-6:

```
admin> read conn taos1link
CONNECTION/taos1link read

admin> set ip-options remote = 10.2.3.4/24

admin> set ip-options rip = routing-off

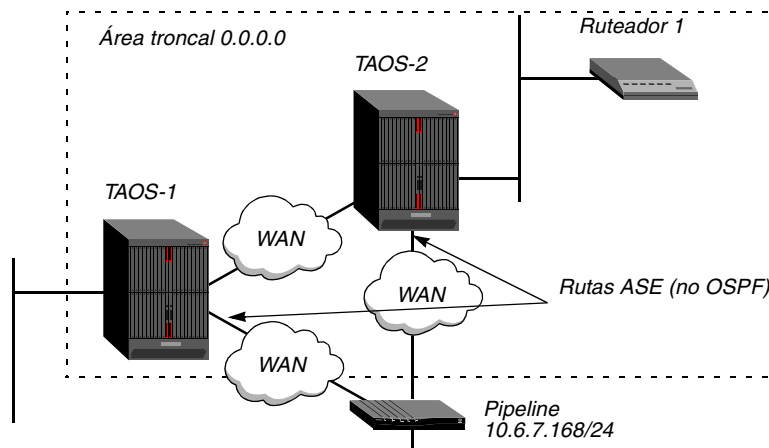
admin> set ip-options ospf active = yes

admin> write
CONNECTION/taos1link written
```

## Ejemplo de integración de una interfaz RIP-v2

En la Figura 3-7 cada unidad TAOS tiene una interfaz de WAN conectada a una unidad Pipeline remota. La unidad Pipeline es un ruteador IP que da soporte a RIP-v2 y que tiene la dirección IP 10.6.7.168/24. La ruta que va a la LAN de la unidad Pipeline y todas las rutas que obtiene la unidad TAOS relacionadas con la unidad Pipeline remota son rutas ASE (externas al sistema autónomo OSPF).

*Figura 3-7. Inclusión de rutas ASE en el entorno OSPF*



Para activar OSPF con el fin de agregar a la tabla de ruteo rutas obtenidas de RIP-v2, puede configurar RIP-v2 normalmente en los perfiles Connection. El parámetro global RIP-ASE-Type del perfil IP-Global determina la métrica ASE que se aplica cuando se importan las rutas a OSPF. Si desea obtener información detallada acerca de RIP-ASE-Type, consulte el apartado “Configuración de opciones de ruta” en la página 3-16.

Sin embargo, en el ejemplo siguiente, RIP se desactiva en el enlace, de modo que la unidad TAOS no reenvía ni recibe actualizaciones de ruteo en la interfaz. Los comandos siguientes especifican un coste de 240 para el enlace con la unidad Pipeline, la desactivación de RIP y la especificación de información sobre ASE para la ruta estática del perfil Connection:

```
admin> read conn pipeline1
CONNECTION/pipeline1 read
admin> set ip-options remote = 10.6.7.168/24
admin> set ip-options rip = routing-off
admin> set ip-options ospf active = no
admin> set ip-options ospf cost = 240
admin> set ip-options ospf ase-type = type-2
admin> set ip-options ospf ase-tag = cfff8000
admin> write
CONNECTION/pipeline1 written
```

La información de ASE-Type y ASE-Tag hace que el ruteador OSPF importe la ruta a 10.6.7.168/24 como un LSA de tipo 2 y la etiqueta con el número hexadecimal especificado. El coste asignado es adecuado para el ancho de banda de una conexión de un único canal B (el coste es 24 veces mayor que en un enlace T1).

## ***Configuración de opciones de ruta***

El perfil IP-Global contiene varios ajustes que solamente se aplican cuando se utiliza el ruteo OSPF. A continuación se muestran los parámetros pertinentes (con los ajustes predeterminados):

```
[in IP-GLOBAL]
pool-ospf-adv-type = type-1
ospf-pref = 10
ospf-ase-pref = 150
rip-tag = c8:00:00:00
rip-ase-type = 1

[in IP-GLOBAL:ospf-global]
as-boundary-router = yes
```

Parámetro	Especifica
Pool-OSPF-Adv-Type	Tipo de métrica ASE que se aplica a las agrupaciones resumidas importadas en OSPF como rutas externas. Pool-Summary debe establecerse en Yes y OSPF debe estar activo para que este ajuste sea efectivo. Type-1 (el valor predeterminado) expresa la métrica en las mismas unidades que el coste de la interfaz. Type-2 se considera mayor que cualquier trayectoria de estado de enlaces. Las importaciones internas agrupan las rutas como rutas internas del área, lo que permite que funcionen con áreas stub.
OSPF-Pref	Valor de preferencia para las rutas obtenidas de OSPF. Los valores válidos se encuentran entre 0 y 255 (10 es el valor predeterminado).



Parámetro	Especifica
OSPF-ASE-Pref	Valor de preferencia para rutas obtenidas de RIP, ICMP u otro protocolo distinto de OSPF. Los valores validos se encuentran entre 0 y 255. De manera predeterminada, se asigna un valor de preferencia de 150 a las rutas obtenidas de forma dinámica de otro protocolo de ruteo.
RIP-Tag	Número hexadecimal que se asocia con las rutas obtenidas de RIP. Los ruteadores de frontera de OSPF pueden utilizar la etiqueta para filtrar un registro.
RIP-ASE-Type	Tipo de métrica ASE que se aplica a las rutas obtenidas de RIP. Type-1 (el valor predeterminado) expresa la métrica en las mismas unidades que el coste de la interfaz. Type-2 se considera mayor que cualquier trayectoria de estado de enlaces.
AS-Boundary-Router	Activa y desactiva los cálculos de ruteador de frontera del sistema autónomo (ASBR) relacionados con rutas externas. Normalmente cuando la unidad TAOS importa rutas externas de RIP (por ejemplo, cuando establece un enlace de WAN con un emisor que no da soporte a OSPF), realiza los cálculos de ASBR para estas rutas. Si es necesario, puede evitar que la unidad TAOS realice cálculos de ASBR estableciendo AS-Boundary-Router en No.

## Ejemplo de importación de una agrupación resumida como ASE

Si desea obtener información acerca de la definición de agrupaciones de direcciones resumidas, consulte el apartado “Ejemplos de configuración de agrupaciones de direcciones resumidas” en la página 2-72. Los comandos siguientes configuran una agrupación resumida y la importan a OSPF con una métrica OSPF de tipo 1:

```
admin> read ip-global
IP-GLOBAL read

admin> set pool-summary = yes

admin> set pool-base-address 1 = 10.12.253.1

admin> set assign-count 1 = 62

admin> set pool-ospf-adv-type = type-1

admin> write
IP-GLOBAL written
```

Cuando Pool-Summary se establece en Yes y OSPF está activo, el subsistema OSPF realiza una búsqueda en el parámetro Pool-OSPF-Adv-Type para decidir cómo importar rutas resumidas en OSPF. Si se establece en Type-1, la métrica de la ruta a una agrupación resumida se expresa en las mismas unidades que la métrica de estado de los enlaces (coste de la interfaz).

Si Pool-OSPF-Adv-Type se establece en Type-2, se supone que el ruteo entre sistemas autónomos es el mayor coste de ruteo de un paquete y que no es necesario convertir los costes externos en métrica de estado de los enlaces interna. Si el parámetro se establece en Internal, las direcciones de la agrupación resumida se importan a OSPF como rutas internas del área, lo que permite que funcionen correctamente con áreas stub.

## Ejemplo de definición de preferencias ASE

Los ajustes de OSPF-Pref y OSPF-ASE-Pref determinan los valores de preferencias asignados a las rutas obtenidas de otros ruteadores OSPF y las rutas que se han importado de otros protocolos de ruteo dinámico. Los ajustes predeterminados asignan una preferencia mucho menor a las rutas OSPF, que se traduce en una mayor probabilidad de utilización de dichas rutas. Los comandos siguientes reducen a 100 el grado de preferencia asignado a rutas ASE (el valor predeterminado es 150):

```
admin> read ip-global
IP-GLOBAL read

admin> set ospf-ase-pref = 100

admin> write
IP-GLOBAL written
```

## Configuración de información de ruta estática OSPF

Los parámetros de IP-Route siguientes (que aparecen con ajustes de ejemplo) se aplican solamente cuando OSPF está activo:

```
in IP-ROUTE/" (new) ]
cost = 1
third-party = no
ase-type = type-1
ase-tag = c0:00:00:00
ase7-adv = N/A
```

Parámetro	Especifica
Cost	Coste del ruteo a la interfaz. Cuanto menor sea el coste asignado a una ruta, mayor será la probabilidad de que se utilice para reenviar tráfico. Consulte el apartado “Métrica configurable del coste” en la página 3-6.
Third-Party	Activa y desactiva el anuncio de rutas a destinos externos en representación de otro gateway (un tercero). Consulte el apartado “Ejemplo de especificación de una ruta de terceros” en la página 3-20.
Ase-Type	Tipo de métrica que se aplica a las rutas que se obtienen de RIP. Type-1 expresa la métrica en las mismas unidades que el coste de la interfaz. Type-2 se considera mayor que cualquier trayectoria de estado de enlaces. Este parámetro se aplica a un perfil Connection solamente cuando OSPF <i>no</i> está activo.
Ase-Tag	Número hexadecimal que aparece en utilidades de gestión y que identifica a la ruta como externa. También pueden utilizarlo los ruteadores de frontera para filtrar este registro. Está activo en un perfil Connection solamente cuando OSPF <i>no</i> está activo.

Parámetro	Especifica
ASE7-Adv	En las versiones anteriores del software este parámetro proporcionaba una manera de desactivar el bit P para rutas estáticas que se importaban a OSPF en una NSSA, con el fin de evitar que estas rutas se propagaran al área troncal. Esta condición ya no se aplica. Ahora el bit P está siempre activo en rutas ASE, de modo que la unidad TAOS pasa por alto el ajuste de este parámetro.

## Ejemplo de configuración de un LSA de tipo 7 en una NSSA

Si desea obtener información complementaria acerca de NSSA, consulte el apartado “Ruteo jerárquico (áreas)” en la página 3-6. Para configurar la unidad TAOS de modo que rutee OSPF en una NSSA, *todas* las interfaces de OSPF de la unidad TAOS deben especificar el tipo de área NSSA.

Para configurar un LSA de tipo 7, debe especificar una ruta estática en un perfil IP-Route. A continuación se muestran los parámetros pertinentes (con los ajustes predeterminados):

```
[in IP-ROUTE/external]
name* = external
dest-address = 10.4.5.0/22
gateway-address = 10.4.5.7
metric = 0
cost = 1
preference = 100
third-party = no
ase-type = type-1
ase-tag = c0:00:00:00
private-route = yes
active-route = yes
ase7-adv = n/a
```

Con el procedimiento siguiente se configura la unidad TAOS para que realice ruteos en una NSSA e importe un LSA de tipo 7 que especifique una ruta externa a través del enlace de WAN:

- 1 Asigne un tipo de área NSSA a cada interfaz IP que ejecute OSPF. Por ejemplo:

```
admin> read ip-int {{ 1 12 1 } 0 }
IP-INTERFACE/{ { shelf-1 slot-12 1 } 0 } read
admin> set ospf area-type = nssa
admin> write
IP-INTERFACE/{ { shelf-1 slot-12 1 } 0 } written
```

- 2 Configure el enlace de WAN que represente una ruta ASE. Por ejemplo:

```
admin> read connection ase-like
CONNECTION/ase-link read
admin> set ip-options remote = 10.4.5.7/22
admin> set ip-options rip = routing-off
admin> set ip-options ospf active = yes
admin> write
CONNECTION/ase-link written
```

- 3 Configure una ruta estática al sitio remoto. Por ejemplo:

```
admin> new ip-route type7
IP-ROUTE/type7 read

admin> set dest = 10.4.5.0/22

admin> set gateway = 10.4.5.7

admin> write
IP-ROUTE/type7 written
```

## Ejemplo de asignación de un coste a una ruta estática

Cuanto menor sea el coste asignado a una ruta, mayor será la probabilidad de que el ruteador elija dicha ruta para reenviar tráfico. Generalmente debe tener en cuenta el ancho de banda de una conexión a la hora de asignar los costes. Por ejemplo, el coste de una conexión de canal único sería 24 veces mayor que el de un enlace T1.

La unidad TAOS tiene el coste predeterminado 1 para una ruta conectada (Ethernet) y 10 para un enlace de WAN. Si dispone de dos trayectorias para el mismo destino, se utilizará aquella cuyo coste sea menor. Preste mucha atención cuando asigne costes ya que una métrica de coste incorrecta puede causar retardos y la congestión de la red. En el ejemplo siguiente un administrador asigna un coste de 25 a una ruta estática:

```
admin> new ip-route 56klink
IP-ROUTE/56klink read

admin> set dest = 10.1.2.0/24

admin> set gateway = 10.9.8.10

admin> set cost = 25

admin> write
IP-ROUTE/56klink written
```

## Ejemplo de especificación de una ruta de terceros

OSPF puede anunciar rutas a destinos externos en representación de otro gateway (un tercero). Esta función se denomina comúnmente anunciar una dirección de reenvío. Si está desactivado el ruteo de terceros, la unidad TAOS se anuncia como dirección de reenvío a un destino externo. Si el ruteo de terceros está activo, la unidad TAOS anuncia la dirección IP de otro gateway.

En función de la topología de la red, es posible que los demás ruteadores puedan utilizar este tipo de LSA de terceros para realizar ruteos directamente a la dirección de reenvío sin implicar al ruteador anunciante, con lo que se incrementaría el rendimiento de la red. Esta función solamente puede utilizarse si todos los ruteadores OSPF saben cómo realizar ruteos a la dirección de reenvío. Para que se conozca la ruta, la dirección de reenvío debe encontrarse en una red local que tenga un ruteador OSPF que actúe de ruteador de reenvío o un ruteador designado debe enviar anuncios LSA para esa red Ethernet en toda las áreas que capten los LSA de dirección de reenvío de la ruta estática. Observe que el ruteo de terceros no puede utilizarse cuando se anuncian ASE de tipo 7 (como se especifica en el documento RFC 1587).

En la siguiente ruta de ejemplo, la unidad TAOS anunciará una ruta de terceros (una dirección de reenvío) para el destino 10.1.2.0. La dirección de reenvío es 10.9.8.10.

```
admin> new ip-route fwd
IP-ROUTE/fwd read

admin> set dest = 10.1.2.0/24

admin> set gateway = 10.9.8.10

admin> set third-party = yes

admin> write
IP-ROUTE/fwd written
```

## ***Soporte multiacceso de no difusión (NBMA) de OSPF***

Una red multiacceso de no difusión (NBMA) de OSPF es cualquier red que tiene varios puntos de acceso (más de dos ruteadores) y que no da soporte a la posibilidad de difusión. El relé de trama y X.25 son generalmente redes NBMA.

Los ruteadores OSPF funcionan en una red NBMA del mismo modo que en una red de difusión, es decir, utilizando el protocolo Hello para formar adyacencias e identificar el ruteador designado (DR). Sin embargo, puesto que los ruteadores no pueden descubrir sus ruteadores contiguos de forma dinámica mediante difusiones, deben especificarse algunos parámetros adicionales.

La unidad TAOS forma adyacencias con otros ruteadores OSPF en una red NBMA. Las adyacencias permiten que la unidad rutee OSPF en redes de relé de trama e interopere con los conmutadores que no dan soporte al modelo serie (punto a punto) en relé de trama.

**Nota:** El parámetro Non-Multicast en los subperfiles OSPF-Options para interfaces IP provoca la conversión del tráfico de difusión múltiple en tráfico dirigido. Este parámetro se utiliza habitualmente con un enlace serie (por ejemplo, una conexión punto a punto en relé de trama) y no está preparado para su utilización con NBMA. Non-Multicast no debe activarse en configuraciones NBMA.

## **Información general de los ajustes de NBMA de OSPF**

A continuación se muestran los parámetros OSPF (con los ajustes predeterminados) relacionados con NBMA:

```
[in IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf]
network-type = Point-to-Point
poll-interval = 0

[in CONNECTION/"":ip-options:ospf-options]
network-type = Point-to-Point
poll-interval = 0

[in OSPF-NBMA-NEIGHBOR/"" (new)]
name* = ""
host-name = ""
ip-address = 0.0.0.0
dr-capable = no
```

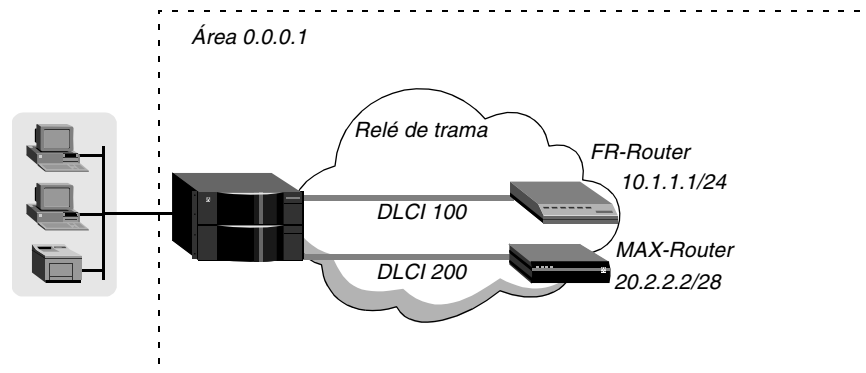
<b>Parámetro</b>	<b>Especifica</b>
Network-Type	Tipo de red con la que se conecta la interfaz: Broadcast, NonBroadcast (multiacceso) o Point-to-Point. Broadcast especifica cualquier red con funciones de difusión, como Ethernet. NonBroadcast (multiacceso) se utiliza para redes que tienen más de dos ruteadores OSPF y que no tienen funciones de difusión, como el relé de trama o X.25. Point-to-Point (el valor predeterminado) se utiliza en interfaces conectadas a otro nodo en el extremo distante.
Poll-Interval	Intervalo, en segundos, en el que se enviarán paquetes Hello a un ruteador contiguo que ha quedado inactivo. El valor predeterminado 0 (cero) significa que no se enviarán paquetes Hello a un ruteador contiguo del que no se hayan recibido paquetes Hello durante el número de segundos que especifica el ajuste Dead-Interval. Si especifica un valor que no sea cero, utilice un valor mayor que el valor predeterminado de Hello-Interval, es decir, de 10 segundos (por ejemplo, 120 segundos).
Name	Nombre del perfil OSPF-NBMA-Neighbor.
Host-Name	Nombre de estación de un perfil Connection local que define la conexión con un ruteador contiguo.
IP-Address	Dirección IP del ruteador contiguo.
DR-Capable	Especifica si el ruteador contiguo puede ser el ruteador designado (DR). Los valores son <i>yes</i> y <i>no</i> (el valor predeterminado).

## **Ejemplo de configuración de NBMA de OSPF**

En una red NBMA, un ruteador con posibilidades de ser el ruteador designado (DR) se configura con una lista de los demás ruteadores OSPF conectados a la red. En el inicio, estos ruteadores se envían paquetes Hello entre ellos para descubrir el DR. El DR empieza a enviar paquetes Hello a toda la lista de ruteadores de la red. Cuando una interfaz NBMA pasa a estar activa en la unidad TAOS, la unidad envía paquetes Hello únicamente a ruteadores contiguos con posibilidades de ser el DR hasta que se le notifica qué ruteador es el DR.

En la Figura 3-8 se muestra una red NBMA de OSPF que utiliza relé de trama. En este ejemplo, se supone que la unidad denominada FR-Router tiene posibilidades de ser el DR y que la unidad MAX-Router no tiene posibilidades de ser el DR.

Figura 3-8. Red multiacceso de no difusión (NBMA) de OSPF



### Ejemplo de configuración de un router contiguo con posibilidades de ser DR

El conjunto de comandos siguiente define un perfil Frame-Relay de ejemplo para la interfaz conectada a FR-Router en la Figura 3-8:

```
admin> new frame-relay fr-dce
FRAME-RELAY/fr-dce read

admin> set active = yes

admin> set link-type = dce

admin> set nailed-up-group = 36

admin> set link-mgmt = ccitt

admin> write
FRAME-RELAY/fr-dce written
```

El conjunto de comandos siguiente define un perfil Connection para la conexión con FR-Router:

```
admin> new conn FR-Router
[in CONNECTION/FR-Router (new)]

admin> set active = yes

admin> set encapsulation-protocol = frame-relay

admin> set ip-options remote-address = 10.1.1.1/24

admin> set ip-options ospf active = yes

admin> set ip-options ospf area = 0.0.0.1

admin> set ip-options ospf network-type = NonBroadcast

admin> set ip-options ospf poll-interval = 60

admin> set telco-options call-type = ft1

admin> set fr-options frame-relay-profile = fr-dce

admin> set fr-options dlci = 100

admin> write
CONNECTION/FR-Router written
```

El conjunto de comandos siguiente activa la unidad TAOS para que forme una adyacencia con FR-Router:

```
admin> new ospf-nbma-neighbor fr-router
[In OSPF-NBMA-NEIGHBOR/fr-router (new)]

admin> set host-name = FR-Router

admin> set ip-address = 10.1.1.1/24

admin> set dr-capable = yes

admin> write
OSPF-NBMA-NEIGHBOR/fr-router written
```

### *Ejemplo de configuración de un ruteador contiguo sin posibilidades de ser un ruteador designado (DR)*

El conjunto de comandos siguiente define un perfil Frame-Relay para operaciones de enlace en la interfaz conectada a la unidad llamada MAX-Router de la Figura 3-8:

```
admin> new frame-relay fr-dte
FRAME-RELAY/fr-dte read

admin> set active = yes

admin> set link-type = dte

admin> set nailed-up-group = 11

admin> set link-mgmt = ccitt

admin> write
FRAME-RELAY/fr-dte written
```

El conjunto de comandos siguiente define un perfil Connection para la conexión con MAX-Router:

```
admin> new conn MAX-Router
[In CONNECTION/MAX-Router (new)]

admin> set active = yes

admin> set encapsulation-protocol = frame-relay

admin> set ip-options remote-address = 20.2.2.2/28

admin> set ip-options ospf active = yes

admin> set ip-options ospf area = 0.0.0.1

admin> set ip-options ospf network-type = NonBroadcast

admin> set ip-options ospf poll-interval = 60

admin> set telco-options call-type = ft1

admin> set fr-options frame-relay-profile = fr-dte

admin> set fr-options dlci = 200

admin> write
CONNECTION/MAX-Router written
```

El conjunto de comandos siguiente activa la unidad TAOS para que forme una adyacencia con FR-Router:

```
admin> new ospf-nbma-neighbor max-router
[In OSPF-NBMA-NEIGHBOR/max-router (new)]
```



```
admin> set host-name = MAX-Router
admin> set ip-address = 20.2.2.2/28
admin> write
OSPF-NBMA-NEIGHBOR/max-router written
```

## ***Desactivación de OSPF***

Para desactivar el protocolo OSPF en toda la unidad, defina el parámetro siguiente (aparece con el valor predeterminado):

```
[in IP-GLOBAL:ospf-global]
enable = yes
```

<b>Parámetro</b>	<b>Especifica</b>
Enable	Activa y desactiva el protocolo OSPF. Los cambios de ajustes entran en vigor inmediatamente una vez grabado el perfil.

Aunque también puede desactivar OSPF manualmente en cada interfaz OSPF, este parámetro proporciona un mecanismo general para desactivar el protocolo. También puede utilizarse para evitar que OSPF se reinicialice varias veces si está modificando un gran número de perfiles relacionados con OSPF. En este caso, establezca el parámetro en `no`, grabe los cambios en OSPF y, a continuación, establezca de nuevo el parámetro en `yes`.



# Protocolo de gestión de túneles de Ascend

Introducción a ATMP . . . . .	4-1
Ajustes de red para ATMP . . . . .	4-2
Configuración de un agente externo. . . . .	4-8
Configuración de agentes locales. . . . .	4-17
Configuración de un agente local y externo. . . . .	4-27
Configuración de IPX sobre ATMP . . . . .	4-31

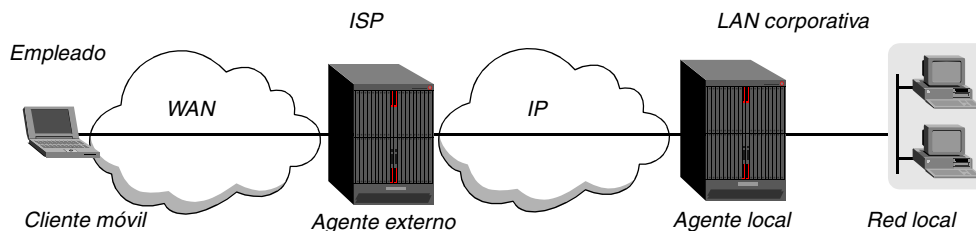
Una Unidad TAOS da soporte a ATMP (Protocolo de gestión de túneles de Ascend) para la conectividad de VPN (Red privada virtual). Si desea obtener información acerca de la utilización de otros protocolos de túneles para la conectividad de VPN, consulte el Capítulo 5, “Túneles L2TP, PPTP e IP en IP”.

## Introducción a ATMP

ATMP es un protocolo basado en UDP/IP para túneles entre dos unidades TAOS en una red IP. Los datos se transportan a través del túnel en GRE (Encapsulación de ruteo genérica), como se describe en el documento RFC 1701. Si desea obtener una descripción completa de ATMP, consulte el documento RFC 2107, K. Hamzeh, *Ascend Tunnel Management Protocol - ATMP*.

En la Figura 4-1 se muestra un ejemplo de utilización de túneles ATMP: los clientes móviles efectúan una llamada de entrada a un ISP local para entrar en una LAN remota a través de Internet. ATMP crea y elimina un túnel a través de Internet entre las dos unidades TAOS. De hecho, el túnel hace que la nube IP parezca haber desaparecido y proporciona la sensación de ser un acceso directo a una red interna.

*Figura 4-1. Túnel ATMP de un ISP a una red interna corporativa*



Un cliente móvil efectúa una llamada de entrada con el agente externo, que autentica el perfil Connection (o el perfil RADIUS) e inicia una conexión IP con el agente local especificado.

El agente externo solicita, a continuación, un túnel para el cliente móvil conectado. El agente local autentica la petición de túnel (por contraseña) y, a continuación, registra el túnel y le asigna un ID. Si el agente local rechaza el túnel, el agente externo desconecta el cliente móvil.

Si el túnel se establece correctamente, el agente local reenvía o rutea los datos enviados por el túnel a la red interna. Si el cliente móvil dispone de una conexión MP+ o MP de varios canales, el túnel permanece activo cuando la conexión agrega o subtrae canales y no se elimina hasta que el canal final de la llamada se desconecta.

El agente local debe poder acceder a la red interna como gateway ATMP o ruteando los paquetes. Si desea obtener una descripción del funcionamiento del agente local como gateway o ruteador, consulte el apartado “Ajustes del perfil ATMP del agente local” en la página 4-17.

## ***Ajustes de red para ATMP***

Los ajustes de red para ATMP son los ajustes relacionados con la conexión IP entre unidades TAOS, los ajustes relacionados con la comunicación UDP necesaria para establecer túneles y los ajustes relacionados con la fragmentación y el reensamblaje de paquetes.

### **Necesidad de reiniciar el sistema**

Cuando se cambia el ajuste del parámetro UDP-Port en el perfil ATMP de un agente local, es necesario reiniciar el sistema para que el subsistema ATMP reconozca el nuevo número de puerto UDP.

Cuando se cambia el parámetro Agent-Mode de su ajuste predeterminado Tunnel-Disabled a otro ajuste, es necesario reiniciar el sistema para que el nuevo valor entre en vigor.

El resto de ajustes de parámetros del perfil ATMP entran en vigor después de que se grabe el perfil.

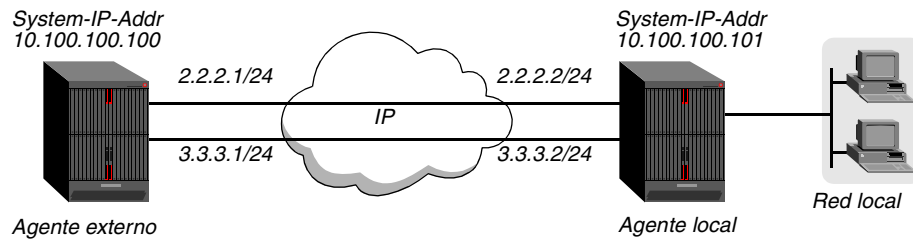
### **Recomendación sobre la dirección IP del sistema**

Es conveniente que establezca el parámetro System-IP-Addr del perfil IP-Global en una Unidad TAOS que funcione como agente ATMP, especialmente si la unidad dispone de varias interfaces con la nube IP que la separa de otros agentes ATMP. Para aplicar esta recomendación deben tenerse en cuenta dos aspectos:

- En un agente externo, el perfil Connection de los clientes móviles debe especificar la dirección IP del sistema de un agente local en lugar de la dirección de interfaz en la que el agente local acepta datos enviados por túnel. Esto ayuda a evitar problemas de comunicación si una ruta cambia en la nube IP.
- Tanto en un agente externo como en un agente local, el enlace con el otro agente puede especificar la dirección IP del sistema de la unidad. Esto no es necesario si RIP está activo en las interfaces entre los dos agentes, pero es aconsejable porque ayuda a simplificar las configuraciones.

En la Figura 4-2 se muestra un agente local y un agente externo, con dos interfaces Ethernet que los conectan (la idea es la misma que si se tratara de dos conexiones WAN entre las unidades).

Figura 4-2. Direcciones IP del sistema y rutas entre agentes ATMP



Cuando RIP está activo en las interfaces IP entre las dos unidades, indica la dirección del sistema en ambos puertos. Por ejemplo, suponga que un agente externo tiene la dirección IP del sistema y la configuración de interfaz IP siguientes:

```
[in IP-GLOBAL]
system-ip-addr = 10.100.100.100

[in IP-INTERFACE { {shelf-1 slot-1 1} 0 } ]
ip-address = 2.2.2.1/24
rip = both-v2

[in IP-INTERFACE { {shelf-1 slot-1 2} 0 } ]
ip-address = 3.3.3.1/24
rip = both-v2
```

y un agente local tiene la dirección IP del sistema y la configuración de interfaz IP siguientes:

```
[in IP-GLOBAL]
system-ip-addr = 10.100.100.101

[in IP-INTERFACE { {shelf-1 slot-7 1} 0 } ]
ip-address = 2.2.2.2/24
rip = both-v2

[in IP-INTERFACE { {shelf-1 slot-7 2} 0 } ]
ip-address = 3.3.3.2/24
rip = both-v2
```

Con esta configuración, el agente externo anuncia, en los dos puertos Ethernet, una ruta a su propia dirección del sistema, 10.100.100.100. Del mismo modo, el agente local indica, en los dos puertos Ethernet, una ruta a su propia dirección del sistema, 10.100.100.101.

Cuando al agente local recibe los anuncios para 10.100.100.100, selecciona uno de los puertos que anuncian la ruta y agrega la ruta a su tabla de ruteo. La próxima vez que el agente local establezca una conexión con el agente externo, utilizará el puerto que indica la tabla de ruteo. Si ese puerto no está disponible (por ejemplo, si el cable está desconectado), el agente local actualiza la tabla de ruteo y utiliza el otro puerto para conectarse con el agente externo.

## Definición del puerto UDP

De manera predeterminada, los agentes ATMP utilizan el puerto UDP 5150 para intercambiar información de control mientras se establece un túnel. Si el perfil ATMP del agente local especifica otro número de puerto UDP, todas las peticiones de túnel hacia ese agente local deben especificar el mismo puerto UDP.

**Nota:** Es necesario reiniciar el sistema para que el subsistema ATMP reconozca el nuevo número de puerto UDP.

## Especificación de límites de reintento de túneles

Los parámetros `Retry-Timeout` y `Retry-Limit` del perfil ATMP funcionan conjuntamente para limitar el número de mensajes `RegisterRequest` (para abrir un túnel) y de mensajes `DeregisterRequest` (para cerrar un túnel) que se envían y los segundos que transcurren entre cada mensaje. Si falla una petición de túnel, el agente externo excede el tiempo de espera, registra un mensaje y desconecta el cliente móvil. Cuando la petición de túnel tiene éxito, el agente local asigna un ID de túnel y el puerto UDP ya no se utiliza para ese túnel. La transferencia real de datos utiliza la conexión IP con GRE.

Los parámetros `Retry-Timeout` y `Retry-Limit` tienen ajustes predeterminados que son adecuados para la mayor parte de los entornos, pero deberá aumentar o disminuir los valores según el tipo de enlace que conecte al agente externo y al agente local. Por ejemplo, si el enlace es una conexión de marcación de salida conmutada, aumente los valores para que haya tiempo suficiente para establecer la conexión. O, si el agente externo y el agente local se encuentran en el mismo segmento de Ethernet, reduzca los valores para proporcionar una respuesta más rápida al cliente móvil cuando el agente local no esté disponible.

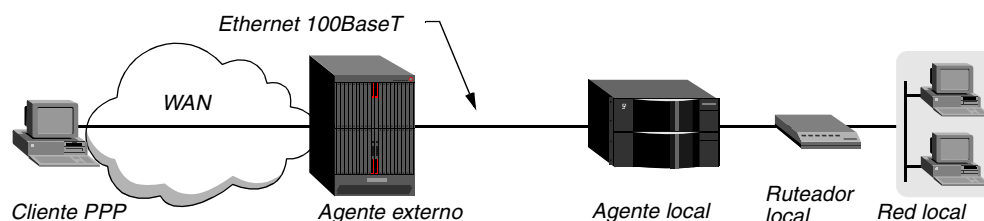
Si aumenta los valores de `Retry-Timeout` y `Retry-Limit`, tenga en cuenta que los valores determinan el tiempo de respuesta para los clientes móviles cuando el agente local no está disponible. Si una petición de túnel llega a un agente local secundario que tampoco está disponible, el cliente móvil espera durante el doble de tiempo que el indicado por el periodo especificado antes de recibir la notificación de que la conexión ha fallado.

## Definición de un límite de MTU

El tipo de enlace que conecta un agente externo y un agente local determina la MTU (Unidad máxima de transmisión). El enlace puede encontrarse en una conexión de marcación de salida conmutada, una conexión de relé de trama o un enlace Ethernet, o puede ser una red local o rutearse a través de varios saltos. Si el enlace entre los dispositivos es de varios saltos (si atraviesa más de un segmento de red), la MTU de ruta es la MTU *mínima* de los segmentos que intervienen.

En la Figura 4-3 se muestra una instalación ATMP en un segmento Ethernet 100BaseT, que limita la MTU de ruta a 1500 bytes.

*Figura 4-3. MTU de ruta en un segmento Ethernet*



Si alguno de los segmentos del enlace entre los agentes tiene una MTU inferior a 1528, se producirá la fragmentación y reensamblaje de algunos paquetes. Puede transferir las tareas de fragmentación y reensamblaje a puntos finales de conexión (un cliente móvil y un dispositivo de la red interna) estableciendo un límite de MTU. A continuación, el software de cliente utiliza mecanismos de descubrimiento de MTU para determinar el tamaño máximo de los paquetes y fragmenta los paquetes antes de enviarlos.

## *Relación entre la MTU y la compresión de enlaces*

La compresión repercute en los paquetes que deben fragmentarse porque los paquetes comprimidos son de menor tamaño que sus equivalentes originales. Si se ha activado algún tipo de compresión (como la compresión de enlaces o cabeceras VJ), la conexión puede transferir paquetes de mayor tamaño sin superar la MRU (Unidad máxima de recepción) de un enlace. Si al comprimir un paquete el tamaño de éste es menor que la MRU, puede enviarse a través de la conexión, mientras que el mismo paquete sin comprimir no puede enviarse.

## *Fragmentación causada por túneles ATMP*

Para transmitir paquetes a través de un túnel ATMP, la Unidad TAOS agrega una cabecera GRE de 8 bytes y una cabecera IP de 20 bytes a las tramas que recibe. La adición de estas cabeceras de paquetes puede hacer que el paquete sea más grande que la MTU del enlace de túnel, en cuyo caso la unidad debe fragmentar el paquete después de encapsularlo o rechazar el paquete.

Fragmentar paquetes después de encapsularlos conlleva varios inconvenientes para el agente externo y para el agente local. Por ejemplo, causa una disminución del rendimiento porque ambos agentes tienen más actividad general de preparación. Significa también que el agente local no puede ser un conmutador GRF (para mantener su elevado rendimiento global, un conmutador GRF no realiza reensamblajes).

## *Transferencia de la tarea de fragmentación a puntos finales de conexión*

Para evitar la actividad general adicional que se genera cuando los agentes ATMP llevan a cabo la fragmentación, puede establecer un enlace entre las dos unidades que tenga una MTU superior a 1528 (lo que significa que no puede incluir segmentos Ethernet) o puede establecer el parámetro MTU-Limit del perfil ATMP en un valor que sea 28 bytes inferior a la MTU de ruta.

Si MTU-Limit se establece en cero (el valor predeterminado), la Unidad TAOS puede que tenga que fragmentar paquetes encapsulados antes de la transmisión. A continuación, el otro agente ATMP debe reensamblar los paquetes.

Si MTU-Limit se establece en un valor que no sea cero, la unidad notifica ese valor como MTU de ruta al software del cliente, lo que hace que el cliente envíe paquetes del tamaño especificado. Esto transfiere la tarea de fragmentación y reensamblaje hacia los puntos finales de conexión, lo que reduce la actividad general de los agentes ATMP.

Por ejemplo, si la Unidad TAOS se está comunicando con otro agente ATMP en un segmento Ethernet, puede establecer el parámetro MTU-Limit en un valor que sea 28 bytes inferior a 1500 bytes, como se muestra en el ejemplo siguiente, a fin de que la unidad envíe paquetes no fragmentados que incluyan la cabecera GRE de 8 bytes y una cabecera IP de 20 bytes:

```
admin> read atmp
ATMP read

admin> set mtu-limit = 1472

admin> write
ATMP written
```

Con este ajuste, el punto final de conexión envía paquetes con un tamaño máximo de 1472 bytes. Cuando la Unidad TAOS los encapsula, agregando 28 bytes al tamaño, los paquetes siguen sin sobrepasar la MTU de 1500 bytes de Ethernet.

## **Cómo forzar la fragmentación para interactuar con clientes anticuados**

Para descubrir la MTU de ruta, algunos clientes normalmente envían paquetes que son de tamaño superior a la MRU negociada y que tienen activado el bit DF (No fragmentar). Estos paquetes se devuelven al cliente con un mensaje ICMP que informa al cliente de que no se puede acceder al host sin realizar la fragmentación. Este funcionamiento previsto y habitual mejora el rendimiento de extremo a extremo al permitir que los puntos finales de conexión lleven a cabo las fragmentaciones y reensamblajes necesarios.

Sin embargo, determinados productos de software de cliente anticuados no manejan este proceso correctamente y siguen enviando paquetes de tamaño mayor al especificado por MTU-Limit. Para que la Unidad TAOS funcione con estos clientes, puede configurarla para que pase por alto el bit DF y realice la fragmentación que normalmente debe llevar a cabo el software del cliente. Esta función se denomina *prefragmentación*.

Cuando el parámetro MTU-Limit está establecido en un valor distinto de cero, puede establecer el parámetro Force-Fragmentation en Yes para que la Unidad TAOS pueda prefragmentar los paquetes que recibe que sean mayores que la MRU negociada y tengan activado el bit DF. La unidad prefragmenta estos paquetes y, a continuación, agrega las cabeceras GRE e IP.

**Nota:** Si el parámetro Force-Fragmentation se establece en Yes, la Unidad TAOS elude el mecanismo de descubrimiento de MTU estándar y fragmenta paquetes de mayor tamaño antes de encapsularlos en GRE. Puesto que esto cambia el funcionamiento previsto, no se recomienda si no es para trabajar con software de cliente anticuado que no maneje la fragmentación de manera adecuada.

## **Clientes móviles con direcciones IP duplicadas**

Un agente externo acepta varias conexiones de clientes móviles con direcciones IP duplicadas siempre que soliciten agentes locales o redes internas diferentes. Este funcionamiento permite que redes privadas independientes utilicen direcciones IP no registradas.

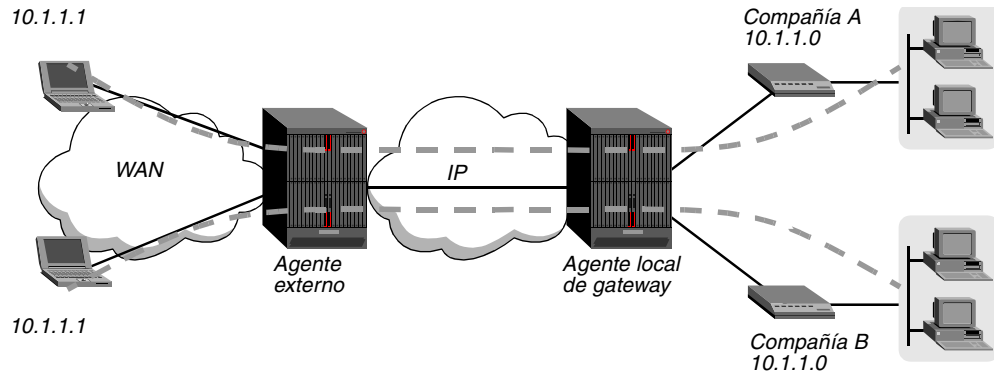
Un agente local no acepta varias conexiones de clientes móviles con la misma red interna y con direcciones IP duplicadas o rangos de subred que se solapan. Si un cliente móvil intenta conectarse con un agente local que dispone de una dirección que duplica o se encuentra en la misma subred de una conexión de cliente móvil ya establecida, el agente local interrumpe de manera inmediata la conexión de cliente *existente*. Este funcionamiento permite que un cliente móvil se vuelva a conectar si su conexión se ha perdido porque no se puede utilizar un agente externo.

### *Aislamiento de la red y direcciones IP duplicadas*

ATMP aísla las redes internas unas de otras, así como de las demás redes IP que haya entre los agentes externos y locales. Por lo tanto, un agente externo puede aceptar varias conexiones de cliente que tengan la misma dirección IP. Por ejemplo, en la Figura 4-4 se muestran dos clientes móviles con el mismo túnel de dirección IP hacia dos redes internas distintas. Las redes internas están aisladas unas de otras, así como de la nube IP que se encuentra entre los puntos finales del túnel.



Figura 4-4. Agente externo que da soporte a direcciones IP de cliente duplicadas



Para proporcionar el aislamiento de la red, el agente externo no crea rutas para los clientes móviles. Del mismo modo, los agentes locales de gateway no crean rutas para conexiones de gateway ATMP ni para clientes móviles registrados (sin embargo, los agentes locales de ruteador *sí* que crean rutas para clientes móviles registrados). El aislamiento de la red también provoca que un cliente móvil o que un ruteador de red interna no reciba una respuesta cuando se intenta realizar una operación ping con un agente externo o un agente local.

### *Direcciones duplicadas que se conectan con la misma red interna*

Si un cliente móvil intenta conectarse con una red interna cuya dirección es un duplicado o se encuentra en la misma subred de una conexión de cliente móvil ya establecida, el agente local interrumpe de manera inmediata la conexión establecida y negocia la petición entrante. Este funcionamiento es necesario para que un cliente móvil pueda volver a conectarse si su conexión se interrumpe cuando un agente externo deja de estar disponible.

Por ejemplo, si un cliente móvil se conecta con una red interna que tiene la siguiente dirección:

10.10.10.10/24

el rango de subred del cliente comprende las direcciones 10.10.10.0 a 10.10.10.255. Si otro cliente móvil intenta conectarse con la siguiente dirección:

10.10.10.199/24

(que ocupa el mismo rango de subred que el primer cliente), el agente local interrumpe la primera conexión y permite que el segundo cliente móvil se conecte.

## Configuración de la conexión de agente a agente

El enlace entre un agente externo y un agente local puede ser cualquier tipo de conexión (conmutada, permanente, de relé de trama, etc.) o un enlace Ethernet. Puede hallarse en una red local o estar ruteado a través de varios saltos. El único requisito es que las dos unidades puedan comunicarse en una red IP.

Por ejemplo, los comandos siguientes de un agente local configuran una conexión IP con un agente externo. En este caso, el agente local utiliza el perfil `atmpfa` para autenticar la conexión telefónica del agente externo.

```
admin> new connection atmpfa
CONNECTION/atmpfa read
```

```
admin> set active = yes
admin> set ppp send-auth = chap-ppp-auth
admin> set ppp send-password = remotepw
admin> set ppp recv-password = localpw
admin> set ip-options remote-address = 1.1.1.1
admin> write
CONNECTION/atmpfa written
```

Si desea obtener información detallada acerca de las conexiones IP, consulte el Capítulo 2, “Ruteo IP”.

**Nota:** Si el agente externo y el agente local residen en la misma Ethernet y utilizan la autenticación RADIUS, debe utilizar servidores RADIUS independientes para que los puntos finales del túnel puedan evitar los bucles de sesión.

## ***Configuración de un agente externo***

Para configurar un agente externo, debe establecer los parámetros del perfil ATMP, configurar un perfil Connection o RADIUS para la conexión con el agente local y configurar perfiles Connection o RADIUS de clientes móviles.

Si desea obtener información acerca de la configuración de una conexión con un agente local, consulte “Configuración de la conexión de agente a agente” en la página 4-7.

### **Ajustes del perfil ATMP del agente externo**

El perfil ATMP contiene los parámetros siguientes (que aparecen con los valores de ejemplo) referentes a la configuración de un agente externo:

```
[in ATMP]
agent-mode = foreign-agent
retry-timeout = 3
retry-limit = 10
mtu-limit = 0
force-fragmentation = no
```

<b>Parámetro</b>	<b>Utilización para la configuración del agente externo</b>
Agent-Mode	Debe especificar Foreign-Agent.
Retry-Timeout	Estos parámetros, juntos, especifican el número de mensajes RegisterRequest y DeregisterRequest que se envían y los segundos que transcurren entre cada mensaje. Los ajustes predeterminados son adecuados para la mayor parte de los entornos. Para obtener información detallada, consulte el apartado “Especificación de límites de reintento de túneles” en la página 4-4.
Retry-Limit	
MTU-Limit	Especifica la MTU de la ruta entre los agentes externos y locales. Para obtener información detallada, consulte el apartado “Definición de un límite de MTU” en la página 4-4.

<b>Parámetro</b>	<b>Utilización para la configuración del agente externo</b>
Force-Fragmentation	Si algún software de cliente anticuado envía paquetes de gran tamaño con el bit DF activado, puede establecer este parámetro de manera que la Unidad TAOS tenga que fragmentar los paquetes de todos modos. Para obtener información detallada, consulte el apartado “Cómo forzar la fragmentación para interactuar con clientes anticuados” en la página 4-6.

## Ajustes de los perfiles mobile-client

Todos los perfiles mobile-client residen en el agente externo del túnel ATMP. Un agente externo puede autenticar un cliente móvil localmente en un perfil Connection o externamente en un perfil RADIUS.

### *Ajustes de los perfiles Connection*

El subperfil Tunnel-Options de un perfil Connection contiene los parámetros siguientes (que aparecen con valores de ejemplo) referentes a una conexión de clientes móviles:

```
[in CONNECTION/mclient-1:tunnel-options]
profile-type = mobile-client
primary-tunnel-server = 2.2.2.2:8877
secondary-tunnel-server = 3.3.3.3:1555
udp-port = 5150
password = tunnel-password
home-network-name = ""
```

<b>Parámetro</b>	<b>Utilización para la configuración de clientes móviles</b>
Profile-Type	Debe especificar Mobile-Client.
Primary-Tunnel-Server	Debe especificar la dirección IP del sistema o el nombre de host de un agente local.
Secondary-Tunnel-Server	Especifica la dirección IP del sistema o el nombre de host de un agente local secundario. Si falla una petición de túnel con el primer agente local, el agente externo lo intenta de nuevo con este host.
UDP-Port	Especifica un puerto UDP para uno de los agentes locales especificados o para ambos. Si la especificación del agente local incluye un número de puerto, ese valor prevalece sobre este parámetro.
Password	Debe especificar la contraseña, si la hay, que se encuentra en el perfil ATMP del agente local (21 caracteres como máximo).
Home-Network-Name	Si el agente local está funcionando en modo de gateway, debe especificar el nombre del perfil de gateway que define la conexión con la red interna.

## *Ajustes de los perfiles RADIUS*

RADIUS utiliza los pares de atributo-valor siguientes para especificar las conexiones de clientes móviles:

<b>Atributo</b>	<b>Valor</b>
Tunnel-Type (64)	Tipo de protocolo utilizado para el túnel. Para garantizar la compatibilidad con versiones posteriores, el atributo Tunneling-Protocol (127), específico de TAOS, se convierte en Tunnel-Type (el valor 4 significa ATMP). Para mantener la compatibilidad con versiones anteriores, la contabilidad de RADIUS sigue generando el atributo Tunneling-Protocol.
Tunnel-Server-Endpoint (67)	Dirección IP del sistema o nombre de host de un agente local. La cadena puede ir seguida de dos puntos y del número de puerto UDP que se utiliza en el agente local ATMP. Para garantizar la compatibilidad con versiones posteriores, el atributo Ascend-Primary-Home-Agent (129), específico de Ascend, se convierte en Tunnel-Server-Endpoint.
Ascend-Secondary-Home-Agent (130)	Dirección IP del sistema o nombre de host de un agente local secundario. Si falla una petición de túnel con el primer agente local, el agente externo lo intenta de nuevo con este host.
Ascend-Home-Agent-UDP-Port (186)	Un puerto UDP para uno de los agentes locales especificados o para ambos. Si la especificación del agente local incluye un número de puerto, ese valor prevalece sobre este parámetro.
Tunnel-Password (69)	Contraseña, si la hay, que se encuentra en el perfil ATMP del agente local, si lo hay (21 caracteres como máximo). Para garantizar la compatibilidad con versiones posteriores, el atributo Home-Agent-Password (184), específico de Ascend, se convierte en Tunnel-Password. Para obtener información detallada, consulte el apartado “Autenticación de túnel” en la página A-34.
Tunnel-Private-Group-ID (81)	Si el agente local está funcionando en modo de gateway, debe utilizar este atributo o el atributo Ascend-Home-Network-Name (185) específico del proveedor para especificar el nombre del perfil de gateway que define la conexión con la red interna.

Cuando está disponible un atributo estándar de RADIUS para los túneles, puede especificar el atributo estándar o el atributo específico de Ascend. Por ejemplo, los perfiles RADIUS siguientes son equivalentes:

```
user1 Password = "pass1"
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Framed-IP-Address = 10.1.1.1,
  Framed-IP-Netmask = 255.255.255.255,
  Tunnel-Type = ATMP,
  Tunnel-Server-Endpoint = "atmp-ha1.example.com",
  Tunnel-Password = "tunnel-password"

user1 Password = "pass1"
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Framed-IP-Address = 10.1.1.1,
```

```
Framed-IP-Netmask = 255.255.255.255,  
Tunneling-Protocol = ATMP  
Ascend-Primary-Home-Agent = "atmp-ha1.example.com",  
Ascend-Home-Agent-Password = "tunnel-password"
```

### *Especificación de direcciones de agentes locales y números de puerto*

Cuando un cliente móvil se conecta con un agente externo, el agente externo envía un mensaje RegisterRequest de ATMP a la dirección IP del agente local primario (si el agente local se ha especificado como un nombre de host, el agente externo efectúa en primer lugar una búsqueda de DNS). Según la configuración de la red, el agente externo puede establecer una conexión telefónica para acceder al agente local.

Si el agente externo no recibe respuesta a su petición, lo intenta de nuevo. El ajuste Retry-Limit del perfil ATMP del agente externo controla el número de intentos.

Si el agente externo sigue sin recibir una respuesta o recibe una respuesta negativa (como la imposibilidad de acceder a la red interna), intenta repetir el procedimiento con la dirección del agente local secundario. Si no se ha especificado ninguna dirección de agente local secundario o si el registro con el agente local secundario también falla, el cliente móvil se desconecta.

Si el perfil ATMP del agente local especifica un número de puerto UDP distinto al predeterminado 5150, puede especificar el número de puerto como parte de la dirección del agente local agregando dos puntos (:) seguidos del número de puerto. Los comandos siguientes especifican la dirección IP del sistema seguida de un número de puerto UDP para un agente local primario y secundario:

```
admin> read connection user1  
CONNECTION/user1 read  
  
admin> set ip-options remote-address = 10.1.1.1/32  
  
admin> set tunnel profile-type = mobile-client  
  
admin> set primary-tunnel-server = 2.2.2.2:8877  
  
admin> set secondary-home-agent = 3.3.3.3:4000  
  
admin> write  
CONNECTION/user1 read
```

O en un perfil RADIUS:

```
user1 Password = "pass1"  
Service-Type = Framed-User,  
Framed-IP-Address = 10.1.1.1,  
Framed-IP-Netmask = 255.255.255.255,  
Tunnel-Type = ATMP,  
Tunnel-Server-Endpoint = "2.2.2.2:8877",  
Ascend-Secondary-Home-Agent = "3.3.3.3",  
Ascend-Home-Agent-UDP-Port = 4000
```

En este caso, el agente externo establece una conexión telefónica con el agente local primario y solicita un túnel en el puerto 8877. Si ese intento falla, establece una conexión telefónica con el agente local secundario y solicita un túnel en el puerto 4000 (si la dirección no especifica un número de puerto, el agente externo utiliza el valor del parámetro UDP-Port del perfil Connection del cliente móvil). Por ejemplo, con los ajustes siguientes:

```
admin> set primary-tunnel-server = 2.2.2.2
admin> set secondary-tunnel-server = ha2.company.com:6789
admin> set udp-port = 8877
```

el agente externo establece una conexión telefónica con el servidor de túnel primario y solicita un túnel en el puerto 8877. Si ese intento falla, establece una conexión telefónica con el servidor de túnel secundario y solicita un túnel en el puerto 6789.

### *Especificación del nombre de la red interna*

Si desea obtener definiciones de los agentes locales de gateway y de ruteador, consulte “Ajustes del perfil ATMP del agente local” en la página 4-17. Si desea crear un túnel de cliente móvil hacia un agente local de *gateway*, debe especificar el nombre del perfil de gateway para la conexión con la red interna. Por ejemplo, para el siguiente perfil de gateway de un agente local:

```
admin> new connection homenet
CONNECTION/homenet read
admin> set active = yes
admin> set tunnel profile-type = gateway-profile
admin> set telco call-type = ft1
admin> set telco nailed-groups = 7
admin> write
CONNECTION/homenet written
```

el perfil del cliente móvil especificaría el nombre de red interna siguiente:

```
admin> set home-network-name = homenet
```

o incluiría uno de los ajustes siguientes en un perfil RADIUS:

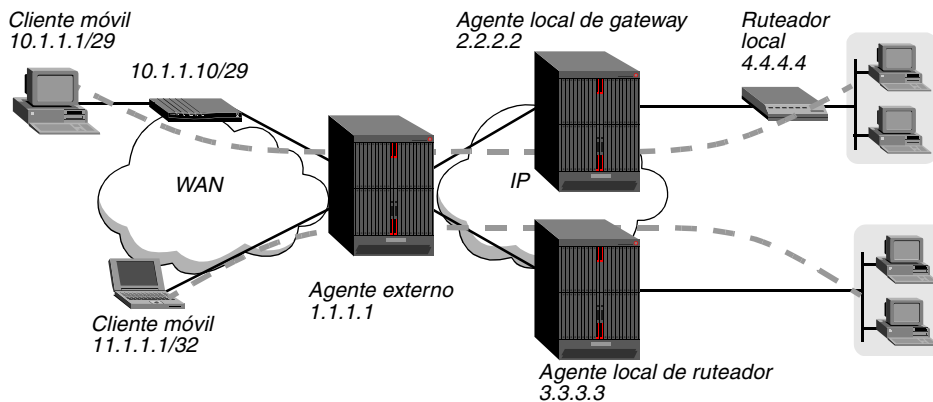
```
Tunnel-Private-Group-ID = "homenet"
Ascend-Home-Network-Name = "homenet"
```

**Nota:** Si el cliente móvil dispone de un túnel con el agente local de *ruteador*, debe dejar en blanco, en los perfiles mobile-client, el parámetro Home-Network u omitir los atributos Tunnel-Private-Group-ID o Ascend-Home-Network-Name.

## **Ejemplo de una configuración de agente externo**

En la Figura 4-5 se muestra un agente externo que se conecta con dos agentes locales a través de conexiones WAN de IP. Uno es un agente local de gateway y el otro es un agente local de ruteador. En la ilustración también se muestran dos conexiones de cliente móvil, una para cada uno de los agentes locales.

Figura 4-5. Túnel de agente externo con dos agentes locales



En este ejemplo, las conexiones de WAN son conexiones PPP de varios canales, que habitualmente negocian una MTU de ruta de 1500 bytes. Los agentes establecen MTU-Limit en 1472 para que los puntos finales de conexión puedan fragmentar paquetes de ese tamaño. Si desea obtener información al respecto, consulte el apartado “Definición de un límite de MTU” en la página 4-4.

### Definición de la dirección del sistema del agente externo

Los comandos siguientes establecen la dirección IP del sistema del agente externo:

```
admin> read ip-global
IP-GLOBAL read
admin> set system-ip-addr = 1.1.1.1
admin> write
IP-GLOBAL written
```

### Configuración del perfil ATMP del agente externo

Los comandos siguientes configuran un perfil ATMP mínimo:

```
admin> read atmp
ATMP read
admin> set agent-mode = foreign-agent
admin> set mtu-limit = 1472
admin> write
ATMP written
admin> reset
```

**Nota:** Cuando cambie el parámetro Agent-Mode de su ajuste predeterminado Tunnel-Disabled a otro ajuste, deberá reiniciar el sistema para que el nuevo valor entre en vigor.

### Configuración de una conexión con un agente local de gateway

En este ejemplo, el agente local de gateway tiene el ajuste de System-IP-Addr siguiente:

```
[in IP-GLOBAL]
system-ip-addr = 2.2.2.2
```

Los comandos siguientes configuran un perfil Connection con el agente local de gateway:

```
admin> read conn hagateway
CONNECTION/hagateway read
admin> set active = yes
admin> set dial-number = 9-1-333-555-1212
admin> set ppp send-auth = chap-ppp-auth
admin> set ppp send-password = remotepw
admin> set ip-options remote = 2.2.2.2
admin> write
CONNECTION/hagateway written
```

A continuación se muestran los perfiles RADIUS equivalentes:

```
route-taos-1 Password = "ascend", Service-Type = Dialout-Framed-User
  Framed-Route = "2.0.0.0 2.2.2.2 1 n hagateway-out"
hagateway-out Password = "ascend", Service-Type = Dialout-Framed-User
  User-Name = "hagateway",
  Framed-Protocol = MPP,
  Ascend-Route-IP = Route-IP-Yes,
  Framed-IP-Address = 2.2.2.2,
  Ascend-Dial-Number = "9-1-333-555-1212",
  Ascend-Send-Auth = Send-Auth-CHAP,
  Ascend-Send-Password = "remotepw"
```

### *Configuración de una conexión con el agente local de ruteador*

En este ejemplo, el agente local de ruteador tiene el ajuste de System-IP-Addr siguiente:

```
[in IP-GLOBAL]
system-ip-addr = 3.3.3.3
```

Los comandos siguientes configuran un perfil Connection para la conexión con un agente local de ruteador:

```
admin> read connection harouter
CONNECTION/harouter read
admin> set active = yes
admin> set dial-number = 9-1-888-555-1234
admin> set ppp send-auth = chap-ppp-auth
admin> set ppp send-password = remotepw
admin> set ip-options remote = 3.3.3.3
admin> write
CONNECTION/harouter written
```

A continuación se muestran los perfiles RADIUS equivalentes:

```
route-taos-1 Password = "ascend", Service-Type = Dialout-Framed-User
  Framed-Route = "3.0.0.0 3.3.3.3 1 n harouter-out"
harouter-out Password = "ascend", Service-Type = Dialout-Framed-User
  User-Name = "harouter",
  Framed-Protocol = MPP,
```



```
Ascend-Route-IP = Route-IP-Yes,  
Framed-IP-Address = 3.3.3.3,  
Ascend-Dial-Number = "9-1-888-555-1234",  
Ascend-Send-Auth = Send-Auth-CHAP,  
Ascend-Send-Password = "remotepw"
```

### *Configuración de una conexión de cliente móvil con el agente local de gateway*

En este ejemplo, el agente local de gateway dispone de un perfil permanente denominado Home-Router para la conexión con la red interna. Tiene además los ajustes siguientes en el perfil ATMP:

```
[in ATMP]  
agent-mode = home-agent  
agent-type = gateway-home-agent  
udp-port = 1555  
password = tunnel-password
```

El grupo de comandos siguiente, introducido en el agente externo, configura una conexión de cliente móvil con el agente local de gateway:

```
admin> read connection mobile-client-1  
CONNECTION/mobile-client-1 read  
  
admin> set active = yes  
  
admin> set ppp recv-password = my-password  
  
admin> set ip-options remote-address= 10.1.1.1/29  
  
admin> set tunnel profile-type = mobile-client  
  
admin> set tunnel primary-tunnel-server = 2.2.2.2:1555  
  
admin> set tunnel password = tunnel-password  
  
admin> set tunnel home-network-name = home-router  
  
admin> write  
CONNECTION/mobile-client-1 written
```

A continuación se muestra un perfil RADIUS equivalente:

```
mobile-client-1 Password = "my-password"  
Service-Type = Framed-User,  
Framed-Protocol = MPP,  
Ascend-IP-Route = Route-IP-Yes,  
Framed-IP-Address = 10.1.1.1,  
Framed-IP-Netmask = 255.255.255.248,  
Tunnel-Type = ATMP,  
Tunnel-Server-Endpoint = "2.2.2.2:1555",  
Tunnel-Password = "tunnel-password"  
Tunnel-Private-Group-ID = "home-router"
```

### *Configuración de una conexión de cliente móvil con el agente local de ruteador*

En este ejemplo, el agente local de ruteador tiene los ajustes siguientes en el perfil ATMP:

```
[in ATMP]  
agent-mode = home-agent  
agent-type = router-home-agent
```

```
udp-port = 8877
password = tunnel-password
```

El grupo de comandos siguiente, introducido en el agente externo, configura una conexión de cliente móvil con el agente local de ruteador:

```
admin> read connection mobile-client-2
CONNECTION/mobile-client-2 read

admin> set active = yes

admin> set ppp recv-password = my-password

admin> set ip-options remote-address= 11.1.1.1/32

admin> set tunnel profile-type = mobile-client

admin> set tunnel primary-tunnel-server = 3.3.3.3:8877

admin> set tunnel password = tunnel-password

admin> write
CONNECTION/mobile-client-2 written
```

A continuación se muestra un perfil RADIUS equivalente:

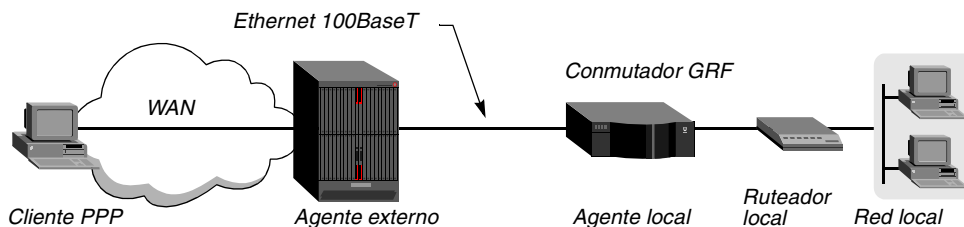
```
mobile-client-2 Password = "my-password", Service-Type= Framed-User
  Framed-Protocol = MPP,
  Ascend-IP-Route = Route-IP-Yes,
  Framed-IP-Address = 11.1.1.1,
  Framed-IP-Netmask = 255.255.255.255,
  Tunnel-Type = ATMP,
  Tunnel-Server-Endpoint = "3.3.3.3:8877",
  Tunnel-Password = "tunnel-password"
```

## **Ejemplo de un agente externo que dispone de un túnel con un conmutador GRF**

Cuando una Unidad TAOS funciona como un túnel de agente externo con un agente local de conmutador GRF, establecer el parámetro MTU-Limit es, más que recomendable, necesario. Para mantener su elevado rendimiento, el GRF no realiza reensamblajes de paquetes. Si no se especifica un valor de MTU-Limit y un cliente móvil envía un paquete de gran tamaño, el agente externo puede verse obligado a fragmentar el paquete antes de enviarlo al agente local. El agente local de conmutador GRF elimina estos paquetes.

En la Figura 4-6 se muestra un túnel de agente externo con un agente local GRF a través de un segmento Ethernet 100BaseT.

*Figura 4-6. Túnel de agente externo con un conmutador GRF*



Los comandos siguientes configuran el perfil ATMP del agente externo para la Unidad TAOS de la Figura 4-6:

```
admin> read atmp
ATMP read

admin> set agent-mode = foreign-agent

admin> set mtu-limit = 1472

admin> write
ATMP written
```

**Nota:** La configuración ATMP del conmutador GRF debe especificar el mismo valor de MTU-Limit.

## Configuración de agentes locales

Para configurar un agente local ATMP, debe establecer parámetros en el perfil ATMP, configurar una conexión IP con el agente externo y configurar la conexión con la red interna.

Si desea obtener información acerca de la configuración de una conexión con el agente externo, consulte “Configuración de la conexión de agente a agente” en la página 4-7.

### Ajustes del perfil ATMP del agente local

El perfil ATMP contiene los parámetros siguientes (que aparecen con valores de ejemplo) referentes a un agente local:

```
[in ATMP]
agent-mode = home-agent
agent-type = gateway-home-agent
udp-port = 5150
password = tunnel-password
retry-timeout = 3
retry-limit = 10
idle-timer = 30
mtu-limit = 0
force-fragmentation = no
```

Parámetro	Utilización para la configuración del agente local
Agent-Mode	Debe especificar Home-Agent.
Agent-Type	Especifica Gateway-Home-Agent (el valor predeterminado) o Router-Home-Agent, según el modo en que el agente local acceda a la red interna.
UDP-Port	Especifica el puerto UDP que los agentes externos deben utilizar para establecer los túneles con el agente local, como se describe en “Definición del puerto UDP” en la página 4-3.
Password	Especifica la contraseña que los agentes externos deben proporcionar para establecer un túnel con esta unidad. Puede especificar hasta 21 caracteres.

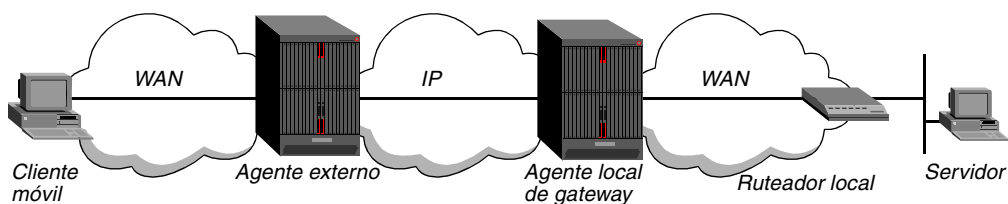
Parámetro	Utilización para la configuración del agente local
Retry-Timeout Retry-Limit	Estos parámetros, juntos, especifican el número de mensajes RegisterRequest y DeregisterRequest que se envían y los segundos que transcurren entre cada mensaje. Los ajustes predeterminados son adecuados para la mayor parte de los entornos, como se describe en “Especificación de límites de reintento de túneles” en la página 4-4.
Idle-Timer	Especifica los minutos durante los que el agente local mantiene un túnel inactivo antes de desconectarlo.
MTU-Limit	Especifica la MTU de la ruta entre los agentes externo y local, como se describe en “Definición de un límite de MTU” en la página 4-4.
Force-Fragmentation	Activa y desactiva la prefragmentación de paquetes que tienen activado el bit DF, como se describe en “Cómo forzar la fragmentación para interactuar con clientes anticuados” en la página 4-6.

### *Especificación de un agente local de gateway*

Un agente local de gateway entrega datos enviados por túnel a la red interna sin ruteo. Un agente local de gateway no puede ejecutar Ping ni tampoco comunicarse con el ruteador local (la misma restricción es aplicable en la dirección opuesta).

Cuando el agente local de gateway recibe datos enviados por túnel, quita la cabecera GRE y reenvía los paquetes al ruteador local, como se muestra en la Figura 4-7.

*Figura 4-7. Funcionamiento de un agente local de gateway*



El enlace con la red interna no puede ser una conexión de marcación de salida conmutada habitual porque el agente local no establecerá la conexión telefónica cuando reciba los datos enviados por el túnel. Si la conexión de gateway está desactivada cuando el agente local recibe una petición de túnel, rechaza la petición. Si desea obtener información detallada acerca de la conexión de gateway con la red interna, consulte “Ajustes del perfil de gateway de la red interna” en la página 4-20.

A continuación se muestra un ejemplo de especificación de un agente local de gateway:

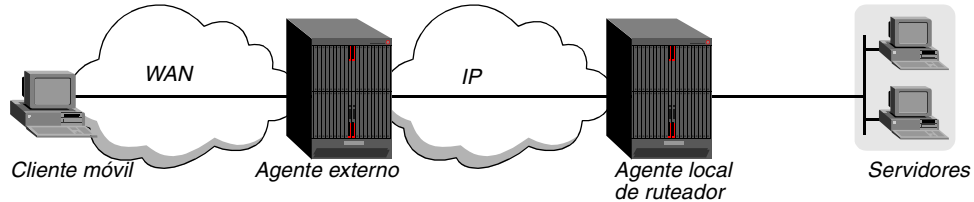
```
admin> read atmp
ATMP read
admin> set agent-mode = home-agent
admin> set agent-type = gateway-home-agent
admin> write
ATMP written
admin> reset
```

**Nota:** Cuando cambie el parámetro Agent-Mode de su ajuste predeterminado Tunnel-Disabled a otro ajuste, deberá reiniciar el sistema para que el nuevo valor entre en vigor.

## Especificación de un agente local de ruteador

Un agente local de ruteador utiliza el ruteo de paquetes para acceder a la red interna.

Figura 4-8. Funcionamiento de un agente local de ruteador



Cuando el agente local de ruteador recibe datos enviados por túnel, quita la encapsulación GRE, pasa los paquetes a su software de ruteador y agrega una ruta al cliente móvil. Si el cliente móvil es un cliente PPP, agrega una ruta de host. Si el cliente móvil es un ruteador, por ejemplo una unidad Pipeline, agrega una ruta normal a las direcciones de subred asignadas a ese ruteador.

A continuación se muestra un ejemplo de especificación de un agente local de ruteador:

```
admin> read atmp
ATMP read

admin> set agent-mode = home-agent
admin> set agent-type = router-home-agent

admin> write
ATMP written

admin> reset
```

**Nota:** Cuando cambie el parámetro Agent-Mode de su ajuste predeterminado Tunnel-Disabled a otro ajuste, deberá reiniciar el sistema para que el nuevo valor entre en vigor.

## Especificación de la contraseña de túnel

El agente local normalmente solicita una contraseña antes de establecer un túnel. El agente externo devuelve una versión cifrada de la contraseña contenida en el perfil mobile-client. Para obtener información detallada, consulte el apartado “Autenticación de túnel” en la página A-34.

## Definición de un temporizador de inactividad para túneles que no se utilizan

Cuando un cliente móvil se desconecta con normalidad, el agente externo envía una petición al agente local para que cierre el túnel. Sin embargo, cuando un agente externo se reinicia, los túneles que se han establecido con un agente local no se eliminan normalmente porque no se notifica al agente local que los clientes móviles ya no están conectados. Los túneles que no se utilizan continúan ocupando memoria del agente local. Para que el agente local pueda reclamar la memoria que ocupan los túneles no utilizados, ahora puede establecer un temporizador de inactividad en un agente local cambiando el valor predeterminado del parámetro siguiente:

```
[in ATMP]
idle-timer = 0
```

El temporizador de inactividad sólo se ejecuta en el agente local. Su valor especifica los minutos (de 1 a 65.535) que el agente local permite que un túnel esté inactivo antes de

desconectarlo. Un valor de 0 desactiva el temporizador, lo que significa que los túneles inactivos permanecen conectados siempre. Este ajuste sólo afecta a los túneles creados después de establecer el temporizador. Los túneles que existían antes de que el temporizador se estableciera no se ven afectados por ello.

## Ajustes del perfil de gateway de la red interna

Cuando un agente local de gateway recibe un mensaje RegisterRequest de túnel del agente externo, comprueba el estado de la conexión con la red interna. Si la conexión está desactivada, el agente local rechaza la petición de túnel y no intenta establecer una conexión telefónica. Si la conexión se desactiva después de que se establezca un túnel, todos los clientes móviles que la estaban utilizando se desconectan.

La conexión de gateway con la red interna puede ser una conexión permanente o una conexión conmutada de marcación de entrada normal. Si se utiliza una conexión de entrada del router local, el administrador de la red interna puede regular cuándo los clientes móviles pueden acceder a la red. Por ejemplo, el administrador de la red interna puede configurar un router de acceso para que establezca una conexión telefónica con el agente local cada día de la semana a las 8:00 AM y para que se desconecte a las 5:00 PM, con lo que se limita a esas horas el acceso de los clientes móviles. En ese caso, la conexión de gateway debe estar activa antes de que los clientes móviles establezcan una conexión telefónica o, si no, sus peticiones de túnel fallarán.

Para configurar un perfil de gateway, establezca una conexión permanente o de llamada de entrada y especifique los parámetros siguientes (que aparecen con ajustes de ejemplo) en el perfil Connection:

```
[in CONNECTION/gwprofile]
station* = gwprofile

[in CONNECTION/gwprofile:tunnel-options]
profile-type = gateway-profile
max-tunnels = 0
atmp-ha-rip = rip-send-v2
```

Parámetro	Utilización para la configuración del perfil de gateway
Station	Especifica el nombre del router local. El valor Home-Network-Name especificado en el perfil mobile-client del agente externo debe especificar el mismo nombre.
Profile-Type	Debe especificar Gateway-Profile.
Max-Tunnels	Especifica el número máximo de clientes móviles que pueden utilizar la conexión al mismo tiempo para acceder a la red interna a través del túnel. El valor predeterminado 0 no establece límite alguno.
ATMP-HA-RIP	Activa y desactiva la construcción de rutas de clientes móviles en respuestas RIP-v2 al router local. Este parámetro no es aplicable a menos que Profile-Type se establezca en Gateway-Profile. El parámetro funciona independientemente del parámetro RIP del subperfil IP-Options. En el caso de perfiles de gateway, el parámetro IP-Options RIP debe ser Off.

### *Limitación del número máximo de túneles*

Si decide limitar el número máximo de túneles a los que puede dar soporte un gateway, debe tener en cuenta el tráfico previsto para cada conexión de cliente móvil, el ancho de banda de la conexión con la red interna y la disponibilidad de los agentes locales alternativos (si los hay). Por ejemplo, cuanto menor sea la cantidad de tráfico generada por cada conexión de cliente móvil, más túneles podrá manejar una conexión de gateway.

### *Activación de RIP en la interfaz con el ruteador local*

El parámetro ATMP-HA-RIP activa al agente local de gateway para que informe al ruteador local sobre las rutas hacia sus clientes móviles. Con esto se elimina la necesidad de que el ruteador local mantenga una ruta estática para cada cliente móvil ATMP. También proporciona la base para una configuración flexible en la que un agente local secundario puede relevar al agente local primario si éste no está disponible.

#### *Notificación al ruteador local de las rutas hacia los clientes móviles*

El ruteador del extremo distante de la conexión definido por el perfil de gateway debe poder rutear de vuelta hacia los clientes móviles. El modo más sencillo de realizarlo es estableciendo el parámetro ATMP-HA-RIP en RIP-Send-v2. Con este ajuste, el agente local de gateway construye un paquete RIP-v2 Response(2) en cada intervalo RIP y lo envía a la red interna desde todos los túneles que utilizan el perfil de gateway. Para cada túnel, el paquete de respuesta contiene la dirección IP del cliente móvil, la máscara de subred, un salto siguiente de 0.0.0.0 y una métrica de 1. No se da soporte a la autenticación RIP-v2 ni a etiquetas de ruta.

Los comandos siguientes activan ATMP-HA-RIP en el perfil de gateway para la conexión con el ruteador local:

```
admin> new connection home-router
CONNECTION/home-router read

admin> set tunnel profile-type = gateway-profile
admin> set tunnel atmp-ha-rip = rip-send-v2
admin> write
CONNECTION/home-router written
```

**Nota:** El agente local no inspeccionará las actualizaciones RIP procedentes de la red interna, independientemente del ajuste de RIP del subperfil IP-Options. Si el agente local recibe actualizaciones RIP de la red interna, reenvía los paquetes de actualizaciones a los clientes móviles, como enviaría cualquier otro tipo de paquete.

#### *La alternativa: mantenimiento de rutas estáticas en el ruteador local*

Si en el perfil de gateway *no* se establece ATMP-HA-RIP en RIP-Send-v2, el administrador de la red interna debe configurar una ruta estática hacia cada cliente móvil. Una ruta estática hacia un cliente móvil puede ser específica del cliente, en cuyo caso el destino de la ruta es la dirección IP del cliente móvil y el ruteador del siguiente salto es la dirección del agente local. Por ejemplo, en la ruta siguiente el cliente móvil es un ruteador (no es una ruta de host) y la dirección del agente local es 2.2.2.2:

```
[in IP-ROUTE/mobile-client]
destination = 10.1.1.10/29
gateway = 2.2.2.2
```

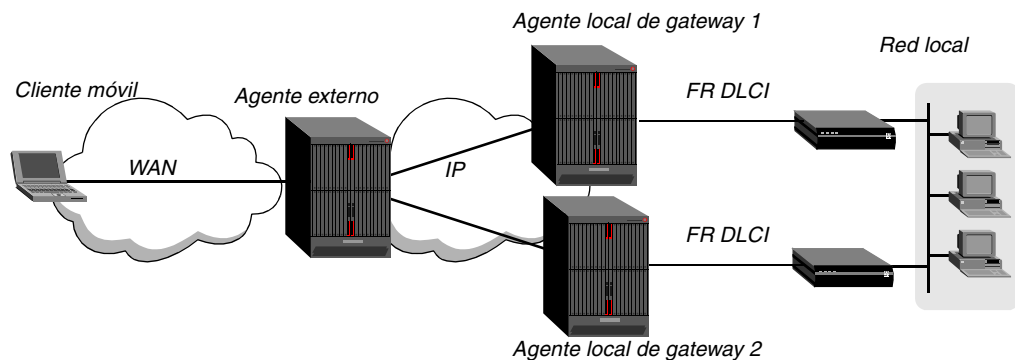
O bien, si los clientes móviles tienen direcciones asignadas del mismo bloque de direcciones (incluidas las direcciones de clientes móviles de ruteador con máscaras de subred de menos de 32 bits) y no hay asignadas direcciones de ese bloque a otros hosts, el administrador de la red interna puede especificar una ruta estática individual que comprenda todos los clientes móviles que utilizan el mismo agente local. Por ejemplo, en la ruta siguiente se asignan direcciones del bloque 10.4.n.n a todos los clientes móviles (y no se asignan direcciones de ese bloque a ningún otro host) y la dirección del agente local es 2.2.2.2:

```
[in IP-ROUTE/mobile-clients]
destination = 10.4.0.0/16
gateway = 2.2.2.2
```

### *Ruteo en una instalación tolerante a errores*

Una instalación ATMP tolerante a errores da soporte a varias rutas ATMP hacia la misma red interna, proporcionando poder de recuperación en caso de que se produzca un fallo en los agentes locales o en el enlace entre el agente local y el ruteador local. Los dos agentes locales pueden conectarse a dos ruteadores locales, como se muestra en la Figura 4-9, o los agentes locales pueden conectarse al mismo ruteador local.

*Figura 4-9. Instalación ATMP tolerante a errores*



Los clientes móviles acceden a la red interna a través de uno de los agentes locales, que no es siempre el mismo. Por lo tanto, una ruta estática mantenida por el ruteador local no permitiría que hosts de la red interna devolvieran de manera fiable paquetes a los clientes móviles. El parámetro ATMP-HA-RIP resuelve los problemas de ruteo que pueden producirse en una configuración tolerante a errores.

En el ejemplo siguiente se muestra un perfil de gateway que puede residir en los dos agentes locales que se muestran en la Figura 4-9:

```
admin> new connection home-router
CONNECTION/home-router read

admin> set active = yes

admin> set tunnel profile-type = gateway-profile

admin> set tunnel max-tunnels = 120

admin> set tunnel atmp-ha-rip = rip-send-v2

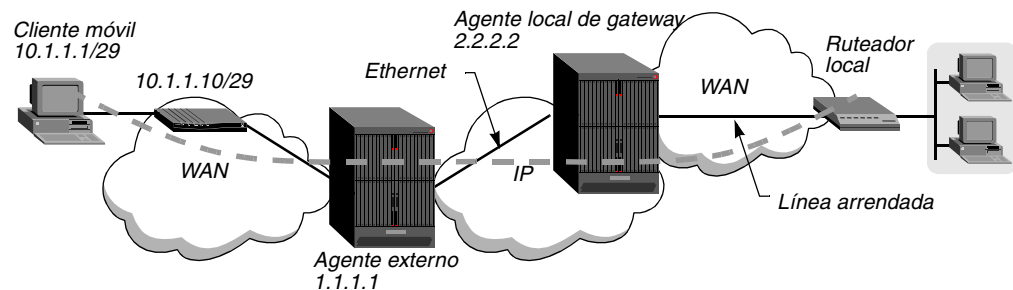
admin> write
CONNECTION/home-router written
```



## Ejemplo de una configuración de agente local de gateway

En la Figura 4-10 se muestra un agente local de gateway con una conexión T1 fraccionada con la red interna. Si desea obtener información detallada acerca de la T1 fraccionada, consulte la publicación *Guía de configuración de la interfaz física de APX 8000/MAX TNT/DSL/TNT*.

Figura 4-10. Agente local de gateway con línea arrendada hacia la red interna



**Nota:** En este ejemplo, el agente externo y el agente local ATMP se encuentran en el mismo segmento de Ethernet, por lo que no se necesitan perfiles Connection para la comunicación.

### Definición de la dirección del sistema del agente local

Los comandos siguientes establecen la dirección IP del sistema del agente local:

```
admin> read ip-global
IP-GLOBAL read

admin> set system-ip-addr = 2.2.2.2

admin> write
IP-GLOBAL written
```

### Configuración del perfil ATMP del agente local

Los comandos siguientes configuran el perfil ATMP del agente local con el ajuste predeterminado Gateway-Home-Agent para el parámetro Agent-Type.

```
admin> read atmp
ATMP read

admin> set agent-mode = home-agent
admin> set udp-port = 1234
admin> set password = tunnel-password
admin> set idle-timer = 30
admin> set mtu-limit = 1472

admin> write
ATMP written

admin> reset
```

**Nota:** Cuando cambie el parámetro Agent-Mode de su ajuste predeterminado Tunnel-Disabled a otro ajuste, deberá reiniciar el sistema para que el nuevo valor entre en vigor.

El agente externo tiene un perfil ATMP como el siguiente:

```
[in ATMP]
agent-mode = foreign-agent
agent-type = gateway-home-agent
udp-port = 5150
password = ""
retry-timeout = 3
retry-limit = 10
idle-timer = 0
mtu-limit = 1472
force-fragmentation = no
```

### *Configuración de un perfil de gateway para la conexión con la red interna*

En el conjunto de comandos siguiente, que configura la interfaz con la red interna, Call-Type se ha establecido en FT1 (permanente) y se asigna un grupo de canales permanentes (número de grupo 7) al enlace. ATMP-HA-RIP se activa en la interfaz.

```
admin> new connection home-router
CONNECTION/home-router read
admin> set active = yes
admin> set tunnel profile-type = gateway-profile
admin> set tunnel atmp-ha-rip = rip-send-v2
admin> set telco call-type = ft1
admin> set telco nailed-groups = 7
admin> write
CONNECTION/home-router written
```

### *Configuración de una conexión de cliente móvil con el agente local de gateway*

Las conexiones de clientes móviles del agente externo necesitarán una configuración de túneles como la siguiente en un perfil Connection:

```
[in CONNECTION/mclient:tunnel-options]
profile-type = mobile-client
primary-tunnel-server = 2.2.2.2:1234
password = tunnel-password
home-network-name = home-router
```

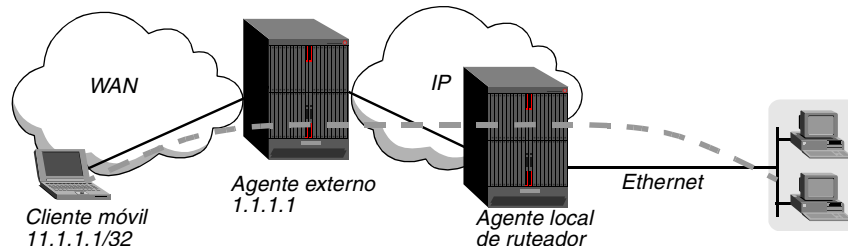
A continuación se muestran los ajustes equivalentes en un perfil RADIUS:

```
mclient Password = "local-password"
Service-Type = Framed-User,
Tunnel-Type = ATMP,
Tunnel-Server-Endpoint = "2.2.2.2:1234",
Tunnel-Password = "tunnel-password",
Tunnel-Private-Group-ID = "home-router"
```

## Ejemplo de una configuración de agente local de ruteador

En la Figura 4-11 se muestra un agente local de ruteador con una conexión Ethernet con la red interna. El agente local y el agente externo ATMP se conectan a través de un enlace PPP de varios canales.

Figura 4-11. Agente local de ruteador en la red interna



Si desea obtener información acerca de la configuración de una conexión con un agente externo, consulte “Configuración de la conexión de agente a agente” en la página 4-7.

### Definición de la dirección del sistema del agente local

Los comandos siguientes establecen la dirección IP del sistema del agente local de ruteador:

```
admin> read ip-global
IP-GLOBAL read

admin> set system-ip-addr = 3.3.3.3

admin> write
IP-GLOBAL written
```

### Configuración del perfil IP-Interface para la conexión con la red interna

Si activa RIP en la interfaz que conduce a la red interna, otros hosts y redes pueden rutear hacia el cliente móvil. La activación de RIP es especialmente útil si la red interna se encuentra a uno o más saltos de distancia. Si RIP está desactivado, los ruteadores implicados necesitan rutas estáticas que especifiquen el agente local como ruta hacia los clientes móviles. También puede activar el protocolo ARP de proxy para que los hosts locales lo utilicen con los clientes móviles. Por ejemplo:

```
admin> read ip-interface {{1 10 1}0}
IP-INTERFACE/{ { 1 10 1 } 0 } read

admin> set ip-address = 3.3.3.3

admin> set proxy-mode = always

admin> set rip-mode = routing-send-and-recv-v2

admin> write
IP-INTERFACE/{ { 1 10 1 } 0 }written
```

### *Configuración del perfil ATMP del agente local*

Los comandos siguientes configuran el perfil ATMP del agente local:

```
admin> read atmp
ATMP read

admin> set agent-mode = home-agent
admin> set agent-type = router
admin> set password = tunnel-password
admin> set idle-timer = 30
admin> set mtu-limit = 1472

admin> write
ATMP written

admin> reset
```

**Nota:** Cuando cambie el parámetro Agent-Mode de su ajuste predeterminado Tunnel-Disabled a otro ajuste, deberá reiniciar el sistema para que el nuevo valor entre en vigor.

El agente externo tiene un perfil ATMP como el siguiente:

```
[in ATMP]
agent-mode = foreign-agent
agent-type = gateway-home-agent
udp-port = 5150
password = ""
retry-timeout = 3
retry-limit = 10
idle-timer = 0
mtu-limit = 1472
force-fragmentation = no
```

### *Configuración de una conexión de cliente móvil con el agente local de ruteador*

Las conexiones de clientes móviles del agente externo necesitarán una configuración de túneles como la siguiente en un perfil Connection:

```
[in CONNECTION/mclient:tunnel-options]
profile-type = mobile-client
primary-tunnel-server = 3.3.3.3
password = tunnel-password
```

A continuación se muestran los ajustes de túneles equivalentes en un perfil RADIUS:

```
mclient Password = "local-password"
Service-Type = Framed-User,
Tunnel-Type = ATMP,
Tunnel-Server-Endpoint = "3.3.3.3",
Tunnel-Password = "tunnel-password"
```

## Configuración de un agente local y externo

En algunas configuraciones, una Unidad TAOS actúa como agente local para algunos clientes móviles y como agente externo para otros clientes móviles. Las dos configuraciones funcionan paralelamente sin conflictos, siempre que se cumplan todos los requisitos para cada tipo de configuración.

### Configuración del perfil ATMP

El perfil ATMP contiene los siguientes parámetros (que aparecen con valores de ejemplo) referentes a la configuración de un agente local y externo:

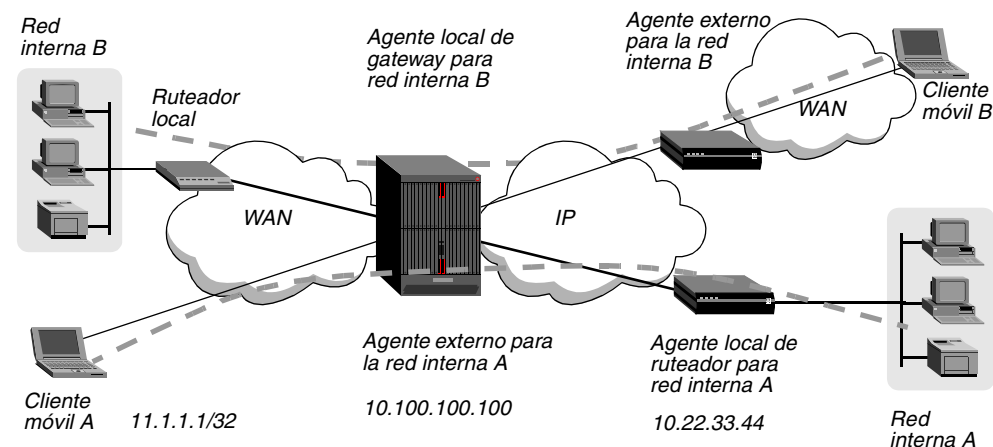
```
[in ATMP]
agent-mode = home-and-foreign-agent
agent-type = gateway-home-agent
udp-port = 5150
password = tunnel-password
retry-timeout = 3
retry-limit = 10
idle-timer = 0
mtu-limit = 1472
force-fragmentation = no
```

El parámetro Agent-Mode debe especificar Home-and-Foreign-Agent. Si desea obtener información detallada acerca de todos los demás ajustes, consulte “Configuración de agentes locales” en la página 4-17 o “Configuración de un agente externo” en la página 4-8.

### Ejemplo de una configuración de agente local y externo

En la Figura 4-12 se muestra una Unidad TAOS que funciona como agente local para la red interna B y como agente externo para los clientes móviles que establecen un túnel con la red interna A.

Figura 4-12. Unidad TAOS actuando como agente local y agente externo



Si desea obtener información acerca de la configuración de conexiones entre agentes locales y agentes externos, consulte “Configuración de la conexión de agente a agente” en la página 4-7.

### *Definición de la dirección del sistema*

Los comandos siguientes establecen la dirección IP del sistema del agente local y externo:

```
admin> read ip-global
IP-GLOBAL read

admin> set system-ip-addr = 10.100.100.100

admin> write
IP-GLOBAL written
```

### *Configuración del perfil ATMP para un agente local y externo*

El conjunto de comandos siguiente configura el perfil ATMP:

```
admin> read atmp
ATMP read

admin> set agent-mode = home-and-foreign-agent

admin> set agent-type = gateway-home-agent

admin> set password = tunnel-password

admin> set udp-port = 1567

admin> set idle-timer = 30

admin> set mtu-limit = 1472

admin> write
ATMP written

admin> reset
```

**Nota:** Cuando cambie el parámetro Agent-Mode de su ajuste predeterminado Tunnel-Disabled a otro ajuste, deberá reiniciar el sistema para que el nuevo valor entre en vigor.

El agente externo de la red interna B tiene un perfil ATMP como el siguiente:

```
[in ATMP]
agent-mode = foreign-agent
agent-type = gateway-home-agent
udp-port = 5150
password = ""
retry-timeout = 3
retry-limit = 10
idle-timer = 0
mtu-limit = 1472
force-fragmentation = no
```

El agente local de la red interna A tiene un perfil ATMP como el siguiente:

```
[in ATMP]
agent-mode = home-agent
agent-type = router-home-agent
udp-port = 8877
password = tunnel-password
retry-timeout = 3
retry-limit = 10
idle-timer = 0
mtu-limit = 1472
force-fragmentation = no
```

## Configuración de un perfil de cliente móvil

El conjunto de comandos siguiente configura un perfil Connection para el cliente móvil A de la Figura 4-12. Para este perfil, la Unidad TAOS funciona como agente externo para que el cliente móvil pueda establecer un túnel con la red interna A:

```
admin> read connection mobile-client-A
CONNECTION/mobile-client-A read

admin> set active = yes

admin> set ip-options remote-address = 11.1.1.1/32

admin> set tunnel profile-type = mobile-client

admin> set tunnel primary-tunnel-server = 10.22.33.44:8877

admin> set tunnel password = tunnel-password

admin> write
CONNECTION/mobile-client-A written
```

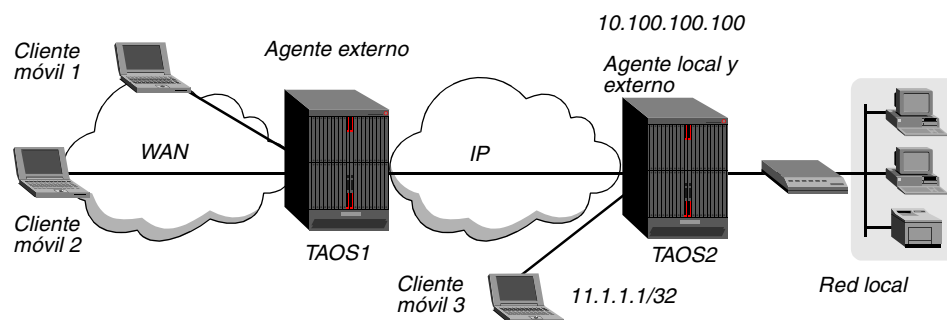
A continuación se muestra un perfil RADIUS equivalente:

```
mobile-client-A Password = "local-password"
  Service-Type = Framed-User,
  Framed-Protocol = MPP,
  Ascend-IP-Route = Route-IP-Yes,
  Framed-IP-Address = 11.1.1.1,
  Framed-IP-Netmask = 255.255.255.255,
  Tunnel-Type = ATMP,
  Tunnel-Server-Endpoint = "10.22.33.44",
  Ascend-UDP-Port = 8877,
  Tunnel-Password = "tunnel-password"
```

## Otro ejemplo de una configuración de agente local y externo

En la Figura 4-13 se muestra otra configuración que utiliza la configuración de agente local y externo. En este ejemplo, los tres clientes móviles desean establecer un túnel con la red interna, utilizando TAOS2 como agente local. Las dos unidades ATMP están separadas geográficamente.

*Figura 4-13. Configuración para que un cliente móvil eluda la conexión con el agente externo*



El cliente móvil 1 y el cliente móvil 2 efectúan llamadas locales para conectarse con el agente externo (TAOS1) y, a continuación, establecen un túnel con el agente local. No obstante, el cliente móvil 3 está geográficamente más cerca de TAOS2 y es preferible realizar una llamada

de entrada directamente a TAOS2. En este caso, TAOS2 está configurada para proporcionar funciones tanto de agente local como de agente externo al cliente móvil 3. No es necesario encapsular en GRE los datos intercambiados con el cliente móvil 3. Los datos llegan en una de las interfaces de TAOS2 y se envían a otra interfaz sin proceso de la encapsulación, pero con todas las ventajas del aislamiento de red que ATMP proporciona.

### *Definición de la dirección IP del sistema*

Los comandos siguientes establecen la dirección IP del sistema del agente local y externo:

```
admin> read ip-global
IP-GLOBAL read

admin> set system-ip-addr = 10.100.100.100

admin> write
IP-GLOBAL written
```

### *Configuración del perfil ATMP para un agente local y externo*

Los comandos siguientes configuran el perfil ATMP de TAOS2:

```
admin> read atmp
ATMP read

admin> set agent-mode = home-and-foreign-agent
admin> set agent-type = gateway-home-agent
admin> set password = tunnel-password
admin> set udp-port = 6789
admin> set idle-timer = 30
admin> set mtu-limit = 1472

admin> write
ATMP written

admin> reset
```

**Nota:** Cuando cambie el parámetro Agent-Mode de su ajuste predeterminado Tunnel-Disabled a otro ajuste, deberá reiniciar el sistema para que el nuevo valor entre en vigor.

TAOS1 tiene un perfil ATMP como el siguiente:

```
[in ATMP]
agent-mode = foreign-agent
agent-type = gateway-home-agent
udp-port = 5150
password = ""
retry-timeout = 3
retry-limit = 10
idle-timer = 0
mtu-limit = 1472
force-fragmentation = no
```



### Configuración de un perfil para el cliente móvil 3

El conjunto de comandos siguiente configura un perfil Connection para el cliente móvil 3 de la Figura 4-13. Para este perfil, la Unidad TAOS funciona como agente externo y agente local.

```
admin> read connection mobile-client-3
CONNECTION/mobile-client-3 read

admin> set active = yes

admin> set ip-options remote-address = 11.1.1.1/32

admin> set tunnel profile-type = mobile-client

admin> set tunnel primary-home-agent = 10.100.100.100:6789

admin> set tunnel password = tunnel-password

admin> write
CONNECTION/mobile-client-3 written
```

A continuación se muestra un perfil RADIUS equivalente:

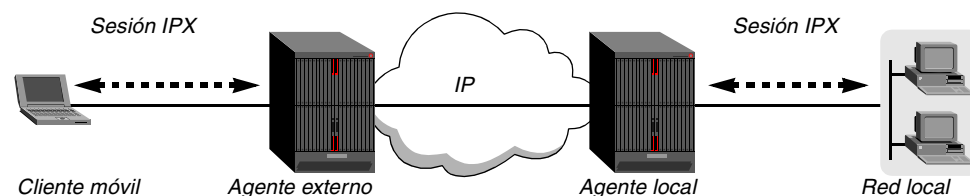
```
mobile-client-3 Password = "local-password"
  Service-Type = Framed-User,
  Framed-Protocol = MPP,
  Ascend-IP-Route = Route-IP-Yes,
  Framed-IP-Address = 11.1.1.1,
  Framed-IP-Netmask = 255.255.255.255,
  Tunnel-Type = ATMP,
  Tunnel-Server-Endpoint = "10.100.100.100:6789",
  Tunnel-Password = "tunnel-password"
```

## Configuración de IPX sobre ATMP

IPX sobre ATMP permite que clientes móviles ATMP establezcan un túnel con una red interna IPX. Los clientes móviles pueden ser clientes IPX de conexión por llamada o adaptadores de terminal de conexión por llamada, pero no pueden ser ruteadores IPX.

Los paquetes IPX se encapsulan (GRE) a través del túnel de manera que la conexión entre el agente externo y el agente local no requiere ruteo de IPX. No obstante, el ruteo de IPX es necesario para la conexión entre el cliente móvil y el agente externo, y para la conexión entre el agente local y la red interna, como se muestra en la Figura 4-14.

Figura 4-14. Conexiones de ruteo de IPX para IPX sobre ATMP



Si desea obtener información detallada acerca de la configuración de IPX, consulte el Capítulo 7, "Ruteo IPX".

Si desea obtener información acerca de la configuración de conexiones entre agentes locales y agentes externos, consulte "Configuración de la conexión de agente a agente" en la página 4-7.

## Configuración de los agentes para el ruteo de IPX

Si desea obtener información detallada acerca de la configuración de la Unidad TAOS para rutear paquetes IPX, consulte el Capítulo 7, “Ruteo IPX”. Los comandos siguientes establecen una configuración de IPX mínima para que una Unidad TAOS pueda rutear paquetes IPX:

```
admin> read ipx-global
IPX-GLOBAL read

admin> set ipx-routing-enabled = yes

admin> set ipx-dialin = cccc1234

admin> write
IPX-GLOBAL written

admin> read ipx-interface { { 1 c 1 } 0 }
IPX-INTERFACE/{ { shelf-1 controller 0 } 0 } read

admin> set ipx-routing-enabled = yes

admin> set ipx-frame = 802.2

admin> set ipx-net-number = 23456789

admin> write
IPX-INTERFACE/{ { shelf-1 controller 0 } 0 } written
```

Además de rutear paquetes IPX, normalmente el agente externo debe definir una red IPX exclusiva que se utilizará para asignar direcciones a clientes NetWare de marcación de entrada. Por ejemplo:

```
admin> read ipx-global
IPX-GLOBAL read

admin> set ipx-dialin = cccc1234

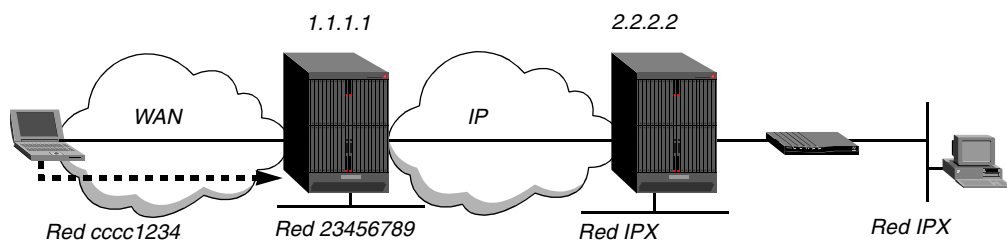
admin> write
IPX-GLOBAL written
```

## Ejemplo de IPX sobre ATMP con un agente local de gateway

Después de configurar la conexión IP entre los dos agentes (como se describe en “Configuración de los agentes para el ruteo de IPX”) y activar el ruteo de IPX en el agente externo, debe configurar las conexiones IPX entre el cliente móvil y el agente externo, y entre el agente local y la red interna.

En este ejemplo, el cliente móvil está ejecutando Windows 98 con IPX activado. Al cliente móvil se le asigna una dirección de la red IPX virtual definida en el perfil IPX-Global del agente externo (CCCC1234).

*Figura 4-15. IPX sobre ATMP con un agente local de gateway*



El agente local de gateway se comunica con una unidad Pipeline configurada para el ruteo IPX (el ruteador local). Después de establecer las configuraciones descritas en los subapartados siguientes, el cliente móvil podrá establecer una conexión telefónica con el agente externo y, una vez conectado, se podrá hacer clic en el icono NetworkNeighborhood para visualizar el servidor NetWare y su contenido.

### *Configuración de una conexión IPX de cliente móvil*

El conjunto de comandos siguiente configura un perfil Connection para el cliente móvil de la Figura 4-15:

```
admin> read connection mobile-client-1
CONNECTION/mobile-client-1 read

admin> set active = yes

admin> set ppp recv-password = mc-password

admin> set ipx ipx-routing-enabled = yes

admin> set ipx peer = dialin

admin> set tunnel profile-type = mobile-client

admin> set tunnel primary-tunnel-server = 2.2.2.2

admin> set tunnel password = tunnel-password

admin> set tunnel home-network-name = home-router

admin> write
CONNECTION/mobile-client-1 written
```

A continuación se muestra un perfil RADIUS equivalente:

```
mobile-client-1 Password = "mc-password"
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Ascend-Route-IPX = Route-IPX-Yes,
  Ascend-IPX-Peer-Mode = IPX-Peer-Dialin,
  Tunnel-Type = ATMP,
  Tunnel-Server-Endpoint = "2.2.2.2",
  Tunnel-Password = "tunnel-password"
  Tunnel-Private-Group-ID = "home-router"
```

### *Ejemplo de una conexión IPX de perfil de gateway*

El enlace entre el agente local de gateway y la red interna puede ser de relé de trama o permanente, pero no puede ser una conexión conmutada (los datos que se reciben a través de un túnel no hacen que el agente local de gateway active el enlace).

El agente local de gateway debe configurarse para IPX (consulte “Configuración de los agentes para el ruteo de IPX” en la página 4-32).

Los comandos siguientes configuran un perfil Connection para la conexión con el ruteador local. Tenga en cuenta que SAP y RIP de IPX están desactivados en el perfil para evitar que la información de SAP y RIP se propague del agente local a la red interna.

```
admin> new connection home-router
CONNECTION/home-router read

admin> set active = yes
```

```
admin> set ppp send-auth = chap-ppp-auth
admin> set ppp send-password = atmp-hrouter
admin> set ppp recv-password = atmp-ha
admin> set ipx ipx-routing-enabled = yes
admin> set ipx peer = router
admin> set ipx rip = off
admin> set ipx sap = off
admin> set telco answer-originate = originate-only
admin> set telco ft1-caller = yes
admin> set telco call-type = ft1-mpp
admin> set telco nailed-groups = 1,2
admin> set tunnel profile-type = gateway-profile
admin> set tunnel max-tunnels = 120
admin> write
CONNECTION/home-router written
```

### *Requisitos del ruteador local IPX*

La unidad Pipeline que actúa como ruteador local necesita un perfil Connection de ruteo de IPX para la conexión con el agente local de gateway y una ruta IPX estática hacia el cliente móvil. Cuando el agente local es un gateway, el ruteador local necesita una ruta IPX estática hacia el cliente móvil. El número de red de destino de esa ruta es el número de red IPX que el cliente móvil utiliza. El número de nodo de destino de la ruta estática debe ser la dirección MAC de Ethernet del puerto Ethernet del controlador del módulo del agente local. El ajuste MAC-Address se puede visualizar en el perfil Ether-Info del agente local. Por ejemplo, el perfil siguiente muestra la dirección MAC 00:c0:7b:6b:9f:d6:

```
admin> get ether-info {1 c 1}
interface-address* = { shelf-1 controller 1 }
mac-address = 00:c0:7b:6b:9f:d6
link-state = unknown
media-speed-mbit = 10
```

En la ruta estática de ejemplo que aparece a continuación, el número de la red de destino es CCCC1234 (la red virtual asignada al cliente por el agente externo) y el número de nodo de destino es la dirección MAC del puerto Ethernet del controlador del módulo del agente local. El parámetro Connection # especifica el número del perfil Connection de ruteo de IPX de la unidad Pipeline para la conexión con el agente local de gateway.

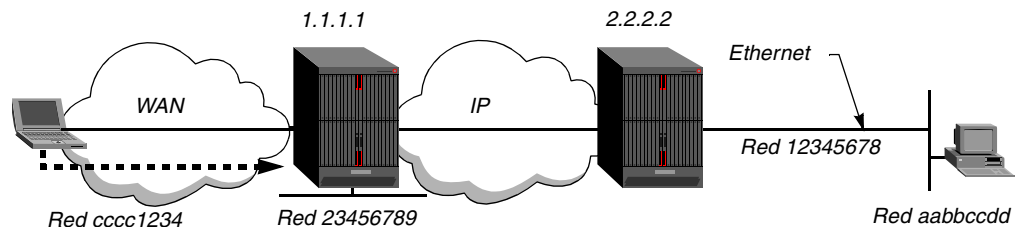
```
Ethernet
  IPX Route
    Mobile-Client-1
      Server Name=
      Active=Yes
      Network=cccc1234
      Node=0c07b6b9fd6
      Socket=
      Server Type=0
      Hop Count=2
      Tick Count=12
      Connection #=1
```

## Ejemplo de IPX sobre ATMP con un agente local de ruteador

Después de configurar la conexión IP entre los dos agentes (como se describe en “Configuración de la conexión de agente a agente” en la página 4-7), debe configurar las conexiones IPX entre el cliente móvil y el agente externo, y entre el agente local y la red interna.

En la Figura 4-16, el cliente móvil está ejecutando Windows 98 con IPX activado. Al cliente móvil se le asigna una dirección de la red IPX virtual definida en el perfil IPX-Global del agente externo (CCCC1234).

Figura 4-16. IPX sobre ATMP con un agente local de ruteador



Después de establecer las configuraciones descritas en los subapartados siguientes, el cliente móvil podrá establecer una conexión telefónica con el agente externo y, una vez conectado, se podrá hacer clic en el icono NetworkNeighborhood para visualizar el servidor NetWare y su contenido.

### Configuración de una conexión IPX de cliente móvil

El conjunto de comandos siguiente configura un perfil Connection para el cliente móvil de la Figura 4-16:

```
admin> read connection mobile-client-1
CONNECTION/mobile-client-1 read

admin> set active = yes

admin> set ppp recv-password = mc-password

admin> set ipx ipx-routing-enabled = yes

admin> set ipx peer = dialin

admin> set tunnel profile-type = mobile-client

admin> set tunnel primary-tunnel-server = 2.2.2.2

admin> set tunnel password = tunnel-password

admin> write
CONNECTION/mobile-client-1 written
```

A continuación se muestra un perfil RADIUS equivalente:

```
mobile-client-1 Password = "mc-password"
Service-Type = Framed-User,
Framed-Protocol = PPP,
Ascend-Route-IPX = Route-IPX-Yes,
Ascend-IPX-Peer-Mode = IPX-Peer-Dialin
Tunnel-Type = ATMP,
```

```
Tunnel-Server-Endpoint = "2.2.2.2",  
Tunnel-Password = "tunnel-password"
```

### *Ejemplo de una configuración de agente local de ruteador IPX*

En este ejemplo el agente local de ruteador reside en la red interna, por lo que no se necesita un perfil Connection (en otras configuraciones, el agente local de ruteador puede comunicarse con otro ruteador IPX a través de una conexión permanente). En el agente local de ruteador, los comandos siguientes configuran una interfaz Ethernet local como red interna IPX:

```
admin> read ipx-global  
IPX-GLOBAL read  
  
admin> set ipx-routing-enabled = yes  
  
admin> write  
IPX-GLOBAL written  
  
admin> read ipx-interface { { 1 c 1 } 0 }  
IPX-INTERFACE/{ { shelf-1 controller 0 } 0 } read  
  
admin> set ipx-routing-enabled = yes  
  
admin> set ipx-frame = 802.2  
  
admin> set ipx-net-number = 12345678  
  
admin> write  
IPX-INTERFACE/{ { shelf-1 controller 0 } 0 } written
```

## Túneles L2TP, PPTP e IP en IP

Protocolo de túnel de capa 2 (L2TP) .....	5-1
Reenvío de capa 2 (L2F) .....	5-18
Protocolo de túnel punto a punto (PPTP) .....	5-24
Resumen del conjunto de atributos de túnel .....	5-29
Encapsulación IP en IP .....	5-33

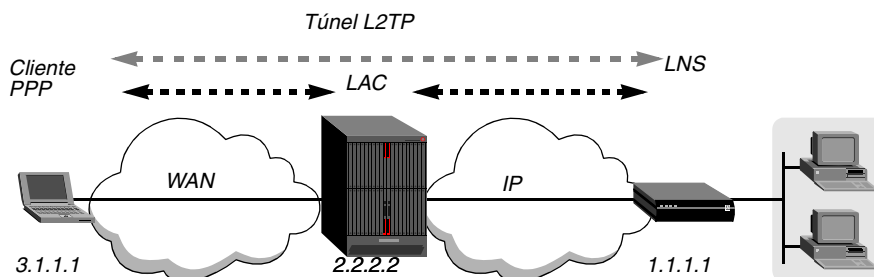
### Protocolo de túnel de capa 2 (L2TP)

El protocolo de túnel de capa 2 (L2TP) proporciona un túnel en la capa 2 de OSI (en la capa HDLC de una conexión PPP). Actualmente, una unidad APX 8000, MAXTNT o DSLTNT puede funcionar solamente como concentrador de acceso L2TP (LAC), lo que significa que la unidad recibe llamadas PPP de entrada e inicia una conexión con un servidor de red L2TP (LNS).

### Componentes de un túnel L2TP

En la Figura 5-1 se muestran los elementos de un túnel L2TP. Un cliente PPP (también llamado *cliente móvil*) efectúa una llamada de entrada a un enlace síncrono o asíncrono utilizando cualquier protocolo que pueda transportarse en PPP. La unidad TAOS responde la llamada y la pasa al LNS. La comunicación de LAC a LNS requiere conexión IP.

Figura 5-1. Túnel L2TP



El cliente móvil puede ser cualquier cliente PPP. Por ejemplo, puede ser una unidad Pipeline que realiza una llamada digital o un PC con Windows NT que efectúa una llamada por módem.

El enlace entre el LAC y el LNS puede ser una conexión conmutada o permanente, o puede ser un enlace Ethernet. La conexión al LNS es un enlace IP, que se compone de un enlace de

control y cero o más enlaces de datos. Tanto el enlace de control como los enlaces de datos utilizan el puerto UDP 1701 y se encapsulan en UDP.

El enlace de control transporta información que se utiliza tanto para consultar si el LNS aceptará la llamada actual como para establecer un túnel. L2TP implementa un mecanismo Hello por el que el LAC y el LNS verifican que el otro está activo. Con este fin se envían uno a otro un mensaje de control aproximadamente cada minuto. Si el mensaje Hello no llega al cabo de varios minutos, el túnel y todas las conexiones de túnel se desactivan.

Los enlaces de datos transportan los datos del cliente, que se componen de tramas PPP. Existe un enlace de datos por conexión de cliente con túnel.

## Configuración de operaciones L2TP

A continuación se muestran los parámetros L2TP globales (aparecen con los valores predeterminados):

```
[in L2-TUNNEL-GLOBAL]
l2tp-mode = disabled
l2tp-auth-enabled = no
l2tp-rx-window = 0

[in TUNNEL-SERVER/""]
server-endpoint* = ""
enabled = yes
shared-secret = ""
```

Parámetro	Especifica
L2TP-Mode	Activa y desactiva operaciones L2TP. Especifique LAC para permitir operaciones L2TP en la unidad TAOS.
L2TP-Auth-Enabled	Activa y desactiva la autenticación de túnel L2TP. Con el ajuste Yes, la unidad TAOS utiliza el valor Shared-Secret para autenticar el LNS antes de activar el canal de control L2TP.
L2TP-Rx-Window	Tamaño de ventana de recepción L2TP anunciado para canales de datos. El valor predeterminado, 0 (cero), especifica que la unidad TAOS solicitará que no se realice control del flujo para cargas útiles L2TP de entrada.
Server-Endpoint	Nombre de host DNS o dirección IP decimal con puntos para el punto final del LNS. Si este ajuste es un nombre de host, la unidad TAOS ejecuta una búsqueda DNS de la dirección del host.
Enabled	Activa y desactiva los túneles establecidos al Server-Endpoint especificado.
Shared-Secret	Autenticación secreta compartida para la autenticación de túneles L2TP. Para obtener información detallada, consulte el apartado "Autenticación de túnel" en la página A-34.

Los comandos siguientes configuran operaciones L2TP con un LNS llamado L2TP-1:

```
admin> read l2-tunnel
L2-TUNNEL-GLOBAL read
admin> set l2tp-mode = lac
```



```
admin> set l2tp-auth-enabled = yes
admin> set l2tp-rx-window = 1024
admin> write
L2-TUNNEL-GLOBAL written
admin> read tunnel-server l2tp-1
TUNNEL-SERVER/l2tp-1 read
admin> set enabled = yes
admin> set shared-secret = secret1
admin> write
TUNNEL-SERVER/l2tp-1 read
```

## Configuración de una conexión con el LNS

Si el LNS se encuentra en una red IP remota, la unidad TAOS requiere un perfil Connection o RADIUS ruteado por IP para conectarse con el LNS. Por ejemplo:

```
admin> read conn l2tp-1
CONNECTION/l2tp-1 read
admin> set active = yes
admin> set dial-number = 9-1-333-555-1212
admin> set ppp send-password = lns-pw
admin> set ppp recv-password = lac-pw
admin> set ip-options remote = 1.1.1.1
admin> write
CONNECTION/l2tp-1 written
```

A continuación se muestran los perfiles RADIUS equivalentes:

```
l2tp-1 Password = "lac-pw"
    Service-Type = Framed-User,
    Framed-Protocol = MPP,
    Framed-IP-Address = 1.1.1.1

route-taos-1 Password = "ascend", Service-Type = Outbound-User
    Framed-Route = "1.0.0.0 1.1.1.1 1 n l2tp-1-out"

l2tp-1-out Password = "lac-pw", Service-Type = Outbound-User
    User-Name = "l2tp-1",
    Ascend-Dial-Number = "9-1-333-555-1212",
    Framed-Protocol = MPP,
    Framed-IP-Address = 1.1.1.1,
    Ascend-Send-Secret = "lns-pw"
```

Si desea obtener información detallada acerca de la configuración de interfaces WAN de IP, consulte el Capítulo 2, "Ruteo IP".

## Configuración de perfiles de cliente móvil L2TP

Si un perfil de cliente PPP está configurado para iniciar un túnel L2TP, la unidad TAOS intenta abrir un túnel tras la autenticación inicial de la conexión. Podrá abrir un túnel después de

autenticar previamente la llamada (mediante la autenticación CLID o DNIS) o después de autenticar el nombre y la contraseña del emisor.

Si el LAC abre un túnel después de autenticar previamente la llamada, el LNS realiza todas las negociaciones PPP y la terminación de la conexión PPP. Aunque el LAC haya autenticado la contraseña de una llamada, el LNS puede (y probablemente debería por motivos de seguridad) realizar de nuevo la autenticación. El LAC y el LNS pueden utilizar diferentes protocolos de autenticación PPP sin restricciones.

**Nota:** Debido a los requisitos del protocolo de túnel, el LNS puede autenticar una llamada de túnel únicamente utilizando un protocolo de autenticación PPP. El LNS no puede utilizar otros métodos de autenticación (como la autenticación CLID, DNIS o del servidor de terminales) para llamadas de túnel. Para que el sistema utilice CLID o DNIS para autenticar previamente una llamada, el conmutador telco debe enviar la información como parte de la llamada y la unidad TAOS debe estar configurada para extraer y utilizar dicha información.

Si desea obtener información detallada acerca de la autenticación previa y la autenticación por contraseña, consulte el Apéndice A, “Métodos de autenticación”.

### *Ajustes de L2TP en perfiles Connection*

A continuación se muestran los parámetros de túnel L2TP (que aparecen con valores de ejemplo) en un perfil Connection:

```
[in CONNECTION/tunnelcx:tunnel-options]
profile-type = mobile-client
tunneling-protocol = l2tp-protocol
primary-tunnel-server = l2tp-1
```

Parámetro	Especifica
Profile-Type	Tipo de perfil del túnel. Especifique Mobile-Client para el túnel L2TP.
Tunneling-Protocol	Protocolo que debe utilizarse cuando se crea un túnel para este perfil. Establézcase en L2TP para pasar el tráfico a un LNS.
Primary-Tunnel-Server	Nombre de host DNS o dirección IP decimal con puntos para el punto final del LNS. Si este ajuste es un nombre de host, la unidad TAOS ejecuta una búsqueda DNS de la dirección del host.

### *Ajustes de L2TP en perfiles RADIUS*

RADIUS utiliza los pares atributo-valor siguientes para especificar túneles L2TP:

Atributo	Valor
Tunnel-Type (64)	Protocolo de túnel que debe utilizarse. Establézcalo en L2TP (3) para el túnel L2TP.
Tunnel-Medium-Type (65)	Medio de transmisión que se utilizará para el túnel. Actualmente sólo se da soporte a IP (1).
Tunnel-Server-Endpoint (66)	Nombre de host DNS o dirección IP decimal con puntos para el punto final del LNS (un valor de serie). Si especifica un nombre de host, la unidad TAOS ejecuta una búsqueda DNS de la dirección del host.

Atributo	Valor
Tunnel-Password (69)	Autenticación secreta compartida para la autenticación de túneles L2TP. Para obtener información detallada, consulte el apartado “Autenticación de túnel” en la página A-34.

### *Ejemplos de apertura de un túnel después de autenticar previamente la llamada*

Para que la unidad TAOS pueda autenticar previamente una llamada, debe estar configurada para extraer y utilizar información CLID o DNIS. Si desea obtener información detallada, consulte el Apéndice A, “Métodos de autenticación”.

### *Ejemplos de utilización de la autenticación CLID*

Los comandos siguientes configuran un perfil que abre un túnel L2TP a un LNS (1.1.1.1) después de verificar el ID del emisor:

```
admin> read conn l2test
CONNECTION/l2test read

admin> set active = yes

admin> set clid = 555-1000

admin> set tunnel profile-type = mobile-client

admin> set tunnel tunneling-protocol = l2tp

admin> set tunnel primary-tunnel-sever = 1.1.1.1

admin> write
CONNECTION/l2test written
```

A continuación se muestra un perfil RADIUS equivalente:

```
5551000 Password = "Ascend-CLID", Service-Type = Outbound-User
    Tunnel-Type = L2TP,
    Tunnel-Medium-Type = IP,
    Tunnel-Server-Endpoint = "1.1.1.1"
```

### *Ejemplos de utilización de DNIS*

Los comandos siguientes configuran un perfil que abre un túnel L2TP a un LNS llamado L2TP-1 si el número marcado es 8001234567:

```
admin> read conn tunnelcx
CONNECTION/tunnelcx read

admin> set active = yes

admin> set callednumber = 8001234567

admin> set tunnel profile-type = mobile-client

admin> set tunnel tunneling-protocol = l2tp

admin> set tunnel primary-tunnel-sever = l2tp-1.example.com

admin> write
CONNECTION/tunnelcx
```

A continuación se muestra un perfil RADIUS equivalente:

```
8001234567 Password = "Ascend-DNIS", Service-Type = Outbound-User
Tunnel-Server-Endpoint = "l2tp-1.example.com",
Tunnel-Type = L2TP,
Tunnel-Medium-Type = IP
```

### *Ejemplos de apertura de un túnel después de la autenticación por contraseña*

En estos ejemplos, la unidad TAOS negocia la llamada PPP, incluida la autenticación por contraseña, y abre el túnel L2TP. Si desea obtener información detallada acerca de la autenticación PPP, consulte el apartado "Autenticación de sesiones de protocolo entramado" en la página A-6.

Los comandos siguientes crean un perfil Connection que incluye una contraseña PPP. La unidad TAOS autentica al emisor antes de activar el túnel con un LNS en 1.1.1.1.

```
admin> read conn l2test
CONNECTION/l2test read

admin> set active = yes

admin> set encapsulation-protocol = ppp

admin> set ppp recv-password = localpw

admin> set tunnel profile-type = mobile-client

admin> set tunnel primary-tunnel-sever = 1.1.1.1

admin> set tunnel tunneling-protocol = l2tp

admin> write
CONNECTION/l2test written
```

A continuación se muestra un perfil RADIUS equivalente:

```
l2test Password = "localpw"
Service-Type = Framed-User,
Framed-Protocol = PPP,
Tunnel-Server-Endpoint = "1.1.1.1",
Tunnel-Type = L2TP,
Tunnel-Medium-Type = IP
```

## **Configuración de la autenticación IPSec**

La unidad TAOS da soporte a la cabecera de autenticación (AH) de IPSec y a los protocolos de carga útil de seguridad de la encapsulación (ESP) para la transmisión segura de paquetes de datos IP. Cada protocolo da soporte a dos modos de utilización: el modo de transporte y el modo de túnel. Para obtener información completa acerca de los protocolos IPSec, consulte los documentos RFC 2401, *Security Architecture for the Internet Protocol* (Noviembre 1998); RFC 2402, *IP Authentication Header* (Noviembre 1998); y RFC 2406, *IP Encapsulating Security Payload (ESP)* (Noviembre 1998).

### *Protocolos de seguridad IPSec*

La AH de IPSec utiliza un secreto compartido (una *clave*) para procesar partes de un paquete de datos mediante algoritmos de síntesis y crear una huella digital electrónica. El sistema receptor realiza el mismo proceso y compara las huellas digitales. Si las huellas digitales

coinciden, el sistema receptor está seguro de que el paquete ha sido enviado por la fuente correcta y que no ha sufrido alteraciones durante el tránsito.

El ESP de IPSec realiza un cifrado completo de la parte de datos de cada paquete. El sistema receptor descifra los paquetes antes de rutearlos. El cifrado y descifrado proporciona la seguridad añadida de que nadie ha visto el contenido del paquete durante el tránsito del paquete.

### *Modos de encapsulación IPSec*

La unidad TAOS da soporte al modo de transporte y al modo de túnel de IPSec.

El *modo de transporte* funciona entre dos hosts. El modo de transporte proporciona servicios de seguridad para protocolos de capa superior, que pueden incluir partes seleccionadas de la cabecera IP y otras opciones seleccionadas.

El *modo de túnel* es necesario para conexiones entre un host que no realiza proceso IPSec y un gateway de seguridad. En el modo de túnel, los paquetes IP se encapsulan en una cabecera IP externa que especifica el destino del proceso IPSec (encapsulación IP en IP).

### *Aplicación de IPSec a un servidor de túnel o en una conexión TCP*

Los perfiles IPSec especifican un punto final IPSec, así como las transformaciones IPSec que deben utilizarse en la corriente de datos que intercambia con dicho punto final. Deben coincidir las configuraciones de los dos puntos finales (los ajustes de la configuración de *envío* de un sistema deben coincidir con los ajustes de la configuración de *recepción* del otro sistema, y viceversa).

En un perfil IPSec, los parámetros siguientes (que aparecen con los valores predeterminados) activan el perfil y especifican el modo de encapsulación y la dirección de punto final IPSec del extremo distante:

```
[in IPSEC/""]
name* = ""
active = no
encap-mode = transport
tunnel-address = 0.0.0.0
```

Parámetro	Especifica
Name	Nombre del perfil IPSec (de 23 caracteres como máximo).
Active	Activa y desactiva el perfil para su utilización.
Encap-Mode	Modo de encapsulación en el que funciona IPSec. Si desea obtener información al respecto, consulte el apartado “Modos de encapsulación IPSec” en la página 5-7. El valor predeterminado es <code>transport</code> (modo de transporte). Si el parámetro se establece en <code>tunnel</code> , se utiliza la encapsulación IP en IP para que la corriente de datos pase por el túnel. El modo de túnel es necesario si las direcciones de punto final IPSec difieren de las direcciones de punto final TCP para sesiones TCP-Clear. Si el parámetro se establece en <code>optimized</code> , el sistema utiliza el modo de transporte si es posible (el modo de transporte es más eficaz) y utiliza el modo de túnel solamente cuando se requiere para una conexión concreta.

Parámetro	Especifica
Tunnel-Address	Dirección IP del punto final IPSec del extremo distante. Para una conexión L2TP, ésta es la dirección IP del servidor de red L2TP (LNS) en el extremo distante del túnel. Para una conexión TCP-Clear, es la dirección de un gateway de seguridad o un host de llamada de entrada.

Por ejemplo, los comandos siguientes especifican que el proceso IPSec funciona en modo de transporte en la corriente de datos que intercambia con 1.1.1.1:

```
admin> new ipsec securegw
IPSEC/l2tp1-ipsec read
admin> set active = yes
admin> set encap-mode = transport
admin> set tunnel-address = 1.1.1.1
admin> write
IPSEC/l2tp1-ipsec written
```

**Nota:** Los comandos del ejemplo anterior no crean un perfil IPSec utilizable. AH o ESP de IPSec (o ambos) deben estar configurados para que el perfil IPSec surta efecto. Para obtener información detallada, consulte los apartados “Configuración de un perfil IPSec para AH de IPSec” en la página 5-9 y “Configuración de un perfil IPSec para ESP de IPSec” en la página 5-11.

### *Aplicación de un perfil IPSec a un LNS*

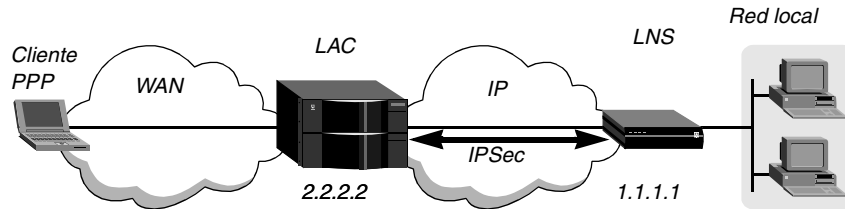
Los parámetros siguientes (que aparecen con los valores predeterminados) asocian un perfil IPSec a un LNS concreto:

```
[in TUNNEL-SERVER/""]
server-endpoint = ""
ipsec-profile = ""
```

Parámetro	Especifica
Server-Endpoint	Nombre o dirección IP del punto final del túnel. Este parámetro debe especificar el mismo host que el parámetro Tunnel-Address en el perfil IPSec para que tenga aplicación.
IPSec-Profile	Nombre del perfil IPSec (de 23 caracteres como máximo) que define las transformaciones y puntos finales para operaciones IPSec en el tráfico que pasa por los túneles L2TP con destino al punto final especificado. Si el perfil Tunnel-Server no especifica un nombre de perfil IPSec, se asigna un zócalo UDP normal y no seguro a la sesión L2TP. Si se especifica un nombre de perfil IPSec, se abre un nuevo zócalo UDP y se le asignan los ajustes del perfil especificado.

En la Figura 5-2 se muestra una unidad TAOS que funciona como concentrador de acceso L2TP (LAC) con una unidad MAX que funciona como LNS.

Figura 5-2. Configuración de un túnel L2TP seguro de IPSec



Los comandos siguientes aplican un perfil IPSec llamado `securegw` al LNS especificado:

```
admin> new tunnel-server
TUNNEL-SERVER/" read

admin> set server-endpoint = 1.1.1.1

admin> set ipsec-profile = securegw

admin> write
TUNNEL-SERVER/1.1.1.1 written
```

### Configuración de un perfil IPSec para AH de IPSec

Para que funcione la AH de IPSec, los dos extremos del túnel L2TP deben especificar un número de índice de parámetros de seguridad (SPI), el tipo de transformación que se utilizará y un secreto compartido (una clave). Estos ajustes deben coincidir en las configuraciones del LAC y el LNS. Además, puede optar por activar la *protección frente a repeticiones*, que se utiliza para contrarrestar ataques de denegación de servicio.

### Información general de los ajustes de AH de IPSec

Los administradores de ambos extremos del túnel deben especificar configuraciones coincidentes de AH de IPSec. A continuación se muestran los parámetros pertinentes de la unidad TAOS (que aparecen con los ajustes predeterminados):

```
[in IPSEC/" :send-ah]
active = no
spi = 1
ah-type = none
key =
replay-protection = no

[in IPSEC/" :recv-ah]
active = no
spi = 1
ah-type = none
key =
replay-protection = no
```

Parámetro	Especifica
Active	Activa y desactiva el proceso AH de IPSec para paquetes enviados o recibidos a través del túnel.

Parámetro	Especifica
SPI	Índice de parámetros de seguridad: un valor numérico de 32 bits del 1 al 2147483647. El SPI del subperfil Send-AH debe coincidir con el SPI de LNS en la configuración AH de recepción, y viceversa. Si el LNS es una unidad TAOS (por ejemplo, una unidad MAX), el administrador de dicha unidad puede utilizar la aplicación SecureConnect Manager™ (SCM) para crear y descargar configuraciones IPsec en perfiles Firewall. Los valores de SPI en SCM son hexadecimales, mientras que los valores de SPI de la unidad TAOS son decimales. Puede especificar el valor del SPI aquí en hexadecimal anteponiendo 0x al valor. Sin embargo, el número todavía se visualiza en decimales en la interfaz de la unidad TAOS.
AH-Type	Tipo de transformación de autenticación que debe utilizarse. Los valores válidos son los siguientes: <ul style="list-style-type: none"><li>• None (el valor predeterminado): sin autenticación</li><li>• MD5: modo MD5, descrito en el documento RFC 1828</li><li>• SHA1: modo SHA1, descrito en el documento RFC 1852 sobre el algoritmo de hash seguro (SHA)</li><li>• MD5-HMAC: MD5 versión 2, actualmente en proyecto</li><li>• SHA1-HMAC: SHA1 versión 2, actualmente en proyecto</li></ul>
Key	Clave de autenticación para hashing: una cadena de texto de 64 bytes que coincide exactamente con la clave que se especifica en la configuración AH de IPsec del LNS.
Replay-Protection	Activa y desactiva el proceso de números de secuencia. El sistema receptor utiliza un número de secuencia para detectar la llegada de paquetes duplicados en una ventana restringida. Si se activa este parámetro en el subperfil Send-AH, la unidad TAOS genera un número de secuencia para los paquetes que envía a través del túnel. En la versión actual del software, la unidad TAOS no verifica la secuencia de paquetes que recibe del LNS, aunque se active Replay-Protection en el subperfil Recv-AH.

### *Ejemplo de configuración de la AH de IPsec*

En el ejemplo siguiente, un administrador crea un perfil IPsec aplicando la AH de IPsec a todos los datos enviados y recibidos mediante un túnel L2TP a un LNS en la dirección IP 1.1.1.1:

```
admin> new ipsec l2tp1-ipsec
IPSEC/l2tp1-ipsec read
admin> set active = yes
admin> set encap-mode = transport
admin> set tunnel-address = 1.1.1.1
```



En los comandos siguientes, la configuración de envío de la unidad TAOS debe coincidir con los parámetros correspondientes en la configuración de recepción IPsec del sistema del LNS, y viceversa:

```
admin> set send-ah active = yes
admin> set send-ah spi = 43981
admin> set send-ah ah-type = md5
admin> set send-ah key = 4142434445464748494A4B4C4D4E4F50
admin> set recv-ah active = yes
admin> set recv-ah spi = 43981
admin> set recv-ah ah-type = md5
admin> set recv-ah key = 4142434445464748494A4B4C4D4E4F50
admin> write
IPSEC/l2tp1-ipsec written
```

Los comandos siguientes aplican el perfil IPsec al LNS:

```
admin> read tunnel-server 1.1.1.1
TUNNEL-SERVER/1.1.1.1 read
admin> set ipsec-profile = l2tp1-ipsec
admin> write
TUNNEL-SERVER/1.1.1.1 written
```

### *Configuración de un perfil IPsec para ESP de IPsec*

El protocolo ESP de IPsec proporciona cifrado de datos, así como protección frente a repeticiones y autenticación. Si configura ESP además de AH de IPsec, puede especificar solamente el cifrado y depender de AH para proporcionar el servicio de autenticación y la protección frente a repeticiones. Si especifica ESP de IPsec sin una configuración AH correspondiente, debe incluir los ajustes de integridad y autenticación para evitar ataques que, de otro modo, podrían comprometer la seguridad que proporciona el cifrado solamente.

### *Información general de los ajustes de ESP de IPsec*

Los administradores de los dos puntos finales IPsec deben especificar configuraciones ESP de IPsec coincidentes. A continuación se muestran los parámetros pertinentes con los ajustes predeterminados:

```
[in IPSEC/"":send-esp]
active = no
spi = 1
version = 0
esp-type = none
iv-len = 32
key =
key2 =
key3 =
auth-type = none
auth-key =
replay-protection = no

[in IPSEC/"":recv-esp]
active = no
```

```
spi = 1
version = 0
esp-type = none
iv-len = 32
key =
key2 =
key3 =
auth-type = none
auth-key =
replay-protection = no
```

Parámetro	Especifica
Active	Activa y desactiva el proceso ESP de IPSec para paquetes enviados o recibidos a través del túnel.
SPI	Índice de parámetros de seguridad: un valor numérico de 32 bits del 1 al 2147483647. El SPI del subperfil Send-ESP debe coincidir con el SPI de LNS en la configuración ESP de recepción, y viceversa. Si el LNS es una unidad TAOS (por ejemplo, una unidad MAX), el administrador de dicha unidad puede utilizar SecureConnect Manager™ (SCM) para crear y descargar configuraciones IPSec en perfiles Firewall. Los valores de SPI en SCM son hexadecimales, mientras que los valores de SPI de la unidad TAOS son decimales. Puede especificar el valor del SPI aquí en hexadecimal anteponiendo 0x al valor. Sin embargo, el número todavía se visualiza en decimales en la interfaz de la unidad TAOS.
Version	Versión de ESP (versión 1 o versión 2).
ESP-Type	Tipo de transformación ESP que debe utilizarse para cifrar la parte de datos de los paquetes IP. Los valores válidos son los siguientes: <ul style="list-style-type: none"><li>• None (el valor predeterminado): sin cifrado</li><li>• DES-CBC: modo DES-CBC, descrito en el documento RFC 1829 sobre el algoritmo de encadenamiento de bloques de cifrado del estándar de cifrado de datos de Estados Unidos</li><li>• 3DES-CBC: modo 3DES-CBC, descrito en el documento RFC 1851 sobre el algoritmo DES-CDC triple</li><li>• 40DES-CBC: modo DES-CBC limitado a 40 bits</li></ul>
IV-Len	Número de bits en el vector de inicialización. Para ESP-v1, puede especificar 32 (vector de 32 bits) o 64 (vector de 64 bits). Para ESP-v2, IV-Len se establece en 64 automáticamente.
Key	Clave de autenticación para ESP: una cadena de texto de 16 bytes que coincide exactamente con la clave especificada en la configuración ESP de IPSec del LNS.
Key2	Segunda clave de autenticación de 16 bytes, que se utiliza para la segunda ejecución del cifrado en modo 3DES-CBC.
Key3	Tercera clave de autenticación de 16 bytes, que se utiliza para la tercera ejecución del cifrado en modo 3DES-CBC.

Parámetro	Especifica
Auth-Type	Tipo de transformación de autenticación que debe utilizarse cuando ESP-v2 está en uso. Los valores válidos son los siguientes: <ul style="list-style-type: none"><li>• None (el valor predeterminado): sin autenticación</li><li>• MD5: modo MD5, descrito en el documento RFC 1828</li><li>• SHA1: modo SHA1, descrito en el documento RFC 1852</li><li>• MD5-HMAC: MD5 versión 2, actualmente en proyecto</li><li>• SHA1-HMAC: SHA1 versión 2, actualmente en proyecto</li></ul>
Auth-Key	Clave de autenticación que se utiliza cuando ESP-v2 está en uso: cadena de texto de 64 bytes que coincide exactamente con la clave especificada en la configuración ESP-v2 de IPsec del LNS. Este ajuste no se aplica si Version se establece en 1.
Replay-Protection	Activa y desactiva el proceso de números de secuencia. El sistema receptor utiliza un número de secuencia para detectar la llegada de paquetes duplicados en una ventana restringida. Si se activa este parámetro en el subperfil Send-AH, la unidad TAOS genera un número de secuencia para los paquetes que envía a través del túnel. En la versión actual del software, la unidad TAOS no verifica la secuencia de paquetes que recibe del LNS, aunque se active Replay-Protection en el subperfil Recv-AH.

### *Ejemplo de configuración de ESP de IPsec para L2TP*

En el ejemplo siguiente, un administrador crea un perfil IPsec aplicando ESP de IPsec y la integridad de secuencia parcial (protección frente a repeticiones) para paquetes intercambiados por túnel con un LNS en la dirección IP 1.1.1.1:

```
admin> new ipsec l2tp1-ipsec
IPSEC/l2tp1-ipsec read
admin> set active = yes
admin> set encap-mode = transport
admin> set tunnel-address = 1.1.1.1
```

En los comandos siguientes, la configuración de envío de la unidad TAOS debe coincidir con los parámetros correspondientes en la configuración de recepción IPsec del sistema del LNS, y viceversa:

```
admin> set send-esp active = yes
admin> set send-esp spi = 26990
admin> set send-esp version = 2
admin> set send-esp esp-type = des-cbc
admin> set send-esp key = 61083D2A76D57ABC
admin> set send-esp esp-version = 2
admin> set send-esp replay-protection = yes
admin> set recv-esp active = yes
admin> set recv-esp spi = 26990
```

```
admin> set recv-esp version = 2
admin> set recv-esp esp-type = des-cbc
admin> set recv-esp key = 61083D2A76D57ABC
admin> set recv-esp esp-version = 2
admin> set recv-esp replay-protection = yes
admin> write
IPSEC/l2tp1-ipsec written
```

Los comandos siguientes aplican el perfil IPsec al LNS:

```
admin> read tunnel-server 1.1.1.1
TUNNEL-SERVER/1.1.1.1 read
admin> set ipsec-profile = l2tp1-ipsec
admin> write
TUNNEL-SERVER/1.1.1.1 written
```

## Configuración de opciones de temporizador de L2TP

Puede configurar opciones de temporizador de L2TP en el subperfil L2TP-Config. Los cambios que realice en estos parámetros entran en vigor cuando el temporizador anterior alcanza su límite. Utilice los parámetros siguientes cuando la unidad TAOS funcione como un concentrador de acceso L2TP (LAC).

**Nota:** Las unidades APX 8000 y DSLTNT sólo funcionan como LAC actualmente. Reciben llamadas de entrada PPP e inician una conexión con un servidor de red L2TP (LNS). Una unidad MAX puede funcionar como LNS.

Parámetro	Especifica
Control-Connect-Establish-Timer	Número máximo de segundos durante los cuales la unidad TAOS puede establecer un túnel L2TP con otra unidad. Introduzca un número entero entre 0 y 600. El valor predeterminado es 60.
First-Retry-Timer	Intervalo inicial, en milisegundos, que espera la unidad TAOS antes de realizar un segundo intento para establecer un túnel L2TP con otra unidad. Introduzca un número entero entre 100 y 5000. El valor predeterminado es 1000.
Hello-Timer	Intervalo, en segundos, entre mensajes Hello que envía la unidad TAOS a otra unidad. Especifique un número entero entre 0 y 600. El valor predeterminado es 60. El ajuste 0 especifica que la unidad TAOS no envía mensajes Hello.
LAC-Incoming-Call-Timer	Número de segundos que la unidad TAOS espera a la finalización del establecimiento de la llamada. Especifique un número entero entre 1 y 600. El valor predeterminado es 60.
Retry-Count	Número máximo de veces que la unidad TAOS intenta establecer un túnel. Especifique un número decimal entre 1 y 10. El valor predeterminado es 10.

## Configuración de los intentos por lista de L2TP

Con MAX TNT TAOS 8.0.0, una unidad TAOS que funcione como servidor de red L2TP (LNS) puede sacar partido de la función de lista DNS para intentar conectarse con una serie de puntos finales de servidor si falla el primer intento.

Para utilizar esta función, la unidad TAOS debe estar configurada para la lista DNS y los servidores DNS locales deben dar soporte a una función de lista que les permita devolver varias direcciones para un nombre de host en respuesta a una consulta DNS. Para obtener información detallada acerca de la configuración de una lista DNS, consulte el apartado “Configuración de búsquedas DNS y la lista DNS” en la página 2-58.

En el ejemplo siguiente se muestra cómo activar la lista DNS con un máximo de 3 hosts en la lista:

```
admin> read ip-global
IP-GLOBAL read

admin> set dns-list-attempt = yes

admin> set dns-list-size = 3

admin> write
IP-GLOBAL written
```

Para que la unidad TAOS utilice la lista DNS al intentar activar un túnel, el perfil Connection o RADIUS del cliente debe especificar un nombre de host que pueda resolverse por DNS como punto final del túnel. Por ejemplo, el comando siguiente muestra un nombre de host especificado como servidor del túnel primario en un perfil Connection:

```
admin> get connection client-1 tunnel-options primary-tunnel-server
[in CONNECTION/client-1:tunnel-options:primary-tunnel-server]
primary-tunnel-server = tunnel-endpoint-1
```

A continuación se muestra un perfil RADIUS con un ajuste equivalente:

```
5551000 Password = "Ascend-CLID", Service-Type = Dialout-Framed-User
      Tunnel-Type = L2TP,
      Tunnel-Medium-Type = IP,
      Tunnel-Server-Endpoint = "tunnel-endpoint-1"
```

Cuando un cliente efectúa una llamada de entrada, el sistema envía una consulta DNS para averiguar el nombre de host del servidor del túnel. Si a cambio recibe una lista de direcciones IP, la unidad TAOS intenta primero conectarse a la primera dirección IP de la lista. Si dicho intento falla, la unidad continúa intentando conectarse a las direcciones IP de la lista hasta que se establece un túnel de forma satisfactoria, la lista DNS no tiene más direcciones IP o la conexión supera el tiempo de espera.

## Configuración de varios puntos finales para sesiones de túnel

Cuando se utiliza la autenticación RADIUS, puede configurar un perfil de usuario para más de dos puntos finales de túnel. Cada punto final puede especificar su propio conjunto de atributos, como el protocolo de túnel y la contraseña. Si desea obtener información detallada acerca de este tipo de configuración RADIUS para conexiones de túnel, consulte la publicación *Guía y referencia de TAOS RADIUS*.

## Servidor de túnel secundario para túneles L2TP y L2F (perfiles locales)

Puede configurar perfiles Connection locales con un punto final de túnel secundario para sesiones de túnel L2TP o L2F. Si desea obtener información detallada acerca del soporte de RADIUS para varios puntos finales, consulte el apartado “Resumen del conjunto de atributos de túnel” en la página 5-29.

A continuación se muestran los parámetros pertinentes con ajustes de ejemplo:

```
[in IP-GLOBAL]
system-ip-addr = 1.1.1.1

[in CONNECTION/test:tunnel-options]
profile-type = mobile-client
tunneling-protocol = l2tp-protocol
primary-tunnel-server = 2.2.2.2
secondary-tunnel-server = 3.3.3.3
```

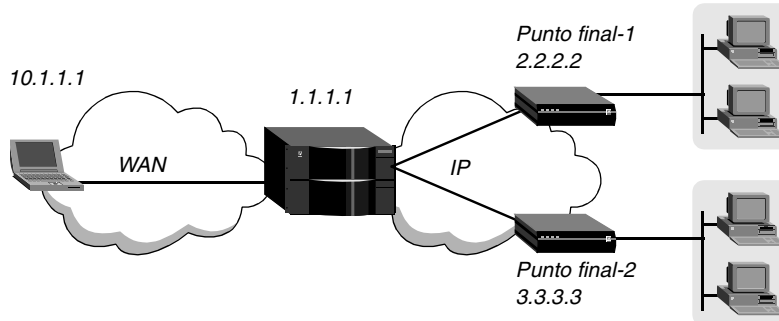
Parámetro	Especifica
System-IP-Addr	Dirección de origen para paquetes que genera el sistema. Establezca el parámetro System-IP-Addr en una unidad TAOS que funcione como LAC, especialmente si la unidad tiene varias interfaces en la nube IP que la separa de los sistemas LNS. Si desea obtener información detallada acerca de este parámetro, consulte la publicación <i>APX 8000/MAX TNT/DSLNT Reference (Referencia de APX 8000/MAX TNT/DSLNT)</i> .
Profile-Type	Para que se apliquen los parámetros del servidor de túnel (los próximos tres parámetros), este parámetro debe establecerse en <code>mobile-client</code> .
Tunneling-Protocol	Protocolo utilizado para las conexiones de túnel. Los ajustes son, entre otros, <code>l2tp-protocol</code> y <code>l2f-protocol</code> .
Primary-Tunnel-Server	Dirección IP o nombre de host del punto final primario para túneles L2TP o L2F. El punto final secundario se utiliza solamente si el primer servidor no está disponible.
Secondary-Tunnel-Server	Dirección IP o nombre de host del punto final secundario del túnel. En versiones anteriores del software, sólo se daba soporte a este ajuste en túneles ATMP. Ahora también se aplica a túneles L2TP y L2F.
	La unidad TAOS abre una sesión de túnel con este servidor solamente si el servidor primario no está disponible. Una vez establecido un túnel con el servidor de túnel secundario, la unidad mantiene dicho túnel hasta que la conexión termina, aunque el servidor primario pase a estar disponible.

### Ejemplo de configuración de un túnel L2TP con dos puntos finales de servidor

En la Figura 5-3 se muestra una unidad TAOS que puede conectarse a uno de dos puntos finales posibles del LNS para crear un túnel L2TP para el cliente de llamada de entrada. En este ejemplo, los puntos finales del LNS se encuentran en una red remota, de modo que el

sistema requiere un perfil Connection o RADIUS para establecer una conexión con uno de los sistemas de punto final.

*Figura 5-3. Puntos finales primario y secundario del túnel L2TP*



Los comandos siguientes configuran la dirección IP del sistema de la unidad TAOS:

```
admin> read ip-global
IP-GLOBAL read
admin> set system-ip-addr = 1.1.1.1
admin> write
IP-GLOBAL written
```

Los comandos siguientes configuran perfiles Connection para los dos sistemas LNS:

```
admin> read connection endpoint-1
CONNECTION/endpoint-1 read
admin> set active = yes
admin> set dial-number = 9-1-333-555-1212
admin> set ppp-options send-password = lns-pw
admin> set ppp-options rcv-password = lac-pw
admin> set ip-options remote = 2.2.2.2
admin> write
CONNECTION/endpoint-1 written
admin> read connection endpoint-2
CONNECTION/endpoint-2 read
admin> set active = yes
admin> set dial-number = 9-1-123-555-1234
admin> set ppp-options send-password = lns-pw
admin> set ppp-options rcv-password = lac-pw
admin> set ip-options remote = 3.3.3.3
admin> write
CONNECTION/endpoint-2 written
```

Los comandos siguientes crean un perfil Connection para el cliente de llamada de entrada:

```
admin> new connection dialin-1
CONNECTION/dialin-1 read
admin> set active = yes
```

```
admin> set clid = 555-1000
admin> set tunnel-options profile-type = mobile-client
admin> set tunnel-options tunneling-protocol = l2tp
admin> set tunnel-options primary-tunnel-server = 2.2.2.2
admin> set tunnel-options secondary-tunnel-server = 3.3.3.3
admin> write
CONNECTION/dialin-1 written
```

## Configuración de un nombre de sistema L2TP optativo

La unidad TAOS puede utilizar un nombre de sistema optativo al establecer túneles L2TP. A continuación se muestra el parámetro pertinente (que aparece con el valor predeterminado):

```
[in L2-TUNNEL-GLOBAL]
l2tp-system-name = ""
```

Parámetro	Especifica
L2TP-System-Name	Nombre (de 31 caracteres como máximo) que debe pasarse al LNS a la hora de iniciar un túnel L2TP. Con el valor predeterminado (null) se envían los nombres de sistema y de dominio del LAC.

Si se especifica un nombre de sistema L2TP, se utiliza en lugar del nombre de sistema y del nombre de dominio de la unidad TAOS al establecer la sesión. Si no se especifica el nombre de sistema L2TP, el LAC proporciona los nombres de sistema y de dominio reales.

Los comandos siguientes establecen el nombre de sistema L2TP:

```
admin> read l2-tunnel-global
L2-TUNNEL-GLOBAL read
admin> set l2tp-system-name = maxtnt-1
admin> write
L2-TUNNEL-GLOBAL written
```

## Reenvío de capa 2 (L2F)

**Nota:** Esta implantación del reenvío de capa 2 (L2F) se ha diseñado para su interacción con IOS 11.3 de Cisco Systems. Es posible que otras versiones de software y homólogos de túnel no reciban soporte.

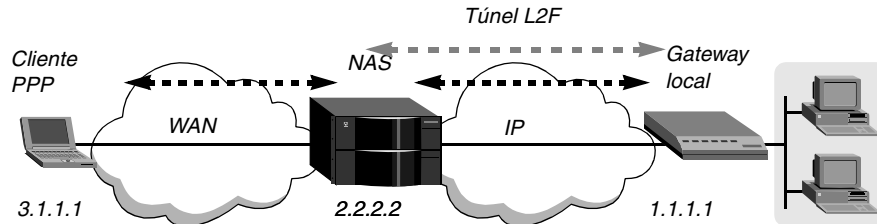
En la versión actual del software, una unidad TAOS puede funcionar como servidor de acceso de red (NAS) L2F en comunicación con un gateway local L2F que es un router Cisco con IOS 11.3.

En la Figura 5-4 se muestran los elementos que componen un túnel L2F. Un cliente PPP realiza una llamada de entrada a través de un enlace síncrono o asíncrono utilizando cualquier protocolo que pueda transportarse dentro de PPP. La unidad TAOS responde la llamada y la



pasa al gateway local (un router Cisco que ejecuta IOS 11.3). La comunicación entre el NAS y el gateway local requiere conectividad IP.

*Figura 5-4. Túnel L2F*



La conexión con el gateway local es un enlace IP, que se compone de un enlace de control y uno o más enlaces de datos. Tanto los enlaces de control como de datos utilizan el puerto UDP 1701 y se encapsulan en UDP.

El enlace de control transporta la información que se utiliza para consultar si el gateway local puede aceptar la llamada actual y establecer un túnel. L2F pone en marcha un mecanismo Hello periódico por el que el NAS y el gateway local verifican que el otro interlocutor todavía está operativo. Si el mensaje Hello no llega en un plazo especificado, se desactivan los túneles.

Cada conexión cliente de túnel tiene un enlace de datos, que transporta tramas PPP.

### **Autenticación de túneles L2F**

La unidad TAOS da soporte a la autenticación de túnel secreta compartida y secreta exclusiva L2F. El método predeterminado es utilizar un secreto compartido entre los puntos finales del túnel (la autenticación de túneles con secreto compartido L2F es similar a la autenticación de túneles L2TP con secreto compartido). Para obtener información detallada, consulte el apartado “Protocolo de túnel de capa 2 (L2TP)” en la página 5-1.

La autenticación secreta exclusiva permite especificar diferentes contraseñas para autenticar el NAS ante el gateway local y el gateway local ante el NAS.

También puede configurar la unidad TAOS para que autentique túneles intentando utilizar primero un secreto compartido y, en caso de que falle, utilizar entonces secretos exclusivos.

En la secuencia de eventos siguiente se describe cómo la unidad TAOS utiliza el secreto de túnel exclusivo para autenticar túneles L2F:

- 1 Un cliente se conecta y se autentica parcialmente. La unidad TAOS busca el perfil Connection asociado (o el perfil RADIUS) por el nombre de cliente y autentica parcialmente al cliente basándose en los ajustes de nombre de usuario y contraseña.
- 2 Si el atributo Tunnel-Type de un perfil RADIUS o el parámetro Tunnel-Protocol en un perfil Connection local especifican un túnel L2F, la unidad TAOS agrega esta conexión de cliente a un túnel existente o crea un túnel nuevo con el punto final de servidor especificado.
- 3 Si el atributo Tunnel-Password de un perfil RADIUS o el parámetro Password en un perfil Connection local presentan la contraseña, la unidad TAOS utiliza dicha contraseña para autenticar el NAS ante el gateway local.

- 4 La unidad TAOS autentica el gateway local comparando el nombre que proporciona el gateway local con el valor especificado en el atributo Tunnel-Server-Endpoint de RADIUS o el parámetro Server-Endpoint en un perfil Connection local.
- 5 La unidad TAOS establece el túnel entre ella y el gateway local.

Si utiliza RADIUS para autenticar túneles L2F con contraseñas exclusivas, asegúrese de lo siguiente:

- El perfil de usuario RADIUS del cliente debe contener un atributo Tunnel-Password con la contraseña que utilizará la unidad TAOS para autenticar el túnel ante el gateway local.
- El gateway local debe tener un perfil de usuario RADIUS. Debido a que no se trata de un perfil de usuario para acceso interactivo, Lucent recomienda que se establezca el atributo Service-Type en Outbound.

En los ejemplos siguientes se muestra un perfil RADIUS de cliente y un perfil RADIUS del gateway local que utilizan secretos exclusivos para la autenticación de túnel:

```
dialup-client Password = "client-pw"
    Tunnel-Type = L2F,
    Tunnel-Server-Endpoint = "1.1.1.1",
    Tunnel-Password = "nas-secret"

hg-name Password = "hg-secret", Service-Type = Outbound
    Reply-Message = ""
```

Como método alternativo, la contraseña del gateway local puede configurarse localmente en un perfil Tunnel-Server.

## *Configuración de operaciones básicas de L2F*

Para permitir que la unidad TAOS funcione como punto final L2F, debe definirse para que se ejecute en modo NAS y configurarla para que reconozca el gateway L2F local (un ruteador Cisco que ejecuta IOS 11.3).

Si el gateway local se encuentra en una red IP remota, la unidad TAOS requiere también un perfil Connection o RADIUS ruteado por IP que defina una conexión con el gateway local. Si desea obtener información detallada acerca de la configuración de interfaces WAN de IP, consulte el apartado “Conexiones WAN” en la página 1-1.

## *Información general de los parámetros globales de L2F*

A continuación se muestran los parámetros globales de L2F (que aparecen con los valores predeterminados) para configurar operaciones de L2F:

```
[in L2-TUNNEL-GLOBAL]
udp-queue-length = 256
l2f-mode = disabled
l2f-system-name = ""
l2f-retry-count = 4
l2f-retry-interval = 0
l2f-tunnel-secret = ""

[in TUNNEL-SERVER/""]
server-endpoint* = ""
enabled = yes
shared-secret = ""
```

Parámetro	Especifica
UDP-Queue-Length	Número máximo de paquetes UDP que pueden residir en la cola de entrada para el NAS de L2F. La longitud predeterminada de la cola para peticiones UDP es 256. Los valores válidos de la longitud de la cola van de 0 a 512.
L2F-Mode	Activa y desactiva operaciones de L2F. Especifique NAS para permitir operaciones L2F en la unidad TAOS. El valor predeterminado es Disabled.
L2F-System-Name	Nombre del sistema de la unidad NAS. Se utiliza para identificar el NAS ante el gateway local L2F durante la creación del túnel.
L2F-Retry-Count	Número de veces que la unidad TAOS reenviará paquetes de control L2F. Los valores están entre 1 y 16. El valor predeterminado es 4.
L2F-Retry-Interval	Intervalo de reintento, en segundos. Los valores están entre 0 y 32 segundos. El valor predeterminado (0) especifica que debe utilizarse un intervalo de reintento adaptativo (basado en el número de reintentos más 1).
L2F-Tunnel-Secret	Método de autenticación que utiliza la unidad TAOS para autenticar túneles L2F. Cuando el parámetro se establece en <code>shared-tunnel-secret</code> (el valor predeterminado), la autenticación de túnel depende de una autenticación secreta compartida entre el NAS y el gateway local. Con el ajuste <code>distinct-tunnel-secrets</code> , la autenticación del túnel es secreta exclusiva para autenticar el NAS ante el gateway local y el gateway local con el NAS. Con el ajuste <code>either-shared-or-distinct-tunnel-secret</code> , la unidad TAOS intenta primero realizar una autenticación secreta compartida. Si falla, la unidad utiliza la autenticación secreta exclusiva para autenticar el túnel. Si desea obtener más información, consulte el apartado “Autenticación de túneles L2F” en la página 5-19.
Server-Endpoint	Nombre de host DNS o dirección IP decimal con puntos para el punto final del túnel. Si el ajuste es un nombre de host, la unidad TAOS ejecuta una búsqueda DNS de la dirección del host.
Enabled	Activa y desactiva los túneles establecidos al Server-Endpoint especificado.
Shared-Secret	Autenticación secreta compartida para túneles L2F. Los túneles L2F puede autenticarse con el mismo valor secreto en ambos extremos de la conexión.

### *Ejemplo de una configuración básica de L2F*

Los comandos siguientes configuran operaciones básicas de L2F con un gateway local llamado `l2f-1`:

```
admin> read l2-tunnel
L2-TUNNEL-GLOBAL read
admin> set l2f-mode = NAS
admin> set l2f-system-name = l2f-1
```

```
admin> write
L2-TUNNEL-GLOBAL written

admin> read tunnel-server l2f-1
TUNNEL-SERVER/l2f-1 read

admin> set server-endpoint = 1.1.1.1

admin> set enabled = yes

admin> set shared-secret = secret1

admin> write
TUNNEL-SERVER/l2f-1 written
```

### *Configuración de perfiles de cliente de L2F*

Cuando un cliente PPP efectúa una llamada de entrada a la unidad TAOS para iniciar un túnel al gateway L2F local, la unidad TAOS debe autenticar primero al cliente con la autenticación PPP. Aunque la unidad TAOS haya proporcionado la autenticación por contraseña para una llamada, el gateway local puede (y probablemente debería por motivos de seguridad) realizar de nuevo una autenticación. El NAS y el gateway local pueden utilizar diferentes protocolos de autenticación PPP sin restricciones.

### *Información general de los ajustes de L2F en perfiles Connection*

A continuación se muestran los parámetros de túnel L2F (aparecen con valores de ejemplo) en un perfil Connection:

```
[in CONNECTION/tunnelcx:tunnel-options]
profile-type = mobile-client
tunneling-protocol = l2f-protocol
primary-tunnel-server = l2f-1
password = "nas-pw"
```

Parámetro	Especifica
Profile-Type	Tipo de perfil del túnel. Especifique Mobile-Client para túneles L2F.
Tunneling-Protocol	Protocolo que debe utilizarse cuando se crea un túnel para este perfil. Establézcalo en l2f-protocol para pasar el tráfico a un gateway local.

<b>Parámetro</b>	<b>Especifica</b>
Primary-Tunnel-Server	Nombre de host DNS o dirección IP decimal con puntos para el punto final del gateway local. Si este parámetro especifica un nombre de host, la unidad TAOS ejecuta una búsqueda DNS de la dirección del host. Si se da soporte a la lista DNS y este parámetro especifica un nombre de host, la unidad TAOS continúa intentando conectarse a las direcciones IP de la lista hasta que se establece el túnel de forma satisfactoria, la lista no tiene más direcciones IP o la conexión supera el tiempo de espera. Para obtener información detallada, consulte el apartado “Configuración de los intentos por lista de L2TP” en la página 5-15.
Password	Autenticación secreta compartida para túneles L2F. Si el parámetro Password está configurado, la unidad TAOS lo utiliza para autenticar túneles L2F y pasa por alto el ajuste Shared-Secret en el perfil Tunnel-Server. El parámetro Password sólo se utiliza para establecer el túnel y se pasa por alto en conexiones posteriores que se agregan al túnel.

### *Información general de los ajustes de L2F en perfiles RADIUS*

RADIUS utiliza los pares atributo-valor siguientes para especificar túneles L2F:

<b>Atributo</b>	<b>Valor</b>
Tunnel-Type (64)	Protocolo de túnel que debe utilizarse. Establézcalo en L2F (2) para túneles L2F.
Tunnel-Medium-Type (65)	Medio de transmisión que se utilizará para el túnel. Actualmente sólo se da soporte a IP (1).
Tunnel-Server-Endpoint (66)	Nombre de host DNS o dirección IP decimal con puntos para el punto final del gateway local (un valor de serie). Si este atributo especifica un nombre de host, la unidad TAOS ejecuta una búsqueda DNS de la dirección del host. Si se da soporte a la lista DNS y este atributo especifica un nombre de host, la unidad TAOS continúa intentando conectarse a las direcciones IP de la lista hasta que se establece el túnel de forma satisfactoria, la lista no tiene más direcciones IP o la conexión supera el tiempo de espera. Para obtener información detallada, consulte el apartado “Configuración de los intentos por lista de L2TP” en la página 5-15.
Tunnel-Password (69)	Autenticación secreta compartida para túneles L2F. Si se utiliza la autenticación secreta exclusiva, Tunnel-Password es el secreto que utiliza el NAS para autenticarse ante el gateway local.
Tunnel-Client-Auth-ID (90)	Nombre que debe utilizarse como nombre NAS durante el establecimiento de un túnel L2F. Observe que este nombre puede ser distinto del que especifica L2F-System-Name. Si se configura, Tunnel-Client-Auth-ID prevalece sobre el parámetro L2F-System-Name.

### *Ejemplos de apertura de un túnel después de la autenticación por contraseña*

En este ejemplo, la unidad TAOS negocia la llamada PPP, incluida la autenticación por contraseña, y abre el túnel L2F. Si desea obtener información detallada acerca de la autenticación PPP, consulte el apartado “Conexiones WAN” en la página 1-1.

Los comandos siguientes crean un perfil Connection que incluye una contraseña PPP. La unidad TAOS autentica al emisor antes de activar un túnel con un gateway local en 1.1.1.1.

```
admin> read conn l2test
CONNECTION/l2test read

admin> set active = yes

admin> set encapsulation-protocol = ppp

admin> set ppp-options recv-password = localpw

admin> set tunnel-options profile-type = mobile-client

admin> set tunnel-options primary-tunnel-sever = 1.1.1.1

admin> set tunnel-options tunneling-protocol = l2f-protocol

admin> write
CONNECTION/l2test written
```

A continuación se muestra un perfil RADIUS equivalente:

```
l2test Password = "localpw"
  Service-Type = Framed,
  Framed-Protocol = PPP,
  Tunnel-Server-Endpoint = "1.1.1.1",
  Tunnel-Type = L2F,
  Tunnel-Medium-Type = IP,
  Tunnel-Password = "shared_secret"
```

## ***Protocolo de túnel punto a punto (PPTP)***

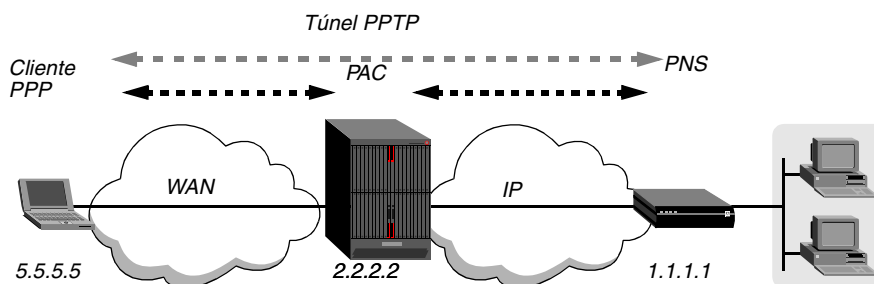
El protocolo de túnel punto a punto (PPTP) proporciona un túnel en la capa 2 de OSI (en la capa HDLC de una conexión PPP). Permite que un cliente PPP se conecte con un servidor Windows NT remoto a través de la unidad TAOS como si la conexión terminara directamente en el servidor.

Una unidad TAOS funciona solamente como concentrador de acceso PPTP (PAC), que significa que la unidad recibe llamadas PPP de entrada e inicia una conexión con el servidor NT configurado como servidor de red PPTP (PNS).

## **Componentes de un túnel PPTP**

En la Figura 5-5 se muestran los elementos de un túnel PPTP. Un cliente PPP efectúa una llamada de entrada a través de un enlace síncrono o asíncrono utilizando cualquier protocolo que pueda transportarse en una conexión PPP. La unidad TAOS responde a la llamada y la pasa al PNS. La comunicación de PAC a PNS requiere una conexión IP.

Figura 5-5. Túnel PPTP



El cliente móvil puede ser cualquier cliente PPP. Por ejemplo, puede ser una unidad Pipeline que realiza una llamada digital o un PC con Windows NT que efectúa una llamada por módem.

El enlace entre el PAC y el PNS puede ser una conexión conmutada o permanente, o puede ser un enlace Ethernet. La conexión PPP del cliente con el PNS es un enlace IP, que consiste en un enlace de control y cero o más enlaces de datos. El enlace de control se ejecuta en TCP y los enlaces de datos se ejecutan en GRE-v2.

El enlace de control transporta información que se utiliza tanto para consultar si el PNS aceptará la llamada actual como para establecer un túnel. PPTP pone en marcha un mecanismo Hello por el que el PAC y el PNS verifican que el otro interlocutor está activo. Con este fin se envían un mensaje de control aproximadamente cada minuto. Si el mensaje Hello no llega al cabo de varios minutos, el túnel y todas las conexiones de túnel se desactivan.

Los enlaces de datos transportan los datos del cliente, que se componen de tramas PPP. Existe un enlace de datos por conexión de cliente con túnel.

## Configuración de operaciones PPTP

A continuación se muestran los parámetros globales de PPTP (que aparecen con los ajustes predeterminados):

```
[in L2-TUNNEL-GLOBAL]
pptp-enabled = no
server-profile-required = no

[in TUNNEL-SERVER/" "]
server-endpoint* = ""
enabled = yes
```

Parámetro	Especifica
PPTP-Enabled	Activa y desactiva operaciones PPTP.
Server-Profile-Required	Activa y desactiva un requisito de un perfil Tunnel-Server para una conexión con el PNS. Con el ajuste Yes, PPTP debe encontrar un perfil Tunnel-Server configurado que coincida con la especificación PNS en un perfil Connection antes de poder crear un túnel con el servidor. Con el ajuste No (el valor predeterminado), PPTP busca primero un perfil Tunnel-Server coincidente y, en caso de encontrar uno, utiliza los ajustes de dicho perfil para crear (o rechazar) el túnel. Sin embargo, si no encuentra un perfil Tunnel-Server coincidente, intenta crear un túnel de todas formas.

Parámetro	Especifica
Server-Endpoint	Nombre de host DNS o dirección IP decimal con puntos para el punto final del PNS. Si se especifica un nombre de host, la unidad TAOS ejecuta una búsqueda DNS de la dirección del host.
Enabled	Activa y desactiva los túneles establecidos al Server-Endpoint especificado.

Los comandos siguientes configuran la unidad TAOS para que se conecte con un PNS llamado PPTP-1:

```
admin> read l2-tunnel
L2-TUNNEL-GLOBAL read

admin> set pptp-enabled = yes

admin> set server-profile-required = yes

admin> write
L2-TUNNEL-GLOBAL written

admin> read tunnel-server pptp-1
TUNNEL-SERVER/pptp-1 read

admin> set enabled = yes

admin> write
TUNNEL-SERVER/pptp-1 read
```

## Configuración de una conexión con el PNS

Si el PNS se encuentra en una red IP remota, la unidad TAOS requiere un perfil Connection o RADIUS de ruteo en IP para una conexión con el LNS. Puede configurar un perfil Connection de la manera siguiente:

```
admin> read conn pptp-1
CONNECTION/pptp-1 read

admin> set active = yes

admin> set dial-number = 9-1-222-555-1212

admin> set ppp send-password = pns-pw

admin> set ppp recv-password = pac-pw

admin> set ip-options remote = 1.1.1.1

admin> write
CONNECTION/pptp-1 written
```

A continuación se muestran los perfiles RADIUS equivalentes:

```
pptp-1 Password = "pac-pw"
  Service-Type = Framed-User,
  Framed-Protocol = MPP,
  Framed-IP-Address = 1.1.1.1

route-taos-1 Password = "ascend", Service-Type = Outbound-User
  Framed-Route = "1.0.0.0 1.1.1.1 1 n pptp-1-out"

pptp-1-out Password = "pac-pw" Service-Type = Outbound-User
  User-Name = "pptp-1",
```



```
Ascend-Dial-Number = "9-1-222-555-1212",  
Framed-Protocol = MPP,  
Framed-IP-Address = 1.1.1.1,  
Ascend-Send-Secret = "pns-pw"
```

Si desea obtener información detallada acerca de la configuración de interfaces WAN de IP, consulte el Capítulo 2, "Ruteo IP".

## Configuración de perfiles de cliente móvil de PPTP

Si se configura un perfil de cliente PPP para iniciar un túnel PPTP, la unidad TAOS intenta abrir un túnel tras la autenticación inicial de la conexión. Podrá abrir un túnel después de autenticar previamente la llamada (mediante la autenticación CLID o DNIS) o después de autenticar el nombre y la contraseña del emisor.

Si el PAC abre un túnel tras autenticar previamente la llamada, el PNS realiza todas las negociaciones PPP y termina la conexión PPP. Aunque el PAC haya autenticado la contraseña de la llamada, el PNS puede (y probablemente debe por motivos de seguridad) autenticarla de nuevo. El PAC y el PNS pueden utilizar diferentes protocolos de autenticación PPP sin restricciones.

**Nota:** Debido a los requisitos de protocolo de túnel, el PNS sólo puede utilizar un protocolo de autenticación PPP para autenticar una llamada del túnel. El PNS no puede utilizar otros métodos de autenticación (como CLID, DNIS o la autenticación del servidor de terminales) para llamadas de túnel.

Para que el sistema utilice CLID o DNIS para autenticar previamente una llamada, el conmutador telco debe enviar la información como parte de la llamada y la unidad TAOS debe estar configurada para extraer y utilizar dicha información.

Si desea obtener información detallada acerca de la autenticación previa y la autenticación por contraseña, consulte el Apéndice A, "Métodos de autenticación".

### *Ajustes de PPTP en perfiles Connection*

A continuación se muestran los parámetros de túnel PPTP (aparecen con valores de ejemplo) en un perfil Connection:

```
[in CONNECTION/tunnelcx:tunnel-options]  
profile-type = mobile-client  
tunneling-protocol = pptp-protocol  
primary-tunnel-server = pptp-1
```

Parámetro	Especifica
Profile-Type	Tipo de perfil del túnel. Especifique Mobile-Client para túneles PPTP.
Tunneling-Protocol	Protocolo que debe utilizarse cuando se crea un túnel para este perfil. Establézcalo en PPTP para pasar el tráfico a un PNS.
Primary-Tunnel-Server	Nombre de host DNS o dirección IP decimal con puntos para el punto final del PNS. Si se especifica un nombre de host, la unidad TAOS ejecuta una búsqueda DNS de la dirección del host.

## *Ajustes PPTP en perfiles RADIUS*

RADIUS utiliza los pares atributo-valor siguientes para especificar túneles PPTP:

<b>Atributo</b>	<b>Valor</b>
Tunnel-Type (64)	Protocolo de túnel que debe utilizarse. Establézcalo en PPTP (1) para túneles PPTP.
Tunnel-Medium-Type (65)	Medio de transmisión que se utilizará para el túnel. Actualmente, sólo se da soporte a IP (1).
Tunnel-Server-Endpoint (66)	Nombre de host DNS o dirección IP decimal con puntos para el punto final del PNS (un valor de serie). Si se especifica un nombre de host, la unidad TAOS ejecuta una búsqueda DNS de la dirección del host.

## *Ejemplos de apertura de un túnel después de autenticar previamente la llamada*

Para que la unidad TAOS pueda autenticar previamente una llamada, debe estar configurada para extraer y utilizar información CLID o DNIS. Si desea obtener información detallada, consulte el Apéndice A, “Métodos de autenticación”.

### *Ejemplos de utilización de la autenticación CLID*

Los comandos siguientes configuran un perfil que abre un túnel PPTP a un PNS (1.1.1.1) después de verificar el ID del emisor:

```
admin> read conn pptp-test
CONNECTION/pptp-test read

admin> set active = yes

admin> set clid = 555-1000

admin> set tunnel profile-type = mobile-client

admin> set tunnel primary-tunnel-sever = 1.1.1.1

admin> set tunnel tunneling-protocol = pptp

admin> write
CONNECTION/pptp-test written
```

A continuación se muestra un perfil RADIUS equivalente:

```
5551000 Password = "Ascend-CLID", Service-Type = Outbound-User
Tunnel-Type = PPTP,
Tunnel-Medium-Type = IP,
Tunnel-Server-Endpoint = "1.1.1.1"
```

### *Ejemplos de utilización de DNIS*

Los comandos siguientes configuran un perfil que abre un túnel con un PNS llamado PPTP-1 si el número marcado es 8001234567:

```
admin> read conn tunnelcx
CONNECTION/tunnelcx read

admin> set active = yes

admin> set callednumber = 8001234567
```

```
admin> set tunnel profile-type = mobile-client
admin> set tunnel tunneling-protocol = pptp
admin> set tunnel primary-tunnel-sever = pptp-1.example.com
admin> write
CONNECTION/tunnelcx
```

A continuación se muestra un perfil RADIUS equivalente:

```
8001234567 Password = "Ascend-DNIS", Service-Type = Outbound-User
Tunnel-Server-Endpoint = "pptp-1.example.com",
Tunnel-Type = PPTP,
Tunnel-Medium-Type = IP
```

### ***Ejemplos de apertura de un túnel después de la autenticación por contraseña***

En estos ejemplos, la unidad TAOS negocia la llamada PPP, incluida la autenticación por contraseña, y abre el túnel PPTP. Si desea obtener información detallada acerca de la autenticación PPP, consulte el apartado “Autenticación de sesiones de protocolo entramado” en la página A-6.

Los comandos siguientes crean un perfil Connection que incluye una contraseña PPP. La unidad TAOS autentica al emisor antes de activar el túnel PPTP con un PNS en 1.1.1.1.

```
admin> read conn pptp-test
CONNECTION/pptp-test read
admin> set active = yes
admin> set encapsulation-protocol = ppp
admin> set ppp recv-password = localpw
admin> set tunnel profile-type = mobile-client
admin> set tunnel primary-tunnel-sever = 1.1.1.1
admin> set tunnel tunneling-protocol = pptp
admin> write
CONNECTION/pptp-test written
```

A continuación se muestra un perfil RADIUS equivalente:

```
pptp-test Password = "localpw"
Service-Type = Framed-User,
Framed-Protocol = PPP,
Tunnel-Server-Endpoint = "1.1.1.1",
Tunnel-Type = PPTP,
Tunnel-Medium-Type = IP
```

## ***Resumen del conjunto de atributos de túnel***

La publicación *RADIUS Attributes for Tunnel Protocol Support Internet-Draft* define un conjunto de atributos RADIUS diseñados para dar soporte a túneles transparentes en redes de llamada de entrada, cuando un túnel se crea automáticamente sin que el usuario realice ninguna acción explícita. Para dar soporte a este tipo de túnel, el perfil del usuario incluye un conjunto de atributos primarios, que especifica todos los valores necesarios para configurar el

túnel, y conjuntos de atributos adicionales, que pueden utilizarse para establecer un túnel si el servidor primario no está disponible.

**Nota:** La utilización de identificadores de atributos de túneles y preferencias requiere el producto NavisRadius™ u otro servidor RADIUS que les ofrezca soporte.

### *Información general de identificadores y conjuntos de atributos*

Un *identificador* es un número del 1 al 31 que se puede agregar a uno o más de los atributos RADIUS que aparecen en “Atributos de túnel que se utilizan con identificadores” en la página 5-31. Los atributos que comparten el mismo identificador forman un conjunto de atributos. Los conjuntos de atributos del mismo perfil de usuario se procesan en orden numérico (el conjunto con el identificador 1 se procesa antes que el conjunto con el identificador 2 y así sucesivamente), a menos que los conjuntos se reordenen mediante el atributo Tunnel-Preference.

Un valor 0 (cero) no se considera identificador. Los conjuntos de atributos sin identificador se procesan antes que los conjuntos de atributos con identificador, a menos que en un ajuste Tunnel-Preference se especifique lo contrario.

Un identificador se separa de un par atributo-valor mediante dos puntos. A continuación se muestra un perfil de ejemplo que especifica tres conjuntos de atributos con los identificadores 1, 2 y 3:

```
joebloggs User-Password = "murphy"
    Tunnel-Type = L2TP : 1,
    Tunnel-Server-Endpoint = "1.1.1.1" : 1,
    Tunnel-Password = "lolloagic" : 1,
    Tunnel-Type = L2TP : 3,
    Tunnel-Server-Endpoint = "3.3.3.3" : 3,
    Tunnel-Password = "i82qb4ip" : 3,
    Tunnel-Type = L2F : 2,
    Tunnel-Server-Endpoint = "2.2.2.2" : 2,
    Tunnel-Password = "itsAsecret" : 2
```

En este perfil se especifica que el NAS (la unidad TAOS) primero debe intentar establecer un túnel L2TP con el LNS en 1.1.1.1. Si ese intento falla, el sistema intenta establecer un túnel L2F con un servidor en 2.2.2.2. Si este intento también falla, el sistema intenta establecer un túnel L2TP con 3.3.3.3.

En la versión actual del software, un perfil de usuario puede especificar hasta 32 conjuntos de atributos de túnel. Sin embargo, puesto que el sistema espera durante un intervalo determinado antes intentar iniciar un túnel y lo vuelve a intentar un determinado número de veces, generalmente la conexión PPP supera el tiempo de espera antes de que puedan realizarse 32 intentos de establecer un túnel. Si desea obtener un ejemplo del temporizador de túnel y ajustes de reintento, consulte el apartado “Configuración de opciones de temporizador de L2TP” en la página 5-14.

### *Protocolos de túnel soportados*

Los identificadores de atributos RADIUS pueden utilizarse para todos los protocolos de túnel soportados. El número de conjuntos de atributos utilizado es limitado en algunos protocolos, como se muestra en la Tabla 5-1.

Tabla 5-1. Protocolos de túnel y conjuntos de atributos con identificadores

Protocolo de túnel	Conjunto de atributos utilizado
L2TP	Se utilizan todos los conjuntos de atributos especificados.
L2F	Se utilizan todos los conjuntos de atributos especificados.
PPTP	Solamente se utiliza el conjunto de atributos con la prioridad más alta. La prioridad se define en el valor de Tunnel-Preference (83) o corresponde al orden de los identificadores.
ATMP	Sólo se utilizan los dos conjuntos con la prioridad más alta (del segundo conjunto de atributos, sólo se utiliza el valor de Tunnel-Server-Endpoint (67). Los demás valores pueden omitirse). La prioridad está definida en el valor de Tunnel-Preference (83) o corresponde al orden de los identificadores.

Puede utilizar la función de intento por lista DNS con los protocolos L2TP y L2F.

Todos conjuntos de atributos de un perfil deben especificar protocolos de túnel similares, sólo túneles de capa 3 (como ATMP) o túneles de capa 2 (como L2TP o L2F). Solamente puede combinar L2TP y L2F. En los ejemplos siguientes se muestran dos casos válidos:

```
JL2 User-Password = example
   Tunnel-Type = L2TP :1,
   Tunnel-Server-Endpoint = LNS-a.example.com :1,
   Tunnel-Type = L2F :2,
   Tunnel-Server-Endpoint = L2FGW.example.com :2

UL3 User-Password = example
   Tunnel-Type = ATMP :1,
   Tunnel-Server-Endpoint = HA-a.example.com :1,
   Tunnel-Server-Endpoint = HA-b.example.com :2,
   Tunnel-Password = HApasword :1,
   Tunnel-Private-Group-ID = MyHomeNet :1
```

### Atributos de túnel que se utilizan con identificadores

A continuación se muestran los pares atributo-valor de túnel pertinentes para los túneles transparentes:

Atributo	Valor
Tunnel-Type (64)	Protocolo o protocolos de túnel que se utilizarán. Solamente L2TP (3) y L2F (2) funcionan con soporte completo de atributos de túnel e identificadores actualmente.
Tunnel-Medium-Type (65)	Medio para establecer el túnel. Actualmente IP (1) es el único valor al que se da soporte.
Tunnel-Server-Endpoint (67)	Dirección IP o nombre de host del punto final del túnel. Si una búsqueda DNS devuelve varias direcciones IP, el sistema intenta establecer un túnel para cada dirección.
Tunnel-Password (69)	Autenticación secreta compartida para el túnel.

<b>Atributo</b>	<b>Valor</b>
Tunnel-Preference (83)	<p>Valor numérico de preferencia para un conjunto de atributos. Si el servidor RADIUS devuelve más de un conjunto de atributos de túnel a la unidad TAOS, el atributo Tunnel-Preference puede incluirse en un conjunto para indicar la preferencia relativa, en la que el valor de preferencia más bajo designará el conjunto preferido.</p> <p>Si no se incluye Tunnel-Preference en ninguno de los conjuntos de atributos, los conjuntos se procesan en el orden de sus números de identificador respectivos.</p> <p>Si algunos conjuntos de atributos incluyen Tunnel-Preference y otros no, aquellos que no lo incluyen serán los conjuntos de menor preferencia.</p> <p>Los conjuntos de atributos con preferencias idénticas se procesan en orden aleatorio.</p>
Tunnel-Client-Auth-ID (90)	<p>Nombre que utiliza el iniciador del túnel (el NAS) para autenticar el servidor del túnel. Actualmente sólo los túneles L2F dan soporte a este atributo. Si no se asigna un valor, se utilizará el valor L2F-System-Name de la configuración del perfil local. Para obtener información detallada, consulte el apartado “Reenvío de capa 2 (L2F)” en la página 5-18.</p>
Ascend-Tunnel-VRouter-Name (31)	<p>Nombre de un ruteador virtual (VRouter) que se utilizará para establecer el túnel L2TP o L2F. El ruteador virtual especificado debe existir en el LAC. Para obtener información detallada, consulte el apartado “Configuración de ruteadores virtuales para conexiones L2TP” en la página 6-14.</p>
Tunnel-Private-Group-ID (81)	<p>Nombre del perfil Connection que define el enlace en el que el agente local ATMP transmite los paquetes que recibe del cliente móvil. Sólo se da soporte a este atributo en túneles ATMP. El valor se utilizará solamente si el agente local se encuentra en modo de gateway. Consulte el atributo Ascend-Home-Network-Name (185) para conocer una alternativa.</p>

Actualmente la unidad TAOS pasa por alto los atributos siguientes si los recibe en una respuesta RADIUS:

- Tunnel-Assignment-ID (82)
- Tunnel-Client-Endpoint (66)

### *Ejemplo de reordenación de conjuntos utilizando Tunnel-Preference*

A continuación se muestra un perfil de ejemplo que especifica tres conjuntos de atributos, con los identificadores 1, 2 y 3 y con un valor de Tunnel-Preference que cambia el orden en el que el NAS intenta establecer un túnel para este usuario:

```
joebloggs Password = "murphy"
  Tunnel-Type = L2TP : 1,
  Tunnel-Server-Endpoint = "1.1.1.1" : 1,
  Tunnel-Password = "loloagic" : 1,
  Tunnel-Type = L2TP : 3,
```

```
Tunnel-Server-Endpoint = "3.3.3.3" : 3,  
Tunnel-Password = "i82qb4ip" : 3,  
Tunnel-Type = L2F : 2,  
Tunnel-Server-Endpoint = "2.2.2.2" : 2,  
Tunnel-Password = "itsAsecret" : 2,  
Tunnel-Preference = 100 : 2,  
Tunnel-Preference = 200 : 1
```

Con estos valores de preferencia, el NAS identifica el conjunto de atributos con el identificador 2 como el conjunto de atributos primario y primero intenta establecer un túnel L2F con un servidor en 2.2.2.2. Intenta establecer un túnel L2TP con el LNS en 1.1.1.1 sólo si falla el intento inicial. Si el segundo intento también falla, el sistema intentará establecer un túnel L2TP con 3.3.3.3.

## Encapsulación IP en IP

IP en IP constituye un modo de alterar el ruteo normal de un paquete IP encapsulándolo en otra cabecera IP. La cabecera de encapsulación especifica la dirección de un ruteador que normalmente no se seleccionaría como ruteador de salto siguiente de acuerdo con la dirección de destino real del paquete. El nodo intermedio elimina la encapsulación del paquete, que seguidamente se rutea al destino de la forma habitual. Si desea obtener información detallada acerca de cómo se lleva a cabo esta operación, consulte el documento RFC 2003, *IP Encapsulation Within IP*.

Este método para volver a rutear paquetes utilizando la encapsulación se denomina *enviar por túnel* el paquete y los *puntos finales* del túnel son el sistema que encapsula los paquetes (el agente externo) y el sistema que elimina la encapsulación de los paquetes (el servidor de túnel).

Si el agente externo recibe un paquete de entrada mayor que el tamaño de la unidad máxima de transmisión (MTU) de IP en IP, el paquete se fragmenta antes de la encapsulación. Cada fragmento se encapsula en su propia cabecera IP. El tamaño de MTU de IP en IP está fijado actualmente en 1480 bytes (1500 - 20).

En la versión actual del software, una unidad TAOS encapsula un paquete IP de entrada en otro paquete IP, con lo que se forma un paquete IP en IP. La unidad no elimina la encapsulación de un paquete IP en IP. En otras palabras, una unidad TAOS funciona solamente como agente externo y no como servidor de túnel. La dirección de origen contenida en la cabecera IP exterior del paquete IP en IP se establece en la dirección IP del agente externo y la dirección IP de destino se establece en la dirección IP del servidor de túnel. El paquete encapsulado se rutea hacia el servidor de túnel de la forma habitual.

## Ajustes de un perfil Connection

A continuación se muestran los parámetros del perfil Connection (que aparecen con ajustes de ejemplo) aplicables a la encapsulación IP en IP:

```
[in CONNECTION/p50:tunnel-options]  
profile-type = mobile-client  
tunneling-protocol = ipinip-protocol  
primary-tunnel-server = "10.2.3.4"
```

Parámetro	Especifica
Profile-Type	Tipo de perfil del túnel. Para el envío de túneles IP en IP, debe especificar Mobile-Client.
Tunneling-Protocol	Protocolo que debe utilizarse cuando se crea un túnel para este perfil. Debe especificar IPINIP-Protocol para encapsular paquetes IP dentro de IP.
Primary-Tunnel-Servidor	Nombre de host DNS o dirección IP decimal con puntos para el punto final del servidor de túnel (el destino intermedio que eliminará la encapsulación de los paquetes IP). Si especifica un nombre de host, la unidad TAOS ejecuta una búsqueda DNS de la dirección del host. Si el nombre no es válido, se pone fin a la llamada del cliente móvil con el motivo de fallo DIS_TS_ERR_HOSTNAME.

## Ajustes de un perfil RADIUS

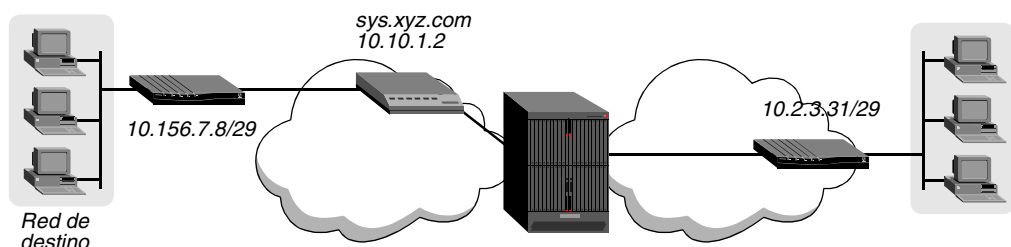
Los atributos RADIUS siguientes pueden utilizarse para indicar la encapsulación IP en IP:

Atributo	Valor
Tunnel-Type (64)	Protocolo que debe utilizarse cuando se crea un túnel para este perfil. Debe establecerse en IP en IP (7) para encapsular paquetes IP dentro de IP.
Tunnel-Server-Endpoint (67)	Nombre de host DNS o dirección IP decimal con puntos para el punto final del servidor de túnel (el destino intermedio que eliminará la encapsulación de los paquetes IP). El valor se acepta como una serie de caracteres. Si se especifica un nombre de host, la unidad TAOS ejecuta una búsqueda DNS de la dirección del host. Si el nombre no es válido, la llamada del cliente móvil finaliza con el motivo de fallo DIS_TS_ERR_HOSTNAME.

## Ejemplos de una conexión IP en IP

La unidad Pipeline que se encuentra a la derecha en la Figura 5-6 efectúa una llamada de entrada a la unidad TAOS para iniciar una sesión en la red de destino. Una vez establecida la conexión, la unidad TAOS encapsula los paquetes IP de esta corriente de datos y los reenvía al router CPE en 10.10.1.2. Este router elimina la encapsulación de los paquetes y los reenvía al destino real.

*Figura 5-6. Túnel IP en IP*





A continuación se muestran los comandos introducidos para configurar un perfil local y las respuestas del sistema:

```
admin> read conn p50
CONNECTION/p50 read
admin> set active = yes
admin> set encapsulation-protocol = ppp
admin> set ip remote-address = 10.2.3.31/29
admin> set ppp recv-password = localpw
admin> set tunnel profile-type = mobile-client
admin> set tunnel tunneling-protocol = ipinip-protocol
admin> set tunnel primary-tunnel-server = sys.xyz.com
admin> write
CONNECTION/p50 read
```

A continuación se muestra un perfil RADIUS equivalente:

```
p50 Password = "localpw"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Framed-IP-Address = 10.2.3.31
    Framed-IP-Netmask = 255.255.255.248
    Tunnel-Type = IP-in-IP,
    Tunnel-Server-Endpoint = "sys.xyz.com"
```



## Ruteadores virtuales

Configuración de ruteadores virtuales .....	6-1
Creación de un ruteador virtual .....	6-3

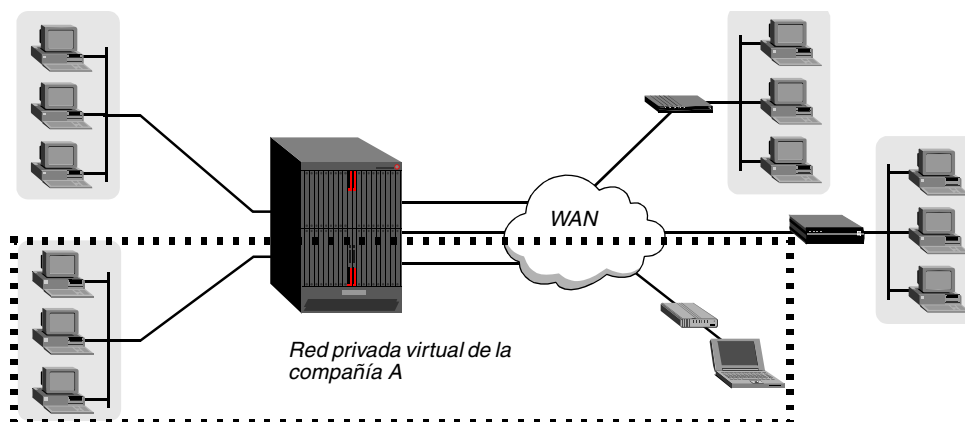
### Configuración de ruteadores virtuales

Un ruteador virtual (también denominado *VRouter*) es un agrupamiento de interfaces en la unidad TAOS. Cada ruteador virtual tiene su propia tabla de ruteo asociada, su tabla ARP, su caché de ruta y sus agrupaciones de direcciones, y mantiene sus propias estadísticas de paquete y de ruteo.

Si no configura ningún ruteador virtual, el ruteador de TAOS funciona exactamente del mismo modo que en las versiones anteriores del software. Cuando se especifican uno o más ruteadores virtuales, el ruteador principal funciona como el ruteador virtual global. Todas las interfaces que no están agrupadas de manera explícita con un ruteador virtual se agrupan con el ruteador virtual global.

En la Figura 6-1 se muestra una unidad TAOS con un ruteador virtual funcionando para la compañía A. Un ruteador virtual agrupa y gestiona las interfaces relacionadas con la compañía A, creando así una red privada virtual para dicha compañía. Las interfaces WAN de la compañía A pueden conectarse a una unidad TAOS local, que puede encontrarse en una red pública, para acceder a las LAN privadas de la compañía A.

Figura 6-1. Ruteo IP virtual



## Repercusión de los ruteadores virtuales en la tabla de ruteo

Cuando los ruteadores virtuales no están definidos, el ruteador de la unidad TAOS mantiene una única tabla de ruteo IP que permite al ruteador acceder a cualquiera de sus muchas interfaces. En esta situación, cada interfaz identificada por el sistema requiere una dirección exclusiva.

Con los ruteadores virtuales, las direcciones deben ser exclusivas dentro del dominio de ruteo del ruteador virtual, pero no necesariamente dentro de la unidad TAOS. Dado que cada ruteador virtual mantiene su propia tabla de ruteo y dado que sólo tiene conocimiento de las interfaces que especifican de manera explícita el mismo ruteador virtual, no es imprescindible que las redes privadas mantengan espacios de direcciones exclusivos.

## Repercusión de los ruteadores virtuales en los comandos de red

Los comandos siguientes dan soporte al ruteo virtual. Si no se especifica ningún nombre de ruteador virtual en la línea de comandos, se presupone que se selecciona el ruteador virtual global. Si se especifica el nombre de un ruteador virtual, los comandos realizan su función habitual, pero sólo se aplican al ruteador virtual especificado:

Comando	Uso con argumentos optativos de ruteador virtual
Netstat	<code>netstat [VRoutername] -options [params]</code>
IProute	<code>iproute add [-r vRouterName] destination/size gateway [pref] [metric]</code> <code>iproute delete [-r vRouterName] destination/size [gateway]</code>
Traceroute	<code>traceroute [-n] [-v] [-m max_ttl] [-p port] [-q nque-ries] [-w waittime] [-r vRouter] [-s src_addr] host-name [datasize]</code>
IPcache	<code>ipcache [-r vRouterName] [debug] [cache]</code>
Ifmgr	<code>ifmgr -r [vRouterName] -option</code> -d: Visualiza entradas de tabla de interfaz. -d ifNum: Muestra detalles de una entrada de tabla i/f dada. -t: Activa y desactiva la visualización de la depuración. <code>ifmgr [up down] [ifNum ifName]</code>
ARPTable	<code>arptable [vRouter] [[-a hostname MAC_address]   [-d hostname]   [-f]]</code> [vRouter]: Ruteador virtual para el que es aplicable este comando ARP [-a hostname MAC_address]: Agrega entrada de nombre de host a la tabla ARP con MAC_address [-d hostname]: Borra nombre de host de una tabla ARP [-f]: Borra una caché ARP completa
IP-Pools	<code>ip-pools [vRouterName]</code>
Ping	<code>ping [-q   -v] [-i sec   -I msec] [-s packet-size] [-r vRouter] [-x source_address] host-name</code>
Telnet	<code>telnet [-a   -b   -t] [-v VRouterName] [-l[e]   -r[e]] host-name [port-number]</code>

## Limitaciones actuales

Actualmente la gestión SNMP no muestra información sobre la unidad TAOS para cada ruteador virtual. Los errores y los eventos no se registran para cada ruteador virtual. El host Syslog definido en el perfil Log del sistema debe ser accesible para el ruteador virtual principal.

Actualmente ATMP presenta paquetes de entrada sólo al ruteador virtual principal. Además, los servidores definidos en los perfiles siguientes deben ser accesibles para el ruteador virtual principal:

- Debug
- Trap
- External-Auth
- IP-Global (para SNTP y difusión múltiple)
- Call-Logging
- SNMP
- SS7-Gateway
- Stacking
- Transaction-Server
- VoIP

## Creación de un ruteador virtual

Cuando al menos hay un perfil VRouter configurado, el parámetro System-IP-Address y el parámetro Global-VRouter del perfil IP-Global son aplicables al ruteador virtual global. Todas las interfaces que no están explícitamente asignadas a otro ruteador virtual se agrupan con el ruteador virtual global.

Por cada ruteador virtual del sistema, se crea una instancia de RIP para procesar las rutas. La nueva instancia de RIP envía y recibe paquetes de actualización sólo en las interfaces asociadas con su ruteador virtual particular y sólo manipula la tabla de ruteo de dicho ruteador. Siempre se crea una instancia predeterminada de RIP para el ruteador virtual global.

Al crear un ruteador virtual, la nueva instancia de RIP envía y recibe paquetes sólo en las interfaces asociadas con dicho ruteador virtual y únicamente manipula la tabla de ruteo de dicho ruteador. Todos los parámetros relacionados con RIP de un perfil VRouter utilizan ajustes predeterminados que se recomiendan para la mayoría de los entornos.

## Ajustes de un perfil VRouter

Un perfil VRouter contiene los siguientes parámetros (que aparecen con los valores predeterminados):

```
[in VROUTER/""]
name* = ""
vrouter-ip-address = 0.0.0.0
pool-base-address = [ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0+
assign-count = [ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 +
```

```
pool-name = [ "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "+
pool-summary = no
rip-policy = Poison-Rvrs
summarize-rip-routes = no
rip-trigger = yes
```

Parámetro	Especifica
Name	Nombre exclusivo del ruteador virtual, de un máximo de 15 caracteres. Las interfaces que pertenecen al ruteador virtual se agrupan especificando este nombre en el perfil IP-Interface o Connection.
VRouter-IP-Address	Dirección IP del sistema para el ruteador virtual.
Pool-Base-Address	Agrupaciones de direcciones IP para el ruteador virtual. Los
Assign-Count	parámetros funcionan exactamente como los parámetros del mismo
Pool-Name	nombre del perfil IP-Global, con la única diferencia de que son
Pool-Summary	exclusivos para un ruteador virtual. Si las agrupaciones de direcciones no se especifican en un perfil VRouter, los ruteadores virtuales pueden compartir las agrupaciones de direcciones definidas en el perfil IP-Global.
RIP-Policy	Criterio para enviar paquetes de actualización que incluyen rutas recibidas en la misma interfaz. Si desea obtener información detallada, consulte “Política RIP para propagar las actualizaciones de vuelta a la subred de origen” en la página 2-46.
Summarize-RIP-Routes	Si el ruteador virtual está ejecutando RIP-v1, el parámetro Summarize-RIP-Routes especifica si hay que resumir la información de subred en los anuncios. Si el ruteador virtual resume las rutas RIP, anuncia una ruta a todas las subredes de una red de la misma clase. Por ejemplo, la ruta a 200.5.8.13/28 (una dirección de clase C) se anunciaría como una ruta a 200.5.8.0. Cuando el ruteador virtual no resume la información, anuncia cada ruta en su tabla de ruteo tal cual.
RIP-Trigger	Activa y desactiva el accionamiento de RIP. Con el ajuste Yes (el valor predeterminado), las actualizaciones de RIP engloban sólo las rutas modificadas. Si desea obtener información detallada, consulte “Activación de RIP” en la página 2-47.

### Ejemplo de definición de un ruteador virtual

Los comandos siguientes crean un ruteador virtual para la compañía A:

```
admin> new vrrouter corpa
VROUTER/corpa read

admin> list
[in VROUTER/corpa (new)]
name* = ""
vrrouter-ip-address = 0.0.0.0
pool-base-address = [ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0+
assign-count = [ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 +
pool-name = [ "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" +
pool-summary = no
rip-policy = Poison-Rvrs
summarize-rip-routes = no
rip-trigger = yes
```

```
admin> set vrouter-ip-addr = 130.200.200.100  
admin> write  
VROUTER/corpa written
```

### *Visualización de las tablas de interfaces y de ruteo del ruteador virtual*

El nuevo ruteador virtual definido para la compañía A en “Ejemplo de definición de un ruteador virtual” mantiene ahora las siguientes tablas mínimas de interfaces y de ruteo:

```
admin> netstat corpa -rn  
Destination      Gateway          IF              Flg    Pref Met      Use      Age  
127.0.0.0/8      -               bh0_corpa      CP      0    0        0      8172  
127.0.0.1/32     -               local          CP      0    0        0      8172  
127.0.0.2/32     -               rj0_corpa      CP      0    0        0      8172  
  
admin> netstat corpa -in  
Name      MTU   Net/Dest      Address      Ipkts    Ierr Opkts  Oerr  
vr0_corpa 1500  130.2.2.2/32  130.2.2.2      0        0      0      0  
lo0_corpa 1500  127.0.0.1/32  127.0.0.1      0        0      0      0  
local     65535 127.0.0.1/32  127.0.0.1      0        0      0      0  
rj0_corpa 1500  127.0.0.2/32  127.0.0.2      0        0      0      0  
bh0_corpa 1500  127.0.0.3/32  127.0.0.3      0        0      0      0
```

### *Visualización de las estadísticas del ruteador virtual*

El ruteador virtual también mantiene sus propias estadísticas IP, TCP, UDP e ICMP. Por ejemplo:

```
admin> netstat corpa -s  
udp:  
    1442 packets received  
    0 packets received with no ports  
    0 packets received with errors  
    0 packets dropped  
    32 packets transmitted  
  
tcp:  
    0 active opens  
    1 passive opens  
    0 connect attempts failed  
    0 connections were reset  
    1 connections currently established  
    858 segments received  
    0 segments received out of order  
    548 segments transmitted  
    0 segments retransmitted  
    0 active closes  
    0 passive closes  
    0 disconnects while awaiting retransmission  
  
icmp:  
    31 packets received  
    0 packets received with errors  
Input histogram:  
    30 echo requests  
    1 netmask requests  
  
    31 packets transmitted
```

```
0 packets not transmitted due to lack of resources
Output histogram:
    30 echo replies
    1 netmask replies

ip:
0 packets received
0 packets received with header errors
0 packets received with address errors
0 packets received forwarded
0 packets received with unknown protocols
0 inbound packets discarded
0 packets delivered to upper layers
0 transmit requests
0 discarded transmit packets
0 outbound packets with no route
0 reassemblies timeout
0 reassemblies required
0 reassemblies succeeded
0 reassemblies failed
0 fragmentation succeeded
0 fragmentation failed
0 fragmented packets created
0 route discards due to lack of memory
64 default ttl

igmp:
0 packets received
0 bad checksum packets received
0 bad version packets received
0 query packets received
0 leave packets received
0 packets transmitted
0 query packets sent
0 resonance packets sent
0 leave packets sent

mcast:
0 packets received
0 packets forwarded
0 packets in error
0 packets dropped
0 packets transmitted
```

**Nota:** No se da soporte a la difusión múltiple de IP para cada ruteador virtual, por lo que las estadísticas IGMP y MCast se refieren sólo al ruteador virtual global.

### *Definición de agrupaciones de direcciones para un ruteador virtual*

Los siguientes comandos definen una agrupación de direcciones para el ruteador virtual de la compañía A definido en “Ejemplo de definición de un ruteador virtual” en la página 6-4:

```
admin> read vrouter corpa
VROUTER/corpa read

admin> set pool-base 1 = 130.100.100.128

admin> set assign-count 1 = 127

admin> write
VROUTER/corpa written
```



A continuación se muestra una definición de agrupación RADIUS equivalente:

```
pools-taos01 Password = "ascend", Service-Type = Outbound-User  
Ascend-IP-Pool-Definition = "1 130.100.100.128 127 corpa"
```

El ruteador virtual de la compañía A mantiene ahora la agrupación de direcciones siguiente:

```
admin> ip-pools corpa
```

Pool#	Base	Count	InUse
1	130.100.100.128	127	0

```
Number of remaining allocated addresses: 0
```

**Nota:** El atributo Ascend-IP-Pool-Definition da soporte a un nombre de ruteador virtual como el último elemento de sintaxis en una definición de agrupación. El valor de Ascend-IP-Pool-Definition utiliza la sintaxis siguiente:

```
"pool-num base-addr assign-count [vrouter-name]"
```

Para obtener más información acerca de las agrupaciones de direcciones, consulte “Configuración y utilización de agrupaciones de direcciones” en la página 2-68. El proceso para definir las agrupaciones de direcciones de un ruteador virtual es el mismo que el descrito en dicha sección.

## Asignación de interfaces a un ruteador virtual

Para asignar la pertenencia de una interfaz a un ruteador virtual, especifique un nombre de ruteador virtual en el perfil de la interfaz. Además de PPP y otras conexiones entramadas, las conexiones TCP-Clear también se gestionan para cada ruteador virtual. Si un perfil Connection o RADIUS está asociado a un ruteador virtual y configurado para TCP-Clear, el sistema sólo localiza el host especificado en la tabla de ruteo del ruteador virtual.

### *Ajustes de los perfiles locales*

Para asignar la pertenencia de una interfaz a un ruteador virtual en los perfiles locales, defina el parámetro VRouter. Por ejemplo:

```
[in IP-INTERFACE/{ { shelf-1 slot-5 5 } 0 } ]  
vrouter = corpa  
  
[in CONNECTION/corpa-client]  
vrouter = corpa
```

Parámetro	Especifica
VRouter	Nombre de un ruteador virtual definido. Al especificar el nombre de ruteador virtual, se agrupa la interfaz con dicho ruteador. El valor nulo predeterminado especifica el ruteador virtual global.

## *Ajustes de los perfiles RADIUS*

RADIUS utiliza el par atributo-valor siguiente para dar soporte al uso de un ruteador virtual:

Atributo	Valor
Ascend-VRouter-Name (102)	Nombre de un ruteador virtual definido. Al especificar el nombre de ruteador virtual, se agrupa la interfaz con dicho ruteador. El valor nulo predeterminado especifica el ruteador virtual global.

## *Ejemplos de cómo asignar la pertenencia de una interfaz a un ruteador virtual*

Los comandos siguientes agrupan tres interfaces WAN con el ruteador virtual `corpa`:

```
admin> new connection dialin-1
CONNECTION/dialin-1 read
admin> set active = yes
admin> set vrouter = corpa
admin> set ip-options remote-address = 10.1.1.1/24
admin> write
CONNECTION/dialin-1 written
admin> new connection dialin-2
CONNECTION/dialin-2 read
admin> set active = yes
admin> set vrouter = corpa
admin> set ip-options remote-address = 11.1.1.1/24
admin> write
CONNECTION/dialin-2 written
admin> new connection dialin-3
CONNECTION/dialin-3 read
admin> set active = yes
admin> set vrouter = corpa
admin> set ip-options remote-address = 12.1.1.1/24
admin> write
CONNECTION/dialin-3 written
```

A continuación se muestran los ajustes equivalentes de perfiles RADIUS:

```
dialin-1 Password = "pwd3"
  Service-Type = Framed-User,
  Framed-Protocol = MPP,
  Framed-IP-Address = 10.1.1.1,
  Framed-IP-Netmask = 255.255.255.0,
  Ascend-Vrouter-Name = "corpa"

dialin-2 Password = "pwd2"
  Service-Type = Framed-User,
  Framed-Protocol = MPP,
  Framed-IP-Address = 11.1.1.1,
  Framed-IP-Netmask = 255.255.255.0,
  Ascend-Vrouter-Name = "corpa"
```

```
dialin-3 Password = "pwd1"
Service-Type = Framed-User,
Framed-Protocol = MPP,
Framed-IP-Address = 12.1.1.1,
Framed-IP-Netmask = 255.255.255.0,
Ascend-Vrouter-Name = "corpa"
```

### *Visualización de interfaces asignadas en las tablas del ruteador virtual*

Tras la asignación de interfaces, según se describe en “Ejemplos de cómo asignar la pertenencia de una interfaz a un ruteador virtual” en la página 6-8, las nuevas interfaces aparecen en las tablas de interfaces y de ruteo del ruteador virtual cuando se activan las interfaces. Por ejemplo:

```
admin> netstat corpa -rn
Destination      Gateway          IF    Flg    Pref  Met  Use  Age
10.0.0.0/24      10.1.1.1        wan30  SG     120   7    0    215
10.1.1.1/32      10.1.1.1        wan30  S      120   7    1    215
11.0.0.0/24      11.1.1.1        wan31  SG     120   7    0    215
11.1.1.1/32      11.1.1.1        wan31  S      120   7    1    215
12.0.0.0/24      12.1.1.1        wan32  SG     120   7    0    215
12.1.1.1/32      12.1.1.1        wan32  S      120   7    1    215
127.0.0.0/8      -               bh0_corpa  CP     0    0    0    1193
127.0.0.1/32     -               local    CP     0    0    0    1193
127.0.0.2/32     -               rj0_corpa  CP     0    0    0    1193

admin> netstat corpa -in
Name      MTU   Net/Dest      Address      Ipkts    Ierr  Opkts  Oerr
vr0_corpa 1500  130.2.2.2/32  130.2.2.2    0        0      0      0
lo0_corpa 1500  127.0.0.1/32  127.0.0.1    0        0      0      0
local      65535 127.0.0.1/32  127.0.0.1    0        0      0      0
rj0_corpa 1500  127.0.0.2/32  127.0.0.2    0        0      0      0
bh0_corpa 1500  127.0.0.3/32  127.0.0.3    0        0      0      0
wan30      1500  10.1.1.1      130.2.2.2    0        0      0      0
wan31      1500  11.1.1.1      130.2.2.2    0        0      0      0
wan32      1500  12.1.1.1      130.2.2.2    0        0      0      0
```

## **Definición de rutas estáticas de ruteador virtual**

Se especifica una ruta estática asociada a un ruteador virtual por una de las siguientes razones:

- Para definir una ruta para cada ruteador virtual.
- Para especificar una ruta entre ruteadores virtuales.

### *Ajustes de un perfil IP-Route*

A continuación se muestran los parámetros relacionados con los ruteadores virtuales (que aparecen con los valores predeterminados) de los perfiles IP-Route:

```
[in IP-ROUTE/""]  
vrouter = ""  
inter-vrouter = ""
```

Parámetro	Especifica
VRouter	Nombre del ruteador virtual que poseerá esta ruta. La ruta formará parte de la tabla de ruteo de dicho ruteador. Si no se especifica ningún nombre (el valor predeterminado), se presupone que se selecciona el ruteador virtual global.
Inter-VRouter	Nombre del ruteador virtual que debe utilizarse como siguiente salto de la ruta. Los paquetes destinados a la dirección de destino de la ruta se envían al ruteador virtual especificado, que consulta su propia tabla de ruteo para seguir ruteando los paquetes. El parámetro Gateway-Address debe establecerse en la dirección cero para que este parámetro sea aplicable.

### *Ajustes de los perfiles RADIUS*

El valor del atributo Framed-Route (22) puede especificar un nombre de ruteador virtual con la sintaxis siguiente:

```
"dest-addr [/prefix] gateway-addr metric [private] [profile]  
[preference] [vrouter-name]"
```

**Nota:** Los campos del valor del atributo Framed-Route son posicionales. A excepción de la especificación optativa de longitud de prefijo, si se especifica cualquiera de los campos optativos, también deben especificarse los campos optativos situados a la izquierda de dicho ajuste.

### *Ejemplos de definición de una ruta para cada ruteador virtual*

A continuación se muestra un ejemplo de cómo definir una ruta estática para la compañía B. Esta ruta se encuentra dentro del dominio del ruteador virtual de la compañía A (el ruteador virtual denominado *corpa* poseerá esta ruta).

```
admin> new ip-route corpa-east  
IP-ROUTE/corpa-east read  
  
admin> set dest = 10.5.6.7/28  
  
admin> set gateway = 10.1.1.1  
  
admin> set vrouter = corpa  
  
admin> write  
IP-ROUTE/corpa-east written
```

A continuación se muestra un perfil RADIUS equivalente:

```
route-taos-1 Password = "ascend", Service-Type = Outbound-User  
Framed-Route = "10.5.6.7/28 10.1.1.1 7 n corpa-out 60 corpa"
```

### *Visualización de la ruta estática en la tabla del ruteador virtual*

La salida de ejemplo siguiente muestra la nueva ruta estática agregada a la tabla de ruteo del ruteador virtual de la compañía A en el apartado “Ejemplos de definición de una ruta para cada ruteador virtual”:

```
admin> netstat corpa -rn
Destination      Gateway          IF    Flg    Pref  Met  Use  Age
10.1.1.0/24      10.1.1.1        wan30  SG     120   7    0    9
10.1.1.1/32      10.1.1.1        wan30  S      120   7    2    9
10.5.6.0/28      10.1.1.1        wan30  SG     60   8    0    9
11.1.1.0/24      11.1.1.1        wan31  SG     120   7    0    9
11.1.1.1/32      11.1.1.1        wan31  S      120   7    1    9
12.1.1.0/24      12.1.1.1        wan32  SG     120   7    0    9
12.1.1.1/32      12.1.1.1        wan32  S      120   7    1    9
127.0.0.0/8      -               bh0_corpa CP      0    0    0  2274
127.0.0.1/32     -               local   CP      0    0    0  2274
127.0.0.2/32     -               rj0_corpa CP      0    0    0  2274
```

### *Especificación de una ruta entre ruteadores virtuales*

En el ejemplo siguiente, la ruta estática especifica el ruteador virtual de la compañía A como siguiente salto de la ruta. Todos los paquetes destinados a la red de destino especificada se envían al ruteador virtual especificado para una decisión de ruteo.

```
admin> new ip-route corpb
IP-ROUTE/corpb read
admin> set dest-address = 11.0.0.0/24
admin> set inter-vrouter = corpa
admin> write
IP-ROUTE/corpb written
```

A continuación se muestra un perfil de ruta RADIUS equivalente:

```
route-taos-1 Password = "ascend", Service-Type = Outbound-User
  Framed-Route = "11.0.0.0/28 0.0.0.0 corpa"
```

### *Visualización de la ruta entre ruteadores virtuales en la tabla global*

En el ejemplo siguiente, la ruta se ha agregado a la tabla de ruteo del ruteador virtual global, no a la del ruteador virtual de la compañía A.

```
admin> netstat -rn
Destination      Gateway          IF    Flg    Pref  Met  Use  Age
0.0.0.0/0        10.1.6.1        ie0    SGP    60   1    59    4
11.0.0.0/24      -               vr0_corpa S      60   8    0    4
20.0.0.0/8       -               ie1-12-1 C      0    0    12  234
20.1.1.2/32      -               local   CP      0    0    0  2347
127.0.0.0/8      -               bh0     CP      0    0    0  2378
127.0.0.1/32     -               local   CP      0    0    0  2378
127.0.0.2/32     -               rj0     CP      0    0    0  2378
130.1.1.1/32     -               sip0    C      0    0    0  2378
130.1.1.252/30   -               rj0     C      0    0    0  2378
100.1.6.0/24     100.1.6.221    wanabe  SG     60   1    0    4
101.1.6.0/24     -               ie0     C      0    0    2531 2378
101.1.6.234/32   -               local   CP      0    0    4152 2378
```

## Ruteadores virtuales

### Creación de un ruteador virtual

---

224.0.0.0/4	-	mcast	CP	0	0	0	2378
224.0.0.1/32	-	local	CP	0	0	0	2378
224.0.0.2/32	-	local	CP	0	0	0	2378
224.0.0.5/32	-	local	CP	0	0	732	2378
224.0.0.6/32	-	local	CP	0	0	0	2378
255.255.255.255/32	-	ie0	P	0	0	422	2378

## Supresión de un ruteador virtual

Al suprimir un perfil VRouter se borra el ruteador virtual. Por ejemplo:

```
admin> delete vrouter corpa
```

Lucent recomienda reiniciar el sistema después de suprimir un ruteador virtual con conexiones activas. Si no es posible reiniciar el sistema, se recomienda que, antes de suprimir el ruteador virtual, se anulen manualmente sus conexiones activas y, a continuación, se modifiquen los perfiles locales Connection, IP-Interface e IP-Route que apuntan al ruteador virtual para que, en su lugar, apunten al ruteador virtual global o a otro ruteador virtual existente.

## Configuración de servidores de nombres de dominio de ruteador virtual

La configuración DNS del ruteador virtual incluye ajustes para servidores DNS primarios y secundarios, servidores de nombres de dominio y servidores DNS de cliente. Los ajustes dirigen las conexiones que pertenecen al ruteador virtual hacia un servicio DNS concreto. Para segmentar por completo la información de DNS del ruteador virtual de cualquier otro host, puede configurar y gestionar la información de DNS por separado para cada ruteador virtual. Las direcciones configuradas para los servidores DNS de cliente se muestran a los usuarios de llamada de entrada durante la negociación del protocolo de control IP (IPCP).

Si la información de DNS no se encuentra en el perfil VRouter, el sistema utiliza la información DNS del perfil IP-Global. La lista DNS y la tabla DNS local mantenida en la RAM son configuraciones DNS de todo el sistema a las que no se da soporte por separado para cada ruteador virtual.

### Información general sobre los ajustes DNS del ruteador virtual

A continuación se muestran los parámetros DNS específicos del ruteador virtual (con los ajustes predeterminados):

```
[in VROUTER/""]
domain-name = ""
sec-domain-name = ""
dns-primary-server = 0.0.0.0
dns-secondary-server = 0.0.0.0
client-primary-dns-server = 0.0.0.0
client-secondary-dns-server = 0.0.0.0
allow-as-client-dns-info = True
```

Parámetro	Especifica
Domain-Name	Nombre de dominio primario (con un máximo de 63 caracteres) que debe utilizarse en las búsquedas DNS de este ruteador virtual. La unidad TAOS agrega este nombre de dominio a los nombres de host al realizar búsquedas.
Sec-Domain-Name	Nombre de dominio secundario que debe utilizarse en las búsquedas DNS si el nombre de host no se encuentra en el dominio primario.
DNS-Primary-Server	Dirección del servidor DNS local primario que debe utilizarse en las búsquedas de este ruteador virtual.
DNS-Secondary-Server	Dirección del servidor DNS local secundario que debe utilizarse en las búsquedas de este ruteador virtual. Sólo se utiliza si no se encuentra el servidor primario.
Client-DNS-Primary-Server	Dirección de un servidor DNS de cliente para los clientes de llamada de entrada de este ruteador virtual.
Client-DNS-Secondary-Server	Dirección de un servidor DNS secundario para los clientes de llamada de entrada de este ruteador virtual.
Allow-As-Client-DNS-Info	Activa y desactiva el uso de información DNS (local) principal si no se encuentran los servidores DNS de cliente. Para aislar información de red local para este ruteador virtual, establézcalo en false.

### *Ejemplo de una configuración DNS clásica de ruteador virtual*

Los comandos siguientes especifican un nombre de dominio primario y secundario para búsquedas DNS de un ruteador virtual denominado xyz:

```
admin> read vrouter xyz
VROUTER/xyz read
admin> set domain-name = xyz.com
admin> set sec-domain-name = eng.xyz.com
admin> write
VROUTER/xyz written
```

Si una búsqueda falla en el primer dominio, el ruteador lo intenta de nuevo con el nombre de dominio secundario. Para activar la unidad TAOS a fin de que utilice DNS para buscar direcciones, especifique direcciones de servidor DNS, como se muestra en el ejemplo siguiente:

```
admin> read vrouter xyz
VROUTER/xyz read
admin> set dns-primary-server = 1.2.2.2
admin> set dns-secondary-server = 1.3.3.3
admin> write
VROUTER/xyz written
```

Si el servidor primario no está disponible, la unidad TAOS intenta realizar una búsqueda en el servidor secundario. Los comandos siguientes configuran un servidor DNS de cliente para este ruteador virtual.

```
admin> read vrouter xyz
VROUTER/xyz read

admin> set client-dns-primary-server = 1.2.2.2
admin> set client-dns-secondary-server = 1.2.2.96
admin> set allow-as-client-dns-info = false
admin> write
VROUTER/xyz written
```

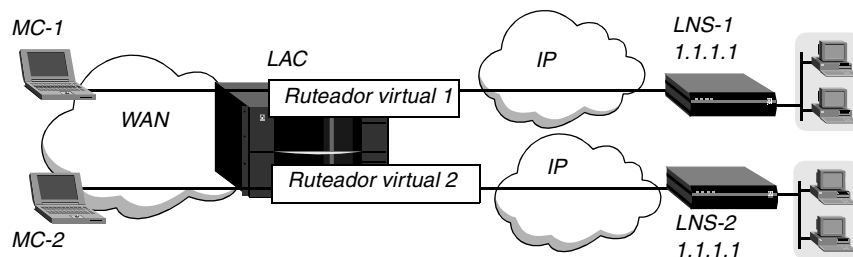
Sólo se accede al servidor secundario si el primario es inaccesible. Si no se puede acceder a ninguno de estos servidores DNS de cliente, la unidad TAOS no permite al cliente acceder a servidores DNS locales. Para obtener información sobre comandos administrativos para DNS de ruteador virtual, consulte la publicación *Guía de administración de APX 8000/MAX TNT/DSLNT*.

## Configuración de ruteadores virtuales para conexiones L2TP

En versiones anteriores, los túneles L2TP sólo utilizaban el ruteador virtual principal. En la versión actual del software, puede construir túneles L2TP en ruteadores virtuales específicos. Los paquetes L2TP (canal de control y datos encapsulados) se envían utilizando el ruteador virtual configurado para dicho túnel.

Dado que cada ruteador virtual mantiene su propia tabla de ruteo y sólo tiene conocimiento de aquellas interfaces que especifican explícitamente el mismo ruteador, esta característica permite al sistema separar el tráfico para diferentes sistemas LNS. Por ejemplo, en la Figura 6-2 se muestran dos clientes de marcación: MC-1 y MC-2. Cada cliente establece un túnel a un LNS diferente, pero los dos sistemas LNS tienen la dirección IP 1.1.1.1. Dado que los túneles están contruidos en ruteadores virtuales independientes, el tráfico se mantiene separado y se dirige al punto final de servidor adecuado.

Figura 6-2. Túneles L2TP contruidos en ruteadores virtuales separados



Observe que la unidad TAOS debe dedicar una interfaz IP a cada ruteador virtual. A continuación se muestran los parámetros, con valores de ejemplo, para dedicar una interfaz WAN de IP o Ethernet a un ruteador virtual:

```
[in IP-INTERFACE/{ { shelf-1 slot-3 1 } 0 }]
vrouter = VRouter-1

[in CONNECTION/LNS-2]
vrouter = VRouter-2
```



Para obtener información detallada acerca de L2TP, consulte “Túneles L2TP, PPTP e IP en IP” en la página 5-1.

### *Establecimiento del perfil Connection*

A continuación se muestra el parámetro (con el valor predeterminado) para especificar un nombre de ruteador virtual:

```
[in CONNECTION/MC-1:tunnel-options]
vrouter = ""
```

Parámetro	Especifica
VRouter	Nombre de un ruteador virtual que se utiliza para establecer el túnel L2TP. El ruteador virtual especificado debe existir en el LAC. Con el valor nulo predeterminado, se utiliza el ruteador virtual global.

Por ejemplo, los comandos siguientes configuran un perfil de cliente móvil para una sesión L2TP que pertenece a un ruteador virtual denominado VRouter-1:

```
admin> new connection MC-1
CONNECTION/MC-1 read
admin> set active = yes
admin> set encapsulation-protocol = ppp
admin> set ppp-options recv-password = localpw
admin> set tunnel-options profile-type = mobile-client
admin> set tunnel-options primary-tunnel-server = 1.1.1.1
admin> set tunnel-options tunneling-protocol = l2tp
admin> set tunnel-options vrouter = VRouter-1
admin> write
CONNECTION/MC-1 written
```

Con este perfil de ejemplo, la unidad TAOS autentica el emisor antes de construir un túnel hacia el LNS en 1.1.1.1 en el ruteador virtual especificado.

### *Establecimiento del perfil RADIUS*

RADIUS utiliza el par atributo-valor siguiente para especificar un nombre de ruteador virtual:

Atributo RADIUS	Valor
Ascend-Tunnel-VRouter-Name (31)	Nombre de un ruteador virtual que se utiliza para establecer el túnel L2F o L2TP. El ruteador virtual especificado debe existir en el LAC. Con el valor nulo predeterminado, se utiliza el ruteador virtual global. Este atributo da soporte al etiquetado. Se utilizan todos los conjuntos de atributos especificados.

Por ejemplo, el perfil de cliente móvil siguiente especifica una sesión L2TP que pertenece a un ruteador virtual denominado VRouter-2:

```
MC-2 Password = "localpw"  
    Service-Type = Framed-User,  
    Framed-Protocol = PPP,  
    Tunnel-Server-Endpoint = "1.1.1.1",  
    Tunnel-Type = L2TP,  
    Ascend-Tunnel-VRouter-Name = "VRouter-2"
```

# Ruteo IPX

# 7

Ruteo IPX en la WAN .....	7-1
Configuración del perfil IPX-Global .....	7-4
Configuración de interfaces IPX de LAN .....	7-5
Configuración de interfaces IPX de WAN .....	7-7
Configuración de rutas IPX estáticas .....	7-13
Definición y aplicación de filtros SAP IPX .....	7-17

## ***Ruteo IPX en la WAN***

Una unidad TAOS configurada para el ruteo IPX permite que los clientes NetWare y las redes Novell distribuidas utilicen los servicios NetWare en la WAN. Lucent ha optimizado el ruteo IPX para la WAN. Esta optimización ha requerido la realización de algunas modificaciones en el funcionamiento de IPX estándar y la adición de extensiones de IPX para que la unidad TAOS funcione como los clientes esperan para las LAN NetWare. En este apartado se describen las cuestiones relacionadas con la adaptación de los protocolos de LAN a la WAN.

### **Utilización de SAP IPX por parte de las unidades TAOS**

La unidad TAOS tiene el funcionamiento estándar de SAP IPX para ruteadores cuando se conecta a través de la WAN a dispositivos IPX en los que no se ejecuta el software TAOS. De todos modos, cuando se conecta con otra unidad TAOS configurada para el ruteo IPX, los dos extremos de la conexión intercambian las tablas SAP completas.

Cuando un cliente NetWare envía una petición SAP para localizar un servicio, la unidad TAOS consulta su tabla SAP y responde con su propia dirección de hardware y con la dirección de red interna del servidor solicitado. Esto es similar a actuar como proxy de peticiones ARP en un entorno IP. El cliente puede transmitir, a continuación, los paquetes cuya dirección de destino es la dirección interna del servidor. Cuando la unidad TAOS recibe estos paquetes, consulta su tabla RIP. Si encuentra una entrada para la dirección de destino de los paquetes, activa la conexión (a menos que ya esté activada) y reenvía los paquetes.

### **Utilización de RIP IPX por parte de las unidades TAOS**

La unidad TAOS tiene el funcionamiento estándar de RIP IPX para ruteadores cuando se conecta a dispositivos IPX en los que no se ejecuta el software TAOS. De todos modos, cuando se conecta con otra unidad TAOS configurada para ruteo IPX, los dos extremos de la conexión

intercambian las tablas RIP completas de manera inmediata. Además, cada unidad TAOS mantiene las entradas RIP importadas como estáticas hasta que se reinicia la unidad o se efectúa un ciclo de apagado/encendido.

### *Funcionamiento de RIP IPX*

RIP IPX es parecido al protocolo de información de ruteo del grupo de protocolos TCP/IP, pero es un protocolo diferente. Los ruteadores IPX difunden actualizaciones de RIP de manera periódica y cada vez que se establece una conexión con una WAN. La unidad TAOS recibe las difusiones RIP IPX de un dispositivo remoto, agrega 1 al recuento de saltos de cada ruta anunciada, actualiza su propia tabla RIP y difunde los paquetes RIP actualizados en las redes conectadas en forma de horizonte dividido.

### *La ruta RIP IPX predeterminada*

La unidad TAOS reconoce el número de red -2 (0xFFFFFFF) como la ruta predeterminada RIP IPX. Cuando recibe un paquete para un destino desconocido, reenvía el paquete al ruteador IPX que anuncia la ruta predeterminada. Por ejemplo, si la unidad TAOS recibe un paquete IPX destinado a la red 77777777 y no dispone de una entrada en la tabla RIP para ese destino, la unidad TAOS reenvía el paquete a la red número FFFFFFFF, si está disponible, en lugar de sencillamente descartar el paquete. Si más de un ruteador IPX anuncia la ruta predeterminada, la unidad toma una decisión sobre la ruta según el recuento de saltos y ciclos de reloj.

## **Soporte para negociación de IPXWAN**

La unidad TAOS da soporte al protocolo IPXWAN, que es imprescindible para establecer comunicaciones con el ruteador multiprotocolo y el software Novell (por ejemplo, NetWare Connect2) que da soporte a conexiones de llamada de entrada. Si desea conocer todas las especificaciones del protocolo IPXWAN, consulte el documento RFC 1634 y la publicación *NetWare Link Services Protocol Specification—IPX WAN Version 2*.

Cuando dos unidades TAOS activan una conexión IPX, negocian todas las opciones durante la fase IPXCP. La negociación de IPXWAN nunca tiene lugar entre dos unidades TAOS, porque ninguna de ellas inicia el proceso de negociación enviando un paquete `Timer_Request` de IPXWAN.

Las conexiones con dispositivos IPX que no ejecutan el software TAOS, pero que utilizan software Novell en PPP, no negocian opciones durante la fase IPXCP, por lo que todas las opciones se negocian durante la fase IPXWAN del establecimiento de enlaces. El dispositivo de extremo distante envía un paquete `Timer_Request` de IPXWAN, que activa la negociación de IPXWAN en la unidad TAOS. Los dispositivos comparan los números de red interna y asignan la función de esclavo a la unidad con el número más bajo. La otra unidad se convierte en el componente maestro de este enlace durante la negociación de IPXWAN. La unidad esclava devuelve un paquete `Timer_Response` de IPXWAN y la unidad maestra inicia un intercambio de información sobre la configuración del ruteador final. La unidad TAOS da soporte a las siguientes opciones de ruteo:

- Ruteo IPX de TAOS (RIP/SAP no numerados sin antigüedad)
- Ruteo Novell (RIP/SAP no numerados sin antigüedad)
- Ninguna (el homólogo es un cliente de llamada de entrada. No hay RIP/SAP si no se solicita y se pueden asignar números de red y de nodo).

La compresión de cabeceras se rechaza como opción de ruteo. Después de que la negociación de IPXWAN finalice, empieza la transmisión de paquetes IPX mediante la opción de ruteo negociada.

## Ampliaciones de IPX estándar

NetWare utiliza el ruteo dinámico y la localización de servicios, por lo que los clientes esperan poder localizar un servidor de manera dinámica, independientemente de dónde esté situado físicamente. Puesto que este esquema se ha diseñado para que funcione en un entorno de LAN y no para operaciones de WAN, TAOS proporciona ampliaciones de IPX estándar. Las funciones agregadas amplían las funciones de WAN, como se muestra en la Tabla 7-1.

*Tabla 7-1. Ampliaciones de IPX de TAOS*

Ampliaciones de IPX de TAOS	Finalidad
Red virtual para clientes de llamada de entrada	Para que puede rutear IPX a no ruteadores (clientes NetWare), la unidad TAOS da soporte a una red IPX virtual definida en su perfil IPX-Global. Por lo tanto, la unidad puede asignar una dirección de red exclusiva al cliente. La conexión del cliente debe especificar que es un homólogo de llamada de entrada.
Aceptación o rechazo de actualizaciones de RIP y SAP	La unidad TAOS puede transmitir actualizaciones de RIP y SAP, recibirlas o ambas cosas, o se pueden desactivar las actualizaciones de RIP o SAP de cualquier conexión de ruteo IPX.
Activación de conexiones en respuesta a una consulta de SAP	La función Dial-Query está diseñada para entornos que dan soporte a muchos clientes y conexiones con sólo unas cuantas redes IPX remotas. La unidad TAOS activa todas las conexiones que activan Dial-Query cuando recibe una consulta de SAP sobre un servidor de archivos (tipo de servicio 0x04) y su tabla SAP no tiene ninguna entrada para ese tipo de servicio.
Rutas estáticas a servidores	Aunque la unidad TAOS conoce sus rutas a través de RIP, borra toda la tabla RIP cuando se reinicia o se apaga. En algunos entornos se configura una ruta IPX estática para que la unidad TAOS pueda abrir una conexión con esa ubicación y descargar la tabla RIP cuando la unidad se enciende.
Filtros SAP	Los filtros SAP IPX evitan que el tamaño de la tabla SAP aumente en exceso al incluir o excluir explícitamente servidores, servicios o tipos de servicio en cualquier interfaz.

## Recomendaciones para software de cliente NetWare

Los clientes NetWare de una WAN no necesitan una configuración especial en la mayor parte de los casos. No obstante, si la red local da soporte a servidores NetWare, los clientes NetWare

deben configurarse con un servidor preferido en la red local y no en una ubicación remota. Si la red local no da soporte a servidores NetWare, debe configurar los clientes locales con un servidor preferido que se encuentre en la red que tenga los costes de conexión más bajos. Si desea obtener más información al respecto, consulte la documentación de NetWare.

A causa de posibles problemas de rendimiento, no es aconsejable ejecutar programas remotamente. Para obtener unos resultados óptimos, copie LOGIN.EXE en la unidad local de cada cliente.

Tanto los clientes Macintosh como los clientes UNIX pueden utilizar IPX para comunicarse con servidores. Sin embargo, los dos tipos de clientes también dan soporte a protocolos nativos: AppleTalk (Macintosh) o TCP/IP (UNIX). Si los clientes Macintosh deben acceder a servidores NetWare a través de la WAN utilizando el software de AppleTalk (en lugar de MacIPX), la unidad TAOS debe dar soporte al ruteo de AppleTalk. De lo contrario, los paquetes de AppleTalk no llegarán a su destino. Si los clientes UNIX acceden a servidores NetWare por medio de TCP/IP (en lugar de UNIXWare), la unidad TAOS también debe configurarse como un ruteador IP. De lo contrario, los paquetes de TCP/IP no llegarán a su destino.

**Nota:** Packet Burst permite que los servidores envíen una corriente de datos a través de la WAN antes de que un cliente envíe un acuse de recibo. La función se incluye de manera automática en el software del servidor y del cliente para NetWare 3.12 o posterior. Si los servidores locales ejecutan NetWare 3.11, deben tener cargado PBURST.NLM. Si desea obtener más información al respecto, consulte la documentación de NetWare.

## ***Configuración del perfil IPX-Global***

Para poder configurar IPX en una interfaz de LAN, debe activar el ruteo IPX globalmente. También tiene la opción de definir una red IPX virtual que deba utilizarse para asignar direcciones IPX a clientes NetWare que no presentan ninguna dirección. A continuación se muestran los parámetros pertinentes con los ajustes de ejemplo:

```
[in IPX-GLOBAL]
ipx-routing-enabled = yes
ipx-dialin-pool = 12:34:56:78
```

Parámetro	Especifica
IPX-Routing-Enabled	Activa y desactiva el ruteo IPX para la interfaz. Cuando se graba el perfil, la unidad TAOS se activa en modo de ruteo IPX. En ese momento, crea un perfil IPX-Interface para cada puerto Ethernet instalado.
IPX-Dialin-Pool	Número de red IPX que debe utilizarse para asignar una dirección IPX a determinados clientes de llamada de entrada. El número debe ser exclusivo en todo el dominio de ruteo IPX. Si desea obtener información detallada al respecto, consulte "Definición de una red IPX virtual para clientes de llamada de entrada".

## Definición de una red IPX virtual para clientes de llamada de entrada

Cuando un cliente NetWare establece una conexión telefónica, la unidad TAOS negocia una sesión de ruteo con el cliente asignando al cliente una dirección en la red virtual IPX. El cliente debe aceptar el número de red, pero si dispone de su propio número de nodo, la unidad TAOS utiliza dicho número para crear la dirección completa de red:nodo. Si el cliente no dispone de un número de nodo, la unidad TAOS le asigna una dirección de nodo exclusiva en la red virtual.

El número de red IPX que asigne debe ser exclusivo en todo el dominio de ruteo IPX de la unidad TAOS. La unidad TAOS anuncia la ruta a esta red IPX virtual.

## Ejemplo de una configuración IPX-Global

A continuación, se muestra un ejemplo en el que se muestra cómo activar el modo de ruteo IPX y cómo definir una red para la asignación de direcciones a clientes de llamada de entrada que no son ruteadores:

```
admin> read ipx-global
IPX-GLOBAL read

admin> set ipx-routing-enabled = yes

admin> set ipx-dialin = cccc1234

admin> write
IPX-GLOBAL written
```

Cuando se graba el perfil, la unidad TAOS entra en modo de ruteo IPX y crea perfiles IPX-Interface para cada interfaz Ethernet. Asegúrese de que el número de red que asigne al parámetro IPX-Dialin es exclusivo en el dominio de ruteo de la unidad TAOS.

## Configuración de interfaces IPX de LAN

Después de activar el ruteo IPX en el perfil IPX-Global, el sistema crea un perfil IPX-Interface para cada interfaz Ethernet del sistema. Los perfiles IPX-Interface no existen hasta que se activa el ruteo IPX globalmente.

**Nota:** Aunque la unidad TAOS no dé soporte al ruteo IPX en la primera o en la segunda interfaz Ethernet del controlador de módulo, IPX-Routing-Enabled debe establecerse en Yes y debe especificarse un tipo de trama IPX válido en el perfil IPX-Interface de los puertos Ethernet del controlador de módulo.

## Información general de los ajustes de IPX de LAN

Los perfiles IPX-Interface contienen los parámetros siguientes, que aparecen con los ajustes predeterminados:

```
[in IPX-INTERFACE/{ { any-shelf any-slot 0 } 0 }
interface-address* = { { any-shelf any-slot 0 } 0 }
ipx-routing-enabled = no
ipx-frame = None
ipx-net-number = 00:00:00:00
```

```
ipx-type-20 = no  
ipx-sap-filter-name = ""
```

Parámetro	Especifica
IPX-Routing-Enabled	Activa y desactiva el ruteo IPX en la interfaz, siempre que se establezca también el parámetro IPX-Frame.
IPX-Frame	Especifica el tipo de trama IPX que la unidad TAOS ruteará y simulará. Con un ajuste None (el ajuste predeterminado), el ruteo IPX se desactiva en la interfaz. Los valores válidos son 802.2 (para NetWare 3.12 o posterior), 802.3 (para NetWare 3.11 o anterior), SNAP y Enet-II.
IPX-Net-Number	Número de red IPX que se utiliza en el segmento. La dirección cero predeterminada permite que el sistema obtenga el número de otros ruteadores IPX de la red.
IPX-Type-20	Activa y desactiva la propagación de paquetes Type-20 en la interfaz de LAN. Si desea obtener información detallada al respecto, consulte “Propagación de paquetes Type-20 de IPX en una interfaz de LAN”.
IPX-SAP-Filter-Name	Nombre de un perfil IPX-SAP Filter que debe aplicarse a la interfaz de LAN. Para obtener información detallada, consulte el apartado “Ejemplo de aplicación de un filtro SAP a una interfaz de LAN” en la página 7-19.

## Activación del ruteo y la simulación de IPX en la interfaz

Para que la unidad TAOS pueda rutear IPX en una interfaz Ethernet, debe establecer el parámetro IPX-Routing-Enabled y el parámetro IPX-Frame. El parámetro IPX-Frame especifica el tipo de trama IPX que la unidad TAOS ruteará y simulará.

**Nota:** Una unidad TAOS sólo rutea y simula un tipo de trama IPX. Si el software NetWare transmite IPX en un tipo de trama distinto del tipo que se especifique, la unidad descartará los paquetes con dicha trama. Si no está familiarizado con el concepto de tramas de paquetes, consulte la documentación de Novell.

Para determinar el tipo de tramas que debe utilizarse en una interfaz de LAN, vaya a la consola de un servidor NetWare de ese segmento y escriba LOAD INSTALL para visualizar el archivo AUTOEXEC.NCF. A continuación se muestra un ejemplo de la línea de AUTOEXEC.NCF que especifica tramas 802.3:

```
Load 3c509 name=ipx-card frame=ETHERNET_8023
```

## Asignación de un número de red IPX

Si hay otros ruteadores (servidores) NetWare en la interfaz de LAN, el número de IPX asignado a la unidad TAOS para esa interfaz debe ser coherente con el número que estén utilizando los demás ruteadores. La mejor manera de garantizar esta coherencia es dejar la dirección nula predeterminada como ajuste para el parámetro IPX-Net-Number. La dirección nula hace que la unidad TAOS obtenga su número de red a partir de otro ruteador de la interfaz o a partir de los paquetes RIP recibidos del servidor IPX local.



Si especifica un número de red IPX que no sea cero, la unidad TAOS se convierte en el ruteador raíz y otros ruteadores pueden obtener su número de red IPX a partir de la unidad. Si desea obtener información detallada acerca de los ruteadores raíz, consulte la documentación de Novell.

## Propagación de paquetes Type-20 de IPX en una interfaz de LAN

Algunas aplicaciones, como NetBIOS sobre IPX, utilizan paquetes Type-20 de IPX para difundir nombres en una red. De manera predeterminada, las difusiones no se propagan en enlaces ruteados (aunque Novell lo recomienda) y no se reenvían en enlaces cuya productividad sea inferior a 1 Mbps. Si está utilizando una aplicación (como NetBIOS sobre IPX) que requiere estos paquetes para funcionar, puede permitir que el ruteador propague paquetes Type-20 de IPX en una interfaz de LAN estableciendo el parámetro IPX-Type-20 en Yes.

## Ejemplo de una configuración de IPX-Interface

A continuación se muestra un ejemplo de entrada que activa la unidad TAOS para rutear tramas 802.3 IPX hacia la interfaz de LAN y desde ésta, así como para propagar paquetes Type-20 de IPX:

```
admin> read ipx-int { {1 12 2 } 0 }  
IPX-INTERFACE/{ { shelf-1 slot-12 2 } 0 } read  
  
admin> set ipx-routing-enabled = yes  
  
admin> set ipx-frame = 802.3  
  
admin> write  
IPX-INTERFACE/{ { shelf-1 slot-12 2 } 0 } written
```

Tenga en cuenta que en este ejemplo no se especifica un valor de IPX-Net-Number, lo que significa que la unidad TAOS es un ruteador no raíz que obtendrá su dirección a partir de otro ruteador IPX de la red o a partir de paquetes RIP recibidos del servidor IPX local.

## Configuración de interfaces IPX de WAN

Las conexiones de ruteo IPX normalmente utilizan la autenticación PPP (que se describe en el apartado “Autenticación de sesiones de protocolo entramado” en la página A-6), porque la unidad TAOS no dispone de un mecanismo de autenticación incorporado, como puede ser la búsqueda de coincidencias de direcciones IPX de un perfil. Además, el perfil IPX-Answer debe activar el ruteo IPX, que es el ajuste predeterminado.

## Información general de los ajustes de conexiones IPX

Puede configurar las conexiones IPX en perfiles de usuario Connection locales o RADIUS.

### *Ajustes de los perfiles Connection*

Las conexiones de ruteo IPX pueden especificar ajustes para una o más de las siguientes opciones de IPX, que aparecen con los valores predeterminados:

```
[in CONNECTION/"":ipx-options]
ipx-routing-enabled = no
peer-mode = router-peer
rip = both
sap = both
dial-query = no
net-number = 00:00:00:00
net-alias = 00:00:00:00
sap-filter = ""
ipx-sap-hs-proxy = no
ipx-sap-hs-proxy-net = [ 0 0 0 0 0 0 ]
ipx-header-compression = no
```

Parámetro	Especifica
IPX-Routing-Enabled	Activa y desactiva el ruteo IPX en la interfaz.
Peer-Mode	Tipo de dispositivo de extremo distante (cliente NetWare de llamada de entrada o ruteador de IPX). Los valores válidos son Router-Peer y Dialin-Peer. Con el ajuste Dialin-Peer, la unidad TAOS asigna un número de red IPX de la red IPX virtual, como se describe en “Definición de una red IPX virtual para clientes de llamada de entrada” en la página 7-5.
RIP	Si Peer-Mode se establece en Router, activa o desactiva las actualizaciones RIP IPX en la interfaz. No es aplicable si Peer-Mode se establece en Dialin-Peer.
SAP	Si Peer-Mode se establece en Router, activa o desactiva las actualizaciones SAP IPX en la interfaz. No es aplicable si Peer-Mode se establece en Dialin-Peer.
Dial-Query	Activa y desactiva el inicio de una conexión después de recibir una consulta SAP sobre el tipo de servicios 0x04 (servidor de archivos) cuando ese tipo de servicio no está presente en la tabla SAP.
Net-Number	Número hexadecimal de cuatro bytes de red IPX para el enlace con el cliente. Sólo es necesario si el dispositivo de extremo distante debe negociar el número antes de establecer la conexión.
Net-Alias	Un segundo número de red IPX que sólo debe utilizarse cuando se establecen conexiones con ruteadores que utilizan interfaces numeradas y no ejecutan software TAOS.
SAP-Filter	Nombre de un perfil IPX-SAP Filter que debe aplicarse a la interfaz de LAN. Para obtener información detallada, consulte el apartado “Ejemplo de aplicación de un filtro SAP a una interfaz de WAN” en la página 7-19.
IPX-SAP-HS-Proxy	Activa y desactiva la función de proxy de servidor inicial de IPX.
IPX-SAP-HS-Proxy-Net	Números de red IPX para un máximo de seis servidores iniciales que se utilizan cuando se activa la función de proxy de servidor inicial.

Parámetro	Especifica
IPX-Header-Compression	Activa y desactiva la compresión de cabeceras IPX, siempre y cuando el método de encapsulación dé soporte para ello.

### *Ajustes de los perfiles RADIUS*

Los perfiles de usuario RADIUS utilizan los pares atributo-valor siguientes para configurar el ruteo IPX:

Atributo	Especifica
Ascend-Route-IPX (229)	Activa y desactiva el ruteo IPX en la interfaz. Los valores válidos son Route-IPX-No (0) y Route-IPX-Yes (1). Route-IPX-No es el valor predeterminado.
Ascend-IPX-Peer-Mode (216)	Tipo de dispositivo de extremo distante (cliente NetWare de llamada de entrada o ruteador de IPX). Los valores válidos son IPX-Peer-Router (0) e IPX-Peer-Dialin (1). Si se especifica IPX Peer-Dialin, la unidad TAOS asigna un número de red IPX en la red virtual IPX, como se describe en “Definición de una red IPX virtual para clientes de llamada de entrada” en la página 7-5.
Framed-IPX-Network (23)	Número hexadecimal de cuatro bytes de red IPX del ruteador de IPX en el extremo remoto de la conexión. Esta dirección se utiliza en paquetes Access-Accept.
Ascend-IPX-Alias (224)	Un segundo número de red IPX que sólo debe utilizarse cuando se establecen conexiones con ruteadores que utilizan interfaces numeradas y no ejecutan software TAOS.

## **Especificación del dispositivo remoto como un ruteador o un cliente de llamada de entrada**

El parámetro Peer-Mode y el atributo Ascend-IPX-Peer-Mode de RADIUS especifican si el sitio remoto es un cliente NetWare de llamada de entrada u otro ruteador IPX. Para establecer un valor predeterminado de Peer-Mode para los perfiles RADIUS, consulte “Ajuste de Answer-Defaults IPX Peer-Mode” en la página 7-10.

Cuando Peer-Mode especifica Dialin-Peer, la unidad TAOS negocia una sesión de ruteo IPX con el cliente NetWare de llamada de entrada asignando al cliente una dirección de nodo en la red IPX virtual definida en el perfil IPX-Global. El cliente debe aceptar el número de red que se le ha asignado. Si el cliente tiene su propio número de nodo, la unidad TAOS utiliza ese número para formar la dirección de red completa. Si el cliente no dispone de número de nodo, la unidad le asigna una dirección de nodo exclusiva en la red virtual.

**Nota:** Cuando se establece una conexión con un cliente Netware de llamada de entrada, la unidad TAOS no envía anuncios RIP ni SAP a través de la conexión y pasa por alto los anuncios RIP y SAP que recibe del extremo distante. Sin embargo, responde las consultas RIP y SAP que recibe de los clientes de llamada de entrada.

## Ajuste de Answer-Defaults IPX Peer-Mode

La unidad TAOS da soporte al parámetro siguiente, que aparece con el valor predeterminado, para establecer un modo homólogo IPX predeterminado para los perfiles RADIUS:

```
[in ANSWER-DEFAULTS:ipx-answer]  
peer-mode = router-peer
```

Cuando Use-Answer-For-All-Defaults se establece en Yes (el valor predeterminado), el sistema utiliza el ajuste IPX-Answer Peer-Mode cuando crea un perfil básico para llamadas autenticadas por RADIUS.

## Control de actualizaciones RIP y SAP al ruteador remoto y desde éste

Cuando el extremo remoto de la conexión es un ruteador, puede especificar cómo manejar los paquetes RIP y SAP a través de esa conexión de WAN. Tanto el parámetro RIP como el parámetro SAP se establecen en Both de manera predeterminada, lo que significa que la unidad TAOS envía actualizaciones a través de la conexión de WAN (informando a los demás ruteadores que existen en la red remota de sus rutas o servicios) y recibe actualizaciones del ruteador remoto (incluidas las rutas o servicios de su tabla RIP o SAP).

Si establece el parámetro RIP en Send, la unidad TAOS envía las rutas al ruteador remoto, pero no recibe ninguna actualización en esta interfaz. Si el parámetro se establece en Recv, la unidad recibe actualizaciones del ruteador remoto, pero no propaga las rutas IPX locales al sitio remoto. Si establece RIP en Off, no se propaga ninguna ruta en ninguna de las direcciones.

Para el parámetro SAP se aplican los mismos ajustes. Si SAP se establece para enviar y recibir difusiones en la interfaz de WAN, la unidad TAOS difunde toda la tabla SAP a la red remota y espera las actualizaciones de la tabla SAP de esa red. Así, ambas redes disponen de una tabla completa de todos los servicios de la WAN. Para controlar los servicios que se anuncian y dónde se anuncian, puede desactivar el intercambio de difusiones SAP a través de una conexión de WAN o especificar que la unidad TAOS sólo enviará o sólo recibirá difusiones SAP en esa conexión.

## Utilización de Dial-Query

Al establecer el parámetro Dial-Query, la unidad TAOS queda configurada para activar una conexión cuando recibe una consulta SAP sobre el tipo de servicio 0x04 (servidor de archivos) y ese tipo de servicio no está presente en la tabla SAP de la unidad TAOS. Si la unidad no dispone de una entrada en la tabla SAP para el tipo de servicio 0x04, activa cada conexión que tiene Dial-Query establecido. Por ejemplo, si 20 perfiles Connection tienen Dial-Query establecido, la unidad TAOS activa las 20 conexiones en respuesta a la consulta.

Si la unidad TAOS dispone de una sola ruta estática de IPX para un servidor remoto, activa esa conexión en lugar de adoptar la solución más costosa que es activar cada conexión que tiene Dial-Query establecido.

## Cuándo debe utilizarse Net-Number y Net-Alias

Net-Number especifica el número de la red IPX del ruteador del extremo remoto. Este parámetro, que es necesario en contadas ocasiones, da cabida a los ruteadores de extremo

remoto para los que es necesario que la unidad TAOS conozca el número de red del ruteador antes de establecer la conexión.

El parámetro Net-Alias especifica un segundo número de red IPX, que sólo debe utilizarse cuando se establecen conexiones con ruteadores que utilizan interfaces numeradas y no ejecutan software TAOS.

## Proxy de servidor inicial

Para clientes móviles NetWare, puede especificar el número de red de uno a seis servidores NetWare que deben recibir consultas SAP a través de la conexión. Si no lo hace, cuando el cliente se encuentra en una ubicación distante y envía una consulta Get Nearest Server Request, las respuestas proceden de los servidores más cercanos a dicha ubicación y no de los servidores iniciales, como se esperaba. Con la función de proxy de servidor inicial, los clientes móviles pueden activar una conexión con los servidores que utilizan habitualmente.

Para activar la función de proxy de servidor inicial, establezca el parámetro IPX-SAP-HS-Proxy en Yes y especifique de uno a seis números de red IPX para el parámetro IPX-SAP-HS-Proxy-Net. La unidad TAOS sólo dirige las consultas SAP del cliente a las redes especificadas.

A continuación se muestra un ejemplo de cómo activar la función de proxy de servidor inicial en un perfil Connection de ruteo IPX:

```
admin> read conn ipxclient
CONNECTION/ipxclient read

admin> set ipx ipx-routing = yes

admin> set ipx ipx-sap-hs-proxy = yes

admin> set ipx ipx-sap-hs-proxy-net 1 = ccff1234

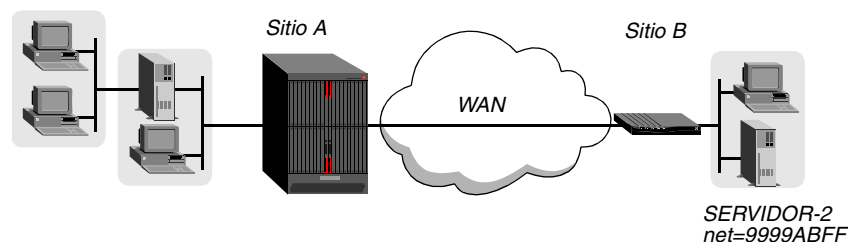
admin> write
CONNECTION/ipxclient written
```

Si IPX-SAP-HS-Proxy se establece en Yes, la función se activa. A continuación, debe especificar como mínimo una dirección de red IPX (y seis como máximo) a la que se dirigirán las difusiones SAP.

## Ejemplos de una conexión con una LAN de Novell

En la Figura 7-1 se muestra una unidad TAOS que proporciona una conexión entre una red IPX, que da soporte a servidores y clientes NetWare, y un sitio remoto que da soporte a una unidad TAOS, así como a servidores y clientes NetWare.

*Figura 7-1. Conexión IPX con servidores NetWare en ambos lados*



En este ejemplo, el servidor NetWare que se encuentra en el Sitio B está configurado con las siguientes especificaciones:

```
Name = SERVER-2
internal net 013DE888
Load 3c509 name = net-card frame = ETHERNET_8023
Bind ipx net-card net = 9999ABFF
```

A continuación se muestra un ejemplo de especificación de una conexión con la unidad TAOS del Sitio B:

```
admin> new conn sitebgw
CONNECTION/sitebgw read

admin> set active = yes

admin> set ppp recv-password = sitebpw

admin> set ipx ipx-routing = yes

admin> set ipx peer = router

admin> set ipx rip = off

admin> write
CONNECTION/sitebgw written
```

A continuación se muestra un perfil RADIUS equivalente:

```
sitebgw Password = "sitebpw"
  Service-Type = Framed-User,
  Framed-Protocol = MPP,
  Ascend-Route-IPX = Route-IPX-Yes,
  Ascend-IPX-Peer-Mode = IPX-Peer-Router
```

Cuando RIP está desactivado en una conexión, es conveniente crear una ruta estática hacia el servidor del sitio remoto. La ruta garantiza que la unidad TAOS pueda activar esta conexión, incluso inmediatamente después de que el sistema se reinicie. En el ejemplo siguiente se muestra cómo configurar una ruta hacia el Server-2 en el Sitio B:

```
admin> new ipx-route SERVER-2
IPX-ROUTE/SERVER-2 read

admin> set server-type = 0004

admin> set dest-network = 013DE888

admin> set server-node = 000000000001

admin> set server-socket = 0451

admin> set profile-name = sitebgw

admin> write
IPX-ROUTE/SERVER-2 written
```

A continuación se muestra un perfil RADIUS equivalente:

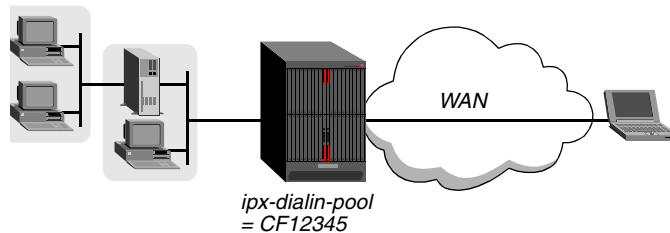
```
ipxroute-sa-1 Password = "ascend", Service-Type = Outbound-User
  Ascend-IPX-Route="sitebgw 013DE888 000000000001 0451 0004 SERVER-2"
```

**Nota:** El número de red de destino es el número de red interna del servidor. Si desea obtener más información acerca de las rutas IPX, consulte “Configuración de rutas IPX estáticas” en la página 7-13.

## Ejemplos de una conexión con un cliente de llamada de entrada

En la Figura 7-2 se muestra un cliente NetWare estableciendo una conexión telefónica con la unidad TAOS para acceder a una red IPX de empresa. El emisor está ejecutando un software de cliente NetWare con software PPP para establecer la conexión telefónica.

*Figura 7-2. Cliente NetWare de llamada de entrada*



Los clientes NetWare de llamada de entrada no disponen de una dirección de red IPX. Los clientes, para establecer una conexión de ruteo IPX con la red local, deben establecer la conexión telefónica mediante el software PPP y el perfil Connection debe tener el parámetro Peer-Mode establecido en Dialin-Peer. Asimismo, la unidad TAOS debe tener una red IPX virtual definida para asignarla a esos clientes. Si desea obtener información acerca de la definición de una red IPX virtual, consulte “Configuración del perfil IPX-Global” en la página 7-4.

A continuación se muestra un ejemplo de entrada en la que se configura una conexión de ruteo IPX para el cliente de la Figura 7-2:

```
admin> new conn client-1
CONNECTION/client-1 read
admin> set ppp rcv-password = client-pw
admin> set ipx ipx-routing = yes
admin> set ipx peer = dialin
admin> write
CONNECTION/client-1 written
```

A continuación se muestra un perfil RADIUS equivalente:

```
client-1 Password = "client-pw"
  Service-Type = Framed-User,
  Framed-Protocol = MPP,
  Ascend-Route-IPX = Route-IPX-Yes,
  Ascend-IPX-Peer-Mode = IPX-Peer-Dialin
```

## Configuración de rutas IPX estáticas

Cuando la unidad TAOS se reinicia o efectúa un ciclo de apagado/encendido, borra las tablas RIP y SAP de la memoria. Las rutas estáticas crean entradas en nuevas tablas RIP y SAP cuando la unidad se inicializa. Las rutas estáticas permiten que la unidad TAOS acceda a un servidor NetWare y descargue de allí unas tablas más completas.

En el caso en el que una unidad TAOS se vaya a conectar con otra unidad TAOS, es conveniente no configurar rutas estáticas. Sin embargo, esto significa que después de un

reinicio o de efectuar un ciclo de apagado/encendido, debe marcar la conexión de ruteo IPX inicial manualmente. Después de que se establezca esa conexión, la unidad TAOS descarga la tabla RIP de la otra unidad TAOS y mantiene las rutas como estáticas hasta el próximo reinicio o ciclo de apagado/encendido.

El inconveniente de las rutas estáticas es que deben actualizarse manualmente siempre que se elimina el servidor especificado o se modifica su dirección. Una ventaja es que garantizan que la unidad TAOS pueda activar la conexión en respuesta a las peticiones SAP de los clientes. Otra ventaja es que ayudan a evitar los tiempos de espera excedidos cuando un cliente tarda mucho tiempo en localizar un servidor en la WAN.

**Nota:** No es necesario crear rutas IPX hacia servidores que se encuentran en la red Ethernet local.

## Información general de los ajustes de rutas IPX

Puede configurar rutas de IPX en perfiles IPX-Route locales o en perfiles de pseudousuario RADIUS.

### *Ajustes de los perfiles IPX-Route locales*

Las rutas IPX estáticas se configuran con los parámetros siguientes, que aparecen con los ajustes predeterminados:

```
[in IPX-ROUTE/""]
name* = ""
server-type = 00:00
dest-network = 00:00:00:00
server-node = 00:00:00:00:00:00
server-socket = 00:00
hops = 8
ticks = 12
profile-name = ""
active-route = yes
```

Parámetro	Especifica
Name	Nombre del perfil IPX-Route, normalmente se trata del nombre del servidor NetWare remoto.
Server-Type	Tipo de servicio NetWare. El tipo de servicio es un número que se incluye en los anuncios SAP. Por ejemplo, los servidores de archivos NetWare son del tipo de servicio SAP 0x04.
Dest-Network	Número de red interna de un servidor NetWare remoto. El administrador de la red asigna un número de red IPX interna a los servidores de archivos NetWare y estos normalmente utilizan el valor predeterminado 000000000001 como un número de nodo en esa red. La dirección de red y de nodo combinada es la dirección de red de destino de las peticiones de lectura y grabación de archivos (si no está familiarizado con los números de red interna, consulte la documentación de NetWare para obtener información detallada al respecto).



Parámetro	Especifica
Server-Node	Dirección de nodo del servidor en la red interna. Los servidores normalmente utilizan la dirección de nodo predeterminada 000000000001 de la red interna.
Server-Socket	Un número de zócalo conocido del servidor. Para obtener información detallada, consulte el apartado “Números de zócalo en rutas estáticas” en la página 7-16.
Hops	Saltos a la red interna del servidor. Normalmente el número de saltos predeterminado 2 es adecuado, pero puede que deba aumentar el valor para servidores que estén muy alejados.
Ticks	Los ciclos de reloj son ciclos de reloj de PC IBM (1/18 de segundo). Las mejores rutas se calculan según el número de ciclos de reloj y no de saltos. Normalmente un número de ciclos de reloj predeterminado de 12 es adecuado, pero puede que deba aumentar el valor para servidores que estén muy alejados.
Profile-Name	Nombre del perfil de llamada de salida Connection o RADIUS que se utiliza para acceder al servidor. El valor predeterminado es nulo. Cuando la unidad TAOS recibe un consulta sobre el servidor especificado o un paquete para ese servidor, busca el perfil referenciado y establece la conexión telefónica.
Active-Route	Activa y desactiva la ruta. Las rutas desactivadas no se utilizan.

### *Ajustes de los perfiles ipxroute de RADIUS*

Un perfil `ipxroute` es un perfil de pseudousuario cuya primera línea tiene el formato siguiente:

```
ipxroute-name-N Password="ascend", Service-Type = Outbound-User
```

El argumento *name* es el nombre del sistema de la unidad TAOS (especificado por el parámetro Name del perfil System) y *N* es un número de una serie secuencial, que empieza por 1. Asegúrese de que no faltan números en la serie que especifica *N*. Si existe un espacio vacío en la secuencia de números, la unidad TAOS deja de recuperar los perfiles cuando encuentra dicho espacio.

**Nota:** Para especificar rutas a las que puede llamar más de un sistema, elimine el argumento *name*. La primera palabra del perfil de pseudousuario es, por lo tanto, `route-N`.

Cada perfil de pseudousuario especifica una o más rutas con el atributo Ascend-IPX-Route. El valor del atributo Ascend-IPX-Route utiliza la sintaxis siguiente:

```
"profile net [node] [socket] [server-type] [hops] [ticks] [server-name]"
```

Elemento de sintaxis	Especifica
<i>profile</i>	Nombre del perfil de usuario de llamada de salida que utiliza la ruta. Cuando la unidad TAOS recibe un consulta sobre el servidor especificado o un paquete para ese servidor, busca el perfil referenciado y establece la conexión telefónica.

Elemento de sintaxis	Especifica
<i>net</i>	Número de red interna de un servidor NetWare remoto. El administrador de la red asigna un número de red IPX interna a los servidores de archivos NetWare y estos normalmente utilizan el valor predeterminado 000000000001 como un número de nodo en esa red. La dirección de red y de nodo combinada es la dirección de red de destino de las peticiones de lectura y grabación de archivos (si no está familiarizado con los números de red interna, consulte la documentación de NetWare para obtener información detallada al respecto).
<i>node</i>	Dirección de nodo del servidor en la red interna. Los servidores normalmente utilizan la dirección de nodo predeterminada 000000000001 en la red interna.
<i>socket</i>	Un número de zócalo conocido del servidor. Para obtener información detallada, consulte el apartado “Números de zócalo en rutas estáticas” en la página 7-16.
<i>server-type</i>	Tipo de servicio NetWare. El tipo de servicio es un número que se incluye en los anuncios SAP. Por ejemplo, los servidores de archivos NetWare son del tipo de servicio SAP 0x04.
<i>hops</i>	Salto a la red interna del servidor. Normalmente el número de saltos predeterminado 2 es adecuado, pero puede que deba aumentar el valor para servidores que estén muy alejados.
<i>ticks</i>	Los ciclos de reloj son ciclos de reloj de PC IBM (1/18 de segundo). Las mejores rutas se calculan según el número de ciclos de reloj y no de saltos. Normalmente un número de ciclos de reloj predeterminado de 12 es adecuado, pero puede que deba aumentar el valor para servidores que estén muy alejados.
<i>server-name</i>	Nombre del servidor NetWare remoto.

## Números de zócalo en rutas estáticas

El número de zócalo que especifique debe ser un número de zócalo conocido. Por ejemplo, los servidores de archivos Novell normalmente utilizan el zócalo 0x451.

Los servicios que utilizan números de zócalo dinámicos pueden utilizar un zócalo diferente cada vez que se cargan y no funcionarán con perfiles IPX Route. Para activar una conexión con un servicio remoto que utilice un número de zócalo dinámico, especifique un servidor maestro con un número de zócalo conocido en la red remota.

## Ejemplos de una ruta IPX estática

En el ejemplo siguiente se muestra cómo crear un perfil IPX-Route nuevo para un servidor remoto denominado Server-1:

```
admin> new ipx-route Server-1
IPX-ROUTE/Server-1 read
admin> set server-type = 0004
admin> set dest-network = cc1234ff
admin> set server-node 1 = 000000000001
```

```
admin> set server-socket = 0451
admin> set profile-name = sitebgw
admin> write
IPX-ROUTE/Server-1 read
```

A continuación se muestra un perfil RADIUS equivalente:

```
ipxroute-sa-1 Password = "ascend", Service-Type = Outbound-User
Ascend-IPX-Route="sitebgw cc1234ff 000000000001 0451 0004 Server-1"
```

## ***Definición y aplicación de filtros SAP IPX***

Los filtros SAP IPX contienen especificaciones que determinan los servicios NetWare remotos que se excluirán o se incluirán en la tabla SAP o en los paquetes de respuestas SAP de la unidad TAOS.

**Nota:** Los filtros SAP sólo funcionan cuando SAP IPX está activo en la interfaz (como lo está de manera predeterminada). Puede evitar que la unidad TAOS envíe o reciba actualizaciones SAP en una interfaz WAN estableciendo SAP en No en el subperfil IPX-Options de un perfil Connection.

## **Información general sobre los ajustes de filtros SAP IPX**

A continuación se muestran los parámetros de los filtros SAP (que aparecen con los valores predeterminados):

```
[in IPX-SAP-FILTER/""]
ipx-sap-filter-name* = ""

[in IPX-SAP-FILTER/":input-ipx-sap-filters:input-ipx-sap-filters [1]]
valid-filter = no
type-filter = exclude
server-type = 00:00
server-name = ""

[in IPX-SAP-FILTER/":output-ipx-sap-filters:output-ipx-sap-filters
[1]]
valid-filter = no
type-filter = exclude
server-type = 00:00
server-name = ""
```

Cada uno de los ocho filtros de entrada y salida tiene los mismos parámetros.

<b>Parámetro</b>	<b>Utilización</b>
IPX-SAP-Filter-Name	Debe asignar un nombre a cada filtro SAP para que pueda aplicarse por el nombre a una interfaz. El nombre que asigne se convertirá en el índice del perfil IPX-SAP-Filter.

<b>Parámetro</b>	<b>Utilización</b>
Input-IPX-SAP-Filters (1–8)	Cada filtro SAP puede contener un máximo de ocho especificaciones de filtro de entrada, que se definen individualmente y se aplican en orden (de 1 a 8) a los paquetes SAP que la unidad TAOS recibe. Los filtros de entrada determinan los servicios remotos a los que los usuarios locales de NetWare pueden acceder.
Output-IPX-SAP-Filters (1–8)	Cada filtro SAP puede contener un máximo de ocho especificaciones de filtro de salida, que se definen individualmente y se aplican en orden (de 1 a 8) a los paquetes de respuestas SAP. La unidad TAOS transmite las respuestas SAP para un paquete de petición SAP. Los filtros de salida determinan los servicios NetWare locales que están disponibles para los usuarios remotos.
Valid-Filter	Activa y desactiva el filtro de entrada o de salida. Con un ajuste No (el valor predeterminado), ese filtro se omite cuando se filtran datos SAP. Establezca este parámetro en Yes para cada filtro definido que pretenda utilizar.
Type-Filter	Especifica si se debe incluir o excluir el servicio especificado por el parámetro Server-Name o Server-Type (o ambos). Excluye es el valor predeterminado. El ajuste Include se utiliza habitualmente para incluir un servicio específico cuando filtros anteriores han excluido un tipo general de servicio.
Server-Type	Especifica un tipo de servicio NetWare. Los tipos de servicio son números hexadecimales que representan un tipo de servicio NetWare. El tipo FFFF representa todos los tipos. El número del servicio de archivos es 0004. Si desea obtener información completa acerca de los tipos de servicio SAP, consulte la documentación de NetWare.
Server-Name	Especifica el nombre de un servidor NetWare local o remoto. Puede utilizar los caracteres comodín * y ? para hallar coincidencias parciales de nombres.

## **Ejemplo de filtrado de un servidor de archivos de la tabla SAP**

En el ejemplo siguiente se muestra cómo crear un filtro SAP que identifique un servidor de archivos concreto y que lo filtre a partir de la tabla SAP. Si la función de servicios de directorios no recibe soporte, los servidores o servicios que no se encuentran en la tabla SAP de la unidad TAOS no serán accesibles para los clientes de otras interfaces de la unidad TAOS.

```
admin> new ipx-sap-filter server_1
IPX-SAP-FILTER/server_1 read

admin> set input 1 valid-filter = yes

admin> set input 1 server-type = 0004

admin> set input 1 server-name = server_1

admin> write
IPX-SAP-FILTER/server_1 written
```

## Ejemplo de filtrado de servicios NetWare remotos de la tabla SAP

En el ejemplo siguiente se muestra cómo crear un filtro SAP que excluya de la tabla SAP de la unidad TAOS todos los servicios NetWare de la interfaz. Cuando este filtro se aplica a un perfil Connection, los usuarios de WAN *pueden* acceder a los servicios locales, pero los usuarios locales no pueden acceder a ningún servicio de la red remota.

```
admin> new ipx-sap-filter nowan
IPX-SAP-FILTER/nowan read

admin> set input 1 valid-filter = yes

admin> set input 1 server-type = FFFF

admin> set input 1 server-name = *

admin> write
IPX-SAP-FILTER/nowan written
```

## Ejemplo de aplicación de un filtro SAP a una interfaz de LAN

Cuando un filtro SAP se aplica a una interfaz de LAN, incluye o excluye servicios locales específicos de la tabla SAP de la unidad TAOS y las respuestas de la unidad a las consultas SAP de la interfaz. Si la función de servicios de directorios no recibe soporte, los servidores o servicios que no se encuentren en la tabla SAP de la unidad TAOS no serán accesibles para los clientes a través de la WAN. Un filtro que se aplica a una interfaz de LAN entra en vigor de manera inmediata.

A continuación se muestra un ejemplo de aplicación de un filtro SAP a una interfaz de LAN:

```
admin> read ipx-interface { { 1 12 2 } 0 }
IPX-INTERFACE/{ { shelf-1 slot-12 2 } 0 } read

admin> set ipx-sap-filter-name = server_1

admin> write
IPX-INTERFACE/{ { shelf-1 slot-12 2 } 0 } written
```

## Ejemplo de aplicación de un filtro SAP a una interfaz de WAN

Puede aplicar un filtro SAP a una interfaz de WAN especificando el nombre del perfil de filtro como el valor del parámetro SAP-Filter. Cuando un filtro SAP se aplica a una interfaz de WAN, incluye o excluye servicios específicos de la tabla SAP de la unidad TAOS y las respuestas de la unidad a las consultas SAP de la interfaz. Un filtro aplicado a una interfaz de WAN entra en vigor cuando la conexión vuelve a activarse.

A continuación se muestra un ejemplo de aplicación de un filtro SAP a una interfaz de WAN:

```
admin> read conn clientnet
CONNECTION/clientnet read

admin> set ipx sap-filter = nowan

admin> write
CONNECTION/client written
```



# Ruteo y acceso remoto de AppleTalk

# 8

Introducción .....	8-1
Configuración del perfil Atalk-Global .....	8-1
Configuración de interfaces AppleTalk de LAN .....	8-2
Configuración de interfaces AppleTalk de WAN .....	8-4

## Introducción

Una unidad TAOS configurada para el ruteo AppleTalk permite conexiones de llamada de entrada del software de cliente AppleTalk Remote Access (ARA), del software de conexión telefónica PPP que da soporte a AppleTalk y de otras unidades TAOS compatibles con AppleTalk.

**Nota:** El ruteo AppleTalk debe estar activado en el controlador del módulo para permitir que el sistema reenvíe paquetes AppleTalk desde la tarjeta en la que se recibe el paquete al controlador del módulo. Este requisito se aplica a cualquier tipo de conexión AppleTalk, incluso si el perfil Connection individual de un dispositivo remoto no utiliza el ruteo.

## Configuración del perfil Atalk-Global

Cuando un cliente PPP Appletalk o ARA efectúa una llamada de entrada, la unidad TAOS asigna al cliente una dirección AppleTalk en una red virtual AppleTalk. Puede definir la red virtual AppleTalk en el perfil Atalk-Global definiendo los parámetros siguientes (que aparecen con los ajustes predeterminados):

```
[in ATALK-GLOBAL]
atalk-dialin-pool-start = 1000
atalk-dialin-pool-end = 1002
```

Se asigna un rango de red a las redes AppleTalk; dicho rango está formado por números enteros consecutivos entre 1 y 65.199. Cada rango de red debe ser exclusivo. Dos redes no pueden utilizar el mismo rango y dos rangos de red no pueden solaparse.

Cada número del rango puede asociarse a un máximo de 253 nodos, de modo que el rango determina el número de clientes que se puede conectar. Por ejemplo, una red con el rango 1001-1002 puede dar soporte a un máximo de 2 x 253, o 506, clientes. A continuación se muestra un ejemplo de definición de una red virtual. En este caso, el rango de red es 1001-1002:

```
admin> read atalk-global
ATALK-GLOBAL read

admin> set atalk-dialin-pool-start = 1001

admin> set atalk-dialin-pool-end = 1002

admin> write
ATALK-GLOBAL written
```

## ***Configuración de interfaces AppleTalk de LAN***

En el perfil Atalk-Interface, puede activar el ruteo AppleTalk y especificar si la unidad TAOS funciona como un ruteador raíz o no raíz en la interfaz. En la versión actual del software, sólo la interfaz Ethernet incorporada en el controlador del módulo puede configurarse como interfaz AppleTalk. El perfil Atalk-Interface contiene los parámetros siguientes (que aparecen con los ajustes predeterminados):

```
[in ATALK-INTERFACE/{ { shelf-1 controller 1 } 0 }]
interface-address* = { { shelf-1 controller 1 } 0 }
atalk-routing-enabled = no
hint-zone = ""
atalk-Router = atlk-router-off
atalk-Net-Start = 0
atalk-Net-End = 0
atalk-Default-Zone = ""
atalk-Zone-List = [ "" "" "" "" "" "" "" "" "" "" ]
```

Parámetro	Especifica
Atalk-Routing-Enabled	Activa y desactiva el ruteo AppleTalk en la interfaz Ethernet del controlador del módulo. Si este parámetro se establece en No, no se aplicará ninguno de los demás parámetros.
Hint-Zone	Nombre de la zona en que reside la unidad TAOS. Se aplica únicamente cuando la unidad TAOS no es un ruteador raíz.
Atalk-Router	Especifica un modo de ruteo. Si este parámetro se establece en Atlk-Router-Off, no se aplicará ninguno de los parámetros restantes. Con el ajuste Atlk-Router-Seed, la unidad se activa con la configuración de red y de zona especificada, que debe coincidir totalmente con las especificaciones correspondientes en otros ruteadores AppleTalk de la interfaz. Con el ajuste Atlk-Router-Nonseed, la unidad obtiene la configuración de zona y red de otro ruteador AppleTalk (un ruteador raíz) de la red.
Atalk-Net-Start	Rango de red para la interfaz. Solamente se aplica a la configuración de ruteadores raíz. Si desea obtener información detallada, consulte “Ejemplo de configuración de un ruteador raíz” en la página 8-3.
Atalk-Net-End	



Parámetro	Especifica
Default-Zone	Zona predeterminada de AppleTalk para la interfaz. Solamente se aplica a la configuración de ruteadores raíz. La zona predeterminada es la zona que se asigna a un servicio de AppleTalk en esta interfaz si el servicio no selecciona una zona en la que residir.
Zone-List	Lista de zonas de la interfaz. Solamente se aplica a la configuración de ruteadores raíz.

## Ejemplo de configuración de un ruteador raíz

Un ruteador raíz tiene su propia configuración de red y zona codificada explícitamente. Los demás ruteadores pueden obtener su configuración de un ruteador raíz. Para configurar la unidad TAOS como un ruteador raíz, debe configurar un rango de red, una lista de zonas y especificar que la unidad es un ruteador raíz.

El rango de red es un rango de números enteros consecutivos entre 1 y 65.199. Cada rango debe ser exclusivo. Dos redes no pueden utilizar el mismo rango y dos rangos de red no pueden solaparse. Cada número del rango puede asociarse a un máximo de 253 nodos, de modo que el rango determina el número de clientes a los que puede dar soporte la interfaz. Por ejemplo, una interfaz con el rango 1006-1010 puede dar soporte a un máximo de 5 x 253, o 1265, clientes.

La lista de zonas es una lista de 1 a 32 nombres de zona AppleTalk. Cada nombre se compone de 1 a 33 caracteres, incluidos los espacios intercalados. Los caracteres deben formar parte del juego de caracteres de impresión estándar y no deben incluirse asteriscos (\*).

Los comandos siguientes configuran un ruteador raíz con el rango de red 1006–1010, tres zonas y la zona predeterminada para la interfaz de LAN:

```
admin> read atalk-int {{1 c 1} 0}
ATALK-INTERFACE/ { { shelf-1 controller 1 } 0 } read
admin> set atalk-routing = yes
admin> set atalk-router = atlk-router-seed
admin> set atalk-net-start = 1006
admin> set atalk-net-end = 1010
admin> set atalk-default-zone = engineering
admin> set atalk-zone-list 1 = admin
admin> set atalk-zone-list 2 = test
admin> set atalk-zone-list 2 = engineering
admin> write
ATALK-INTERFACE/ { { shelf-1 controller 1 } 0 } written
```

## Configuración de un ruteador no raíz

Un ruteador no raíz obtiene la configuración de zona y red de otro ruteador de la red. Si la unidad TAOS está configurada en modo no raíz, debe disponer de un ruteador raíz en el momento del inicio o, de lo contrario, la unidad TAOS no podrá activarse en modo de ruteo

AppleTalk (si la unidad TAOS se activa sin ruteo AppleTalk porque no hay no ruteadores raíz disponibles en el inicio, debe reiniciar el sistema cuando disponga de un ruteador raíz).

Cuando se reinicia el sistema, envía un paquete de petición ZipGetNetInfo para obtener la configuración de un ruteador raíz. Si especifica el nombre de la zona AppleTalk en la que reside la unidad TAOS (el procedimiento recomendado), el sistema puede incluir el nombre de la zona especificada en el paquete ZipGetNetInfo y el ruteador puede devolver un rango de red válido para dicha zona.

Los comandos siguientes configuran la unidad TAOS como ruteador no raíz:

```
admin> read atalk-int {{1 c 1} 0}
ATALK-INTERFACE/ { { shelf-1 controller 1 } 0 } read
admin> set atalk-routing = yes
admin> set atalk-router = atlk-router-non-seed
admin> set hint-zone = engineering
admin> write
ATALK-INTERFACE/ { { shelf-1 controller 1 } 0 } written
```

## ***Configuración de interfaces AppleTalk de WAN***

PPP y ARA son los protocolos de encapsulación que se utilizan para la conexión telefónica de AppleTalk en la unidad TAOS. El software de cliente PPP y ARA de AppleTalk lo distribuyen Apple Computer (tanto ARA y PPP reciben soporte en ARA 3.0) y otros proveedores; por ejemplo, Netmanage Pacer PPP. Tanto PPP como ARA de AppleTalk pueden utilizarse mediante un módem o una conexión de adaptador de terminal (TA) V.120 ISDN. Asimismo, PPP de AppleTalk puede utilizarse en una conexión síncrona PPP cuando la unidad que realiza la llamada es una unidad Pipeline o MAX.

**Nota:** El ruteo AppleTalk debe estar activo en un perfil Connection para conexiones PPP de entrada, pero no es necesario para conexiones de clientes ARA.

Puede configurar una conexión para AppleTalk de las maneras siguientes:

- Conexión cliente ARA
- Conexión PPP de llamada de entrada (PPP de AppleTalk)
- Conexión PPP síncrona con una unidad Pipeline o MAX (ruteo AppleTalk)
- Gateway DDP-IP (IP sobre AppleTalk)

## **Ajustes del perfil Answer-Defaults**

Para permitir conexiones de clientes ARA, debe activar ARA-Answer en el perfil Answer-Defaults. Además, si tiene previsto permitir el acceso como invitado de ARA, establezca el parámetro Profiles-Required en No (habitualmente está establecido en Yes por motivos de seguridad). A continuación se muestran los parámetros pertinentes:

```
[in ANSWER-DEFAULTS]
profiles-required = no

[in ANSWER-DEFAULTS:ara-answer]
enabled = yes
```

A continuación se muestra un ejemplo de entrada que activa ARA-Answer y desactiva el acceso como invitado de ARA:

```
admin> read answer
ANSWER-DEFAULTS read

admin> set ara-answer enabled = yes

admin> set profiles-required = yes

admin> write
ANSWER-DEFAULTS written
```

(Establecer Profiles-Required en Yes desactiva el acceso como invitado de ARA.)

## Ajustes de un perfil Connection

Puede configurar las conexiones ARA o PPP de AppleTalk utilizando los parámetros siguientes (que aparecen con ajustes de ejemplo):

```
[in CONNECTION/""]
encapsulation-protocol = ara

[in CONNECTION/":ara-options]
recv-password = test
ara-enabled = yes
maximum-connect-time = 0

[in CONNECTION/":appletalk-options]
atalk-routing-enabled = no
atalk-static-ZoneName = ""
atalk-static-NetStart = 0
atalk-static-NetEnd = 0
atalk-Peer-Mode = router-peer
```

Parámetro	Especifica
Encapsulation-Protocol	Método de encapsulación. En conexiones ARA, especifique ARA.
Recv-Password	Contraseña que se espera del cliente que efectúa la llamada de entrada.
ARA-Enabled	Activa y desactiva el procesamiento de ARA para la conexión.
Maximum-Connect-Time	Número máximo de minutos que una sesión de ARA puede permanecer conectada. El ajuste predeterminado, 0 (cero), desactiva el temporizador. Si se especifica un tiempo máximo de conexión, la unidad TAOS inicia una desconexión de ARA cuando se cumple el tiempo especificado. El enlace de ARA realiza una desconexión con previo aviso, pero los usuarios remotos no reciben ninguna notificación. Los usuarios verán que el enlace de ARA ha desaparecido sólo cuando intenten acceder a un dispositivo.
Atalk-Routing-Enabled	Activa y desactiva el ruteo AppleTalk para la conexión. Si no se ha activado el ruteo AppleTalk en el perfil Atalk-Interface o si el perfil Answer-Defaults no activa ARA-Answer, este parámetro no tendrá ningún efecto.

<b>Parámetro</b>	<b>Especifica</b>
Atalk-Static-Zonename	Nombre de zona que utiliza la unidad TAOS a la hora de rutear paquetes a un sitio remoto para una conexión AppleTalk de salida. Observe que actualmente sólo se da soporte a AppleTalk de entrada.
Atalk-Static-Netstart Atalk-Static-Netend	Rango de red para los paquetes que rutea la unidad TAOS al sitio remoto para la conexión AppleTalk de salida. Observe que actualmente sólo se da soporte a AppleTalk de entrada.
Atalk-Peer-Mode	Tipo de cliente de llamada de entrada (ruteador u homólogo de llamada de entrada). Con el ajuste Dialin-Peer, la unidad TAOS negocia una sesión de ruteo con el cliente de llamada de entrada asignando al cliente una dirección de nodo en la red virtual AppleTalk definida en el perfil Atalk-Global. El cliente debe aceptar el número de red que se le ha asignado.

## Ajustes de un perfil RADIUS

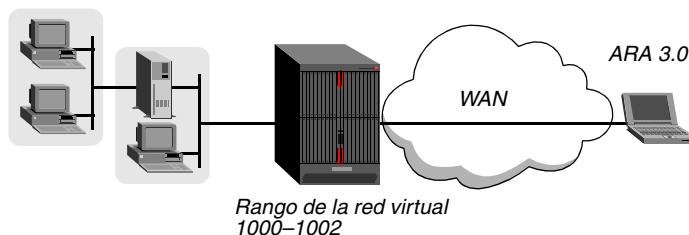
RADIUS utiliza los pares atributo-valor siguientes para configurar conexiones de ruteo ARA y AppleTalk:

<b>Atributo</b>	<b>Valor</b>
Framed-Protocol (7)	Método de encapsulación. En conexiones ARA, especifique ARA (255).
Ascend-Send-Secret (214)	Contraseña que el cliente de llamada de entrada envía al servidor.
Ascend-Route-Appletalk (118)	Activa y desactiva el ruteo AppleTalk para la conexión. Los valores válidos son Route-Appletalk-No (0) y Route-Appletalk-Yes (1).
Ascend-Appletalk-Peer-Mode (117)	Tipo de cliente de llamada de entrada. Los valores válidos son Appletalk-Peer-Router (0) y Appletalk-Peer-Dialin (1). Con el ajuste Appletalk-Peer-Dialin, la unidad TAOS negocia una sesión de ruteo con el cliente de llamada de entrada asignando al cliente una dirección de nodo en la red virtual AppleTalk definida en el perfil Atalk-Global. El cliente debe aceptar el número de red que se le ha asignado.

## Ejemplos de configuración de una conexión de cliente ARA

Una conexión de cliente ARA utiliza el protocolo de encapsulación ARA y no requiere ruteo AppleTalk. En la Figura 8-1, el cliente de llamada de entrada ejecuta ARA 3.0, con la encapsulación ARA seleccionada y con un módem interno. En este ejemplo, al cliente se le asignará una dirección de red en la red virtual 1000–1002 y un tiempo máximo de conexión ARA de 60 minutos.

*Figura 8-1. Conexión telefónica de un cliente ARA*



Los comandos siguientes configuran un perfil Connection para el cliente ARA:

```
admin> read connection araclient
CONNECTION/araclient read

admin> set active = yes
admin> set encaps = ara
admin> set ara-enabled = yes
admin> set ara recv-password = ara-password
admin> set maximum-connect-time = 60
admin> write
CONNECTION/araclient written
```

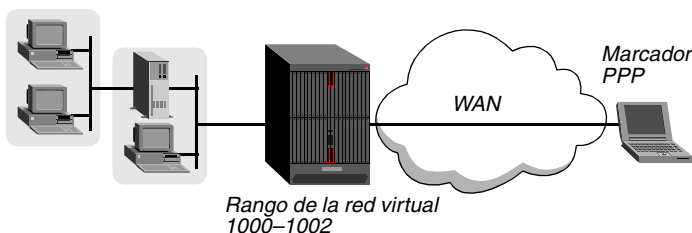
A continuación se muestra un perfil RADIUS equivalente:

```
araclient Password = "ara-password"
  Service-Type = Framed-User,
  Framed-Protocol = ARA,
  Ascend-Send-Secret = "ara-password"
```

## **Ejemplos de configuración de una conexión telefónica PPP de AppleTalk**

Una conexión de cliente de llamada de entrada PPP de AppleTalk utiliza el protocolo de encapsulación PPP. En la Figura 8-2, el cliente de llamada de entrada ejecuta ARA 3.0 y ha seleccionado la encapsulación PPP o utiliza otro marcador PPP que da soporte a AppleTalk. Al cliente se le asignará una dirección de red en la red virtual 1000-1002.

*Figura 8-2. Conexión de AppleTalk utilizando un marcador PPP*



Los comandos siguientes configuran un perfil Connection para el cliente PPP:

```
admin> new connection ppp-ataalk
CONNECTION/ppp-ataalk read

admin> set active = yes

admin> set encapsulation-protocol = ppp

admin> set ppp rcv-password = localpw

admin> set appletalk atalk-routing-enabled = yes

admin> set appletalk atalk-peer-mode = dialin

admin> write
CONNECTION/ppp-ataalk written
```

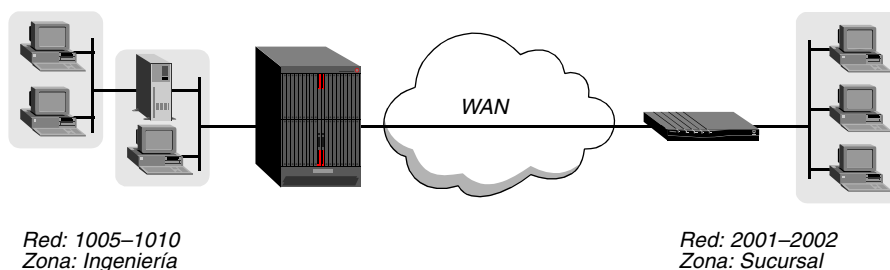
A continuación se muestra un perfil RADIUS equivalente:

```
ppp-ataalk Password = "localpw"
Service-Type = Framed-User,
Framed-Protocol = PPP,
Ascend-Route-Appletalk = Route-Appletalk-Yes,
Ascend-Appletalk-Peer-Mode = Appletalk-Peer-Dialin
```

## Ejemplos de configuración de una conexión con un ruteador AppleTalk

Una conexión de un ruteador AppleTalk utiliza el protocolo de encapsulación PPP o una de sus variantes multienlace (MP o MP+). En la Figura 8-3, se configura la unidad Pipeline remota como un ruteador AppleTalk que se encuentra en la red AppleTalk 2000-2001 ampliada en la zona Sucursal.

*Figura 8-3. Conexión del ruteo AppleTalk*



Los comandos siguientes configuran una conexión con el ruteador remoto:

```
admin> read connection atalk-router
CONNECTION/atalk-router read

admin> set active = yes

admin> set encaps = ppp

admin> set ppp rcv-password = rtr-password

admin> set appletalk atalk-routing enabled = yes

admin> set appletalk atalk-peer-mode = router-peer

admin> write
CONNECTION/atalk-router written
```

A continuación se muestra un perfil RADIUS equivalente:

```
atalk-router Password = "rtr-password"
Service-Type = Framed-User,
Framed-Protocol = PPP,
Ascend-Route-Appletalk = Route-Appletalk-Yes,
Ascend-Appletalk-Peer-Mode = Appletalk-Peer-Router
```

## Ejemplos de una conexión de IP sobre AppleTalk

Para rutear IP y AppleTalk, la unidad TAOS debe estar configurada como ruteador IP y ruteador AppleTalk. Si desea obtener información detallada acerca de la configuración del ruteador IP y las conexiones individuales IP, consulte el Capítulo 2, "Ruteo IP". Para dar soporte a IP, el perfil Connection del cliente de llamada de entrada debe especificar una configuración IP y el cliente debe configurar el software TCP/IP para Macintosh (por ejemplo, Open Transport). En la Tabla 8-1 se describen las configuraciones de TCP/IP para Macintosh en una conexión PPP.

*Tabla 8-1. Ajustes de TCP/IP para Macintosh en conexiones PPP*

Software de Macintosh	Ajustes de IP para una conexión PPP de AppleTalk
Open Transport	El Panel de control TCP/IP debe especificar una conexión PPP y la dirección IP del cliente. Si el perfil Connection tiene una dirección IP codificada explícitamente, escriba la dirección manualmente en el Panel de control. Si el perfil Connection especifica la asignación dinámica de direcciones, defina el Panel de control para obtener una dirección del servidor PPP.
MacTCP	En el Panel de control MacTCP debe seleccionar el icono de PPP y la dirección IP del cliente. Si el perfil Connection tiene una dirección IP codificada explícitamente, escriba la dirección manualmente en el Panel de control. Si el perfil Connection especifica la asignación dinámica de direcciones, defina el Panel de control para obtener una dirección de un servidor. (No se da soporte a la opción Dynamic en MacTCP.)

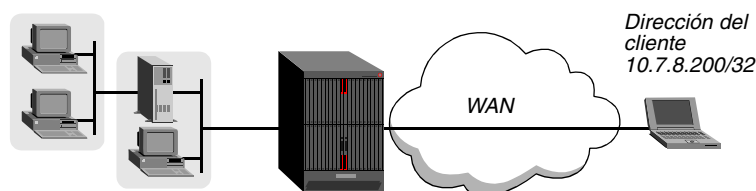
Cuando se utiliza la encapsulación de ARA, la unidad TAOS maneja los paquetes IP encapsulándolos en DDP. En la Tabla 8-2 se describen las configuraciones de TCP/IP para Macintosh en una conexión PPP.

*Tabla 8-2. Ajustes de TCP/IP para Macintosh en conexiones ARA*

Software de Macintosh	Ajustes de IP para una conexión ARA
Open Transport	El Panel de control TCP/IP debe especificar una conexión vía Mac-IP y la dirección IP del cliente. Si el perfil Connection tiene una dirección IP codificada explícitamente, escriba la dirección manualmente en el Panel de control. Si el perfil Connection especifica la asignación dinámica de una dirección, defina el Panel de control para obtener una dirección del servidor Mac-IP.
MacTCP	En el Panel de control MacTCP debe seleccionar el icono de ARA y la dirección IP del cliente. Si el perfil Connection tiene una dirección IP codificada explícitamente, escriba la dirección manualmente en el Panel de control. Si el perfil Connection especifica la asignación dinámica de direcciones, defina el Panel de control para obtener una dirección de un servidor. (No se da soporte a la opción Dynamic en MacTCP.)

En la Figura 8-4, el cliente de llamada de entrada ejecuta ARA 3.0 (que incluye funciones de túnel DDP-IP) y una aplicación IP, por ejemplo Telnet, para comunicarse con un host IP en la interfaz local de la unidad TAOS. El cliente tiene una dirección IP codificada explícitamente.

*Figura 8-4. Conexión ARA que encapsula paquetes IP en DDP*



Los comandos siguientes configuran un perfil que permite al cliente utilizar ARA 3.0 para efectuar la llamada de entrada y, a continuación, iniciar una conexión Telnet con un host en la red IP de la unidad TAOS:

```
admin> read connection ddpip-client
CONNECTION/ddpip-client read
admin> set active = yes
admin> set encaps = ara
admin> set ara ara-enabled = yes
admin> set ara recv-password = ara-password
admin> set ip-options remote = 10.7.8.200/32
admin> write
CONNECTION/ddpip-client written
```



A continuación se muestra un perfil RADIUS equivalente:

```
ddpip-client Password = "ara-password"  
Service-Type = Framed-User,  
Framed-Protocol = ARA,  
Framed-IP-Address = 10.7.8.200,  
Framed-IP-Netmask = 255.255.255.255,  
Ascend-Appletalk-Peer-Mode = Appletalk-Peer-Dialin
```



# Filtros de paquetes

Información general sobre filtros . . . . .	9-1
Definición de filtros genéricos . . . . .	9-7
Definición de filtros IP . . . . .	9-12
Definición de filtros de tipo de servicio (TOS) . . . . .	9-19
Definición de filtros IPX . . . . .	9-25
Definición de filtros de ruta . . . . .	9-28
Definición de filtros remotos dinámicos . . . . .	9-30
Aplicación de un filtro a una interfaz. . . . .	9-34

## ***Información general sobre filtros***

Un filtro consiste en especificaciones que describen paquetes y las acciones que se deben realizar con los paquetes que coinciden con las descripciones. Tras aplicar un filtro a una interfaz, la unidad TAOS supervisa la corriente de datos de dicha interfaz.

En función de la definición de un filtro, éste se puede aplicar a paquetes de entrada, a paquetes de salida o a ambos. Asimismo, los filtros son lo suficientemente flexibles como para especificar que se debe realizar una acción (como reenviar o descartar) en aquellos paquetes que coincidan con las especificaciones o en todos los paquetes *excepto* los que coincidan con las especificaciones.

## **Tipos básicos de filtros**

Cada perfil Filter contiene hasta 12 filtros de entrada (aplicados a paquetes de entrada) y 12 filtros de salida (aplicados a paquetes de salida). Cada una de las 24 especificaciones puede ser de uno de los tipos básicos de filtros siguientes:

- Filtros genéricos
- Filtros IP
- Filtros de tipo de servicio (TOS)
- Filtros IPX (solamente perfiles Filter locales)
- Filtros de ruta (solamente perfiles Filter locales)

Los filtros genéricos examinan el contenido de bytes o bits de cualquier paquete, comparando los bytes o bits especificados con un valor definido en el filtro. Según el resultado de esta comparación, el filtro especifica una acción de reenvío. Para utilizar los filtros genéricos de forma eficiente, es necesario conocer el contenido de determinados bytes en los paquetes que desea filtrar. Las especificaciones de protocolo son generalmente la mejor fuente de dicha información.

Los filtros IP solamente son válidos para paquetes relativos a IP. Especifican una acción de reenvío en función de los campos de nivel superior en paquetes IP (por ejemplo, la dirección de origen o de destino, o el número de protocolo). Funcionan con información lógica, que es relativamente fácil de obtener.

Los filtros de tipo de servicio (TOS) establecen bits de prioridad en la cabecera TOS de los paquetes IP. A continuación, otros ruteadores pueden utilizar la información para asignar una prioridad a los enlaces y seleccionarlos para corrientes de datos concretas.

Los filtros IPX solamente son válidos para paquetes NetWare. Especifican una acción de reenvío en función de los campos de nivel superior, por ejemplo red de origen o de destino, nodo y número de zócalo. Al igual que los filtros IP, los filtros IPX funcionan con información lógica, que es relativamente fácil de obtener.

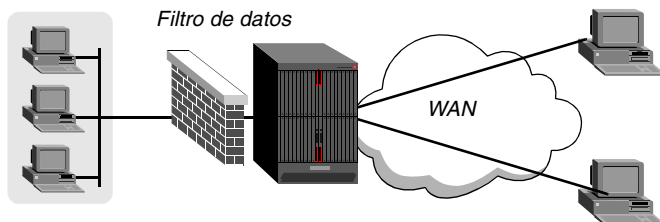
Los filtros de ruta solamente son válidos para paquetes de actualización de RIP. Especifican si las rutas coincidentes en un paquete RIP se aceptan, se rechazan o se aceptan con un aumento de métrica en la tabla de ruteo. Los filtros de ruta también pueden especificar una dirección de origen, lo que significa que pueden intervenir en todas las actualizaciones de dicha dirección.

## **Filtros de datos y de llamada**

Los filtros de datos se utilizan habitualmente por razones de seguridad, pero también son válidos siempre que se requiera el descarte o reenvío de paquetes específicos por parte de la unidad TAOS. Normalmente la función principal es evitar la entrada de tráfico no deseado a una LAN. Por ejemplo, puede utilizar filtros de datos para descartar paquetes dirigidos a determinados hosts o para evitar que las difusiones atraviesen la WAN. También puede utilizar filtros de datos para permitir a los usuarios acceder solamente a dispositivos específicos de la WAN.

Cuando se aplica un filtro de datos, la acción de reenvío (reenvío o descarte) afecta a la corriente de datos real evitando que determinados paquetes alcancen la Ethernet desde la WAN, y viceversa. Los filtros de datos no afectan al temporizador de inactividad y un filtro de datos aplicado a un perfil Connection no afecta al proceso de respuesta.

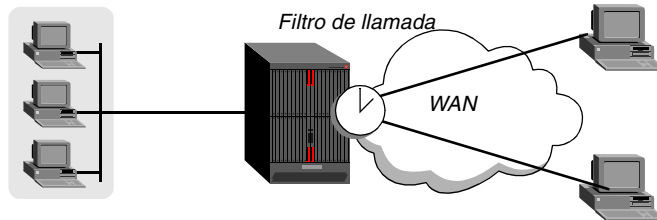
*Figura 9-1. Los filtros de datos eliminan o reenvían determinados paquetes*



Los filtros de llamada evitan que se efectúen conexiones innecesarias y ayudan a la unidad TAOS a distinguir entre el tráfico activo y el “ruido”. De manera predeterminada, el tráfico

hacia un sitio remoto desencadena una llamada y el tráfico a través de una conexión activa reinicia el temporizador de inactividad de la conexión.

*Figura 9-2. Los filtros de llamada evitan que determinados paquetes reinicien el temporizador*



Cuando se aplica un filtro de llamada, la acción de reenvío (reenvío o descarte) *no* afecta a los paquetes que se envían a través de una conexión activa. La acción de reenvío de un filtro de llamada determina los paquetes que pueden iniciar una conexión o reiniciar un temporizador de sesión. Cuando el temporizador de inactividad de una sesión alcanza su límite, se interrumpe dicha sesión. Con el ajuste predeterminado del temporizador de inactividad de 120 segundos, la unidad TAOS interrumpe una conexión que ha estado inactiva durante dos minutos.

## Funcionamiento de los filtros

Un perfil Filter puede incluir hasta 12 especificaciones de filtro de entrada y 12 especificaciones de filtro de salida (filtros). Cada filtro posee su propia acción de reenvío (reenvío o descarte). Los filtros se aplican secuencialmente. Cuando se produce la primera comparación satisfactoria entre un filtro y el paquete que se examina, el proceso de filtrado se detiene y la acción de reenvío especificada en dicho filtro se aplica al paquete. Dado que la acción de reenvío no tiene ningún efecto para los filtros de ruta, cuando la comparación es satisfactoria se aplica al paquete otro tipo de acción del filtro.

Si ninguna comparación es satisfactoria, el paquete no coincide con el filtro. Sin embargo, esto no significa que se reenvíe el paquete. Cuando no hay ningún filtro en uso, la unidad TAOS reenvía todos los paquetes, pero la aplicación de un filtro a una interfaz permite cambiar este comportamiento predeterminado. Por razones de seguridad, la unidad no reenvía automáticamente los paquetes no coincidentes. Se requiere un filtro que permita explícitamente el paso de dichos paquetes. Para obtener información sobre un filtro de entrada de ejemplo que reenvía los paquetes que no coinciden con un filtro previo, consulte “Ejemplos de un filtro IP para evitar la suplantación de direcciones locales” en la página 9-16.

**Nota:** Para que un filtro de llamada evite que una interfaz permanezca activa de forma innecesaria, debe definir filtros tanto para los paquetes de entrada como de salida. De lo contrario, si solamente se definen filtros de entrada, los paquetes de salida mantendrán activa una conexión, y viceversa.

### *Filtros genéricos*

En un filtro genérico, todos los ajustes de una especificación de filtro funcionan conjuntamente para especificar una ubicación en un paquete y un número para comparar con dicha ubicación. También se debe especificar el tipo de comparación que constituye una coincidencia (igual o desigual). Si falla una comparación, el paquete se somete a la comparación siguiente. Cuando

una comparación es satisfactoria, el proceso de filtrado se detiene y la acción de reenvío especificada en dicho filtro se aplica al paquete.

Si se aplica un filtro genérico como filtro de llamada y se obtiene una comparación satisfactoria, la acción de reenvío puede suponer el reinicio o no del temporizador de inactividad, en función de la definición del filtro. Si se aplica un filtro genérico como filtro de datos, la acción de reenvío puede suponer el reenvío del paquete o su descarte.

## *Filtros IP*

En un filtro IP, cada especificación de filtro incluye un conjunto de comparaciones que se llevan a cabo en un orden definido. Si falla una comparación, el paquete se somete a la comparación siguiente. Cuando una comparación es satisfactoria, el proceso de filtrado se detiene y la acción de reenvío especificada en dicho filtro se aplica al paquete. Las pruebas del filtro IP se realizan en el orden siguiente:

- 1 Se aplica el valor Source-Address-Mask al valor Source-Address y se compara el resultado con la dirección de origen del paquete. Si no son iguales, la comparación falla.
- 2 Se aplica el valor Dest-Address-Mask al valor Dest-Address y se compara el resultado con la dirección de destino del paquete. Si no son iguales, la comparación falla.
- 3 Si el parámetro Protocol es cero (es decir, coincide con cualquier protocolo), la comparación es satisfactoria. Si es distinto de cero y no es igual al campo de protocolo del paquete, la comparación falla.
- 4 Si el parámetro Src-Port-Cmp no tiene el valor None, se compara el número Source-Port con el número del puerto de origen del paquete. Si no coinciden como especifica el parámetro Src-Port-Cmp, la comparación falla.
- 5 Si el parámetro Dst-Port-Cmp no tiene el valor None, se compara el número Dest-Port con el número de puerto de destino del paquete. Si no coinciden como especifica el parámetro Dst-Port-Cmp, la comparación falla.
- 6 Si el parámetro TCP-Estab tiene el valor Yes y el número de protocolo es 6, la comparación es satisfactoria.

Si se aplica un filtro IP como filtro de llamada y se obtiene una comparación satisfactoria, la acción de reenvío puede suponer el reinicio o no del temporizador de inactividad, en función de la definición del filtro. Si se aplica un filtro IP como filtro de datos, la acción de reenvío puede suponer el reenvío del paquete o su descarte.

## *Tipo de filtros de servicio*

En un filtro TOS de IP, cada especificación de filtro incluye un conjunto de comparaciones que se llevan a cabo en un orden definido. Si falla una comparación, el paquete se somete a la comparación siguiente. Cuando una comparación es satisfactoria, el proceso de filtrado se detiene y la acción especificada en dicho filtro se aplica al paquete. Las pruebas del filtro TOS se realizan en el orden siguiente:

- 1 Se aplica el valor Source-Address-Mask al valor Source-Address y se compara el resultado con la dirección de origen del paquete. Si no son iguales, la comparación falla.
- 2 Se aplica el valor Dest-Address-Mask al valor Dest-Address y se compara el resultado con la dirección de destino del paquete. Si no son iguales, la comparación falla.

- 3 Si el parámetro Protocol es cero (es decir, coincide con cualquier protocolo), la comparación es satisfactoria. Si es distinto de cero y no es igual al campo de protocolo del paquete, la comparación falla.
- 4 Si el parámetro Src-Port-Cmp no tiene el valor None, se compara el número Source-Port con el número del puerto de origen del paquete. Si no coinciden como especifica el parámetro Src-Port-Cmp, la comparación falla.
- 5 Si el parámetro Dst-Port-Cmp no tiene el valor None, se compara el número Dest-Port con el número de puerto de destino del paquete. Si no coinciden como especifica el parámetro Dst-Port-Cmp, la comparación falla.

Si una comparación es satisfactoria, el sistema establece los bits de prioridad y la clase de servicio (en función de la definición de filtro) en la cabecera TOS del paquete.

## *Filtros IPX*

En un filtro IPX, cada especificación de filtro incluye un conjunto de comparaciones que se llevan a cabo en un orden definido. Si falla una comparación, el paquete se somete a la siguiente comparación. Cuando una comparación es satisfactoria, el proceso de filtrado se detiene y la acción de reenvío especificada en dicho filtro se aplica al paquete. Las pruebas del filtro IPX se realizan en el orden siguiente:

- 1 Se compara el número Src-Net-Address con el número de red de origen del paquete. Si no son iguales, la comparación falla.
- 2 Se compara el número Dest-Net-Address con el número de red de destino en el paquete. Si no son iguales, la comparación falla.
- 3 Se compara el número Src-Node-Address con el número de nodo de origen del paquete. Si no son iguales, la comparación falla.
- 4 Se compara el número Dest-Node-Address con el número de nodo de destino en el paquete. Si no son iguales, la comparación falla.
- 5 Si el parámetro Src-Socket-Cmp no tiene el valor None, se compara el número Src-Socket con el número de zócalo de origen del paquete. Si no coinciden como especifica el parámetro Src-Socket-Cmp, la comparación falla.
- 6 Si el parámetro Dst-Socket-Cmp no tiene el valor None, se compara el número Dest-Socket con el número de zócalo de destino del paquete. Si no coinciden como especifica el parámetro Dst-Socket-Cmp, la comparación falla.

Si se aplica un filtro IPX como filtro de llamada y se obtiene una comparación satisfactoria, la acción de reenvío puede suponer el reinicio o no del temporizador de inactividad, en función de la definición del filtro. Si se aplica un filtro IPX como filtro de datos, la acción de reenvío puede suponer el reenvío del paquete o su descarte.

## *Filtros de ruta*

En un filtro de ruta, cada especificación de filtro incluye un conjunto de comparaciones que se llevan a cabo en un orden definido. Si falla una comparación, el paquete RIP se somete a la comparación siguiente. Cuando una comparación es satisfactoria, el proceso de filtrado se detiene y la acción especificada en dicho filtro se aplica a la ruta o paquete coincidente. Las pruebas del filtro de ruta se realizan en el orden siguiente:

- 1 Se aplica el valor Source-Address-Mask al valor Source-Address y se compara el resultado con la dirección de origen del paquete. Si no son iguales, la comparación falla.

- 2 Se aplica el valor Route-Mask al valor Route-Address y se compara el resultado con las rutas en el paquete. Si no coinciden, la comparación falla.

Si una comparación es satisfactoria, el sistema lleva a cabo una de las acciones siguientes, en función de la definición del filtro:

- Si el parámetro Action tiene el valor Add, se aumenta el campo métrico de las rutas coincidentes mediante el valor Add-Metric y, a continuación, se agregan las rutas a la tabla de ruteo.
- Si el parámetro Action tiene el valor Accept, se agregan las rutas coincidentes a la tabla de ruteo.
- Si el parámetro Action tiene el valor Deny, se rechazan las rutas coincidentes (no se agregan a la tabla de ruteo).

## Especificación de la dirección de un filtro

Un perfil Filter local puede definir hasta 12 especificaciones de filtro de entrada y 12 especificaciones de filtro de salida. A continuación se muestran los parámetros pertinentes (que aparecen con los ajustes predeterminados):

```
[in FILTER/"":input-filters:input-filters[1]]
valid-entry = no

[in FILTER/"":output-filters:output-filters[1]]
valid-entry = no
```

Parámetro	Especifica
Input-Filters (1–12)	Cada filtro puede contener hasta 12 especificaciones de filtro de entrada, las cuales se definen por separado y se aplican ordenadamente (1–12) en la corriente de paquetes de entrada. El orden en que se definen los filtros de entrada es importante.
Output-Filters (1–12)	Cada filtro puede contener hasta 12 especificaciones de filtro de salida, las cuales se definen por separado y se aplican ordenadamente (1–12) en la corriente de paquetes de salida. El orden en que se definen los filtros de salida es importante.
Valid-Entry	Activa y desactiva la especificación de filtro. Con un ajuste No (el ajuste predeterminado), la especificación se omite cuando se filtra la corriente de datos. Establezca este parámetro en Yes para cada filtro definido que pretenda utilizar.

En un perfil RADIUS, cada filtro se especifica por separado utilizando los atributos Ascend-Data-Filter y Ascend-Call-Filter. Como sucede siempre con los filtros, el orden en que se aplican en el perfil de usuario es importante.

En una definición de filtro RADIUS, debe especificar la dirección en que se controla la corriente de datos bien como `in` o bien como `out`. Este ajuste proporciona la misma función que los parámetros Input-Filters y Output-Filters de un perfil local. El ejemplo siguiente muestra una definición de filtro de entrada en RADIUS:

```
test-user Password = "test-pw"
Ascend-Data-Filter = "ip in forward tcp dstport > 1023"
```



## Especificación de una acción de reenvío de un filtro

Para filtros genéricos, IP o IPX, cada filtro de entrada o de salida de un perfil Filter local especifica una acción de reenvío para los paquetes que coinciden con el filtro. A continuación se muestra el parámetro pertinente (que aparece con el ajuste predeterminado):

```
[in FILTER/"":input-filters:input-filters[1]]
forward = no

[in FILTER/"":output-filters:output-filters[1]]
forward = no
```

Parámetro	Especifica
Forward	Acción de reenvío para el filtro. Cuando no hay ningún filtro en uso, la unidad TAOS reenvía de forma predeterminada todos los paquetes. Cuando hay un filtro en uso, el valor predeterminado es descartar los paquetes coincidentes (Forward = No).

**Nota:** Para los filtros de ruta y de tipo de servicio, la acción de reenvío no tiene ningún efecto. Estos filtros realizan un tipo de acción diferente con los paquetes coincidentes.

En una definición RADIUS, debe especificar la acción que realiza un filtro como `forward` o `drop`. Este ajuste proporciona la misma función que el parámetro Forward en un perfil local. En el ejemplo siguiente se muestra un filtro de entrada cuya acción de reenvío es descartar los paquetes coincidentes:

```
test-user Password = "test-pw"
Ascend-Data-Filter = "ip in drop tcp dstport > 1023"
```

## Definición de filtros genéricos

Los filtros genéricos pueden coincidir con cualquier paquete, independientemente del tipo de protocolo o de los campos de cabecera. Las especificaciones de filtro funcionan conjuntamente para definir una ubicación en un paquete y un valor hexadecimal para compararlo.

## Ajustes de un perfil Filter local

En un perfil Filter local, un filtro genérico utiliza los parámetros siguientes (que aparecen con los ajustes predeterminados):

```
[in FILTER/"":input-filters:input-filters[1]]
type = generic-filter

[in FILTER/"":input-filters:input-filters[1]:gen-filter]
offset = 0
len = 0
more = no
comp-neq = no
mask = 00:00:00:00:00:00:00:00:00:00:00:00
value = 00:00:00:00:00:00:00:00:00:00:00:00
```

Los mismos parámetros también están disponibles en el subperfil Output-Filters. Si establece los parámetros en un filtro de entrada, solamente se examinarán los paquetes de entrada. Si los establece en un filtro de salida, solamente se examinarán los paquetes de salida.

Parámetro	Especifica
Type	Tipo de filtro. Los valores válidos son Generic-Filter (el valor predeterminado), IP-Filter, IPX-Filter, Route-Filter y TOS-Filter. Solamente serán válidos los parámetros en el subperfil correspondiente.
Offset	Desplazamiento en bytes a partir del que se debe empezar a comparar el contenido del paquete con el ajuste Value especificado en el filtro. Para obtener información detallada, consulte el apartado “Especificación del desplazamiento de los bytes que se deben examinar” en la página 9-10.
Len	Número de bytes que se deben analizar en un paquete; se empieza por el byte especificado por el parámetro Offset. Para obtener información detallada, consulte el apartado “Especificación del número de bytes que se deben analizar” en la página 9-10.
More	Activa y desactiva la aplicación del filtro siguiente antes de determinar si el paquete coincide con la especificación. Si More tiene el valor Yes, la especificación actual se enlaza con la inmediatamente posterior. La coincidencia solamente se produce si <i>ambas</i> especificaciones coinciden. Debe activarse la siguiente especificación ya que, de lo contrario, la unidad TAOS pasa por alto la especificación de filtro en la que More tiene el valor Yes. El parámetro More permite crear un filtro que examina múltiples bytes no contiguos en un paquete antes de adoptar la decisión de reenvío.
Comp-Neq	Tipo de comparación que se debe realizar. Si Comp-Neq (Compare-Not-Equals) tiene el valor Yes, la comparación es satisfactoria (el filtro coincide) si el contenido es distinto del valor especificado. Si un filtro requiere que el contenido del paquete sea igual al valor especificado, establezca Comp-Neq en No.
Mask	Máscara binaria. El sistema aplica la máscara al valor especificado por el parámetro Value antes de compararlo con los bytes del paquete especificado por el parámetro Offset. Para obtener información detallada, consulte el apartado “Enmascaramiento del valor antes de la comparación” en la página 9-11.
Value	Número hexadecimal que debe compararse con los datos del paquete identificados mediante los cálculos Offset, Length y Mask. Tras introducir el número, el sistema incluye dos puntos (:) en los límites de byte.

## Ajustes de un perfil RADIUS

En RADIUS, una entrada de filtro genérico es un valor de los atributos Ascend-Call-Filter o Ascend-Data-Filter. Para especificar un valor de filtro genérico, utilice el formato siguiente:

```
"generic dir action offset mask value compare [more]"
```

Palabra clave o argumento	Valor
<i>generic</i>	Tipo de filtro. Los tipos válidos especificados por los atributos Ascend-Data-Filter y Ascend-Call-Filter son <i>generic</i> (el valor predeterminado) e <i>ip</i> .
<i>dir</i>	Especifica la dirección de los paquetes. Puede especificar bien <i>in</i> (para filtrar los paquetes que llegan a la unidad TAOS ) o bien <i>out</i> (para filtrar los paquetes que salen de la unidad TAOS).
<i>action</i>	Especifica la acción que realiza la unidad TAOS con un paquete que coincide con el filtro. Puede especificar <i>forward</i> o <i>drop</i> .
<i>offset</i>	Desplazamiento en bytes en un paquete a partir del que se debe empezar a comparar el contenido del paquete con el <i>value</i> especificado en el filtro. Para obtener información detallada, consulte el apartado “Especificación del desplazamiento de los bytes que se deben examinar” en la página 9-10.
<i>mask</i>	Máscara binaria. El sistema aplica la <i>mask</i> al <i>value</i> especificado antes de compararlo con los bytes especificados por <i>offset</i> . Para obtener información detallada, consulte el apartado “Enmascaramiento del valor antes de la comparación” en la página 9-11.
<i>value</i>	Número hexadecimal para comparar con el contenido del paquete en el <i>offset</i> especificado. La longitud del número debe ser igual a la longitud de la máscara (hasta 12 bytes).
<i>compare</i>	Operador de comparación que determina la manera en que la unidad TAOS compara el contenido del paquete con el valor del filtro. Puede especificar <i>=</i> (igual a) o <i>!=</i> (distinto de). El valor predeterminado es <i>=</i> (igual a).
<i>more</i>	Si el indicador <i>more</i> está presente, la unidad TAOS aplica al paquete actual la siguiente definición de filtro del perfil antes de decidir si reenviarlo o descartarlo. El sentido y la acción de reenvío del filtro siguiente debe ser igual a la del filtro actual pues, de lo contrario, la unidad TAOS pasa por alto este indicador.

## Especificación del desplazamiento de los bytes que se deben examinar

El desplazamiento en un filtro genérico es un desplazamiento en bytes desde el inicio de un paquete hasta el inicio de los datos del paquete que se deben analizar. Por ejemplo, con la especificación de filtro siguiente:

```
[in FILTER/"":input-filters:input-filters[1]:gen-filter]
offset = 2
len = 8
more = no
comp-neq = no
mask = 0f:ff:ff:ff:00:00:00:f0:00:00:00:00
value = 07:fe:45:70:00:00:00:90:00:00:00:00
```

o la definición de filtro RADIUS equivalente:

```
Ascend-Data-Filter = "generic in drop 2 0ffffff000000f
07fe45700000009"
```

y el contenido del paquete siguiente:

```
2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

los dos primeros bytes en el paquete (2A y 31) se pasan por alto a causa del desplazamiento de dos bytes.

## Especificación del número de bytes que se deben analizar

En un perfil RADIUS, la longitud de la máscara debe ser igual a la longitud de Value. El sistema analiza este número de bytes en el paquete, empezando por el desplazamiento especificado. En un perfil Filter local, el ajuste Len especifica el número de bytes que se deben analizar en un paquete, empezando por el byte especificado por el parámetro Offset. Se supone que el ajuste Mask tiene el mismo número de octetos que los datos especificados por el parámetro Len.

Por ejemplo, con la especificación de filtro siguiente:

```
[in FILTER/"":input-filters:input-filters[1]:gen-filter]
offset = 2
len = 8
more = no
comp-neq = no
mask = 0f:ff:ff:ff:00:00:00:f0:00:00:00:00
value = 07:fe:45:70:00:00:00:90:00:00:00:00
```

y el contenido del paquete siguiente:

```
2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

el filtro analiza al valor del byte tres (97) al byte diez (99).

## Enmascaramiento del valor antes de la comparación

Un filtro genérico puede incluir una máscara que se debe aplicar al valor especificado por el parámetro Value antes de que la unidad TAOS lo compare con los bytes a partir del desplazamiento especificado. Puede utilizar la máscara para especificar exactamente los bits que desea comparar. Se supone que la máscara tiene el mismo número de octetos que los datos especificados por el parámetro Len.

La unidad TAOS convierte a un formato binario tanto la máscara como el valor especificado por el parámetro Value y, a continuación, aplica un AND lógico a los resultados. Cada 0 (cero) binario de la máscara oculta un bit en la posición correspondiente en el valor. Una máscara compuesta exclusivamente por unos (FF:FF:FF:FF:FF:FF:FF) no enmascara ningún bit, por lo que todo el valor especificado debe coincidir con el contenido del paquete. Por ejemplo, con la especificación de filtro siguiente:

```
[in FILTER/"":input-filters:input-filters[1]:gen-filter]
offset = 2
len = 8
more = no
comp-neq = no
mask = 0f:ff:ff:ff:00:00:00:f0:00:00:00:00
value = 07:fe:45:70:00:00:00:90:00:00:00:00
```

o la definición de filtro RADIUS equivalente:

```
Ascend-Data-Filter = "generic in drop 2 0ffffff000000f
07fe45700000009"
```

y el contenido del paquete siguiente:

```
2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

el ajuste Value coincide con los datos del paquete tras la aplicación de la máscara.

	Desplazamiento de 2 bytes	Comparación de 8 bytes
	2A 31	97 FE 45 70 12 22 33 99 B4 80 75
Máscara .....		0F FF FF FF 00 00 00 F0
Resultado de máscara .....		07 FE 45 70 00 00 00 90
Valor que analizar .....		07 FE 45 70 00 00 00 90

Suponiendo que el parámetro Forward tenga el valor No, el paquete se descarta dado que coincide con el filtro. La comparación de bytes funciona de la forma siguiente:

- La unidad TAOS pasa por alto 2A y 31 debido al desplazamiento de dos bytes.
- El 9 en el tercer byte también se pasa por alto dado que la máscara muestra un 0 (cero) en su lugar. El 7 en el tercer byte coincide con el 7 del parámetro Value para dicho byte.
- En el cuarto byte, F y E coinciden con el cuarto byte especificado por el parámetro Value.
- En el quinto byte, 4 y 5 coinciden con el quinto byte especificado por el parámetro Value.
- En el sexto byte, 7 y 0 coinciden con el sexto byte especificado por el parámetro Value.
- El séptimo (12), octavo (22) y noveno (33) byte se pasan por alto porque la máscara muestra ceros en su lugar.

- En el décimo byte, 9 coincide con el 9 del parámetro Value para dicho byte. El segundo 9 en el décimo byte del paquete se pasa por alto dado que la máscara muestra un 0 (cero) en su lugar.

## Ejemplo de un filtro de llamada genérico

El ejemplo siguiente se explica cómo definir un filtro de llamada genérico. El objetivo del filtro es evitar que los paquetes de entrada reinicien el temporizador de la sesión.

En el filtro de entrada, los valores predeterminados permanecen inalterados en el subperfil Gen-Filter, con lo que todos los paquetes coinciden. Además, la acción de reenvío se mantiene en el valor predeterminado No. En el filtro de salida, los valores predeterminados coinciden de nuevo con todos los paquetes, pero la acción de reenvío se establece en Yes. Por lo tanto, el filtro no evita que los paquetes de salida reinicien el temporizador o hagan una llamada.

```
admin> new filter out-only
FILTER/out-only read

admin> set input 1 valid = yes
admin> set output 1 valid = yes
admin> set output 1 forward = yes
admin> write
FILTER/out-only written
```

A continuación se muestra una definición del filtro RADIUS equivalente:

```
test-user Password = "test-pw"
Ascend-Call-Filter = "generic in drop"
Ascend-Call-Filter = "generic out forward"
```

## Definición de filtros IP

Los filtros IP afectan solamente a los paquetes IP y a los paquetes relacionados. Utilizan información de alto nivel de los paquetes (por ejemplo, números de protocolo, direcciones lógicas y puertos TCP o UDP).

## Ajustes de un perfil Filter local

El subperfil IP-Filter contiene los parámetros siguientes (que aparecen con los valores predeterminados):

```
[in FILTER/"":input-filters:input-filters[1]]
type = ip-filter

[in FILTER/"":input-filters:input-filters[1]:ip-filter]
protocol = 0
source-address-mask = 0.0.0.0
source-address = 0.0.0.0
dest-address-mask = 0.0.0.0
dest-address = 0.0.0.0
Src-Port-Cmp = none
source-port = 0
Dst-Port-Cmp = none
```

```
dest-port = 0  
tcp-estab = no
```

Los mismos parámetros también están disponibles en el subperfil Output-Filters. Si establece los parámetros en un filtro de entrada, solamente se examinarán los paquetes de entrada. Si los establece en un filtro de salida, solamente se examinarán los paquetes de salida.

Parámetro	Especifica
Type	Tipo de filtro. Los valores válidos son Generic-Filter (el valor predeterminado), IP-Filter, IPX-Filter, Route-Filter y TOS-Filter. Solamente serán válidos los parámetros en el subperfil correspondiente.
Protocol	Número de protocolo. El valor 0 (cero) coincide con todos los protocolos. Si especifica un número distinto de cero, la unidad TAOS lo compara con el campo Protocol en cada paquete. Para obtener una lista de los números de protocolo asignados, consulte el documento RFC 1700, <i>Assigned Numbers</i> , por Reynolds, J. y Postel, J.; octubre de 1994.
Source-Address-Mask	Máscara que se debe aplicar al valor Source-Address antes de compararlo con la dirección de origen de un paquete.
Source-Address	Dirección IP. Tras aplicar el valor Source-Address-Mask, la unidad TAOS compara el resultado con la dirección de origen de un paquete. Para obtener información detallada, consulte el apartado “Filtrado por dirección de origen o de destino” en la página 9-15.
Dest-Address-Mask	Máscara que se debe aplicar al valor Dest-Address antes de compararlo con la dirección de destino de un paquete.
Dest-Address	Dirección IP. Tras aplicar el valor Dest-Address-Mask, la unidad TAOS compara el resultado con la dirección de origen de un paquete. Para obtener información detallada, consulte el apartado “Filtrado por dirección de origen o de destino” en la página 9-15.
Src-Port-Cmp	Tipo de comparación que se debe realizar al comparar números de puerto de origen. Con un ajuste None (el ajuste predeterminado), no se efectúa ninguna comparación. Puede especificar que el filtro coincida con el paquete si el número de puerto de origen del paquete es Less (menor que), Eql (igual a), Gtr (mayor que) o Neq (distinto de) que el valor Source-Port.
Source-Port	Número de puerto que se debe comparar con el puerto de origen de un paquete. Por lo general, los números de puerto TCP y UDP se asignan a servicios. Para obtener información detallada, consulte el apartado “Filtrado por números de puerto” en la página 9-16.
Dst-Port-Cmp	Tipo de comparación que se debe realizar al comparar números de puerto de destino. Con un ajuste None (el ajuste predeterminado), no se efectúa ninguna comparación. Puede especificar que el filtro coincida con el paquete si el número de puerto de destino del paquete es Less (menor que), Eql (igual a), Gtr (mayor que) o Neq (distinto de) que el valor Dest-Port.

Parámetro	Especifica
Dest-Port	Número de puerto que se debe comparar con el puerto de destino de un paquete. Por lo general, los números de puerto TCP y UDP se asignan a servicios. Para obtener información detallada, consulte el apartado “Filtrado por números de puerto” en la página 9-16.
TCP-Estab	Activa y desactiva la aplicación del filtro solamente a paquetes de una sesión TCP establecida. Solamente es válido si el número de protocolo es 6 (TCP).

## Ajustes de un perfil RADIUS

En RADIUS, una entrada de filtro IP es un valor de los atributos Ascend-Call-Filter o Ascend-Data-Filter. Para especificar un valor de filtro IP, utilice el formato siguiente:

```
"ip dir action [ dstip n.n.n.n/nn ] [ srcip n.n.n.n/nn ] [[ proto ]  
[ destport cmp value ] [ srcport cmp value ] [est]]"
```

**Nota:** Una definición de filtro no puede contener indicadores de línea nueva. Se muestra la sintaxis en dos líneas para fines exclusivamente de impresión.

Palabra clave o argumento	Valor
<i>ip</i>	Tipo de filtro. Los tipos válidos especificados por los atributos Ascend-Data-Filter y Ascend-Call-Filter son <i>generic</i> (el valor predeterminado) e <i>ip</i> .
<i>dir</i>	Especifica la dirección de los paquetes. Puede especificar bien <i>in</i> (para filtrar los paquetes que llegan a la unidad TAOS ) o bien <i>out</i> (para filtrar los paquetes que salen de la unidad TAOS).
<i>action</i>	Especifica la acción que realiza la unidad TAOS con un paquete que coincide con el filtro. Puede especificar <i>forward</i> o <i>drop</i> .
<i>dstip n.n.n.n/nn</i>	Si después de la palabra clave <i>dstip</i> aparece una dirección IP válida, el filtro coincidirá solamente con los paquetes que presenten dicha dirección de destino. Si una parte de la máscara de subred de la dirección está presente, la unidad TAOS compara solamente los bits enmascarados. Si después de la palabra clave <i>dstip</i> aparece una dirección cero (0.0.0.0) o si dicha palabra clave y su especificación de dirección IP no están presentes, el filtro coincide con todos los paquetes IP. Para obtener información detallada, consulte el apartado “Filtrado por dirección de origen o de destino” en la página 9-15.



<b>Palabra clave o argumento</b>	<b>Valor</b>
<code>srcip n.n.n.n/nn</code>	Si después de la palabra clave <code>srcip</code> aparece una dirección IP válida, el filtro coincidirá solamente con los paquetes que presenten dicha dirección de origen. Si una parte de la máscara de subred de la dirección está presente, la unidad TAOS compara solamente los bits enmascarados. Si después de la palabra clave <code>srcip</code> aparece una dirección cero (0.0.0.0) o si dicha palabra clave y su especificación de dirección IP no están presentes, el filtro coincide con todos los paquetes IP. Para obtener información detallada, consulte el apartado “Filtrado por dirección de origen o de destino” en la página 9-15.
<code>proto</code>	Número de protocolo. El valor cero coincide con todos los protocolos. Si especifica un número que no sea cero, la unidad TAOS lo compara con el campo Protocol de los paquetes. Para obtener una lista de números de protocolo, consulte el documento RFC 1700.
<code>dstport cmp value</code>	Si después de la palabra clave <code>dstport</code> aparece un símbolo de comparación y un número, el número se compara con el puerto de destino de un paquete. El símbolo de comparación puede ser < (menor que), = (igual a), > (mayor que) o != (distinto de). El valor del puerto puede ser uno de los nombres o números siguientes: ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514) o talk (517). Para obtener información detallada, consulte el apartado “Filtrado por números de puerto” en la página 9-16.
<code>srcport cmp value</code>	Si después de la palabra clave <code>srcport</code> aparece un símbolo de comparación y un número, el número se compara con el puerto de origen de un paquete. El símbolo de comparación puede ser < (menor que), = (igual a), > (mayor que) o != (distinto de). El valor del puerto puede ser uno de los nombres o números siguientes: ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514) o talk (517). Para obtener información detallada, consulte el apartado “Filtrado por números de puerto” en la página 9-16.
<code>est</code>	Si el indicador <code>est</code> está presente, restringe la aplicación del filtro a los paquetes de una sesión TCP establecida. El número de protocolo se debe establecer en 6 (TCP) o, de lo contrario, se pasa por alto el indicador.

## Filtrado por dirección de origen o de destino

Cuando especifica una dirección de origen o de destino en un filtro IP, la unidad TAOS aplica la acción de reenvío del filtro a los paquetes recibidos o enviados desde dicha dirección. Si también especifica una máscara de subred, la unidad TAOS aplica la máscara al valor de

dirección antes de comparar el valor resultante con la dirección de origen o de destino de un paquete.

Para aplicar la máscara, la unidad TAOS convierte los valores de máscara y dirección a formato binario y, a continuación, utiliza un AND lógico para aplicar la máscara a la dirección. La máscara oculta los bits cuyas posiciones coinciden con las de los ceros binarios en la máscara. Una máscara compuesta exclusivamente por ceros (el valor predeterminado) enmascara todos los bits. Si el valor de dirección también se compone exclusivamente de ceros (el valor predeterminado), el filtro coincide con cualquier dirección de origen o de destino. Una máscara compuesta exclusivamente por unos (255.255.255.255) no enmascara ningún bit, por lo que la dirección de origen completa de un host individual se compara con el valor de dirección.

Puede utilizar la máscara de dirección para enmascarar, por ejemplo, la parte de host de una dirección o la parte de host y de subred, con el fin de que la especificación coincida con la dirección de origen o de destino de cualquier host de una determinada subred.

## Filtrado por números de puerto

Los filtros IP pueden especificar un número de puerto que se debe comparar con el puerto de origen o de destino (o ambos) de un paquete. Un número de puerto igual a cero no coincide con nada. Por lo general, los números de puerto TCP y UDP se asignan a servicios. Para obtener una lista de asignaciones de puerto conocidas, consulte el documento RFC 1700, *Assigned Numbers*.

**Nota:** Por motivos de seguridad, debe filtrar todos los servicios exteriores a su dominio que no sean necesarios. Los servicios basados en UDP hacen que su red sea especialmente vulnerable a determinados tipos de ataques de seguridad.

El tipo especificado de comparación determina cuándo se produce una coincidencia. Si no se especifica ningún operador de comparación en el filtro, no se efectúa ninguna comparación. Puede especificar que el filtro coincida con el paquete si el número de puerto del paquete es menor, igual, mayor o distinto del número de puerto especificado en el filtro.

## Ejemplos de un filtro IP para evitar la suplantación de direcciones locales

La suplantación de direcciones IP se produce habitualmente cuando un dispositivo remoto obtiene ilegalmente una dirección local y la utiliza para intentar atravesar un filtro de datos. En esta sección se muestra un ejemplo de un filtro de datos que evita la suplantación de direcciones IP. Si desea obtener información al respecto, consulte el apartado “Ejemplos de verificación de la dirección de origen por sesión” en la página 2-23.

El filtro de ejemplo define primero tres filtros de entrada. El primer filtro descarta los paquetes cuya dirección de origen se encuentra en la red IP local. El segundo filtro descarta los paquetes cuya dirección de origen es la dirección de prueba de bucle (127.0.0.0). El tercer filtro de entrada acepta todas las direcciones de origen restantes (mediante la especificación de una dirección de origen 0.0.0.0) y las reenvía a la red local.

En este ejemplo, la red IP local presenta una dirección IP 192.100.50.128, con una máscara de subred 255.255.255.192. Estos valores son solamente ejemplos arbitrarios.

**Nota:** Si aplica este filtro a la interfaz Ethernet, la unidad TAOS descartará los paquetes IP procedentes de la LAN local y no podrá establecer una conexión Telnet con la unidad.

La serie de comandos siguiente crea el primer filtro de entrada, estableciendo el tipo en IP-Filter. El primer filtro especifica la máscara y la dirección de origen de la red local. Si un paquete de entrada presenta la dirección local, la unidad TAOS lo descarta en lugar de reenviarlo a la red Ethernet, puesto que el parámetro Forward tiene el valor No (el valor predeterminado).

```
admin> new filter ip-spoof
FILTER/ip-spoof read

admin> set input 1 valid = yes

admin> set input 1 type = ip-filter

admin> set input 1 ip-filter source-address-mask = 255.255.255.192

admin> set input 1 ip-filter source-address = 192.100.50.128
```

La serie de comandos siguiente crea el segundo filtro de entrada, estableciendo el tipo en IP-Filter. El segundo filtro especifica la dirección de origen de prueba de bucle. Si un paquete de entrada presenta la dirección de prueba de bucle, la unidad TAOS lo descarta en lugar de reenviarlo a la red Ethernet, puesto que el parámetro Forward tiene el valor No.

```
admin> set input 2 valid = yes

admin> set input 2 type = ip-filter

admin> set input 2 ip-filter source-address-mask = 255.0.0.0

admin> set input 2 ip-filter source-address = 127.0.0.0
```

La serie de comandos siguiente crea el tercer filtro de entrada, estableciendo el tipo en IP-Filter y el parámetro Forward en Yes. A excepción de Forward=Yes, el tercer filtro utiliza todos los valores predeterminados. Dado que el parámetro Forward tiene el valor Yes, la unidad TAOS reenvía el resto de paquetes (aquellos que presentan direcciones de origen no locales) a la red Ethernet.

```
admin> set input 3 valid = yes

admin> set input 3 forward = yes

admin> set input 3 type = ip-filter
```

La serie de comandos siguiente crea un filtro de salida, estableciendo el tipo en IP-Filter y la acción de reenvío en Yes. Este filtro especifica la máscara y la dirección de origen de la red local (los paquetes que se originan en la red local se deben reenviar a través de la WAN).

```
admin> set output 1 valid = yes

admin> set output 1 type = ip-filter

admin> set output 1 forward = yes

admin> set output 1 ip-filter source-address-mask = 255.255.255.192

admin> set output 1 ip-filter source-address = 192.100.50.128

admin> write
FILTER/ip-spoof written
```

A continuación se muestra una definición de filtro RADIUS equivalente:

```
test-user Password = "test-pw"
Ascend-Data-Filter = "ip in drop srcip 192.100.50.128/26"
Ascend-Data-Filter = "ip in drop srcip 127.0.0.0/8"
Ascend-Data-Filter = "ip in forward"
Ascend-Data-Filter = "ip out forward srcip 192.100.50.128/26"
```

## Ejemplos de un filtro IP para cuestiones más complejas de seguridad

En esta sección se ilustran algunas de las cuestiones que debería considerar al escribir sus propios filtros IP. Sin embargo, el filtro de ejemplo que aquí se expone no aborda los puntos más precisos de seguridad de la red. Utilice este filtro como punto de partida y aumentelo según sus necesidades de seguridad.

En este ejemplo, la red local da soporte a un servidor de Web y el administrador necesita llevar a cabo las siguientes tareas:

- Proporcionar acceso por marcación a la dirección IP del servidor
- Restringir el tráfico de llamadas de entrada al resto de hosts de la red local

Sin embargo, muchos hosts IP locales necesitan conectarse a Internet y utilizar aplicaciones basadas en IP, como Telnet o FTP, con lo que sus paquetes de respuesta necesitan ser dirigidos al host de origen adecuadamente. En este ejemplo, la dirección IP del servidor de Web es 192.9.250.5. El filtro se aplicará a los perfiles Connection como un filtro de datos.

La serie de comandos siguiente crea el primer filtro de entrada, establece el tipo en IP-Filter y el parámetro Forward en Yes, y configura el primer filtro para que los paquetes puedan alcanzar la dirección de destino del servidor de Web en un puerto TCP de destino que se pueda utilizar para Telnet o FTP:

```
admin> new filter web-access
FILTER/web-access read
admin> set input 1 valid = yes
admin> set input 1 forward = yes
admin> set input 1 type = ip-filter
admin> set input 1 ip-filter protocol = 6
admin> set input 1 ip-filter dest-address-mask = 255.255.255.255
admin> set input 1 ip-filter dest-address = 192.9.250.5
admin> set input 1 ip-filter dst-port-cmp = eq1
admin> set input 1 ip-filter dest-port = 80
```

La serie de comandos siguiente crea el segundo filtro de entrada, establece el tipo en IP-Filter y el parámetro Forward en Yes. Este filtro admite paquetes TCP de entrada en respuesta a una petición Telnet de salida de usuario local mediante la especificación de que los paquetes TCP se deben reenviar si su número de puerto de destino es mayor que el del puerto de origen (las peticiones Telnet se envían desde el puerto 23 y las respuestas se reciben en algún puerto aleatorio superior al puerto 1023).

```
admin> set input 2 valid = yes
admin> set input 2 forward = yes
```

```
admin> set input 2 type = ip-filter
admin> set input 2 ip-filter protocol = 6
admin> set input 2 ip-filter dst-port-cmp = gtr
admin> set input 2 ip-filter dest-port = 1023
```

La serie de comandos siguiente crea el tercer filtro de entrada, establece el tipo en IP-Filter y el parámetro Forward en Yes. Este filtro admite actualizaciones RIP de entrada mediante la especificación de que los paquetes UDP de entrada se deben reenviar si el número de puerto de destino es mayor que el del puerto de origen (por ejemplo, supongamos que un paquete RIP se envía como un paquete UDP al puerto de destino 520. La respuesta a esta petición se recibe en un puerto de destino aleatorio mayor que el puerto 1023).

```
admin> set input 3 valid = yes
admin> set input 3 forward = yes
admin> set input 3 type = ip-filter
admin> set input 3 ip-filter protocol = 17
admin> set input 3 ip-filter dst-port-cmp = gtr
admin> set input 3 ip-filter dest-port = 1023
```

La serie de comandos siguiente crea el cuarto filtro de entrada, establece el tipo en IP-Filter y el parámetro Forward en Yes. El cuarto filtro utiliza todos los valores predeterminados, lo que permite Pings y Traceroutes sin restricciones. A diferencia de TCP y UDP, ICMP no utiliza puertos, por lo que no es necesaria una comparación de puertos.

```
admin> set input 4 valid = yes
admin> set input 4 forward = yes
admin> set input 4 type = ip-filter
admin> write
FILTER/web-access written
```

A continuación se muestran definiciones de filtro RADIUS equivalentes:

```
Ascend-Data-Filter="ip in forward dstip 192.9.250.5/32 dstport = 80
proto 6"
Ascend-Data-Filter="ip in forward dstport > 1023 proto 6"
Ascend-Data-Filter="ip in forward dstport > 1023 proto 6"
Ascend-Data-Filter="ip in forward"
```

## ***Definición de filtros de tipo de servicio (TOS)***

Para activar proxy-QoS para todos los paquetes que coinciden con una especificación de filtro específica, puede definir de manera local un filtro TOS en un perfil Filter y, a continuación, aplicar el filtro a cualquier número de perfiles Connection o RADIUS (el atributo Filter-ID puede aplicar un perfil Filter local a perfiles de usuario RADIUS). También puede definir filtros TOS directamente en un perfil de usuario RADIUS estableciendo el atributo Ascend-Filter. Para los filtros TOS, la acción de reenvío del filtro no tiene ningún efecto.

## Ajustes de un perfil Filter local

La definición de un filtro TOS local requiere establecer los parámetros siguientes (que aparecen con los ajustes predeterminados):

```
[in FILTER/"":input-filters:input-filters[1]]
type = tos-filter

[in FILTER/"":input-filters:input-filters[1]:tos-filter]
protocol = 0
source-address-mask = 0.0.0.0
source-address = 0.0.0.0
dest-address-mask = 0.0.0.0
dest-address = 0.0.0.0
Src-Port-Cmp = none
source-port = 0
Dst-Port-Cmp = none
dest-port = 0
precedence = 000
type-of-service = normal
```

Parámetro	Especifica
Protocol	Número de protocolo. El valor cero coincide con todos los protocolos. Si especifica un número distinto de cero, la unidad TAOS lo compara con el campo Protocol de cada paquete. Para obtener una lista de números de protocolo, consulte el documento RFC 1700.
Source-Address-Mask	Máscara que se debe aplicar al valor Source-Address antes de compararlo con la dirección de origen de un paquete.
Source-Address	Dirección IP. Tras aplicar el valor Source-Address-Mask, la unidad TAOS compara el resultado con la dirección de origen de un paquete. Para obtener información detallada, consulte el apartado “Filtrado por dirección de origen o de destino” en la página 9-15.
Dest-Address-Mask	Máscara que se debe aplicar al valor Dest-Address antes de compararlo con la dirección de destino de un paquete.
Dest-Address	Dirección IP. Tras aplicar el valor Dest-Address-Mask, la unidad TAOS compara el resultado con la dirección de origen de un paquete. Para obtener información detallada, consulte el apartado “Filtrado por dirección de origen o de destino” en la página 9-15.
Src-Port-Cmp	Tipo de comparación que se debe realizar al comparar números de puerto de origen. Con un ajuste None (el ajuste predeterminado), no se efectúa ninguna comparación. Puede especificar que el filtro coincida con el paquete si el número de puerto de origen del paquete es Less (menor que), Eql (igual a), Gtr (mayor que) o Neq (distinto de) que el valor Source-Port.
Source-Port	Número de puerto que se debe comparar con el puerto de origen de un paquete. Por lo general, los números de puerto TCP y UDP se asignan a servicios. Para obtener información detallada, consulte el apartado “Filtrado por números de puerto” en la página 9-16.

<b>Parámetro</b>	<b>Especifica</b>
Dst-Port-Cmp	Tipo de comparación que se debe realizar al comparar números de puerto de destino. Con un ajuste None (el ajuste predeterminado), no se efectúa ninguna comparación. Puede especificar que el filtro coincida con el paquete si el número de puerto de destino del paquete es Less (menor que), Eql (igual a), Gtr (mayor que) o Neq (distinto de) que el valor Dest-Port.
Dest-Port	Número de puerto que se debe comparar con el puerto de destino de un paquete. Por lo general, los números de puerto TCP y UDP se asignan a servicios. Para obtener información detallada, consulte el apartado “Filtrado por números de puerto” en la página 9-16.
Precedence	<p>Nivel de prioridad de la corriente de datos. Los tres bits más significativos del byte TOS son bits de prioridad utilizados para determinar la prioridad para la puesta en cola por prioridades. Cuando se activa el filtro TOS y el paquete coincide con el filtro, se puede establecer uno de los valores siguientes para los bits (el bit más significativo primero):</p> <ul style="list-style-type: none"><li>• 000: Prioridad normal</li><li>• 001: Nivel de prioridad 1</li><li>• 010: Nivel de prioridad 2</li><li>• 011: Nivel de prioridad 3</li><li>• 100: Nivel de prioridad 4</li><li>• 101: Nivel de prioridad 5</li><li>• 110: Nivel de prioridad 6</li><li>• 111: Nivel de prioridad 7 (la prioridad más alta)</li></ul>
Type-of-Service	<p>Tipo de servicio de la corriente de datos. El valor de este atributo establece los cuatro bits siguientes a los tres bits más significativos del byte TOS. Estos cuatro bits se utilizan para elegir un enlace de acuerdo con el tipo de servicio. Cuando se activa el filtro TOS y el paquete coincide con el filtro, se puede establecer uno de los valores siguientes en el paquete:</p> <ul style="list-style-type: none"><li>• Normal: Servicio normal</li><li>• Cost: Minimizar coste económico</li><li>• Reliability: Maximizar fiabilidad</li><li>• Throughput: Maximizar rendimiento</li><li>• Latency: Minimizar retardo</li></ul>

## Ajustes de un perfil RADIUS

En RADIUS, una entrada de filtro TOS es un valor del atributo Ascend-Filter. Para especificar un valor de filtro TOS, utilice el formato siguiente:

```
iptos dir [ dstip n.n.n.n/nn ] [ srcip n.n.n.n/nn ] [ proto ] [ destport  
cmp value ] [ srcport cmp value ] [ precedence value ] [ type-of-service  
value ]
```

**Nota:** Una definición de filtro no puede contener indicadores de línea nueva. Se muestra la sintaxis en múltiples líneas para fines exclusivamente de impresión.

Palabra clave o argumento	Descripción
<code>iptos</code>	Especifica un filtro TOS de IP.
<code>dir</code>	Especifica la dirección de los paquetes. Puede especificar bien <code>in</code> (para filtrar los paquetes que llegan a la unidad TAOS ) o bien <code>out</code> (para filtrar los paquetes que salen de la unidad TAOS).
<code>dstip n.n.n.n/nn</code>	Si después de la palabra clave <code>dstip</code> aparece una dirección IP válida, el filtro TOS establecerá bytes solamente en los paquetes con dicha dirección de destino. Si una parte de la máscara de subred de la dirección está presente, la unidad TAOS compara solamente los bits enmascarados. Si después de la palabra clave <code>dstip</code> aparece una dirección cero (0.0.0.0) o si dicha palabra clave y su especificación de dirección IP no están presentes, el filtro coincide con todos los paquetes IP. Para obtener información detallada, consulte el apartado “Filtrado por dirección de origen o de destino” en la página 9-15.
<code>srcip n.n.n.n/nn</code>	Si después de la palabra clave <code>srcip</code> aparece una dirección IP válida, el filtro TOS establecerá bytes solamente en los paquetes con dicha dirección de origen. Si una parte de la máscara de subred de la dirección está presente, la unidad TAOS compara solamente los bits enmascarados. Si después de la palabra clave <code>srcip</code> aparece una dirección cero (0.0.0.0) o si dicha palabra clave y su especificación de dirección IP no están presentes, el filtro coincide con todos los paquetes IP. Para obtener información detallada, consulte el apartado “Filtrado por dirección de origen o de destino” en la página 9-15.
<code>proto</code>	Número de protocolo. El valor cero coincide con todos los protocolos. Si especifica un número distinto de cero, la unidad TAOS lo compara con el campo Protocol de los paquetes. Para obtener una lista de números de protocolo, consulte el documento RFC 1700.



Palabra clave o argumento	Descripción
<code>dstport cmp value</code>	Si después de la palabra clave <code>dstport</code> aparece un símbolo de comparación y un puerto, el puerto se compara con el puerto de destino de un paquete. El símbolo de comparación puede ser < (menor que), = (igual a), > (mayor que) o != (distinto de). El valor del puerto puede ser uno de los nombres o números siguientes: ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514) o talk (517). Para obtener información detallada, consulte el apartado “Filtrado por números de puerto” en la página 9-16.
<code>srcport cmp value</code>	Si después de la palabra clave <code>srcport</code> aparece un símbolo de comparación y un puerto, el puerto se compara con el puerto de origen de un paquete. El símbolo de comparación puede ser < (menor que), = (igual a), > (mayor que) o != (distinto de). El valor del puerto puede ser uno de los nombres o números siguientes: ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514) o talk (517). Para obtener información detallada, consulte el apartado “Filtrado por números de puerto” en la página 9-16.
<code>precedence value</code>	<p>Especifica el nivel de prioridad de la corriente de datos. Los tres bits más significativos del byte TOS son bits de prioridad utilizados para determinar la prioridad para la puesta en cola por prioridades. Si un paquete coincide con el filtro, los bits se establecen en el valor especificado (el bit más significativo primero). Especifique uno de los valores siguientes:</p> <ul style="list-style-type: none"><li>• 000: Prioridad normal</li><li>• 001: Nivel de prioridad 1</li><li>• 010: Nivel de prioridad 2</li><li>• 011: Nivel de prioridad 3</li><li>• 100: Nivel de prioridad 4</li><li>• 101: Nivel de prioridad 5</li><li>• 110: Nivel de prioridad 6</li><li>• 111: Nivel de prioridad 7 (la prioridad más alta)</li></ul>

### Definición de filtros de tipo de servicio (TOS)

## Ejemplos de definición de un filtro TOS

```
admin> new filter jfans-tos-filter
FILTER/jfans-tos-filter read

admin> list input 1
[in FILTER/jfans-tos-filter:input-filters[1] (new)]
valid-entry = no
forward = no
Type = generic-filter
gen-filter = { 0 0 no no 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00+
00:00:00:0+
ip-filter = { 0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 none 0 none 0 no }
route-filter = { 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0 none }
ipx-filter = { 00:00:00:00 00:00:00:00 00:00:00:00:00:00:00 00:00:00+
tos-filter = { 0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 none 0 none 0 000
norma+

admin> set valid = yes

admin> set type = tos-filter

admin> list tos
[in FILTER/jfans-tos-filter:input-filters[1]:tos-filter (changed)]
protocol = 0
source-address-mask = 0.0.0.0
source-address = 0.0.0.0
dest-address-mask = 0.0.0.0
```

```
dest-address = 0.0.0.0
Src-Port-Cmp = none
source-port = 0
Dst-Port-Cmp = none
dest-port = 0
precedence = 000
type-of-service = normal

admin> set protocol = 6

admin> set dest-address-mask = 255.255.255.255

admin> set dest-address = 10.168.6.24

admin> set dst-port-cmp = eql

admin> set dest-port = 23

admin> set precedence = 010

admin> set type-of-service = latency

admin> write
FILTER/jfans-tos-filter written
```

A continuación se muestra un perfil de usuario RADIUS que contiene una definición de filtro equivalente:

```
jfan-pc Password = "secret"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Framed-IP-Address = 10.168.6.120,
    Framed-IP-Netmask = 255.255.255.0,
    Ascend-Filter = "iptos in dstip 10.168.6.24/32 dstport = 23 prece-
dence
    010 type-of-service latency"
```

**Nota:** Las definiciones de filtro no pueden contener indicadores de línea nueva. Los ejemplos anteriores muestran el valor Ascend-Filter en dos líneas para fines exclusivamente de impresión.

## ***Definición de filtros IPX***

RADIUS no da soporte a las especificaciones de filtro IPX. Éstas afectan solamente a paquetes NetWare y su principal objetivo es identificar redes, hosts o servicios específicos. En un perfil Filter local, el subperfil IPX-Filter contiene los parámetros siguientes (que aparecen con los valores predeterminados):

```
[in FILTER/"":input-filters:input-filters[1]]
type = ipx-filter

[in FILTER/""):input-filters:input-filters[1]:ipx-filter]
src-net-address = 00:00:00:00
dest-net-address = 00:00:00:00
src-node-address = 00:00:00:00:00:00
dest-node-address = 00:00:00:00:00:00
src-socket = 00:00
src-socket-cmp = none
dest-socket = 0
dst-socket-cmp = none
```

Los mismos parámetros también están disponibles en el subperfil Output-Filters. Si establece los parámetros en un filtro de entrada, solamente se examinarán los paquetes de entrada. Si los establece en un filtro de salida, solamente se examinarán los paquetes de salida.

Parámetro	Especifica
Type	Tipo de filtro. Los valores válidos son Generic-Filter (el valor predeterminado), IP-Filter, IPX-Filter, Route-Filter y TOS-Filter. Solamente serán válidos los parámetros en el subperfil correspondiente.
Src-Net-Address	Parte de número de red de la dirección IPX de origen.
Dest-Net-Address	Parte de número de red de la dirección IPX de destino.
Src-Node-Address	Parte de número de nodo de la dirección IPX de origen.
Dest-Node-Address	Parte de número de nodo de la dirección IPX de destino.
Src-Socket	Número de zócalo de origen.
Src-Socket-Cmp	Tipo de comparación que debe realizarse con el número de zócalo de origen. Puede especificar que el filtro coincida con el paquete si el número de zócalo de origen del paquete es Less (menor que), Eql (igual a), Gtr (mayor que) o Neq (distinto de) que el número de zócalo de origen especificado en el filtro.
Dest-Socket	Número de zócalo de destino.
Dst-Socket-Cmp	Tipo de comparación que debe realizarse con el número de zócalo de destino. Puede especificar que el filtro coincida con el paquete si el número de zócalo de origen del paquete es Less (menor que), Eql (igual a), Gtr (mayor que) o Neq (distinto de) que el número de zócalo de origen especificado en el filtro.

## Filtrado por dirección de origen o de destino

Los parámetros de dirección de red y dirección de nodo se han diseñado para funcionar conjuntamente y especificar un servidor NetWare de origen o de destino. Una dirección de red IPX completa utiliza el formato siguiente:

*número-red:número-nodo*

Los parámetros Src-Net-Address y Dest-Net-Address especifican la parte del número de red de la dirección. El número de red es un número hexadecimal de 8 bytes exclusivo y común a todos los hosts de una determinada LAN. Los servidores NetWare disponen de un número de red interno que es la dirección de red de destino para peticiones de lectura o escritura de archivos (si no está familiarizado con los números de red interna, consulte la documentación de NetWare para obtener información detallada al respecto).

Los parámetros Src-Node-Address y Dest-Node-Address especifican la parte del número de nodo de la dirección. El número de nodo es un número hexadecimal de 12 bytes que es exclusivo para cada nodo de una LAN. Cualquier filtro que especifique un número de red IPX también debe especificar el correspondiente número de nodo (por ejemplo, si especifica un valor para Src-Net-Address en un filtro, también debe especificar un valor para Src-Node-Address).

Habitualmente una dirección de servidor NetWare tiene el número de nodo 1 (00:00:00:00:00:01) en la red interna del servidor. Un número de nodo compuesto exclusivamente por unos (FF:FF:FF:FF:FF:FF) coincide con todos los nodos de una LAN.

## Filtrado por número de zócalo

Los servidores NetWare utilizan un número de zócalo concreto para cada servicio. Por ejemplo, el servicio de archivos NetWare utiliza habitualmente el zócalo 0451 (04:51). Algunos servicios utilizan números de zócalo dinámicos, que pueden cambiar cada vez que se cargan. Un número de zócalo compuesto exclusivamente por unos (FF:FF) coincide con cualquier zócalo del servidor especificado.

Si especifica un número de zócalo NetWare, también debe indicar la manera de comparar el número de zócalo de un paquete con la especificación del filtro. El parámetro Src-Socket-Cmp especifica el método de comparación para el número de zócalo de origen. Puede especificar que el filtro coincida con el paquete si el número de zócalo de origen del paquete es Less (menor que), Eql (igual a), Gtr (mayor que) o Neq (distinto de) que el número de zócalo de origen especificado en el filtro.

El parámetro Dst-Socket-Cmp especifica el método de comparación para el número de zócalo de destino. Puede especificar que el filtro coincida con el paquete si el número de zócalo de destino del paquete es Less (menor que), Eql (igual a), Gtr (mayor que) o Neq (distinto de) que el número de zócalo de destino especificado en el filtro.

## Ejemplo de un filtro IPX de salida

Cuando el filtro IPX de ejemplo siguiente se aplica como filtro de datos a una interfaz de WAN, la unidad TAOS descarta todos los paquetes IPX de salida que tienen una dirección de red IPX de destino 00003823, independientemente del número de zócalo o nodo IPX de destino en los paquetes. El resto de paquetes se reenvía.

```
admin> new filter dstipx
FILTER/dstipx read

admin> set output 1 valid = yes

admin> set output 1 type = ipx-filter

admin> set output 1 ipx dest-net-address = 00003823

admin> set output 1 ipx dest-node-address = ffffffff

admin> set output 2 forward = yes

admin> write
FILTER/dstipx read
```

## Ejemplo de un filtro IPX de entrada

Cuando el filtro IPX de ejemplo siguiente se aplica como filtro de datos a una interfaz de WAN, la unidad TAOS descarta todos los paquetes IPX de entrada procedentes de un origen específico. En este ejemplo, el filtro hace que la unidad TAOS descarte los paquetes procedentes de la dirección de red IPX de origen 00000005:00abcde12345 y con número de zócalo de origen 4002. El resto de paquetes se reenvía.

```
admin> new filter srcipx
FILTER/srcipx read
admin> set input 1 type = ipx-filter
admin> set input 1 ipx src-net = 00000005
admin> set input 1 ipx src-node = 00abcde12345
admin> set input 1 ipx src-socket = 4002
admin> set input 1 ipx src-socket-cmp = eq1
admin> set input 2 forward = yes
admin> write
FILTER/srcipx read
```

## ***Definición de filtros de ruta***

RADIUS no da soporte a las especificaciones de filtro de ruta. Los filtros de ruta afectan solamente a los paquetes RIP. Para los filtros de ruta, la acción de reenvío del filtro no tiene ningún efecto.

En un perfil Filter local, el subperfil Route-Filter contiene los parámetros siguientes (que aparecen con los valores predeterminados):

```
[in FILTER:input-filters:input-filters[1]]
type = route-filter

[in FILTER:input-filters:input-filters[1]:route-filter]
source-address-mask = 0.0.0.0
source-address = 0.0.0.0
route-mask = 0.0.0.0
route-address = 0.0.0.0
add-metric = 0
action = none
```

Los mismos parámetros también están disponibles en el subperfil Output-Filters. Si establece los parámetros en un filtro de entrada, solamente se examinarán los paquetes de entrada. Si los establece en un filtro de salida, solamente se examinarán los paquetes de salida.

Parámetro	Especifica
Type	Tipo de filtro. Los valores válidos son Generic-Filter (el valor predeterminado), IP-Filter, IPX-Filter, Route-Filter y TOS-Filter. Solamente serán válidos los parámetros en el subperfil correspondiente.
Source-Address-Mask	Máscara que se debe aplicar al valor Source-Address antes de compararlo con la dirección de origen de un paquete de actualización de RIP.
Source-Address	Dirección IP. Tras aplicar el valor Source-Address-Mask, la unidad TAOS compara el resultado con la dirección de origen de un paquete RIP. Si desea obtener información al respecto, consulte el apartado “Filtrado por dirección de origen o de destino” en la página 9-26.
Route-Mask	Máscara que se debe aplicar a la dirección de destino de una ruta.

Parámetro	Especifica
Route-Address	Dirección IP. Tras aplicar el valor Route-Mask, la unidad TAOS compara el resultado con las rutas de un paquete RIP. Si encuentra una ruta con un destino coincidente, realiza la acción especificada.
Add-Metric	Número del 1 al 15, que se debe sumar al valor de métrica de una ruta que coincide con la especificación de filtro, si el valor especificado para el parámetro Action es Add.
Action	Acción que se debe llevar a cabo en una ruta que coincide con la especificación de filtro. Los valores válidos son None (el valor predeterminado), Accept (aceptar la ruta permitiendo que afecte a la tabla de ruteo), Deny (rechazar la ruta sin permitir que afecte a la tabla de ruteo) o Add (sumar el valor del parámetro Add-Metric a la métrica de la ruta y aceptar la ruta).

## Ejemplo de un filtro que excluye una ruta

En este ejemplo, los filtros de entrada definidos aceptan todos los paquetes RIP de entrada excepto aquellos cuyo destino es 90.0.0.0. A continuación se muestran los comandos introducidos para definir el filtro y las respuestas del sistema:

```
admin> new filter route-test
FILTER/route-test read
admin> set input 1 valid = yes
admin> set input 1 type = route-filter
admin> set input 1 route route-mask = 255.0.0.0
admin> set input 1 route route-address = 90.0.0.0
admin> set input 1 route action = deny
admin> set input 2 valid = yes
admin> set input 2 type = route-filter
admin> set input 2 route action = accept
admin> write
FILTER/route-test written
```

En este filtro de ruta de ejemplo, se rechaza cualquier ruta que coincida con el filtro 1 y se acepta el resto de las rutas (porque coinciden con el filtro 2).

## Ejemplo de un filtro que configura la métrica de una ruta

En este ejemplo, un filtro de salida identifica la ruta 11.0.0.0 en paquetes RIP de salida y asigna una métrica superior a dicha ruta. A continuación se muestran los comandos introducidos y las respuestas del sistema:

```
admin> new filter metrics
FILTER/metrics read
admin> set output 1 valid = yes
admin> set output 1 type = route-filter
admin> set output 1 route route-mask = 255.0.0.0
```

```
admin> set output 1 route route-address = 11.0.0.0

admin> set output 1 route add-metric = 7

admin> set output 1 route action = add

admin> write
FILTER/metrics written
```

## Definición de filtros remotos dinámicos

Puede crear perfiles de pseudousuario RADIUS que definan filtros de datos y aplicar los filtros a varios perfiles Connection o RADIUS locales haciendo referencia al nombre de perfil de pseudousuario.

Si la unidad TAOS recibe un ID de filtro en un paquete Access-Accept procedente de RADIUS, la unidad busca un filtro local coincidente. Si no encuentra ninguno, la unidad TAOS solicita el filtro del servidor RADIUS. Puede especificar la manera en que el sistema debe comportarse si no se encuentra el filtro al que se hace referencia en un perfil. El sistema puede establecer la sesión y registrar un mensaje referente al filtro que falta o sencillamente dar por terminada la llamada.

Los filtros definidos de forma externa se guardan localmente en la caché durante un intervalo que se puede configurar. El comando FiltCache muestra las estadísticas acerca de cada perfil de filtro RADIUS guardado en la caché y le permite borrar los perfiles de la caché. Para obtener más información sobre el comando FiltCache, consulte la publicación *Guía de administración de APX 8000/MAX TNT/DSLNT*.

## Limitaciones actuales

En la versión actual del software, la implantación de filtro remoto está sujeta a las limitaciones siguientes:

- En esta versión no se permiten filtros aplicados a llamadas de salida.
- En esta versión no se permiten filtros de llamada, filtros de ruta ni filtros TOS. Actualmente sólo se da soporte a filtros de datos.

## Información general sobre los ajustes de un perfil local

A continuación se muestran los parámetros locales (que aparecen con los valores predeterminados) relacionados con filtros remotos dinámicos:

```
[in ANSWER-DEFAULTS:session-info]
filter-required = no

[in CONNECTION:session-options]
filter-required = no
data-filter = ""

[in IP-GLOBAL]
default-filter-cache-time = 1440
```



<b>Parámetro</b>	<b>Especifica</b>
Filter-Required	Define si el acceso al filtro es obligatorio para la sesión. Con el valor predeterminado <code>No</code> , el sistema establece la sesión aunque no se encuentre el filtro especificado. Si el parámetro tiene el valor <code>Yes</code> , el sistema desconecta la llamada si no se encuentra el filtro. Este parámetro no se aplica si el perfil no hace referencia a un filtro por su nombre.  En el perfil <code>Answer-Defaults</code> , este parámetro se utiliza para perfiles de usuario <code>RADIUS</code> que aplican un filtro y no especifican un valor para <code>Ascend-Filter-Required</code> (50).
Data-Filter	Nombre de un perfil <code>Filter</code> asociado a la conexión. El nombre puede ser el de un perfil local o el de un perfil de pseudousuario en <code>RADIUS</code> . Sin embargo, si un perfil <code>Connection</code> local no utiliza la autenticación, no puede especificar un perfil de filtro <code>RADIUS</code> .
Default-Filter-Cache-Time	Número de minutos durante los que se deben guardar en la caché los perfiles de filtro <code>RADIUS</code> que no incluyen ningún valor para <code>Ascend-Cache-Time</code> (57). El valor predeterminado es <code>1440</code> (24 horas). Al alcanzar su límite el temporizador de la caché, los perfiles guardados en la caché se eliminan de la memoria del sistema. La próxima vez que se precise un filtro remoto, el sistema recuperará el perfil de <code>RADIUS</code> y lo almacenará de nuevo en la caché. Si se guarda un perfil en la caché, se aumenta el rendimiento al establecer sesiones que utilizan el filtro, a expensas de ocupar algo de espacio de la memoria del sistema. Si este parámetro tiene el valor <code>0</code> (cero), el temporizador predeterminado está desconectado, de modo que únicamente se guardarán en la caché los perfiles <code>RADIUS</code> que especifiquen un tiempo de permanencia en la caché.

## Información general sobre los ajustes del perfil de usuario `RADIUS`

El soporte de perfil de usuario `RADIUS` para perfiles de filtro lo proporcionan los atributos específicos del proveedor (VSA) siguientes:

<b>Atributo</b>	<b>Especifica</b>
Filter-ID (11)	Nombre de un perfil de filtro local o remoto asociado a la conexión.
Ascend-Filter-Required (50)	Define si el acceso al filtro es obligatorio para la sesión. Con el valor predeterminado <code>Required-No</code> (0), el sistema establece la sesión aunque no se encuentre el filtro especificado. Si el atributo tiene el valor <code>Required-Yes</code> (1), el sistema desconecta la llamada si no se encuentra el filtro. Este atributo no se aplica si el perfil no hace referencia a un filtro por su nombre. Si no se especifica ningún valor para este atributo, se utiliza el ajuste del parámetro <code>Filter-Required</code> en el perfil <code>Answer-Defaults</code> para determinar el comportamiento del sistema si no se encuentra el filtro especificado.

## Filtros de paquetes

### Definición de filtros remotos dinámicos

---

Un perfil de filtro es un perfil de pseudousuario cuyas dos primeras líneas tienen el formato siguiente:

```
nombre-perfil Password = "ascend" Service-Type = Outbound
```

El valor *nombre-perfil* es el nombre asignado al perfil. No se permiten nombres de filtro duplicados. Si ya hay guardado un perfil Filter local, la unidad TAOS no recupera un perfil de filtro del mismo nombre del servidor RADIUS. Las definiciones de perfil Filter pueden incluir los pares atributo-valor siguientes:

Atributo	Especifica
Ascend-Data-Filter (242)	Definición de filtro en formato no binario que utiliza uno de los siguientes formatos:  "generic dir action offset mask value compare [more]"  "ip dir action [ dstip n.n.n.n/nn ] [ srcip n.n.n.n/nn ] [[ proto ] [ destport cmp value ] [ srcport cmp value ] [est]]"
Ascend-Cache-Refresh (56)	Define si el temporizador para las rutas en caché de este perfil debe reiniciarse cada vez que se active una nueva sesión que haga referencia al perfil de pseudousuario. Con el valor Refresh-No (0), no se reinicia el temporizador. Con el valor Refresh-Yes (1), se reinicia el temporizador de la caché cada vez que se activa una sesión que hace referencia al perfil.
Ascend-Cache-Time (57)	Número de minutos durante los que se debe guardar el perfil en la caché. Al alcanzar su límite el temporizador de la caché para un perfil RADIUS, el perfil se elimina de la memoria del sistema. La próxima vez que se necesite, el sistema lo recuperará de RADIUS y lo almacenará de nuevo en la caché. Si se guarda un perfil en la caché, aumenta el rendimiento de las búsquedas de ruta, aunque a expensas de ocupar algo de la memoria del sistema. El tiempo en caché mínimo posible es 0 minutos, con lo que el sistema recupera el perfil cada vez que se necesita. Este valor no suele ser recomendable. Si no se ha especificado ningún valor para este atributo, se utiliza el ajuste definido para el parámetro Default-Filter-Cache-Time en el perfil IP-Global.

Para utilizar estos atributos, el servidor RADIUS debe permitir atributos específicos del proveedor (VSA) y la unidad TAOS debe estar configurada en el modo de compatibilidad con VSA. A continuación se muestran los ajustes pertinentes:

```
[in EXTERNAL-AUTH]
auth-type = radius

[in EXTERNAL-AUTH:rad-auth-client]
auth-radius-compatible = vendor-specific
```

Si desea obtener información detallada acerca de estos ajustes, consulte la publicación *APX 8000/MAX TNT/DSLNT Reference (Referencia de APX 8000/MAX TNT/DSLNT)*.

## *Ejemplos de configuración de un perfil de filtro en RADIUS*

A continuación se muestra un perfil de filtro RADIUS de ejemplo:

```
filter-c Password = "ascend", Service-Type = Outbound
  Ascend-Cache-Time = 20,
  Ascend-Cache-Refresh = Refresh-Yes,
  Ascend-Data-Filter = "ip out forward tcp dstip 10.1.1.3/16",
  Ascend-Data-Filter = "ip out drop"
```

El temporizador de la caché se ha establecido en 20 minutos y se reinicia cada vez que se aplica el filtro a una sesión.

Los comandos siguientes configuran el tiempo en caché predeterminado para perfiles de filtro RADIUS:

```
admin> read ip-global
IP-GLOBAL read

admin> set default-filter-cache-time = 180

admin> write
IP-GLOBAL written
```

A continuación se muestra un perfil de filtro RADIUS de ejemplo que utiliza el valor predeterminado en lugar de especificar un valor para Ascend-Cache-Time (57):

```
filter-e Password = "ascend", Service-Type = Outbound
  Ascend-Data-Filter = "ip out forward tcp dstip 10.2.2.2/28",
  Ascend-Data-Filter = "ip out drop"
```

## *Ejemplos de aplicación de filtros remotos*

Los comandos siguientes modifican un perfil Connection de modo que la sesión utiliza un filtro remoto y el sistema desconecta la llamada si no se encuentra el filtro:

```
admin> read connection p50-v2
CONNECTION/p50-v2 read

admin> set session-options data-filter = filter-c

admin> set session-options filter-required = yes

admin> write
CONNECTION/p50-v2 written
```

El perfil RADIUS siguiente aplica el mismo perfil de filtro y tiene los mismos requisitos. Este perfil también especifica cómo se guardan en la caché los filtros para esta conexión.

```
p50-v2 Password = "my-password", Service-Type = Framed
  Framed-Protocol = PPP,
  Framed-IP-Address = 10.1.1.1,
  Framed-IP-Netmask = 255.0.0.0,
  Filter-ID = "filter-c",
  Ascend-Filter-Required = Required-Yes
```

Los comandos siguientes configuran el sistema para rechazar llamadas de entrada si el perfil de usuario RADIUS especifica un filtro que no se encuentra y el perfil de usuario no indica explícitamente lo que se debe hacer si no se encuentra dicho filtro:

```
admin> read answer-defaults
ANSWER-DEFAULTS read

admin> set session-info filter-required = yes

admin> write
ANSWER-DEFAULTS written
```

A continuación se muestra un perfil RADIUS de ejemplo que utiliza el valor predeterminado en lugar de especificar un valor para Ascend-Filter-Required (55):

```
p50-v2 Password = "my-password", Service-Type = Framed
    Framed-Protocol = PPP,
    Framed-IP-Address = 10.1.1.1,
    Framed-IP-Netmask = 255.0.0.0,
    Filter-ID = "filter-c"
```

## ***Aplicación de un filtro a una interfaz***

Si aplica un filtro a una interfaz de WAN, éste entra en vigor cuando se activa la conexión.

Los paquetes pueden atravesar tanto un filtro de datos como un filtro de llamada en una interfaz de WAN. Cuando ambos filtros, de datos y de llamada, se aplican a la misma interfaz, el filtro de datos se aplica primero.

## **Ajustes de los perfiles locales**

Para aplicar un filtro a una interfaz, establezca los parámetros siguientes (que aparecen con los ajustes predeterminados):

```
[in ANSWER-DEFAULTS]
use-answer-for-all-defaults = yes

[in ANSWER-DEFAULTS:session-info]
call-filter = ""
data-filter = ""
filter-persistence = no

[in CONNECTION/":session-options]
call-filter = ""
data-filter = ""
filter-persistence = no

[in CONNECTION/":ip-options]
route-filter = ""
tos-filter = ""

IP-INTERFACE { { any-shelf any-slot 0 } 0}
route-filter = ""
```

```
ETHERNET { any-shelf any-slot 0 }  
filter-name= ""
```

Parámetro	Especifica
Call-Filter	Nombre de un perfil Filter. Para obtener información detallada, consulte el apartado “Ejemplos de aplicación de un filtro de llamada a una interfaz de WAN” en la página 9-37. El ajuste contenido en el perfil Answer-Defaults se utiliza solamente para conexiones autenticadas por RADIUS que no incluyen un filtro de llamada.
Data-Filter	Nombre de un perfil Filter. Para obtener información detallada, consulte el apartado “Ejemplos de aplicación de un filtro de datos a una interfaz de WAN” en la página 9-36. El ajuste contenido en el perfil Answer-Defaults se utiliza solamente para conexiones autenticadas por RADIUS que no incluyen un filtro de datos.
Filter-Persistence	Activa y desactiva la persistencia del filtro en cambios de estado de la conexión.
Route-Filter	Nombre de un perfil Filter. Para obtener información detallada, consulte el apartado “Ejemplos de aplicación de un filtro de ruta a una interfaz IP de WAN o LAN” en la página 9-39.
TOS-Filter	Nombre de un perfil Filter. Para obtener información detallada, consulte el apartado “Ejemplos de aplicación de un filtro TOS a una interfaz de WAN” en la página 9-38.
Filter-Name	Nombre de un perfil Filter. Para obtener información detallada, consulte el apartado “Ejemplo de aplicación de un filtro a una interfaz de LAN” en la página 9-39.

## Ajustes de los perfiles RADIUS

Los pares atributo-valor de RADIUS siguientes se utilizan para aplicar un filtro a una conexión WAN:

Atributo	Valor
Ascend-Call-Filter (243)	<p>Definición de filtro en formato no binario que utiliza uno de los formatos siguientes:</p> <pre>"generic dir action offset mask value compare [more]"</pre> <pre>"ip dir action [ dstip n.n.n.n/nn ] [ srcip n.n.n.n/nn ] [[ proto ] [ destport cmp value ] [ srcport cmp value ] [est]]"</pre> <p>Para obtener información detallada, consulte los apartados “Definición de filtros genéricos” en la página 9-7 y “Definición de filtros IP” en la página 9-12.</p>

Atributo	Valor
Ascend-Data-Filter (242)	<p>Definición de filtro en formato no binario que utiliza uno de los formatos siguientes:</p> <pre>"generic dir action offset mask value compare [more]"</pre> <pre>"ip dir action [ dstip n.n.n.n/nn ] [ srcip n.n.n.n/nn ] [[ proto ] [ destport cmp value ] [ srcport cmp value ] [est]]"</pre> <p>Para obtener información detallada, consulte los apartados “Definición de filtros genéricos” en la página 9-7 y “Definición de filtros IP” en la página 9-12.</p>
Ascend-Filter (90)	<p>Especificación de filtro en formato de serie de caracteres que utiliza el siguiente formato:</p> <pre>iptos dir [ dstip n.n.n.n/nn ] [ srcip n.n.n.n/nn ][ proto ] [ destport cmp value ] [ srcport cmp value ] [ precedence value ] [ type-of-service value ]</pre> <p>Para obtener información detallada, consulte el apartado “Definición de filtros de tipo de servicio (TOS)” en la página 9-19.</p>
Filter-ID (11)	<p>Nombre de un perfil Filter local que define un filtro de datos. La próxima vez que la unidad TAOS acceda al perfil de usuario RADIUS en el que aparece este atributo, el filtro al que se hace referencia se aplicará a la conexión.</p>

## Utilización por parte del sistema de los ajustes del perfil Answer-Defaults

Si el parámetro Use-Answer-For-All-Defaults tiene el ajuste Yes (el ajuste predeterminado), la unidad TAOS utiliza los ajustes contenidos en el perfil Answer-Defaults para crear un perfil inicial para las llamadas autenticadas por RADIUS. La unidad utiliza los valores iniciales para los ajustes que no se especifican en el perfil RADIUS del emisor. Por ejemplo, si el perfil RADIUS del emisor no aplica un filtro de datos, ni un filtro de llamada, ni ambos, y el parámetro Use-Answer-for-All-Defaults tiene el valor Yes, cualquier filtro aplicado al perfil Answer-Defaults se aplica a la conexión autenticada. Pero si el perfil del emisor sí que aplica un filtro de datos o de llamada, se utilizan los filtros aplicados en el perfil Answer-Defaults.

## Ejemplos de aplicación de un filtro de datos a una interfaz de WAN

Cuando se aplica un filtro de datos, la acción de reenvío (reenvío o descarte) afecta a la corriente de datos real evitando que determinados paquetes alcancen la red Ethernet desde la WAN, y viceversa. Los filtros de datos no afectan al temporizador de inactividad y un filtro de datos aplicado a un perfil Connection no afecta al proceso de respuesta. En los ejemplos siguientes, la unidad TAOS permite los dos perfiles Filter locales siguientes:

```
admin> dir filter
370  09/13/1998 15:04:31  ip-spoof
372  09/13/1998 15:04:43  web-access
```

A continuación se muestra un ejemplo de aplicación de un filtro de datos:

```
admin> read conn tlynch
CONNECTION/tlynch read

admin> set session data-filter = ip-spoof

admin> write
CONNECTION/tlynch written
```

A continuación se muestra un perfil RADIUS equivalente:

```
tlynch Password = "secret"
      Service-Type = Framed-User,
      Framed-Protocol = MPP,
      Framed-IP-Address = 10.10.10.64,
      Framed-IP-Netmask = 255.255.255.0,
      Filter-Id = "ip-spoof"
```

El siguiente perfil RADIUS hace referencia a ambos filtros locales:

```
tlynch Password = "secret"
      Service-Type = Framed-User,
      Framed-Protocol = MPP,
      Framed-IP-Address = 10.10.10.64,
      Framed-IP-Netmask = 255.255.255.0,
      Filter-Id = "ip-spoof",
      Filter-Id = "web-access"
```

Como sucede siempre con los filtros, el orden en que se aplican en el perfil de usuario es importante. Si la unidad TAOS permite varios perfiles Filter con nombres similares, intenta hacer coincidir el primer perfil Filter con los caracteres especificados en el perfil de usuario.

A continuación se muestra un ejemplo de definición de un filtro de protección frente a engaños dentro del perfil RADIUS de usuario:

```
tlynch Password = "secret"
      Service-Type = Framed-User,
      Framed-Protocol = MPP,
      Framed-IP-Address = 10.10.10.64,
      Framed-IP-Netmask = 255.255.255.0,
      Ascend-Data-Filter = "ip in drop srcip 192.100.50.128/26"
      Ascend-Data-Filter = "ip in drop srcip 127.0.0.0/8"
      Ascend-Data-Filter = "ip in forward"
      Ascend-Data-Filter = "ip out forward srcip 192.100.50.128/26"
```

## Ejemplos de aplicación de un filtro de llamada a una interfaz de WAN

Los filtros de llamada evitan que se efectúen conexiones innecesarias y ayudan a la unidad TAOS a distinguir entre el tráfico activo y el “ruido”. De manera predeterminada, el tráfico hacia un sitio remoto desencadena una llamada y el tráfico a través de una conexión activa reinicia el temporizador de inactividad de la conexión.

Los comandos siguientes aplican un filtro a una conexión WAN y establecen el temporizador de inactividad en 20 segundos. Si ningún paquete atraviesa el filtro de llamada en cualquier sentido durante 20 segundos, la conexión se desactiva.

```
admin> read conn bob
CONNECTION/bob read
```

## Filtros de paquetes

### Aplicación de un filtro a una interfaz

---

```
admin> set session call-filter = out-only

admin> set session idle-timer = 20

admin> write
CONNECTION/bob written
```

A continuación se muestra un perfil RADIUS equivalente:

```
bob Password = "secret"
  Service-Type = Framed-User,
  Framed-Protocol = MPP,
  Framed-IP-Address = 10.10.10.23,
  Framed-IP-Netmask = 255.255.255.0,
  Ascend-Idle-Limit = 20
  Ascend-Call-Filter = "generic in drop"
  Ascend-Call-Filter = "generic out forward"
```

## Ejemplos de aplicación de un filtro TOS a una interfaz de WAN

Los filtros TOS dan instrucciones al sistema para que establezca bits de prioridad y clases de servicio TOS (Tipo de servicio) en nombre de las aplicaciones del usuario. La unidad TAOS no pone en marcha la puesta en cola por prioridades, pero define información que pueden utilizar los ruteadores de carga para asignar una prioridad a los enlaces y seleccionarlos para corrientes de datos concretas. Los filtros TOS especifican los bits que deben establecerse en la cabecera TOS de los paquetes IP.

La serie de comandos siguiente aplica un filtro TOS a un perfil Connection. Cuando la corriente de datos de entrada contiene paquetes que coinciden con la especificación de filtro TOS, los ajustes proxy-QoS y TOS especificados en el filtro se establecen en estos paquetes.

```
admin> read connection jfan-pc
CONNECTION/jfan-pc read

admin> set ip-options tos-filter = jfans-tos-filter

admin> write
CONNECTION/jfan-pc written
```

A continuación se muestra un perfil RADIUS equivalente en el que se especifica el filtro TOS mediante el atributo Filter-ID:

```
jfan-pc Password = "johnfan"
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Framed-IP-Address = 10.168.6.120
  Framed-IP-Netmask = 255.255.255.0
  Filter-ID = "jfans-tos-filter"
```

A continuación se muestra un perfil RADIUS en el que el filtro TOS se especifica dentro del perfil:

```
jfan-pc Password = "johnfan"
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Framed-IP-Address = 10.168.6.120
  Framed-IP-Netmask = 255.255.255.0
```



```
Ascend-Filter = "iptos in dstip 10.1.1.1/32 dstport = 23 precedence  
010 type-of-service latency"
```

**Nota:** Las definiciones de filtro no pueden contener indicadores de línea nueva. El ejemplo anterior muestra la especificación en dos líneas para fines exclusivamente de impresión.

## Ejemplos de aplicación de un filtro de ruta a una interfaz IP de WAN o LAN

Los filtros de ruta especifican las rutas de los paquetes de actualización de RIP que podrán afectar a la tabla de ruteo. También se pueden utilizar para aumentar la métrica asignada a una ruta antes de añadirla a la tabla de ruteo.

Cuando se aplica un filtro de ruta a una interfaz IP, la unidad TAOS supervisa los paquetes RIP en dicha interfaz y efectúa una acción específica si una ruta coincide con las especificaciones de filtro. En función de la manera en que se defina el filtro, se puede aplicar a paquetes RIP de entrada, paquetes RIP de salida o ambos. Los filtros de ruta solamente se permiten en perfiles Filter definidos localmente en la interfaz de línea de comandos y no en filtros definidos en RADIUS.

Los filtros de ruta no interrumpen el reenvío de paquetes de actualización de RIP. Al contrario, su acción determina si el sistema añade rutas coincidentes a la tabla de ruteo.

A continuación se muestra un ejemplo de aplicación de un filtro a un perfil Connection:

```
admin> read conn bdv  
CONNECTION/bdv read  
  
admin> set ip-options route-filter = route-test  
  
admin> write  
CONNECTION/bdv written
```

A continuación se muestra un ejemplo de aplicación de un filtro de ruta a una interfaz IP local:

```
admin> read ip-interface { { 1 c 1 } 0 }  
IP-INTERFACE/{ { shelf-1 controller 1 } 0 } read  
  
admin> set route-filter = route-test  
  
admin> write  
IP-INTERFACE/{ { shelf-1 controller 1 } 0 } written
```

## Ejemplo de aplicación de un filtro a una interfaz de LAN

Las interfaces Ethernet son rutas conectadas, por lo que los filtros de llamada no son válidos. Sin embargo, puede aplicar un filtro de datos que determine qué paquetes pueden entrar o salir de la red Ethernet. Un filtro que se aplica a una interfaz Ethernet entra en vigor de manera inmediata. Si cambia un ajuste en un perfil Filter, los cambios se aplicarán tan pronto como guarde el perfil Filter.

**Nota:** Cuando aplique un filtro a una interfaz Ethernet, hágalo con mucho cuidado. Podría, sin darse cuenta, hacer que la unidad TAOS sea inaccesible desde la LAN local.

## Filtros de paquetes

### *Aplicación de un filtro a una interfaz*

---

La siguiente serie de comandos aplica un filtro a una interfaz de red local:

```
admin> read ether {1 12 1}
ETHERNET/{ shelf-1 slot-12 1 } read
admin> set filter-name = dstipx
admin> write
ETHERNET/{ shelf-1 Slot-12 1 } written
```

Fax IP de almacenamiento y reenvío . . . . .	10-1
Configuración de la unidad TAOS para el fax IP. . . . .	10-5

## Fax IP de almacenamiento y reenvío

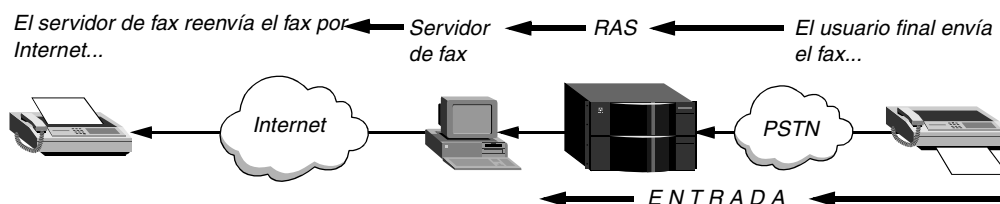
La función de almacenamiento y reenvío del fax IP permite que la unidad TAOS interactúe con un servidor de fax de otros fabricantes, como los servidores proporcionados por Open Port Technology, Inc. La tecnología Fax sobre IP hace posible que los ISP y los concentradores corporativos puedan utilizar Internet para entregar faxes.

Cuando se activa la función de fax IP en la unidad TAOS, el sistema actúa como servidor de acceso remoto (RAS), pues acepta llamadas de fax en los mismos puertos y líneas telefónicas utilizadas para las conexiones de llamada de entrada por módem. La unidad también ejecuta funciones de llamada de salida por módem para entregar faxes de Internet a las máquinas de fax conectadas a la red telefónica pública conmutada (PSTN).

## Faxes IP de entrada y de salida

En la Figura 10-1 se muestra la estructura básica del funcionamiento de un fax IP de entrada. La unidad TAOS recibe un *fax de entrada* de la red PSTN e interactúa con el servidor de fax para transferirlo a Internet. La transferencia a Internet es transparente para la persona que envía el fax, debido a que hay un dispositivo de hardware llamado *remarcador* conectado a la máquina de fax. El remarcador intercepta el número marcado en la máquina de fax e inicia una llamada a la unidad TAOS en su lugar. Cuando el servidor de fax empieza a transferir el fax a Internet, el remarcador y la unidad TAOS se convierten en canales transparentes para los datos de fax.

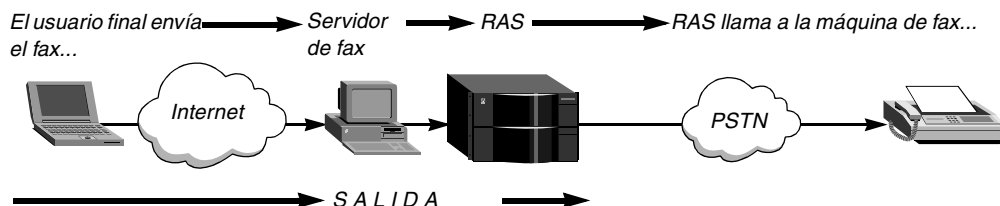
Figura 10-1. Fax IP de entrada de una máquina de fax a Internet



En la Figura 10-2 se muestra la estructura básica del funcionamiento de un fax IP de salida. El servidor de fax recibe un *fax de salida* de Internet e interactúa con la unidad TAOS para transferirlo a la red PSTN. El servidor de fax se conecta con la unidad TAOS y se autentica

antes de tomar el control de uno de los módems de la unidad para realizar la llamada de salida a la máquina de fax de destino.

Figura 10-2. Fax IP de salida de Internet a la máquina de fax



## Parámetros del sistema para el uso del fax-módem IP

Para enviar faxes, el servidor de fax se conecta con la unidad TAOS, toma el control de uno de sus módems y realiza la llamada de salida. La configuración del servidor de fax especifica la dirección IP de la unidad TAOS y (opcionalmente) uno o varios grupos de líneas troncales para el uso del fax IP. Además de los parámetros de inicio de sesión y de puerto del fax IP que permiten al servidor de fax conectarse, y que se describen en el apartado siguiente, los parámetros siguientes del perfil System repercuten en los recursos disponibles para las llamadas de fax de salida (los ajustes que aparecen son los predeterminados).

```

[in SYSTEM]
use-trunk-groups = no
num-digits-trunk-groups = 1
parallel-dialing = 2

[in T1/{ any-shelf any-slot 0 }:line-interface]
default-call-type = digital

[in T1/{ any-shelf any-slot 0 }:line-interface:channel-config[1]]
trunk-group = 9

[in E1/{ any-shelf any-slot 0 }:line-interface]
default-call-type = digital

[in E1/{ any-shelf any-slot 0 }:line-interface:channel-config[1]]
trunk-group = 9

[in SWAN { any-shelf any-slot 0 }:line-config]
trunk-group = 9

[in CALL-ROUTE { { { any-shelf any-slot 0 } 0 } 0}]
trunk-group = 0

```

### Parámetro

### Especifica

Use-Trunk-Groups

Activa y desactiva el uso de grupos de líneas troncales en la unidad TAOS. Con el ajuste predeterminado **no**, no se aplican los ajustes Num-Digits-Trunk-Groups ni Trunk-Group. Con el ajuste **yes**, deben asignarse números de grupo de líneas troncales a todos los canales.

Parámetro	Especifica
Num-Digits-Trunk-Groups	Número de dígitos que se debe permitir para los grupos de líneas troncales. Actualmente el servidor de fax IP admite grupos de líneas troncales de 2 dígitos, pero la especificación del número de grupo de líneas troncales debe estar dentro del rango de 2 a 9. La unidad TAOS debe tener el mismo el número de dígitos del número de grupo de líneas troncales que el servidor de fax; de lo contrario, los números de teléfono no se analizarán correctamente y las llamadas fallarán. Para obtener información detallada al respecto, consulte la publicación <i>Guía de configuración de la interfaz física de APX 8000/MAX TNT/DSLNT</i> .
Parallel-Dialing	Número total de llamadas de salida que la unidad TAOS puede efectuar al mismo tiempo.
Default-Call-Type	Tipo de llamada predeterminada para las llamadas en líneas T1 o E1 que no son ISDN. Este parámetro debe establecerse en voice para fax IP sobre señalización en banda.
Trunk-Group	Número de grupo de líneas troncales (de 2 a 9). Para una línea de red, este parámetro asigna canales a un grupo de líneas troncales. En un perfil Call-Route, especifica que las llamadas recibidas en ese grupo de líneas troncales se rutearán al módulo, ranura y puerto especificados en el índice del perfil.

### *Asignación de ancho de banda para el uso habitual del fax IP*

Una vez que el servidor de fax tiene el control de un módem digital, realiza la llamada en cualquier canal disponible, a menos que la configuración del servidor de fax especifique un número de grupo de líneas troncales. En ese caso, el servidor de fax utiliza un canal disponible dentro de dicho grupo de líneas troncales. Si no hay ningún canal disponible en el grupo de líneas troncales, la unidad TAOS devuelve un código Trunk Group Not Available al servidor de fax, que intenta volver a realizar la llamada más adelante.

Por ejemplo, los comandos siguientes configuran el sistema para que utilice grupos de líneas troncales de 2 dígitos y asignan toda una línea T1 al grupo de líneas troncales 5 (pueden asignarse menos de 24 canales a un grupo de líneas troncales si es necesario). Si la configuración del servidor de fax también especifica grupos de líneas troncales de 2 dígitos y un grupo de líneas troncales 5, estos canales estarán disponibles para el uso del fax IP.

```
admin> read system
SYSTEM read

admin> set use-trunk-groups = yes

admin> set num-digits-trunk-groups = 2

admin> write
SYSTEM read

admin> read t1 { 1 5 7 }
T1/{ shelf-1 slot-5 7 } read

admin> set line default-call-type = voice

admin> set line channel 1 trunk = 5

admin> set line channel 2 trunk = 5
```

```
admin> set line channel 3 trunk = 5
admin> set line channel 4 trunk = 5
admin> set line channel 5 trunk = 5
admin> set line channel 6 trunk = 5
admin> set line channel 7 trunk = 5
admin> set line channel 8 trunk = 5
admin> set line channel 9 trunk = 5
admin> set line channel 10 trunk = 5
admin> set line channel 11 trunk = 5
admin> set line channel 12 trunk = 5
admin> set line channel 13 trunk = 5
admin> set line channel 14 trunk = 5
admin> set line channel 15 trunk = 5
admin> set line channel 16 trunk = 5
admin> set line channel 17 trunk = 5
admin> set line channel 18 trunk = 5
admin> set line channel 19 trunk = 5
admin> set line channel 20 trunk = 5
admin> set line channel 21 trunk = 5
admin> set line channel 22 trunk = 5
admin> set line channel 23 trunk = 5
admin> set line channel 24 trunk = 5
admin> write
T1/{ shelf-1 slot-5 7 } written
```

### *Configuración de un perfil Call-Route normal*

Una vez que ha asignado el grupo de líneas troncales, debe crear un perfil Call-Route para dirigir las llamadas de salida a la línea recién configurada si van a utilizar el grupo de líneas troncales 5. Por ejemplo:

```
admin> new call-route { { { shelf-1 slot-5 7 } 0 } 0 }
CALL-ROUTE/{ { { shelf-1 slot-5 7 } 0 } 0 } read
admin> set trunk-group = 5
admin> set call-route-type = trunk-call
admin> write
CALL-ROUTE/{ { { shelf-1 slot-5 7 } 0 } 0 } written
```

### *Especificación del número máximo de llamadas de salida paralelas*

El parámetro Parallel-Dialing limita el número de llamadas de salida que el sistema puede efectuar a la vez. Si se está procesando el número máximo de llamadas de salida y se efectúa una petición de llamada de salida, el sistema coloca la petición en cola y la procesa a la mínima oportunidad.

Esta operación es transparente para el servidor de fax, excepto en caso de que los módems agoten el tiempo de espera si una petición de llamada de salida se retrasa más de 30 a 40 segundos. A continuación se muestra un ejemplo que establece el parámetro Parallel-Dialing en el valor máximo para T1:

```
admin> read system
SYSTEM read

admin> set parallel-dialing = 64

admin> write
SYSTEM read
```

## Configuración de la unidad TAOS para el fax IP

A continuación se muestran los parámetros del fax IP que permiten que la unidad TAOS interactúe con un servidor de fax de otro fabricante. Los ajustes que aparecen son los valores predeterminados.

```
[in IP-FAX]
ip-fax-enabled = no
outgoing-fax-port = 10001
server-login = ""
server-password = ""
incoming-fax-port = 0
all-calls-are-fax = no

[in IP-FAX:fax-dnis]
fax-dnis[1] = ""
fax-dnis[2] = ""
fax-dnis[3] = ""
fax-dnis[4] = ""
fax-dnis[5] = ""
fax-dnis[6] = ""
fax-dnis[7] = ""
fax-dnis[8] = ""

[in IP-FAX:fax-servers]
fax-servers[1] = 0.0.0.0
fax-servers[2] = 0.0.0.0
fax-servers[3] = 0.0.0.0
fax-servers[4] = 0.0.0.0
fax-servers[5] = 0.0.0.0
```

Parámetro	Especifica
IP-Fax-Enabled	Activa y desactiva el soporte de fax IP en la unidad TAOS. De manera predeterminada, está desactivado.
Outgoing-Fax-Port	Puerto TCP en el que se aceptan los datos de fax de salida de un servidor de fax (los datos de fax de salida se reciben de Internet y requieren una llamada de salida a una máquina de fax de destino). El valor predeterminado es 10001.

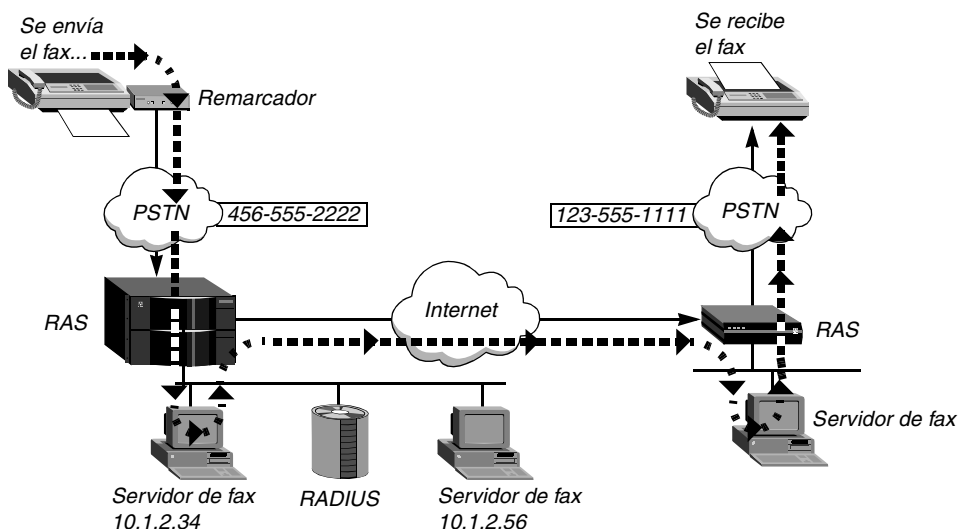
<b>Parámetro</b>	<b>Especifica</b>
Server-Login Server-Password	Nombre y contraseña utilizados para autenticar el servidor de fax como parte de una sesión de fax de salida. Cuando el servidor de fax recibe un fax de Internet, se conecta a la unidad TAOS y envía un nombre y una contraseña. La unidad TAOS compara los valores con los ajustes de Server-Login y Server-Password.
Incoming-Fax-Port	Puerto TCP en el que el servidor de fax espera la recepción de datos de fax de entrada (los datos de fax de entrada se reciben de un remarcador de máquina de fax). El valor predeterminado es cero.
All-Calls-Are-Fax	Activa y desactiva la gestión de todas las llamadas de entrada como llamadas de fax IP. Cuando este parámetro se establece en <code>no</code> (el valor predeterminado), la unidad TAOS reconoce las llamadas de fax de entrada comparando el número DNIS del emisor con uno de los números Fax-DNIS especificados por Fax-DNIS [1-8]. Con el ajuste <code>yes</code> , se da soporte al servicio de fax IP si no hay un número DNIS disponible.
Fax-DNIS [1-8]	Hasta ocho números DNIS. La unidad TAOS compara el número DNIS suministrado en el mensaje de configuración PRI de una llamada de entrada con los números configurados. Si no coinciden exactamente, la unidad no iniciará la función de fax IP.
Fax-Servers [1-5]	<p>Dirección IP de hasta cinco servidores de fax. Los sistemas de servidor de fax se encuentran normalmente en la red IP local, pero la conectividad local no es un requisito.</p> <p>La unidad TAOS intenta primero conectarse con el servidor de fax en la dirección especificada en primer lugar. Si la unidad no recibe ninguna respuesta, intenta conectarse en la segunda dirección. Si la unidad sigue sin recibir ninguna respuesta, intenta con la tercera, y así sucesivamente. Una vez que la unidad TAOS logra conectarse con un servidor de fax, utilizará esa misma dirección para las conexiones posteriores hasta que falle un intento de conexión, momento en que intentará conectarse con la siguiente dirección configurada.</p>

## **Ejemplo de una configuración de fax IP para faxes de entrada**

En la Figura 10-3 se muestra cómo una unidad TAOS recibe un fax de entrada a través de la red PSTN. La unidad inicia una sesión TCP con un servidor de fax, que autentica la llamada de entrada (el servidor de fax puede utilizar RADIUS, como se muestra en la Figura 10-3, o un método exclusivo de ese servidor). Si el servidor de fax autentica la llamada correctamente, realiza una llamada de salida al servidor de fax remoto en uno de los módems de la unidad TAOS. Una vez finalizada la transmisión del fax, el servidor de fax termina la sesión TCP y la unidad TAOS vuelve a obtener el control de su módem.

*Figura 10-3. Recepción y reenvío de faxes IP de entrada*





A continuación se muestra un ejemplo de una configuración de fax IP que permite que la unidad TAOS gestione las llamadas de fax de entrada como se muestra en la Figura 10-3:

```
admin> new ip-fax
IP-FAX read

admin> set ip-fax-enabled = yes

admin> set incoming-fax-port = 1234

admin> set fax-dnis 1 = 2222

admin> set fax-servers 1 = 10.1.2.34

admin> set fax-servers 2 = 10.1.2.56

admin> list
ip-fax-enabled = yes
outgoing-fax-port = 10001
server-login = ""
server-password = ""
incoming-fax-port = 1234
all-calls-are-fax = no
fax-dnis = [ 2222 "" "" "" "" "" "" "" ]
fax-servers = [ 10.1.2.34 10.1.2.56 0.0.0.0 0.0.0.0 0.0.0.0 ]

admin> write
IP-FAX written
```

Con esta configuración, el fax IP se procesa de la manera siguiente:

- 1 Un usuario final envía un fax al 123-555-1111.
- 2 La máquina que envía el fax recibe un tono de marcación del remarcador (que está conectado directamente a la máquina de fax) y marca el 123-555-1111.
- 3 El remarcador intercepta la llamada, almacena el número de teléfono de destino y marca su número configurado para la unidad TAOS (456-555-2222).
- 4 La unidad TAOS recibe la llamada y la identifica como una llamada de fax comparando el número DNIS de la llamada con los valores Fax-DNIS del perfil IP-Fax.
- 5 Si los números DNIS coinciden (o si la unidad está configurada para que considere todas las llamadas de entrada como llamadas de fax IP), la unidad TAOS genera un tono de

respuesta a 400 Hz para iniciar una comunicación DTMF (Multifrecuencia de dos tonos) con el remarcador. A continuación, la unidad descodifica la secuencia DTMF de entrada del remarcador, que contiene el número de cuenta del remarcador y el número de teléfono de destino 123-555-1111.

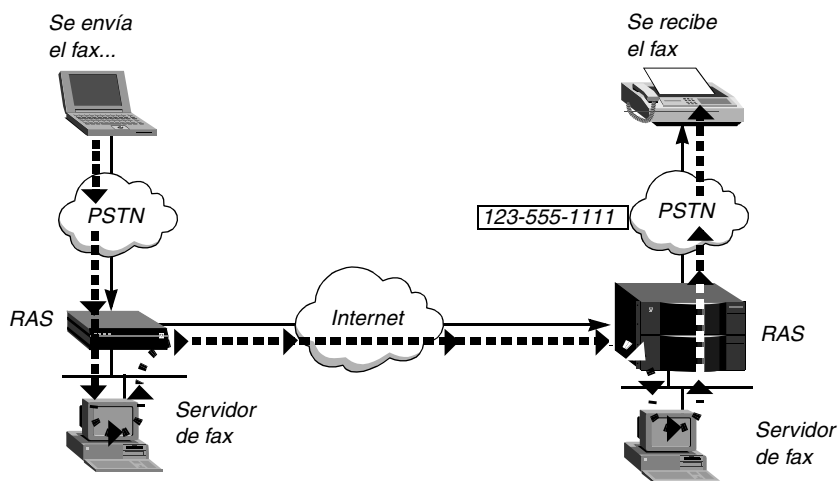
- 6 La unidad TAOS inicia una conexión con el servidor de fax, enviando el número de cuenta del emisor y el número de teléfono de destino en el primer paquete TCP.
- 7 Si el servidor de fax autentica correctamente la llamada con esta información, la unidad TAOS contesta la llamada del fax de entrada. Si la autenticación falla, finaliza la conexión.
- 8 Cuando la autenticación es correcta, la unidad TAOS y el servidor de fax establecen una sesión TCP, y la unidad TAOS transfiere el control de un módem disponible al servidor de fax para la llamada de entrada. Si no se produce ninguna actividad de envío o de recepción durante más de 2 minutos, se termina la sesión y se liberan los recursos.

**Nota:** A efectos contables, se inicia una sesión de fax cuando se asigna un recurso de módem y se detiene cuando se termina la sesión.

## Ejemplo de una configuración de fax IP para faxes de salida

En la Figura 10-4 se muestra cómo una unidad TAOS reenvía un fax recibido por el servidor de fax de Internet. El servidor de fax se conecta a la unidad TAOS, introduciendo los valores de Server-Login y Server-Password especificados, e inicia una sesión de llamada de salida por módem para reenviar el fax por la red PSTN. Una vez finalizada la transmisión del fax, el servidor de fax termina la sesión TCP y la unidad TAOS vuelve a obtener el control de su módem.

*Figura 10-4. Envío de un fax IP de salida a una máquina de fax*



A continuación se muestra un ejemplo de una configuración de fax IP que permite que la unidad TAOS gestione las llamadas de fax de salida, como se muestra en la Figura 10-4:

```
admin> new ip-fax
IP-FAX read

admin> set ip-fax-enabled = yes

admin> set server-login = ipfax

admin> set server-password = works
```

```

admin> list
ip-fax-enabled = yes
outgoing-fax-port = 10001
server-login = ipfax
server-password = works
incoming-fax-port = 0
All calls are Fax = no
fax-dnis = [ "" "" "" "" "" "" "" "" ]
fax-servers = [ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 ]

admin> write
IP-FAX written

```

Con esta configuración, la unidad TAOS procesa un fax IP de la manera siguiente:

- 1 El servidor de fax de la red local recibe los datos de fax a través de Internet desde un servidor de fax remoto.
- 2 El servidor de fax inicia una conexión con la unidad TAOS enviando su nombre de inicio de sesión y su contraseña en el primer paquete TCP.
- 3 Si el nombre de inicio de sesión y la contraseña coinciden con los valores de Server-Login y Server-Password, respectivamente, del perfil del fax IP, la unidad TAOS establece una sesión TCP con el servidor de fax. Si la autenticación falla, finaliza la conexión.
- 4 Una vez lograda la autenticación, la unidad TAOS transfiere el control de un módem disponible al servidor de fax.
- 5 El servidor de fax envía comandos de módem encapsulados en paquetes TCP, inicia una conexión con la máquina de fax de destino y envía los datos mediante una operación periférica simultánea en línea (*spool*). Si no se produce ninguna actividad de envío ni de recepción durante más de 2 minutos, se termina la sesión y se liberan los recursos.

**Nota:** A efectos contables, se inicia una sesión de fax cuando se asigna un recurso de módem y se detiene cuando se termina la sesión.

## Códigos de colgar fax y códigos de causa de la desconexión

Conexant suministra dos códigos de colgar fax:

- +FHNG 1: cuando los tonos de fax son reconocidos, pero el establecimiento de enlace falla
- +FHNG 11: cuando no se reconoce ningún tono de fax en el extremo distante

Los códigos de causa de la desconexión ISDN se devuelven cuando las llamadas de fax fallan, si están disponibles como parte de los códigos de colgar fax. Para evitar los problemas con los códigos devueltos por los módems y con los códigos devueltos por otras unidades, los códigos de causa de fax agregan 1000 a los códigos estándar, de modo que estén dentro del rango 1000–1255. Por ejemplo, Far End Busy (código ISDN 17) se devuelve como +FHNG 1017 y Far End Did Not Answer (es decir, no descuelga) se devuelve como +FHNG 1018.

## Contabilidad de llamadas de fax IP

En versiones anteriores del software, había más información contable disponible para una llamada de entrada que para una llamada de salida. Debido a que la función de fax IP crea un gran volumen de llamadas de salida, la información contable de las llamadas SNMP, RADIUS

y Syslog se ha ampliado y ahora incluye la siguiente información contable adicional para las llamadas de fax IP de salida:

- Indicación de la hora de conexión de la llamada, que muestra la duración de ésta
- El grupo de líneas troncales utilizado para canales específicos en una llamada de salida
- El número de teléfono de destino marcado desde la unidad TAOS
- El módulo, ranura, línea y número de canal en los que se origina la llamada
- El número total de bytes enviados y recibidos (sólo en SNMP y RADIUS)
- La velocidad de transmisión y de recepción en baudios (sólo en SNMP y RADIUS)

**Nota:** A efectos contables, una sesión de fax se inicia cuando se asigna un recurso de módem y se detiene cuando se termina la sesión.

## **Cambios SNMP para el funcionamiento del fax IP**

SNMP proporciona información adicional sobre la llamada en los campos siguientes:

<b>Nombre de campo MIB</b>	<b>Indica</b>
eventCurrentService: ipFax (19)	Service ipFax está disponible para una llamada de fax IP cuando el tipo de evento es callOriginated(1).
eventTrunkGroup (24)	El grupo de líneas troncales utilizado solamente para las llamadas de salida. Esta información está disponible cuando el tipo de evento es callCleared (9).
eventCalledPartyID	Número de teléfono marcado para una llamada de salida. Actualmente eventCalledPartyID es equivalente al ID de número marcado DNIS para una llamada de entrada. En la llamada de salida, este campo representa el número de teléfono marcado. Esta información está disponible cuando el tipo de evento es callCleared (9).
eventSlotNumber	Número de ranura en el que se originó la llamada. Esta información está disponible cuando el tipo de evento es callCleared(3).
eventSlotLineNumber	Línea en la que se originó la llamada. Esta información está disponible cuando el tipo de evento es callCleared(3).
eventSlotChannelNumber	Canal en el que se originó la llamada. Esta información está disponible cuando el tipo de evento es callCleared(3).
eventTimeStamp	Para una llamada de fax IP, hora a la que se reserva el módem para una petición de llamada de salida. Para cualquier otro tipo de llamada, este campo informa sobre el tiempo real de conexión. Esta información está disponible cuando el tipo de evento es callCleared(3).
eventInOctets	Número total de bytes recibidos para la llamada. Esta información está disponible cuando el tipo de evento es callCleared(3).
eventOutOctets	Número total de bytes transmitidos para la llamada. Esta información está disponible cuando el tipo de evento es callCleared(3).

<b>Nombre de campo MIB</b>	<b>Indica</b>
eventXmitRate	Velocidad de transmisión en baudios negociada que se utiliza en la llamada. Esta información está disponible cuando el tipo de evento es callCleared(3). Para el fax IP, las velocidades en baudios de transmisión y de recepción son las mismas.
eventDataRate	Velocidad de recepción en baudios negociada que se utiliza en la llamada. Esta información está disponible cuando el tipo de evento es callCleared(3). Para el fax IP, las velocidades en baudios de transmisión y de recepción son las mismas.
eventUserIPAddress	Dirección IP del usuario. Esta información está disponible cuando el tipo de evento es nameChanged(5).
eventUserName	Nombre de usuario. Esta información está disponible cuando el tipo de evento es callOriginated(1).
eventModemSlotNumber	Ranura en la que está ubicado el módem. Esta información está disponible cuando el tipo de evento es callOriginated(1).
eventModemOnSlot	Módem en uso. Esta información está disponible cuando el tipo de evento es callOriginated(1).
ssnActiveUserName	Nombre de usuario activo.
ssnActiveUserIPAddress	Dirección IP de usuario activo.
ssnActiveCurrentService: ipFax(19)	El servicio ipFax(19) está en uso para una llamada de fax IP de salida.

## Soporte RADIUS para el funcionamiento del fax IP

Los atributos RADIUS siguientes, que aparecen en los paquetes Accounting Stop, proporcionan valores de llamada de salida y de entrada para las llamadas de fax IP:

<b>Atributo RADIUS</b>	<b>Valor</b>
NAS-Port	Módulo, ranura, línea y número de canal en los que se origina la llamada de salida. El valor aparece en el formato binario siguiente:  FFSS SSSL LLLC CCCC  FF especifica el número de módulo.  SSSS especifica el número de ranura.  LLLLL especifica el número de línea.  CCCC especifica el número de canal.  Para cada valor se empieza a contar a partir de cero. Por ejemplo, dado el número decimal 13348, cuyo equivalente binario es 0011 0100 0010 0100:  00=número de módulo 1  1101=número de ranura 14  00001=número de línea 2  0100=número de canal 5

<b>Atributo RADIUS</b>	<b>Valor</b>
Acct-Session-Time	Tiempo total de conexión para una llamada. Para una llamada de fax IP de salida, el periodo de tiempo empieza cuando se reserva el módem y finaliza cuando se termina la llamada.
Client-Port-DNIS	Número llamado para una llamada de salida.
Ascend-Modem-PortNo	Puerto de módem utilizado para la llamada.
Ascend-Modem-SlotNo	Número de la ranura en que está ubicada físicamente la tarjeta de módem.
Ascend-Modem-ShelfNo	Número del módulo en que está ubicada la tarjeta de módem.
Acct-Input-Octets	Número total de bytes recibidos para la llamada.
Acct-Output-Octets	Número total de bytes transmitidos para la llamada.
Ascend-Xmit-Rate	Velocidad de transmisión en baudios negociada para la llamada. Para el fax IP, las velocidades en baudios de transmisión y de recepción son las mismas.
Ascend-Data-Rate	Velocidad de recepción en baudios negociada para la llamada. Para el fax IP, las velocidades en baudios de transmisión y de recepción son las mismas.

Además, el atributo Ascend-CBCP-Trunk-Group (115) se aplica a las llamadas de fax IP de salida.

<b>Atributo</b>	<b>Valor</b>
Ascend-CBCP-Trunk-Group (115)	<p>Asigna la devolución de llamada o llamada de fax IP de salida al grupo de líneas troncales de una unidad TAOS. El valor de Ascend-CBCP-Trunk-Group se agrega al final del número que la unidad TAOS marca para una devolución de llamada o una llamada de fax de salida. Especifique un número de grupo de líneas troncales entre 1 y 9.</p> <p>Ascend-CBCP-Trunk-Group sólo es aplicable si se da una de estas condiciones o ambas a la vez:</p> <ul style="list-style-type: none"> <li>• Callback Control Protocol (CBCP) se negocia para realizar una conexión.</li> <li>• La llamada es una llamada de fax IP de salida y los grupos de líneas troncales se han activado en el perfil System.</li> </ul>

## **Soporte Syslog para el funcionamiento del fax IP**

El mensaje Syslog siguiente refleja la hora en la que se ha reservado un módem:

```
LOG info, Shelf 1, Controller, Time: 15:36:40--
[1/1/13/0] [MBID 13] Assigned to Port
```

El mensaje siguiente muestra el número de llamada de salida, el grupo de líneas troncales, la ranura de módem y el número de módem al efectuar una llamada:

```
LOG info, Shelf 1, Controller, Time: 15:37:07--  
[1/1/13/0] [MBID 13; ->97476799] Outgoing Call, 97476799, Trunk 8
```

Cuando se conecta la llamada, el mensaje siguiente muestra su módulo, ranura, línea y canal:

```
LOG info, Shelf 1, Controller, Time: 15:37:13--  
[1/14/2/5] [MBID 13; ->97476799] Call Connected
```

Al terminar la llamada, se muestra la hora, la ranura de módem y el número de módem.

```
LOG info, Shelf 1, Controller, Time: 15:38:00--  
[1/1/13/0] [MBID 13; ->97476799] Call Terminated
```

## **Soporte de remarcador en la tarjeta MultiDSP para fax de almacenamiento y reenvío**

Cuando se conecta un dispositivo remarcador a una máquina de fax, éste espera un tono a 400 Hz. Tras recibir el tono, el remarcador transmite el número de fax de destino a la unidad TAOS en forma de dígitos DTMF. Con la versión actual de software, la tarjeta MultiDSP transmite el tono a 400 Hz y detecta los dígitos DTMF de entrada.





# Redes de transacciones de corta duración

# 11

Información general sobre las redes de transacciones de corta duración .....	11-1
Perfiles Transaction-Server .....	11-2
Conexiones de llamada de entrada para clientes de transacciones .....	11-5

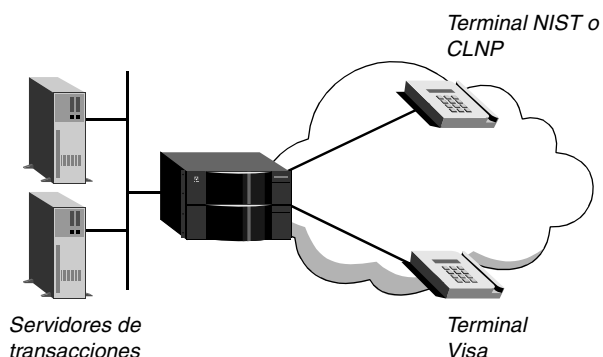
## Información general sobre las redes de transacciones de corta duración

La unidad TAOS da soporte a la interacción con servidores de transacciones para conducir transacciones de corta duración a través de redes basadas en IP. SDTN es una característica protegida mediante código hash. Los parámetros relacionados pueden verse en la interfaz de línea de comandos, pero no están activos a menos que se haya comprado a Lucent Technologies la licencia de software correspondiente. Puede verificar que la licencia de SDTN está activa en el perfil predeterminado Transaction-Server utilizando el comando siguiente:

```
admin> get transaction-server enabled
enabled = yes
```

Para dar soporte a transacciones de corta duración, la unidad TAOS recibe llamadas de aplicaciones cliente de transacciones y las transmite de forma transparente a un servidor de transacciones. En la Figura 11-1 se muestra un ejemplo de configuración de SDTN, con servidores de transacciones en una interfaz Ethernet local de 100 Mb.

Figura 11-1. Ejemplo de configuración de SDTN



Las llamadas de datos de transacción proceden de terminales NIST (*National Institute of Standards and Technology*, Instituto nacional de estándares y tecnología), terminales CLNP (Protocolo de red sin conexiones) o terminales Visa. La unidad TAOS responde a las llamadas y las envía al servidor de transacciones mediante QTP (Protocolo de transacción rápida).

QTP es un protocolo simétrico que opera sobre UDP en ambas direcciones entre la unidad TAOS y los servidores de transacciones. QTP establece y finaliza la conexión virtual entre sistemas, transporta el tráfico de la transacción e intercambia periódicamente mensajes de informe de estado.

La unidad TAOS utiliza una tabla de selección para determinar el servidor que se debe emplear para una petición de proceso de transacciones concreta. El sistema mantiene actualizados los datos sobre estado y disponibilidad de los servidores en la tabla aplicando métricas configurables a la información obtenida de los mensajes de informe de estado de QTP, así como a partir de eventos en tiempo real, por ejemplo el hecho de no recibir una respuesta a una petición de llamada.

## ***Perfiles Transaction-Server***

El perfil Transaction-Server establece parámetros que afectan a la métrica utilizada en la tabla de selección de servidor. La tabla contiene una lista primaria y otra secundaria de servidores de transacciones que se han introducido en la lista mediante QTP. La unidad TAOS sólo utiliza la lista primaria, a menos que no quede ningún servidor disponible en dicha lista; en tal caso, empieza a utilizar la lista secundaria. Cuando un servidor se agrega a la lista, la unidad TAOS genera uno de los mensajes Syslog siguientes:

```
TS Address [x.x.x.x] has been entered into the Primary List
TS Address [x.x.x.x] has been entered into the Secondary List
```

Cada entrada de la lista especifica una dirección IP del servidor de transacciones, el puerto UDP utilizado por QTP en dicho servidor y una métrica que indica la disponibilidad del servidor para la unidad TAOS. En esta versión, la unidad TAOS busca en la lista en orden cíclico y selecciona el primer servidor disponible (en esta versión, la métrica no se utiliza para ponderar la selección. Se utiliza para eliminar servidores de la lista cuando su estado o disponibilidad atraviesa un umbral métrico. En próximas versiones, se dará soporte a mecanismos de búsqueda adicionales). Cuando la unidad TAOS se elimina a sí misma de la lista, genera uno de los mensajes Syslog siguientes:

```
TS Address [x.x.x.x] has been removed from Primary List
TS Address [x.x.x.x] has been removed from Secondary List
```

Los ajustes de los parámetros del perfil Transaction-Server se utilizan para asociar la métrica con los eventos que mantienen actualizada la tabla: mensajes de informe de estado de QTP, eventos como peticiones de llamada y respuestas, y la recepción periódica de informes de estado de QTP. Si estos eventos no tienen lugar del modo previsto, el sistema puede modificar una métrica de servidor de transacciones en función de ello.

Los mensajes de informe de estado de QTP procedentes de servidores de transacciones pueden contener los atributos de control de flujo siguientes, que indican lo ocupado que está el servidor:

- Available (0x01)
- Partly Congested (0x02)
- Congested (0x03)
- Shutdown (0x04)

Los mensajes de informe de estado de QTP también pueden contener los atributos de estado Primary Station (0x01) o Secondary Station (0x02), que indican si el servidor se encuentra en la lista primaria o en la secundaria.

## Configuración de los ajustes de servidor de transacciones

Los parámetros siguientes (que aparecen con los valores predeterminados) se utilizan para configurar los algoritmos y umbrales métricos empleados para la selección del servidor de transacciones:

```
[in TRANSACTION-SERVER]
enabled = yes
hunting-mechanism = cyclic
selection-timeout = 10000
data-ack-timeout = 10000
keep-alive-timeout = 30
qtp-port = 3350
metric-max = 15
no-conn-ack-increment = 8
call-reject-increment = 4
call-ack-decrement = 1
available-metric = 1
partly-congested-metric = 4
congested-metric = 10
shutdown-metric = 14
no-first-status-metric = 10
no-second-status-metric = 16
max-qtp-pdu-size = 512
```

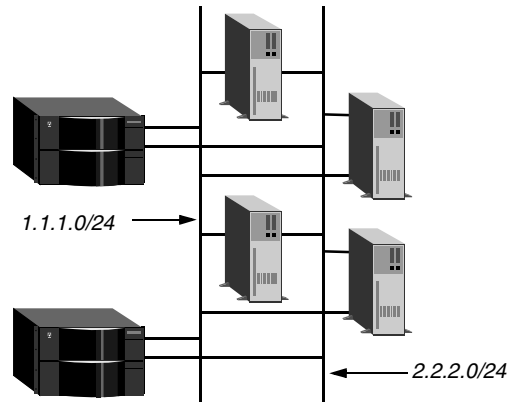
Parámetro	Especifica
Enabled	Estado de la licencia de SDTN (sólo lectura). Está establecido en <i>yes</i> cuando la licencia está activa. Si el valor es <i>No</i> , la licencia está desactivada y este perfil no tiene ningún efecto.
Hunting-Mechanism	Método de búsqueda en la lista primaria (o secundaria) de servidores de transacciones. En esta versión, sólo se da soporte al ajuste predeterminado <i>cyclic</i> , que indica que se busca en la lista en un orden cíclico.
Selection-Timeout	Número de milisegundos (de 0 a 65000) antes de que el intento de establecer una conexión QTP con un servidor de transacciones agote el tiempo de espera. El ajuste predeterminado es 10000 milisegundos.
Data-Ack-Timeout	Número de milisegundos (de 500 a 30000) que la unidad TAOS espera a que un servidor de transacciones envíe un acuse de recibo QTP en respuesta a un mensaje de datos de QTP. El ajuste predeterminado es 10000 milisegundos.
Keep-Alive-Timeout	Número de segundos (de 1 a 300) que la unidad TAOS espera a recibir una actualización de estado de QTP procedente de un servidor de transacciones. El ajuste predeterminado es 30 segundos.
QTP-Port	Puerto UDP en el que QTP debe recibir las conexiones QTP de entrada. Los números de puerto UDP pueden ser de 0 a 65535. El número de puerto predeterminado para QTP es 3350.

<b>Parámetro</b>	<b>Especifica</b>
Metric-Max	Número, de 0 a 255, que indica la métrica máxima, por encima de la cual un servidor de transacciones se elimina de la lista activa. La métrica máxima predeterminada es 15.
No-Conn-Ack-Increment	Número, de 0 a 255, en el que se aumenta la métrica actual de un servidor de transacciones si no envía un acuse de recibo de conexión QTP en respuesta a una petición de conexión QTP enviada por la unidad TAOS. El ajuste predeterminado es 8.
Call-Reject-Increment	Número, de 0 a 255, en el que se aumenta la métrica actual de un servidor de transacciones si envía un rechazo de llamada de QTP en respuesta a una petición de conexión QTP enviada por la unidad TAOS (un intento de conexión QTP ha fallado). El ajuste predeterminado es 4.
Call-Ack-Decrement	Número, de 0 a 255, en el que se disminuye la métrica actual de un servidor de transacciones si envía un acuse de recibo de llamada de QTP en respuesta a una petición de conexión QTP enviada por la unidad TAOS (un intento de conexión QTP ha tenido éxito). El ajuste predeterminado es 1.
Available-Metric	Número, de 0 a 255, que se utiliza como métrica actual de un servidor de transacciones si envía un mensaje de estado QTP con un atributo Flow Control establecido en Available. El ajuste predeterminado es 1.
Partly-Congested-Metric	Número, de 0 a 255, que se utiliza como métrica actual de un servidor de transacciones si envía un mensaje de estado QTP con un atributo Flow Control establecido en Partly-Congested. El ajuste predeterminado es 4.
Congested-Metric	Número, de 0 a 255, que se utiliza como métrica actual de un servidor de transacciones si envía un mensaje de estado QTP con un atributo Flow Control establecido en Congested. El ajuste predeterminado es 10.
Shutdown-Metric	Número, de 0 a 255, que se utiliza como métrica actual de un servidor de transacciones si envía un mensaje de estado QTP con un atributo Flow Control establecido en Shutdown. El ajuste predeterminado es 14.
No-First-Status-Metric	Número, de 0 a 255, que se utiliza como métrica actual de un servidor de transacciones la primera vez que no envía un mensaje de estado QTP dentro del intervalo del tiempo de espera. El ajuste predeterminado es 10.
No-Second-Status-Metric	Número, de 0 a 255, que se utiliza como métrica actual de un servidor de transacciones la segunda vez que no envía un mensaje de estado QTP dentro del intervalo del tiempo de espera. El ajuste predeterminado es 16.
Max-QTP-PDU-Size	Número máximo de bytes (de 1 a 1460) que puede contener un mensaje de QTP enviado por la unidad TAOS. El ajuste predeterminado es 512 bytes.

## Ejemplo de configuración de un servidor de transacciones

En la Figura 11-2 se muestra un ejemplo de configuración de SDTN con dos estaciones de unidad TAOS. Por cuestiones de redundancia y de velocidad de acceso, cada unidad TAOS y cada servidor de transacciones da soporte a una interfaz Ethernet de 100 Mbps en dos subredes locales. Dado que los informes de estado QTP de los servidores de transacciones contienen las direcciones IP de las dos interfaces Ethernet de cada servidor, un único servidor aparece como dos entidades accesibles en la tabla de selección de los servidores. Estas conexiones proporcionan cierta redundancia si se produce un fallo en una subred o puerto Ethernet, puesto que aún se puede acceder al servidor en la otra subred o el otro puerto.

*Figura 11-2. Servidores de transacciones con conexiones Ethernet redundantes*



En la mayoría de los entornos, los ajustes predeterminados del perfil Transaction-Server son la configuración de SDTN más eficaz.

## Conexiones de llamada de entrada para clientes de transacciones

La unidad TAOS reconoce las conexiones de marcación HDLC-NRM (HDLC-modo de respuesta normal) y Visa-II para el proceso de transacciones.

Cualquier conexión de cliente de transacciones requiere una gestión rápida para evitar superar los tiempos de espera. Si la llamada se realiza por módem, puede configurar una cadena AT personalizada que especifique la temporización de módem requerida, los tipos de modulación, la velocidad y otros parámetros del módem. Esta personalización ayuda a evitar retardos provocados por el ajuste del módem.

## Ajustes del perfil Answer-Defaults

El perfil Answer-Defaults contiene dos subperfiles nuevos para los protocolos de encapsulación de capa de enlace HDLC-NRM y Visa-II. A continuación se muestran los parámetros pertinentes, con los ajustes predeterminados:

```
[in ANSWER-DEFAULTS:hdlc-nrm-answer]
enabled = yes

[in ANSWER-DEFAULTS:visa2-answer]
enabled = yes
```

De manera predeterminada, el sistema no rechaza las llamadas HDLC-NRM o Visa-II basándose en los tipos de encapsulación. Con los ajustes predeterminados, el sistema responde a las llamadas si pasan la autenticación.

En el caso de conexiones HDLC-NRM y Visa-II, se requiere autenticación CLID o DNIS. Por ejemplo, los comandos siguientes configuran la unidad para que necesite DNIS:

```
admin> read answer
ANSWER-DEFAULTS read

admin> set clid-auth-mode = dnis-require

admin> write
ANSWER-DEFAULTS written
```

## Configuración de conexiones HDLC-NRM

La unidad TAOS da soporte a HDLC-NRM como protocolo de encapsulación de capa de enlace. Cuando recibe una llamada HDLC-NRM, el sistema debe autenticarla primero mediante CLID o DNIS. Si la llamada pasa la autenticación, el sistema la responde, completa las negociaciones HDLC y envía los paquetes al software de QTP, que los rutea a través de UDP a un servidor de transacciones.

HDLC-NRM es similar al protocolo LAPB (Procedimiento de acceso al enlace en modo simétrico) y a otros protocolos HDLC de capa 2. El paquete HDLC-NRM inicial es SNRM (Paso a modo de respuesta normal). A diferencia del protocolo LAPB, en el que las estaciones conectadas son homólogas y están activadas para enviar datos en cualquier momento, HDLC-NRM es un protocolo semidúplex, de modo que sólo una estación puede enviar datos en un momento dado. Para ello, una de las estaciones conectadas es la estación primaria (normalmente la unidad TAOS) y la otra es la estación secundaria (normalmente el terminal NIST o CLNP). La estación primaria puede enviar paquetes de datos en cualquier momento. La estación secundaria se debe sondear (mediante RR) antes de que pueda enviar paquetes de datos como tramas-I síncronas. De manera predeterminada, la estación primaria elimina los paquetes de datos que recibe de la estación secundaria cuando la estación no está autorizada para transmitir (tramas-I asíncronas).

### *Información general sobre los ajustes de HDLC-NRM*

Los parámetros siguientes, que aparecen con los valores predeterminados, se utilizan para configurar conexiones HDLC-NRM:

```
[in CONNECTION/dgtnt]
encapsulation-protocol = hdlc-nrm
sdtm-packets-server = no

[in CONNECTION/dgtnt:hdlc-nrm-options]
enabled = no
snrm-response-timeout = 20000
snrm-retry-counter = 2
poll-timeout = 60000
poll-rate = 5000
poll-retry-counter = 2
primary = yes
async-drop = yes
```

Parámetro	Especifica
Encapsulation-Protocol	Protocolo de encapsulación que debe utilizarse para esta conexión. Debe establecerse en <code>hdlc-nrm</code> para clientes HDLC-NRM.
SDTN-Packets-Server	Activa y desactiva el envío de paquetes a un servidor de transacciones mediante QTP. Establezca este parámetro en <code>yes</code> para las conexiones HDLC-NRM. Si está establecido en <code>no</code> (el ajuste predeterminado) para una conexión HDLC-NRM, el sistema establece la conexión, pero elimina los datos.
Enabled	Activa y desactiva la función de respuesta a una llamada HDLC-NRM que coincida con este perfil.
SNRM-Response-Timeout	SNRM (Paso a modo de respuesta normal) es el paquete HDLC-NRM inicial enviado. Este ajuste especifica el número de milisegundos (500-5000) que hay que esperar una respuesta. El ajuste predeterminado es 2000.
SNRM-Retry-Counter	Número de veces (de 0 a 255) que se reintentará enviar un paquete SNRM tras el tiempo de espera de respuesta. El ajuste predeterminado es 2.
Poll-Timeout	Número de milisegundos (de 0 a 255000) que hay que esperar una respuesta del emisor (la estación secundaria) a un sondeo enviado por la unidad TAOS (la estación primaria). El ajuste predeterminado es 60000.
Poll-Rate	Número de milisegundos (de 500 a 5000) entre sondeos. El ajuste predeterminado es 5000.
Poll-Retry-Counter	Número de veces (de 0 a 255) que se reintentará el sondeo tras el tiempo de espera de respuesta. El ajuste predeterminado es 2.
Primary	Estado de la estación primaria o secundaria de la unidad de llamada de entrada. El ajuste predeterminado es <code>no</code> porque los terminales de marcación suelen actuar como estaciones secundarias. Si establece este parámetro en <code>yes</code> , la unidad TAOS actúa como estación secundaria para esta conexión (normalmente para pruebas).
Async-Drop	Dado que HDLC-NRM es un protocolo semidúplex, la estación primaria debe eliminar las tramas-I asíncronas que recibe de una estación secundaria. Cuando este parámetro está establecido en <code>yes</code> (el ajuste predeterminado) y la unidad TAOS es la estación primaria, el sistema elimina las tramas-I recibidas de la estación secundaria. Si el parámetro está establecido en <code>no</code> , el sistema procesa normalmente las tramas-I que recibe. El hecho de establecer el parámetro en <code>no</code> activa la comprobación dos a dos en la unidad TAOS.

### *Ejemplo de una configuración típica de cliente HDLC-NRM*

En este ejemplo, los comandos siguientes configuran un perfil Connection para un cliente HDLC-NRM:

```
admin> new conn hstation-1  
CONNECTION/hstation-1 read
```

```
admin> set active = yes
admin> set encapsulation-protocol = hdlc-nrm
admin> set sdtm-packets-server = yes
admin> set dial-number = 853784
admin> set calledNumber = 3783
admin> set telco-options dialout-allowed = yes
admin> set hdlc-nrm-options enabled = yes
admin> write
CONNECTION/hstation-1 written
```

## Configuración de conexiones Visa-II

La unidad TAOS da soporte a Visa-II como protocolo de encapsulación de capa de enlace. Cuando recibe una llamada de un terminal Visa, el sistema debe autenticar primero la llamada mediante CLID o DNIS. Si la llamada pasa la autenticación, el sistema la responde y envía los paquetes al software de QTP, que los rutea a través de UDP a un servidor de transacciones.

En el caso de las conexiones Visa-II, la gestión del protocolo tiene lugar entre el servidor de transacciones y el terminal Visa. Para los datos de entrada procedentes del terminal, la unidad TAOS realiza un análisis mínimo, como definen los ajustes de Visa-II en el perfil Connection del emisor. En cuanto a los datos que van del servidor al terminal, la unidad TAOS sencillamente los transmite de forma transparente.

### *Información general sobre los ajustes de Visa-II*

Los siguientes parámetros, que aparecen con los valores predeterminados, se utilizan para configurar Visa-II:

```
[in CONNECTION/dgtnt]
encapsulation-protocol = visa2
sdtn-packets-server = no

[in CONNECTION/dgtnt:visa2-options]
enabled = no
idle-character-delay = 10000
first-data-forward-character = 04
second-data-forward-character = 06
third-data-forward-character = 15
fourth-data-forward-character = 05
1-char-sequence = 03
2-char-sequence = 00:03:00:00
```

Parámetro	Especifica
Encapsulation-Protocol	Protocolo de encapsulación que debe utilizarse para esta conexión. Debe establecerse en <i>visa2</i> para las conexiones de terminal Visa.
SDTN-Packets-Server	Activa y desactiva el envío de paquetes a un servidor de transacciones mediante QTP. Establezca este parámetro en <i>yes</i> para las conexiones de terminal Visa. Si está establecido en <i>no</i> (el ajuste predeterminado) para una conexión de terminal Visa, el sistema establece la conexión, pero elimina los datos.



<b>Parámetro</b>	<b>Especifica</b>
Enabled	Activa y desactiva la función de respuesta a una llamada Visa-II que coincida con este perfil.
Idle-Character-Delay	Número de milisegundos de tiempo de inactividad tras recibir un carácter antes de enviar datos. Entre 0 y 30.000 ms. El ajuste predeterminado es 10.000 ms.
First-Data-Forward-Character	Valor hexadecimal de un carácter que se debe utilizar como desencadenante para enviar datos. El ajuste predeterminado es 04.
Second-Data-Forward-Character	Valor hexadecimal de un carácter que se debe utilizar como desencadenante para enviar datos. El ajuste predeterminado es 06.
Third-Data-Forward-Character	Valor hexadecimal de un carácter que se debe utilizar como desencadenante para enviar datos. El ajuste predeterminado es 15.
Fourth-Data-Forward-Character	Valor hexadecimal de un carácter que se debe utilizar como desencadenante para enviar datos. El ajuste predeterminado es 05.
1-Char-Sequence	Valor hexadecimal de un carácter que se debe utilizar como desencadenante para enviar datos y el carácter siguiente. El ajuste predeterminado es 03.
2-Char-Sequence	Dos valores de caracteres de una secuencia que se deben utilizar como desencadenantes para enviar datos y los dos caracteres siguientes tras la secuencia. El ajuste predeterminado es 00:03:00:00. Observe que tan sólo los dos primeros valores de caracteres de esta secuencia tienen un significado. Los dos últimos valores se pasan por alto.

### *Ejemplo de una configuración típica de terminal Visa-II*

Por ejemplo, los comandos siguientes configuran un perfil Connection para un terminal o emulador de terminal Visa:

```
admin> new conn visa-1
CONNECTION/visa-1 read
admin> set active = yes
admin> set encapsulation-protocol = visa2
admin> set sdtn-packets-server = yes
admin> set dial-number = 853784
admin> set calledNumber = 34343
admin> set telco dialout-allowed = yes
admin> set visa2 enabled = yes
admin> write
CONNECTION/visa-1 written
```

### *Prevención de retardos de ajuste para llamadas de transacciones por módem*

Cuando se inicia o se responde por módem a una llamada de transacción, la unidad TAOS debe preparar el módem antes de establecer la conexión. Para que los terminales de marcación para procesos de transacciones se conecten rápidamente con el mínimo ajuste del módem posible, puede establecer una cadena AT que especifique la temporización de módem requerida, los

tipos de modulación, la velocidad y otros parámetros del módem. Esta personalización ayuda a evitar retardos provocados por el ajuste del módem.

### *Ajuste para personalizar la cadena AT*

A continuación se muestra el parámetro correspondiente con el valor predeterminado:

```
[in CONNECTION/""]  
at-string = ""
```

Con el valor nulo predeterminado, el sistema realiza el ajuste del módem del modo habitual. El valor de este parámetro se puede establecer en comandos AT válidos de hasta 58 caracteres. No empiece la cadena con las letras AT. La secuencia AT se agrega de manera automática al principio de esta cadena antes de que se envíe al módem. Tampoco incluya ningún comando A (respuesta) ni D (marcación) en ningún punto de la cadena. Un comando A se agrega automáticamente al final de esta cadena para las llamadas de entrada, mientras que un comando D en la cadena de respuesta provocaría que la llamada fallase. Un comando D se agrega al final de la cadena especificada para las llamadas de salida.

**Nota:** Preste mucha atención al introducir comandos AT en este parámetro. El sistema no impide que se introduzcan cadenas incorrectas.

### *Ejemplo de cadena AT personalizada*

Los comandos siguientes configuran una conexión HDLC-NRM y definen la cadena AT para obligar al módem a responder como un módem de tipo Bell 212A:

```
admin> new conn hstation-1  
CONNECTION/hstation-1 read  
admin> set active = yes  
admin> set encapsulation-protocol = hdlc-nrm  
admin> set dial-number = 853784  
admin> set calledNumber = 3783  
admin> set telco dialout-allowed = yes  
admin> set hdlc enabled = yes  
admin> set at-string = B1+MS=69,1,1200,1200;  
admin> write  
CONNECTION/hstation-1 written
```

El ajuste de AT-String del ejemplo provoca que la cadena siguiente se envíe al módem, lo cual le obliga a responder como un módem de tipo Bell 212A en modo automático.

```
ATB1+MS=69,1,1200,1200;
```

# Métodos de autenticación

# A

Introducción . . . . .	A-1
Gestión de contraseñas RADIUS . . . . .	A-2
Autenticación de sesiones de protocolo entramado . . . . .	A-6
Autenticación de inicios de sesión de usuario . . . . .	A-22
Autenticación por tarjeta de testigo . . . . .	A-26
Autenticación de túnel . . . . .	A-34
Autenticación previa (CLID o DNIS) . . . . .	A-36
Devolución de llamada . . . . .	A-44

## Introducción

La autenticación es la primera línea de defensa frente al acceso no autorizado a su red. Esta función utiliza un intercambio de información para verificar la identidad de un usuario. La información suele estar cifrada en ambos extremos.

Cuando determine el tipo de autenticación que se va a utilizar, debe tener en cuenta si la llamada se efectúa entre dos máquinas o entre un ser humano y una máquina y, a continuación, decidir cómo debe ser de estricto el mecanismo de autenticación.

Por ejemplo, si la conexión se negocia entre dos máquinas, debe considerar si la otra ubicación es fiable, si la máquina protege sus propias redes frente a ataques de seguridad y si es físicamente accesible para varios usuarios.

Si la conexión se negocia con un usuario que debe escribir un testigo o una contraseña, debe considerar cuán segura es la contraseña y con qué frecuencia desea que cambie. Una vez autenticada la conexión de un usuario, puede utilizar restricciones de autorización para impedir que el emisor acceda a sistemas o redes que desea proteger. Para obtener información detallada acerca de las opciones de autorización, consulte el Apéndice B, “Opciones de autorización”.

## Autenticación de contraseña para sesiones de protocolo entramado

Para las sesiones de protocolo entramado, el proceso de autenticación se realiza normalmente mediante protocolos de acceso como el Protocolo de autenticación de contraseñas (PAP), el Protocolo de autenticación de establecimiento de enlace con desafío (CHAP) o la extensión de CHAP de Microsoft (MS-CHAP). Todos los protocolos de autenticación disponibles, excepto

PAP, incluyen el cifrado de contraseñas. El cifrado de contraseñas protege frente a ataques pasivos, en los que un usuario no autorizado controla información que se está transmitiendo con la intención de utilizarla para establecer lo que parece ser una sesión válida.

## **Autenticación de inicios de sesión en el servidor de terminales**

Para los inicios de sesión, en los que los usuarios realizan una llamada de entrada al software de servidor de terminales para acceder a los hosts locales, los administradores suelen configurar secuencias de comandos Expect-Send para automatizar el proceso de petición y recepción de un nombre y una contraseña. Para los inicios de sesión autenticados en RADIUS, puede hacer uso de la caducidad de contraseña como medida para reforzar la seguridad.

## **Autenticación de contraseña por tarjeta de testigo**

La autenticación de contraseña más segura utiliza tarjetas de testigo para contrarrestar las limitaciones de las contraseñas estáticas. Las tarjetas de testigo protegen frente a ataques pasivos y ataques de repetición, en los que un usuario no autorizado graba información válida de autenticación intercambiada entre sistemas y, posteriormente, la repite para obtener acceso. Como las tarjetas de testigo proporcionan contraseñas de un solo uso, éstas cambian muchas veces al día, con lo que la repetición resulta imposible.

## **Autenticación previa mediante información de llamada**

El ID de línea de llamada (CLID) y el Servicio de información de número de marcación (DNIS) son elementos informativos que pueden proporcionarse como parte de la llamada mediante el conmutador telco. Puede utilizar estos elementos para verificar el número desde el que se llama y el número marcado, respectivamente, antes de que la unidad TAOS responda a la llamada.

## **Utilización de la devolución de llamada como refuerzo de la seguridad**

Una vez concluida la autenticación, la unidad TAOS puede colgar y devolver la llamada, con lo que se garantiza que la conexión se realice sólo con un número fiable.

## ***Gestión de contraseñas RADIUS***

Las entradas de usuario RADIUS constan de tres partes:

```
User-Name Check-Items  
          Reply-Items
```

User-Name debe estar justificado a la izquierda. Normalmente es el nombre del emisor (o dispositivo llamador), pero puede ser también un número de teléfono (para la autenticación CLID o DNIS), una cadena especial que indique un perfil de pseudousuario o la cadena DEFAULT (para el perfil de usuario predeterminado).

Check-Items debe estar en la misma línea que User-Name y debe estar separado de éste por un espacio en blanco (espacio o tabulación). Check-Items incluye cero o más pares atributo-valor que deben coincidir con los atributos presentes en el paquete Access-Request para la

autenticación del usuario. En Check-Items se incluye habitualmente la contraseña para la entrada.

Reply-Items debe estar sangrado y separado de User-Name y Check-Items por un salto de línea (si Reply-Items no está sangrado, se interpreta como User-Name de una nueva entrada). Reply-Items incluye ninguno o varios pares atributo-valor que se devuelven en mensajes Access-Accept con el fin de autorizar servicios para el usuario.

## Contraseñas RADIUS reservadas

Los servidores RADIUS pueden reservar determinados valores del atributo Password (2) para usos específicos. Por ejemplo, algunos servidores interpretan la contraseña UNIX como una instrucción para utilizar la autenticación UNIX para el perfil. Algunos servidores RADIUS utilizan las contraseñas ACE y SAFEWORD para solicitar validación desde un servidor Security Dynamics ACE/Server y un servidor Enigma Logic SafeWord, respectivamente (consulte “Autenticación por tarjeta de testigo” en la página A-26).

La unidad TAOS reserva los valores siguientes para el atributo Password (2):

Valores de Password	Descripción
Ascend	Utilizado para perfiles de pseudousuario y otros perfiles del sistema. Cuando se utiliza esta contraseña, el atributo Service-Type debe especificar siempre Outbound-User, a fin de evitar que los emisores accedan a la red mediante una contraseña conocida. <i>Aunque el sistema no rechaza un perfil que no incluya el ajuste Outbound-User, su omisión supone un riesgo grave para la seguridad.</i>
Ascend-CLID o Ascend-DNIS	Especifican la utilización de información CLID o DNIS, respectivamente, para autenticar llamadas previamente. Cuando se utiliza una de estas contraseñas, el atributo Service-Type debe especificar siempre Outbound-User, a fin de evitar que los emisores accedan a la red mediante una contraseña conocida. <i>Aunque el sistema no rechaza un perfil que no incluya el ajuste Outbound-User, su omisión supone un riesgo grave para la seguridad.</i>

## Caducidad de la contraseña

Muchos servidores RADIUS dan soporte a las funciones de caducidad y antigüedad de las contraseñas y proporcionan un método para que los usuarios que realizan una llamada de entrada en el servidor de terminales puedan reemplazar las contraseñas caducadas. La función de caducidad de contraseñas no funciona para las contraseñas que no están almacenadas en la base de datos RADIUS (contraseñas autenticadas en UNIX o contraseñas de tarjeta de testigo) ni para las contraseñas reservadas (como Ascend).

La unidad TAOS utiliza los pares atributo-valor siguientes para permitir la función de caducidad y antigüedad de las contraseñas:

Atributo	Valor
Ascend-PW-Expiration (21)	Fecha de caducidad de la contraseña del usuario (una fecha consistente en una especificación de día, mes y año). El valor puede actualizarse automáticamente cuando un usuario renueva una contraseña. Debe ser un elemento de verificación.
Ascend-PW-Lifetime (208)	Número de días durante los que una contraseña puede ser válida (número entero de 0 a 65535). El valor predeterminado 0 (cero) desactiva la caducidad de la contraseña. Si el atributo tiene un valor que no sea cero, cuando el usuario cambie la contraseña la unidad TAOS agrega el valor a la fecha actual y actualiza la fecha de Ascend-PW-Expiration. Esta rutina proporciona un método para especificar nuevas fechas de caducidad de forma automática en lugar de codificar explícitamente una fecha.
Ascend-PW-Warntime (207)	Número de días antes de la fecha de caducidad en los que se advertirá al usuario de que la contraseña está a punto de caducar (número entero de 0 a 65535).

A continuación se muestra un ejemplo de perfil cuya contraseña caduca el 1 de enero de 1999:

```
brian Password = "localpw", Ascend-PW-Expiration = "Jan. 1, 1999"
    Ascend-PW-Lifetime = 30,
    Ascend-PW-Warntime = 2,
    ...
```

Un usuario que realice una llamada de entrada el 30 de diciembre de 1998 recibirá un mensaje en que se le indica que su contraseña caducará en dos días. Si el usuario cambia la contraseña en ese momento (mediante el comando Password del servidor de terminales), el servidor RADIUS actualiza la contraseña, agrega 30 días a la fecha actual y actualiza la fecha de Ascend-PW-Expiration a 29 de enero de 1999.

Un usuario que realice una llamada de entrada el 1 de enero de 1999 recibirá un mensaje en que se le indica que su contraseña ha caducado y se le solicita que introduzca la contraseña caducada y una nueva contraseña. El sistema solicita dos veces la nueva contraseña a fin de verificar la entrada. Si el usuario introduce la información incorrectamente, el sistema muestra otro indicador y el usuario puede intentarlo de nuevo un total de tres veces.

Si la actualización se realiza correctamente, el sistema envía la nueva contraseña al servidor RADIUS y muestra el mensaje siguiente, seguido inmediatamente del indicador del servidor de terminales:

```
Password Updated
ascend%
```

Si la actualización falla por el motivo que sea, aparece el mensaje siguiente:

```
Password NOT Changed
```

No hay ninguna indicación del motivo del fallo del cambio de contraseña. El servidor RADIUS puede rechazar el cambio de contraseña por cualquiera de los motivos siguientes:

- El sistema de archivos que contiene el archivo `users` de RADIUS está lleno.
- El archivo `users` de RADIUS está protegido frente a escritura.
- La contraseña del usuario está almacenada en UNIX.

## El perfil de usuario DEFAULT

Puede colocarse un perfil de usuario especial denominado `DEFAULT` al final del archivo `users` para especificar cómo se debe proceder con los usuarios que no tienen un perfil en el archivo `users`. Sólo se permite una entrada `DEFAULT` y debe ser la última entrada del archivo. Por ejemplo, la entrada siguiente permite a los usuarios del servidor de terminales iniciar una sesión con su contraseña y nombre de cuenta UNIX:

```
DEFAULT Password = "UNIX"  
Service-Type = Login-User,  
Login-Service = Telnet
```

## Secretos compartidos e intercambios seguros

Los secretos compartidos se utilizan para autenticar paquetes intercambiados entre la unidad TAOS y el servidor RADIUS, así como para cifrar contraseñas de emisores de entrada antes de enviarlas por la red local. Un secreto compartido es un valor individual conocido en ambos sistemas.

En el servidor RADIUS, los secretos compartidos se especifican en el archivo `clients`. Por ejemplo, para un sistema denominado `TAOS-01`, la entrada siguiente en el archivo `clients` especifica un secreto compartido de `nas-secret`:

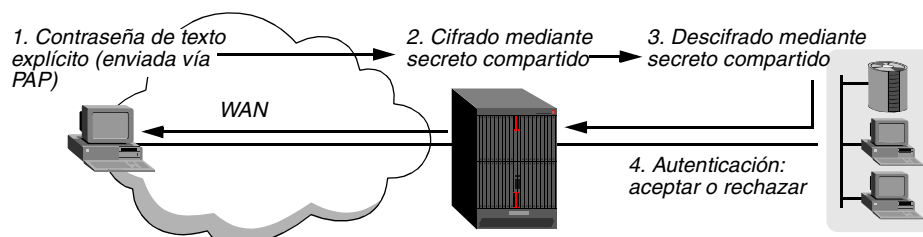
```
TAOS-01 nas-secret
```

La unidad TAOS especifica la misma cadena de secreto compartido como valor del parámetro `Auth-Key` en el perfil `External-Auth`. Por ejemplo:

```
admin> read external-auth  
EXTERNAL-AUTH read  
  
admin> set rad-auth-client auth-key = nas-secret  
  
admin> write  
EXTERNAL-AUTH written
```

En la Figura A-1 se muestra un ejemplo básico de cómo se gestionan las contraseñas presentadas por llamadas de entrada entre los sistemas.

Figura A-1. Secreto compartido utilizado entre la unidad TAOS y un servidor RADIUS



La unidad TAOS utiliza el secreto compartido para cifrar la contraseña de la llamada de entrada antes de que la unidad envíe la contraseña por la red local a un servidor RADIUS. El cifrado utiliza el secreto compartido, el campo Authenticator y un método de codificación, como MD5, CHAP o DES.

Para las llamadas de salida, el servidor RADIUS envía la contraseña de extremo distante al servidor de acceso de red (NAS). El servidor RADIUS debe cifrar las contraseñas antes de enviarlas a NAS si el perfil de llamada de salida utiliza el atributo Ascend-Send-Secret (214) para especificar la contraseña. Si el perfil especifica Ascend-Send-Secret y el servidor RADIUS no cifra la contraseña, la autenticación fallará.

En cambio, si el perfil de llamada de salida utiliza el atributo Ascend-Send-Passwd (232) para especificar la contraseña, el servidor RADIUS no realiza ningún cifrado antes de enviar la contraseña a NAS. Este ajuste puede ser necesario si se utiliza un servidor RADIUS que no permite el cifrado de contraseñas de salida.

A menos que se utilice un servidor RADIUS que no permita Ascend-Send-Secret, se recomienda su utilización en lugar de Ascend-Send-Passwd como protección frente a programas de exploración de paquetes locales que detectan contraseñas de llamada de salida.

## Autenticación de sesiones de protocolo entramado

Durante el establecimiento de un enlace de datos PPP, las unidades de marcación y respuesta utilizan paquetes de protocolo de control de enlaces (LCP) para negociar el protocolo de autenticación. Una vez concluidas las negociaciones LCP, la unidad TAOS utiliza el protocolo de autenticación acordado para autenticar al usuario. A continuación, negocia el protocolo de control de redes (NCP) de capa superior para configurar los protocolos de capa de red del enlace.

Si el enlace está configurado de forma que requiere autenticación, las unidades de ambos extremos del enlace negocian un protocolo de autenticación. La unidad de respuesta siempre determina el método de autenticación que se debe utilizar para la llamada. Una conexión multienlaces empieza con la autenticación de un canal base, y los canales subsiguientes se autentican por separado al agregarse a la llamada.

## Especificación de un protocolo de autenticación obligatorio para llamadas de entrada

Para especificar un protocolo de autenticación como obligatorio para la autenticación de nombre y contraseña de las sesiones entramadas, debe establecer el parámetro siguiente (que aparece con el ajuste predeterminado):

```
[in ANSWER-DEFAULTS:ppp-answer]
receive-auth-mode = no-ppp-auth
```

Parámetro	Especifica
Receive-Auth-Mode	Protocolo de autenticación obligatorio para la autenticación de llamadas de entrada. Los valores válidos son No-PPP-Auth (el valor predeterminado), PAP-PPP-Auth, CHAP-PPP-Auth, MS-CHAP-PPP-Auth y Any-PPP-Auth.



El parámetro Receive-Auth-Mode normalmente especifica un ajuste general para permitir el rango más amplio de protocolos de autenticación. Por ejemplo:

```
admin> read answer
ANSWER-DEFAULTS read

admin> set ppp receive-auth-mode = any-ppp-auth

admin> write
ANSWER-DEFAULTS written
```

Si establece este parámetro en un valor distinto al predeterminado No-PPP-Auth, la unidad TAOS utiliza LCP para solicitar determinadas opciones de autenticación y el emisor debe aceptar una de las opciones que le ofrece el sistema. Con el ajuste predeterminado, la unidad TAOS no solicita autenticación alguna.

PAP-PPP-Auth especifica el Protocolo de autenticación de contraseñas (PAP), que proporciona un método sencillo para que la unidad TAOS establezca su identidad en un establecimiento de enlace bidireccional. El dispositivo remoto debe permitir PAP.

CHAP-PPP-Auth especifica el Protocolo de autenticación de establecimiento de enlace con desafío (CHAP), que es más seguro que PAP. Mientras la unidad TAOS utiliza CHAP para autenticar el dispositivo remoto, el sistema puede verificar periódicamente la identidad del dispositivo remoto mediante un cifrado y un establecimiento de enlace tridireccional. El dispositivo remoto debe permitir CHAP.

MS-CHAP-PPP-Auth especifica la extensión de CHAP de Microsoft, que utiliza el cifrado DES y MD4. Lo utilizan principalmente los sistemas Windows NT y LAN Manager.

Any-PPP-Auth especifica que se acepta cualquier protocolo de autenticación. La unidad TAOS acepta llamadas PPP de entrada que admiten cualquiera de los métodos de autenticación, pero descarta las conexiones que no aceptan ningún protocolo de autenticación durante la negociación LCP.

## Especificación de un protocolo de autenticación mediante RADIUS

También puede utilizar el atributo específico del proveedor (VSA) Ascend-Auth-Type (81) en un perfil de usuario RADIUS para especificar el tipo de autenticación PPP que se debe utilizar, con lo que se anula la especificación de Answer-Defaults.

Algunos clientes y proveedores que compran el acceso a un ISP desean utilizar la autenticación CHAP para las llamadas PPP, mientras que otros clientes desean utilizar PAP. En la mayoría de los casos, la puesta de ambas autenticaciones (PAP y CHAP) a disposición de los clientes no presenta ningún problema. Sin embargo, los usuarios que utilizan Microsoft Windows 95, Windows 98 o Windows NT no pueden configurar sus unidades para que rechacen CHAP. Si Receive-Auth-Mode tiene el valor `any-ppp-auth`, la unidad TAOS ofrece la autenticación CHAP antes que el PAP. Por lo tanto, los clientes de Windows siempre utilizan CHAP. En esta versión, puede configurar RADIUS para que seleccione otro tipo de autenticación PPP.

El atributo Ascend-Auth-Type se devuelve como parte de la autorización resultante de la autenticación DNIS o CLID de primer nivel. Si especifica un valor para Ascend-Auth-Type, éste anula la especificación Receive-Auth-Mode del perfil Answer-Defaults.

Atributo	Valor
Ascend-Auth-Type (81)	<p>Especifica el tipo de autenticación PPP que utiliza la conexión durante la autenticación CLID o DNIS de primer nivel.</p> <p>Especifique uno de los valores siguientes:</p> <ul style="list-style-type: none"><li>• Auth-None (0): La autenticación de nombre y contraseña de segundo nivel no es obligatoria. La especificación de este valor tiene el mismo efecto que el establecimiento de Ascend-Require-Auth en Not-Require-Auth.</li><li>• Auth-Default (1): La conexión utiliza el ajuste Receive-Auth-Mode.</li><li>• Auth-Any (2): La conexión debe utilizar PAP, CHAP o MS-CHAP.</li><li>• Auth-PAP (3): La conexión debe utilizar PAP. El extremo remoto envía su contraseña como texto explícito. La contraseña no está cifrada.</li><li>• Auth-CHAP (4): La conexión debe utilizar CHAP. El extremo remoto no envía su contraseña como texto explícito. En su lugar, se envían un desafío aleatorio y una síntesis MD5 (algoritmo de síntesis de mensajes 5) calculada a partir de la contraseña.</li><li>• Auth-MS-CHAP (5): La conexión debe utilizar MS-CHAP.</li></ul>

Si los valores que se transmiten de RADIUS a la unidad TAOS no son los que se acaban de describir, entonces la unidad TAOS utiliza el perfil predeterminado Answer-Defaults o el valor predeterminado de fábrica.

## Funcionamiento de PAP

PAP es un método de establecimiento de enlace bidireccional para establecer la identidad de un emisor. Utilizado una vez, durante el establecimiento inicial del enlace de datos, no resulta un método de autenticación muy potente. Las contraseñas se envían como texto sin formato en la WAN, de modo que cualquier curioso con el equipo y el software adecuados puede detectar y reutilizar contraseñas correctas.

La autenticación PAP se utiliza generalmente porque el método o base de datos de contraseñas disponibles lo precisa. Por ejemplo, si se utiliza el archivo de contraseñas UNIX para la autenticación (vía RADIUS), la unidad TAOS fuerza al homólogo a utilizar PAP.

Si se utiliza PAP con la autenticación RADIUS, la unidad TAOS hace uso del secreto compartido para cifrar la contraseña de texto que recibe del emisor antes de enviar la contraseña al servidor a través de la red. El servidor RADIUS utiliza el mismo secreto

compartido para descifrar la contraseña antes de efectuar la autenticación o transmitirla a otro servidor de autenticación, como un host UNIX o un servidor de tarjeta de testigo.

## Funcionamiento de CHAP y MS-CHAP

La autenticación CHAP verifica la identidad del emisor empleando un enlace tridireccional al establecerse inicialmente el enlace y, posiblemente, repitiendo el establecimiento de enlace cualquier número de veces. El autenticador envía un desafío al emisor, que responde con una síntesis MD5 calculada a partir de la contraseña. A continuación, el autenticador compara la síntesis con su propio cálculo del valor hash previsto a fin de autenticar la llamada. Puede enviarse un nuevo desafío a intervalos aleatorios.

CHAP es un método de autenticación más potente que PAP, ya que la contraseña no se envía como texto sin formato. Además, la utilización de desafíos repetidos limita el tiempo de exposición a cualquier intento individual de desglosar el código de cifrado, y el autenticador controla cuándo y con qué frecuencia se envían los desafíos.

Microsoft CHAP (MS-CHAP) es un derivado de CHAP muy parecido a éste. Sin embargo, CHAP está designado para autenticar el software seguro con soporte para WAN. Su utilización para dar soporte a las estaciones de trabajo remotas no está muy extendida. Dicha utilización puede requerir un inicio de sesión mediante texto sin formato poco seguro. MS-CHAP resuelve este problema y, además, integra los algoritmos de cifrado y hash utilizados en las redes Windows. Las plataformas Microsoft Windows NT y LAN Manager utilizan MS-CHAP.

La autenticación MS-CHAP se permite en perfiles Connection locales o en perfiles RADIUS. La versión actual del software proporciona una clave para el cifrado DES de contraseñas cuando se utiliza la autenticación MS-CHAP. No se requiere ningún parámetro en los perfiles locales.

Cuando se utiliza CHAP o MS-CHAP con la autenticación RADIUS, se producen los eventos siguientes:

- 1 La unidad TAOS envía un desafío aleatorio de 128 bits a la unidad que realiza la llamada.
- 2 Esta unidad calcula una síntesis MD5 utilizando su contraseña, el desafío y el ID de paquete PPP.
- 3 La unidad que realiza la llamada envía la síntesis MD5, el desafío y el ID de paquete PPP (pero no la contraseña) a la unidad TAOS. La unidad TAOS nunca obtiene la contraseña del emisor.
- 4 La unidad TAOS envía la síntesis, junto con el desafío original y el ID de paquete PPP, al servidor RADIUS. No es necesario realizar ningún cifrado, puesto que MD5 crea un código monodireccional que no puede descodificarse.
- 5 El servidor RADIUS busca la contraseña del emisor en una base de datos local y calcula una síntesis MD5 basada en la versión local del secreto, el desafío y el ID de paquete PPP remotos recibidos desde la unidad TAOS.
- 6 El servidor RADIUS compara la síntesis MD5 calculada con la síntesis recibida desde la unidad TAOS. Si las síntesis son iguales, las contraseñas coinciden y se acepta la llamada.

## Funcionamiento de la autenticación CHAP bidireccional

La autenticación CHAP bidireccional entre el dispositivo PPP que realiza la llamada y el dispositivo PPP al que se llama refuerza el cumplimiento de la norma RFC 1994 para la

autenticación CHAP de PPP. Tenga en cuenta que esta función no se aplica a la autenticación basada en PAP (PAP, PAP-TOKEN o PAP-TOKEN-CHAP).

**Nota:** Como se indica en el documento RFC 1994, puede producirse un fallo de seguridad al hacer uso de la autenticación bidireccional para una llamada de entrada si los secretos utilizados en ambas direcciones son idénticos. La autenticación bidireccional en TAOS ha sido desarrollada para evitar el fallo de seguridad, incluso en el caso de que los secretos sean idénticos. Sin embargo, para obtener unos resultados óptimos, Lucent recomienda especificar un secreto distinto para cada dirección de autenticación.

La autenticación CHAP bidireccional tiene soporte localmente y a través de RADIUS.

### Configuración de la autenticación CHAP bidireccional en una unidad TAOS

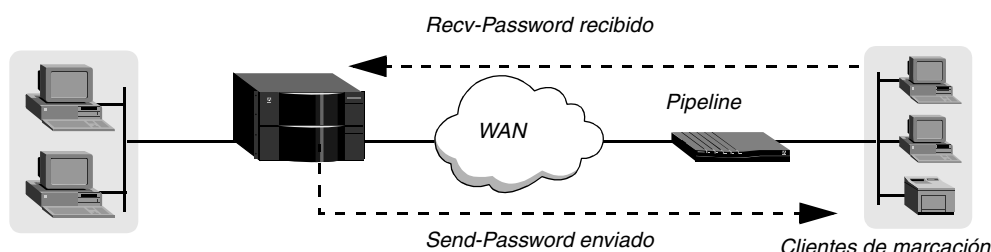
En las secciones siguientes se describe cómo se configura la autenticación CHAP bidireccional en perfiles locales. Puede elegir una o varias de las configuraciones siguientes:

- Configuración de la autenticación CHAP bidireccional para todas las llamadas de entrada
- Configuración de la autenticación CHAP bidireccional para llamadas de entrada seleccionadas
- Configuración de la autenticación CHAP bidireccional para las llamadas de salida

#### Configuración de la autenticación CHAP bidireccional para todas las llamadas de entrada

En la Figura A-2 se muestra una configuración en la que una unidad TAOS y sus clientes de llamada de entrada se autentican los unos a los otros mediante la autenticación CHAP bidireccional. Uno o varios clientes pueden realizar una marcación en la unidad TAOS. La unidad TAOS autentica cada dispositivo llamador mediante un perfil Connection y cada cliente de llamada de entrada autentica la unidad TAOS mediante el valor Send-Password.

Figura A-2. Autenticación CHAP bidireccional para todas las llamadas de entrada a la unidad TAOS



Para configurar la autenticación CHAP bidireccional en la unidad TAOS para todas las llamadas de entrada, proceda del modo siguiente:

- 1 Utilice Answer-Defaults como su perfil de trabajo.
- 2 Visualice el subperfil PPP-Answer.
- 3 Establezca Receive-Auth-Mode en `any-ppp-auth` o `chap-ppp-auth`.
- 4 Establezca Bi-Directional-Auth en `required` o `allowed`. Required especifica que debe efectuarse la autenticación bidireccional o, de lo contrario, se descarta la llamada. Allowed especifica que la autenticación *puede* ser bidireccional. La unidad TAOS

identifica el dispositivo que realiza la llamada, y este dispositivo puede identificar la unidad TAOS, pero esto último no es necesario para que se acepte la llamada.

- 5 Grabe el perfil Answer-Defaults.
- 6 Para cada llamada de entrada, cree o lea un perfil Connection y utilícelo como su perfil de trabajo.
- 7 Visualice el subperfil PPP-Options.
- 8 Especifique Send-Password mediante cualquier cadena de texto. La contraseña que especifique es la enviada a la unidad que realiza la llamada durante la autenticación iniciada por dicha unidad.
- 9 Especifique Recv-Password mediante cualquier cadena de texto. La contraseña que especifique es la enviada por la unidad que realiza la llamada durante la autenticación iniciada por la unidad TAOS.
- 10 Grabe el perfil Connection.

**Nota:** Si el parámetro Receive-Auth-Mode tiene el valor `any-ppp-auth`, la unidad TAOS puede aceptar tanto la autenticación PAP como la autenticación CHAP. El ajuste Bi-Directional-Auth sólo se utiliza si se ha negociado una forma de autenticación CHAP durante la negociación del protocolo de control de enlaces (LCP). Si se ha negociado alguna forma de autenticación PAP y Bi-Directional-Auth tiene el valor `required`, la unidad TAOS autentica la unidad que realiza la llamada y la autenticación tiene lugar en una única dirección.

A continuación se muestra un ejemplo de configuración:

```
admin> read answer-defaults
ANSWER-DEFAULTS read

admin> set ppp-answer receive-auth-mode = chap-ppp-auth
admin> set ppp-answer bidirectional-auth = required
admin> write
ANSWER-DEFAULTS written

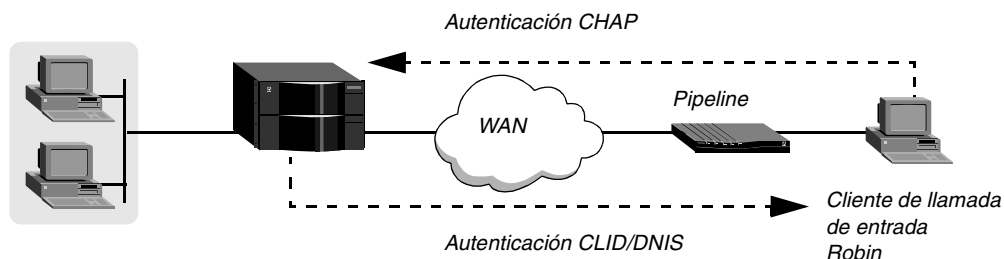
admin> read connection robin
CONNECTION/robin read

admin> set ppp-options send-password = sendpw
admin> set ppp-options recv-password = recvpw
admin> write
CONNECTION/robin written
```

### *Configuración de la autenticación CHAP bidireccional para llamadas de entrada seleccionadas*

En la Figura A-3 se muestra una configuración en la que la unidad TAOS autentica el dispositivo que realiza la llamada mediante la autenticación CLID (ID de línea de llamada) o DNIS (Servicio de información de número de marcación). A continuación, el cliente de llamada de entrada y la unidad TAOS se autentican el uno al otro mediante CHAP.

Figura A-3. Autenticación CHAP bidireccional para llamadas seleccionadas



Para configurar la autenticación CHAP bidireccional en la unidad TAOS para llamadas de entrada seleccionadas, proceda del modo siguiente:

- 1 Utilice Answer-Defaults como su perfil de trabajo.
- 2 Establezca Profiles-Required en yes.
- 3 Establezca CLID-Auth-Mode en `clid-require`, `clid-prefer`, `dnis-require` o `dnis-prefer`.
- 4 Visualice el subperfil PPP-Answer.
- 5 Establezca Bi-Directional-Auth en `none` o `allowed`.
- 6 Grabe el perfil Answer-Defaults.
- 7 Seleccione o cree el perfil Connection para el que desea configurar la autenticación CHAP bidireccional y utilícelo como su perfil de trabajo.
- 8 Si CLID-Auth-Mode está establecido en `clid-require` o `clid-prefer`, establezca el valor CLID en CLID.
- 9 Si CLID-Auth-Mode está establecido en `dnis-require` o `dnis-prefer`, establezca el valor CalledNumber en el número que marca el emisor de la llamada.
- 10 Visualice el subperfil PPP-Options.
- 11 Especifique Send-Password mediante cualquier cadena de texto. La contraseña que especifique es la enviada a la unidad que realiza la llamada durante la autenticación iniciada por dicha unidad.
- 12 Especifique Recv-Password mediante cualquier cadena de texto. La contraseña que especifique es la enviada por la unidad que realiza la llamada durante la autenticación iniciada por la unidad TAOS.
- 13 Establezca Send-Auth-Mode en `chap-ppp-auth`. Este valor indica el modo para la autenticación de las llamadas de entrada y de salida.
- 14 Establezca Bi-Directional-Auth en `required` o `allowed`. Required especifica que debe efectuarse la autenticación bidireccional o, de lo contrario, se descarta la llamada. Allowed especifica que la autenticación *puede* ser bidireccional. La unidad TAOS identifica el dispositivo que realiza la llamada, y este dispositivo puede identificar la unidad TAOS, pero esto último no es necesario para que se acepte la llamada.
- 15 Grabe el perfil Connection.

A continuación se muestra un ejemplo de configuración:

```
admin> read answer-defaults
ANSWER-DEFAULTS read
admin> set profiles-required = yes
admin> set clid-auth-mode = clid-require
```

```
admin> set ppp-answer bidirectional-auth = allowed
admin> write
ANSWER-DEFAULTS written
admin> read connection robin
CONNECTION/robin read
admin> set clid = 1234567
admin> set ppp-options send-password = "passin"
admin> set ppp-options recv-password = "passout"
admin> set ppp-options send-auth-mode = chap-ppp-auth
admin> set ppp-options bi-directional-auth = allowed
admin> write
CONNECTION/robin written
```

### *Configuración de la autenticación CHAP bidireccional para las llamadas de salida*

Para configurar la autenticación CHAP bidireccional para llamadas de salida en la unidad TAOS, proceda del modo siguiente:

- 1 Utilice el perfil Connection como su perfil de trabajo.
- 2 Visualice el subperfil PPP-Options.
- 3 Establezca Send-Auth-Mode en chap-ppp-auth, cache-token-ppp-auth o ms-chap-ppp-auth. Si especifica otra modalidad de autenticación, no se llevará a cabo la autenticación bidireccional, aunque Bi-Directional-Auth esté establecido en allowed o required.
- 4 Establezca Bi-Directional-Auth en required o allowed. Required especifica que debe efectuarse la autenticación bidireccional o, de lo contrario, se descarta la llamada. Allowed especifica que la autenticación *puede* ser bidireccional. La unidad TAOS identifica el dispositivo al que se llama si éste acepta la autenticación y dicho dispositivo puede identificar la unidad TAOS, pero no es necesario para que se acepte la llamada.
- 5 Defina Send-Password con una cadena texto que especifique la contraseña enviada al dispositivo al que se llama durante la autenticación iniciada por la unidad TAOS.
- 6 Defina Recv-Password con una cadena de texto que especifique la contraseña enviada por la unidad a la que se llama durante la autenticación iniciada por dicha unidad.
- 7 Especifique Substitute-Recv-Name mediante una cadena de texto. Se compara el nombre del receptor de la llamada con el valor que se especifique. Si el nombre del receptor de la llamada es diferente, no se establece la llamada. Si no se especifica un valor para Substitute-Recv-Name, se compara el nombre del receptor de la llamada con el nombre del perfil de llamada de salida.
- 8 Grabe el perfil Connection.

A continuación se muestra un ejemplo de configuración:

```
admin> read connection robin
CONNECTION/robin read
admin> set ppp-options send-auth-mode = chap-ppp-auth
admin> set ppp-options bi-directional-auth = required
admin> set ppp-options send-password = sendpw
```

## Métodos de autenticación

### Autenticación de sesiones de protocolo entramado

---

```
admin> set ppp-options recv-password = recvpw
admin> set ppp-options substitute-recv-name = subname
admin> write
CONNECTION/robin written
```

Answer-Defaults > PPP-Answer, Connection > PPP-Options

Parámetro	Especifica
Bi-Directional-Auth	<p>Si la autenticación CHAP debe ser bidireccional. Especifique uno de los valores siguientes:</p> <ul style="list-style-type: none"><li>• None: La autenticación es unidireccional. El dispositivo al que se llama identifica al dispositivo que realiza la llamada. La unidad TAOS impide la autenticación en la que el emisor de la llamada identifica al receptor de la llamada. Es el valor predeterminado.</li><li>• Allowed: La autenticación puede ser bidireccional. Cuando la unidad TAOS es el dispositivo al que se llama, identifica al dispositivo que realiza la llamada. El sistema también permite al dispositivo que realiza la llamada autenticar la unidad TAOS, pero esta autenticación no es obligatoria. Por lo tanto, si el dispositivo que llama no autentica la unidad TAOS, la unidad TAOS aún puede aceptar la llamada. Cuando la unidad TAOS es el dispositivo que realiza la llamada, ésta responde a la autenticación iniciada por el dispositivo al que se llama. La unidad TAOS también intenta negociar la autenticación en la dirección opuesta, pero si el dispositivo al que se llama rechaza esta segunda opción de autenticación, aún se establece la llamada.</li><li>• Required: La autenticación debe ser bidireccional. La unidad TAOS requiere que tanto el dispositivo que realiza la llamada como el dispositivo al que se llama se autenticuen mutuamente. Si la autenticación no se efectúa en ambas direcciones, la unidad TAOS rechaza la llamada (en caso de una llamada de entrada) o desconecta la llamada (en caso de una llamada de salida).</li></ul>
Substitute-Recv-Name	<p>Nombre del dispositivo PPP al que se llama durante las llamadas de salida. Dado que la autenticación bidireccional proporciona una manera de autenticar formalmente el dispositivo al que se llama durante una llamada de salida, el nombre del dispositivo debe compararse con el nombre definido localmente. El nombre puede ser el nombre del perfil de llamada de salida o un nombre substituido. Especifique una cadena de un máximo de 23 caracteres. El valor predeterminado es dejarlo en blanco.</p>



## *Configuración de la autenticación CHAP bidireccional en RADIUS*

En las secciones siguientes se describe cómo se configura la autenticación CHAP bidireccional en RADIUS. Puede utilizar una de las configuraciones siguientes:

- Configuración de la autenticación CHAP bidireccional en RADIUS para las llamadas de entrada
- Configuración de la autenticación CHAP bidireccional en RADIUS para las llamadas de salida
- Configuración de la autenticación CHAP bidireccional selectiva con devolución de llamada
- Configuración de una llamada de salida con búsquedas RADIUS dobles

### *Configuración de la autenticación CHAP bidireccional en RADIUS para las llamadas de entrada*

Puede configurar la autenticación bidireccional selectiva utilizando la autenticación previa CLID o DNIS en un perfil de pseudousuario y, a continuación, especificar dos contraseñas en el perfil de usuario.

En el perfil de pseudousuario, especifique la autenticación CLID o DNIS y, a continuación, establezca el atributo Ascend-Bi-Directional-Auth en Bi-Directional-Auth-Allowed o Bi-Directional-Auth-Required:

- Bi-Directional-Auth-Allowed especifica que la autenticación puede ser bidireccional. La unidad TAOS identifica el dispositivo que realiza la llamada. El sistema también permite al dispositivo que realiza la llamada autenticar la unidad TAOS, pero esta autenticación no es obligatoria. Por lo tanto, si el dispositivo que llama no autentica la unidad TAOS, la unidad TAOS aún puede aceptar la llamada.
- Bi-Directional-Auth-Required especifica que la autenticación debe ser bidireccional.

En el perfil de pseudousuario siguiente, la autenticación bidireccional es obligatoria:

```
111886067 Password = "Ascend-CLID"  
Service-Type = Framed,  
Ascend-Require-Auth = Require-Auth,  
Ascend-Auth-Type = Auth-CHAP,  
Ascend-Send-Auth = Send-Auth-CHAP,  
Ascend-Bi-Directional-Auth = Bi-Directional-Auth-Required
```

En el perfil de usuario, Ascend-Send-Secret se establece en la contraseña enviada al dispositivo al que se llama durante la autenticación iniciada por la unidad TAOS:

```
Mikel Password = "passin"  
Service-Type = Framed,  
Ascend-Send-Secret = "passout",  
Framed-Protocol = PPP  
Framed-IP-Address = 111.5.1.1  
Framed-IP-Netmask = 255.255.255.255  
Ascend-Data-Svc = Switched-64K  
Ascend-Route-IP = Route-IP-Yes
```

Tenga en cuenta que el perfil Answer-Defaults debe contener la modalidad de autenticación bidireccional deseada (*none*, *required* o *allowed*) si no se utiliza la autenticación previa CLID o DNIS. El perfil de pseudousuario puede suprimirse (no utilizarse) y el perfil de usuario debe contener el atributo Ascend-Bi-Directional-Auth.

### *Configuración de la autenticación CHAP bidireccional en RADIUS para las llamadas de salida*

Para configurar un perfil RADIUS de llamada de salida que utilice la autenticación bidireccional, proceda del modo siguiente:

- 1 Configure User-Name con el nombre del receptor de la llamada y especifique la contraseña *ascend*.
- 2 Establezca Ascend-Send-Auth en *send-auth-chap*.
- 3 Configure Ascend-Send-Secret con el texto del secreto enviado al dispositivo al que se llama.
- 4 Configure Ascend-Receive Secret con el texto del secreto recibido del dispositivo al que se llama.
- 5 Establezca Ascend-Bi-Directional-Auth en *bi-directional-auth-allowed* o *bi-directional-auth-required*.
- 6 Configure Ascend-Recv-Name con el nombre del receptor de la llamada.

Por ejemplo:

```
Mikel-out Password = "ascend"
    Service-Type = Outbound,
    User-Name = "Mikel",
    Framed-Protocol = PPP,
    Framed-IP-Address = 111.5.1.1,
    Framed-IP-Netmask = 255.255.255.0,
    Ascend-Dial-Number = 90492386067,
    Ascend-Data-Svc = Switched-64K,
    Ascend-Send-Auth = Send-Auth-CHAP,
    Ascend-Send-Secret = "passout",
    Ascend-Receive-Secret = "passin",
    Ascend-Bi-Directional-Auth = Bi-Directional-Auth-Required,
    Ascend-Route-IP = 1

route-tnt-pat-1 Password = "ascend"
    Service-Type = Outbound,
    Framed-Route = "111.5.1.0/30 111.5.1.1 1 n Mikel-out"
```

### *Configuración de la autenticación CHAP bidireccional selectiva con devolución de llamada*

Para configurar la autenticación CHAP bidireccional con devolución de llamada, debe efectuar los pasos siguientes:

- Crear un perfil de pseudousuario de primer nivel.
- Crear un perfil de usuario de segundo nivel.

En el perfil de pseudousuario de primer nivel, proceda del modo siguiente:

- 1 Configure User-Name con el nombre del receptor de la llamada y especifique la contraseña ascend.
- 2 Establezca Ascend-Require-Auth en require-auth.
- 3 Establezca Ascend-Send-Auth en send-auth-chap.
- 4 Establezca Ascend-Bi-Directional-Auth en bi-directional-auth-allowed o bi-directional-auth-required.

Para una devolución de llamada CHAP bidireccional global, no se utiliza el perfil de pseudousuario de primer nivel. En el perfil de usuario de segundo nivel, proceda del modo siguiente:

- 1 Establezca Ascend-Send-Auth en send-auth-chap.
- 2 Establezca Ascend-Bi-Directional-Auth en bi-directional-auth-allowed o bi-directional-auth-required.
- 3 Establezca Ascend-Callback en callback-yes.

En el ejemplo siguiente se muestra la configuración necesaria para una devolución de llamada. En el perfil de pseudousuario de primer nivel, la autenticación bidireccional se determina de forma selectiva durante la autenticación previa DNIS y el sistema efectúa la autenticación bidireccional para las llamadas de entrada y de salida. El perfil de usuario de segundo nivel está configurado para la autenticación CHAP bidireccional con devolución de llamada.

```
8940 Password = "Ascend-DNIS"
    Service-Type = Outbound,
    Ascend-Require-Auth = Require-Auth,
    Ascend-Auth-Type = Auth-CHAP,
    Ascend-Send-Auth = Send-Auth-CHAP,
    Ascend-Bi-Directional-Auth = Bi-Directional-Auth-Required

Mikel_cb Password = "passin"
    Service-Type = Framed,
    Ascend-Send-Secret = "pass",
    Framed-Protocol = MP,
    Ascend-Base-Channel-Count = 2,
    Ascend-Minimum-Channels = 1,
    Ascend-Maximum-Channels = 2,
    Framed-IP-Address = 111.5.1.1,
    Framed-IP-Netmask = 255.255.255.255,
    Ascend-Dial-Number = 90492386067,
    Ascend-Data-Svc = Switched-64K,
    Ascend-Send-Auth = Send-Auth-CHAP,
    Ascend-Bi-Directional-Auth = Bi-Directional-Auth-Required,
    Ascend-Callback = Callback-Yes,
    Ascend-Callback-Delay = 10,
    Ascend-Route-IP = 1
```

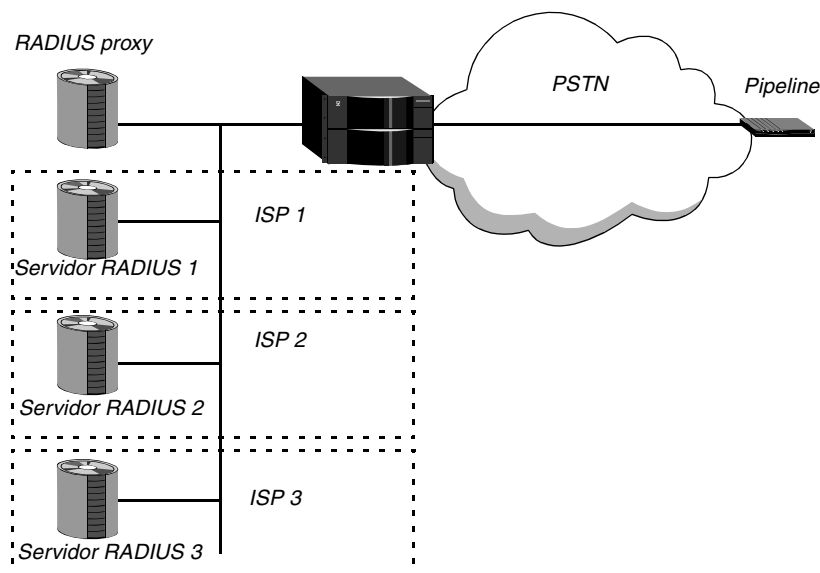
#### *Configuración de una llamada de salida con búsquedas RADIUS dobles*

En esta sección se analiza lo siguiente:

- Las circunstancias en las que se pueden utilizar búsquedas RADIUS dobles
- El procedimiento para configurar búsquedas RADIUS
- La secuencia de mensajes durante las búsquedas RADIUS

En redes grandes, varios ISP pueden estar alojados en una misma red física, como la que se muestra en la Figura A-4. Normalmente cada ISP posee su propio servidor RADIUS, mientras que el proveedor de la red utiliza un servidor RADIUS proxy. La unidad TAOS sólo interactúa con el servidor RADIUS proxy. El servidor proxy puede responder a algunas peticiones localmente y enviar otras peticiones al servidor RADIUS de un ISP. Normalmente un ISP requiere que todos los usuarios sean autenticados por su propio servidor RADIUS, y no por el equipo del proveedor de la red.

*Figura A-4. Autenticación CHAP bidireccional en una red de varios proveedores*



Durante una llamada de salida con autenticación bidireccional, la unidad TAOS recupera en primer lugar el perfil de llamada de salida. Una vez establecida la llamada, la unidad TAOS debe autenticar el receptor de la llamada, en este caso una Pipeline. La decisión de autenticación debe tomarla el servidor RADIUS del ISP, lo que requiere una segunda búsqueda RADIUS.

Cuando se configuran búsquedas RADIUS dobles, el perfil de llamada de salida se divide en dos perfiles: el perfil de llamada de salida de primer nivel y el perfil de llamada de salida de segundo nivel. El perfil de llamada de salida contiene todos los parámetros de llamada de salida necesarios para establecer la llamada de salida y el perfil de usuario contiene información para autenticar el dispositivo al que se llama.

Observe el siguiente perfil de llamada de salida de primer nivel, configurado para la autenticación CHAP bidireccional:

```
pipe-pat-out Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = PPP,
    Framed-IP-Address = 10.4.8.8,
    Framed-IP-Netmask = 255.255.255.0,
    Ascend-Dial-Number = 90492386067,
    Ascend-Data-Svc = Switched-64K,
    Ascend-Send-Auth = Send-Auth-CHAP,
    Ascend-Send-Secret = "passin",
    Ascend-Bi-Directional-Auth = Bi-Directional-Auth-Required,
    Ascend-Recv-Name = "pipe-pat",
    Ascend-Route-IP = 1
```

Para realizar la segunda búsqueda RADIUS, el nombre del perfil de llamada de salida (en este ejemplo, pipe-pat-out) debe ser distinto del nombre del dispositivo al que se llama en el perfil de usuario. El atributo Ascend-Recv-Name especifica el nombre del dispositivo al que se llama, en este caso pipe-pat.

En el perfil de usuario de segundo nivel siguiente, el nombre del receptor de la llamada es pipe-pat y la contraseña de recepción es pass.

```
pipe-pat Password = "pass"
    Service-Type = Framed
    Ascend-Route-IP = 1"
```

Puede desactivar la función de búsqueda RADIUS doble asignando al perfil de llamada de salida el nombre del homólogo y omitiendo el atributo Ascend-Recv-Name. Utilice el atributo User-Name para cambiar el nombre del perfil (en este caso por pipe-pat):

```
pipe-pat-out Password = "ascend"
    Service-Type = Outbound,
    User-Name = "pipe-pat",
    Framed-Protocol = PPP,
    Framed-IP-Address = 10.4.8.8,
    Framed-IP-Netmask = 255.255.255.0,
    Ascend-Dial-Number = 90492386067,
    Ascend-Data-Svc = Switched-64K,
    Ascend-Send-Auth = Send-Auth-CHAP,
    Ascend-Send-Secret = "passin",
    Ascend-Bi-Directional-Auth = Bi-Directional-Auth-Required,
    Ascend-Receive-Secret = "pass",
    Ascend-Route-IP = 1
```

Una llamada que utiliza dos búsquedas RADIUS pasa por la secuencia de mensajes siguiente:

- 1 La unidad TAOS solicita un perfil de llamada de salida de RADIUS.
- 2 RADIUS envía el perfil de llamada de salida a la unidad TAOS.
- 3 La unidad TAOS realiza una llamada ISDN al dispositivo remoto.
- 4 Se conecta la llamada ISDN.
- 5 La unidad TAOS y el receptor de la llamada realizan intercambios LCP.
- 6 El receptor de la llamada envía una petición de desafío a la unidad TAOS.
- 7 La unidad TAOS responde con una respuesta de desafío.

## Métodos de autenticación

### Autenticación de sesiones de protocolo entramado

---

- 8 El receptor de la llamada informa a la unidad TAOS sobre si el primer nivel de autenticación ha sido correcto o no.
- 9 Si la primera autenticación ha sido correcta, la unidad TAOS envía una petición de desafío al receptor de la llamada.
- 10 El receptor de la llamada responde con una respuesta de desafío.
- 11 La unidad TAOS envía la petición de autenticación a RADIUS, que efectúa una segunda búsqueda.
- 12 El servidor RADIUS informa a la unidad TAOS sobre si la autenticación ha sido correcta o no.
- 13 Si ha sido correcta, la unidad TAOS informa al receptor de la llamada de que ha sido autenticado.

RADIUS utiliza los pares atributo-valor siguientes para la configuración de la autenticación CHAP bidireccional. Para obtener información adicional acerca de estos atributos, consulte la publicación *Guía y referencia de TAOS RADIUS*.

Atributo	Valor
Ascend-Bi-Directional-Auth (46)	Especifica si la autenticación CHAP debe ser bidireccional.
Ascend-Recv-Name (45)	Nombre del dispositivo PPP al que se llama, que se compara con el nombre definido localmente. Puede ser el nombre del perfil de llamada de salida o un nombre substituido.

## Petición de un protocolo para utilizarlo en las llamadas de salida

Los perfiles Connection y los perfiles RADIUS de llamada de salida pueden especificar el protocolo de autenticación y la contraseña utilizada para enviar información de autenticación al extremo distante.

### Ajustes de los perfiles Connection

A continuación se muestran los parámetros del perfil Connection (que aparecen con los ajustes predeterminados) para solicitar un protocolo de autenticación en una llamada de salida:

```
[in CONNECTION/"":ppp-options]
send-auth-mode = no-ppp-auth
send-password = ""
```

Parámetro	Especifica
Send-Auth-Mode	Protocolo de autenticación solicitado para una llamada de salida. Con el ajuste predeterminado, no se negocia ninguna autenticación. Otros valores son PAP-PPP-Auth, No-PPP-Auth, CHAP-PPP-Auth, MS-CHAP-PPP-Auth y Any-PPP-Auth.
Send-Password	Contraseña que la unidad TAOS envía al extremo distante como parte del establecimiento de enlace inicial.

## *Ajustes de los perfiles RADIUS*

RADIUS utiliza los pares atributo-valor siguientes para solicitar un protocolo de autenticación en un perfil de llamada de salida.

<b>Atributo</b>	<b>Valor</b>
Ascend-Authen-Alias (203)	Nombre de inicio de sesión para la unidad TAOS, que debe enviarse como parte del proceso de autenticación de una llamada de salida. El ajuste predeterminado es el valor del parámetro Name en el perfil System.
Ascend-Send-Auth (231)	Protocolo de autenticación solicitado para una llamada de salida. Con el valor predeterminado Send-Auth-None (0), no se negocia ninguna autenticación. Otros valores son Send-Auth-PAP (1) y Send-Auth-CHAP (2).
Ascend-Send-Secret (214)	Contraseña enviada al extremo distante durante la autenticación de la llamada de salida. Si el servidor no dispone de este atributo, utilice en su lugar Ascend-Send-Passwd (232). Para obtener información detallada, consulte el apartado “Secretos compartidos e intercambios seguros” en la página A-5.

## *Ejemplos de solicitud de autenticación CHAP para una llamada de salida*

Los comandos siguientes crean un perfil que solicita la autenticación CHAP al realizar una llamada de salida al extremo distante:

```
admin> new connection hanif
CONNECTION/hanif read
admin> set active = yes
admin> set encapsulation-protocol = ppp
admin> set dial-number = 555-1212
admin> set ip remote-address = 10.1.2.3/29
admin> set ppp send-auth-mode = chap-ppp-auth
admin> set ppp send-password = remotepw
admin> set ppp recv-password = localpw
admin> write
CONNECTION/hanif written
```

A continuación se muestran los perfiles RADIUS equivalentes:

```
hanif Password = "localpw"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Framed-IP-Address = 10.1.2.3,
    Framed-IP-Netmask = 255.255.255.248

route-taos-1 Password = "ascend", Service-Type = Outbound-User
    Framed-Route = "10.1.2.3/29 10.1.2.3 1 n hanif-out"

hanif-out Password = "localpw", Service-Type = Outbound-User
    User-Name = "hanif",
    Ascend-Dial-Number = "555-1212",
```

```
Framed-Protocol = PPP,  
Framed-IP-Address = 10.1.2.3  
Framed-IP-Netmask = 255.255.255.248,  
Ascend-Send-Auth = Send-Auth-PAP,  
Ascend-Send-Secret = "remotepw"
```

## Autenticación de inicios de sesión de usuario

Una conexión del servidor de terminales la inicia un módem análogo o un módem ISDN (como un adaptador de terminales V.120). Según el software de cliente que se utilice para iniciar el enlace, puede tratarse de una llamada PPP asíncrona o una sesión de inicio de sesión de un usuario.

Al recibir la llamada, el servidor de terminales espera a recibir de un paquete PPP durante un período de tiempo breve. Si se agota el tiempo de espera, envía un indicador de inicio de sesión. Si recibe un nombre y una contraseña que coinciden con un perfil configurado, autentica la llamada y proporciona al usuario el nivel autorizado de acceso al propio servidor de terminales o a un host de la red. Para obtener información detallada acerca de la autorización de acceso para sesiones de conexión, consulte el Apéndice B, “Opciones de autorización”.

Si el servidor de terminales recibe un paquete PPP, responde con un paquete PPP. Se inician las negociaciones LCP, incluida la autenticación PPP. Si la autenticación es correcta, la unidad TAOS envía la llamada al software del ruteador y establece una sesión PPP normal. Salvo en el proceso inicial, la unidad TAOS trata una llamada PPP asíncrona igual que cualquier llamada PPP normal. Para obtener información detallada acerca de la autenticación de sesiones de protocolo entramado, consulte “Autenticación de sesiones de protocolo entramado” en la página A-6.

## Secuencias de comandos de inicio de sesión Expect-Send

Si un emisor realiza una llamada de entrada utilizando un paquete de comunicaciones y un TA ISDN o de módem con PPP desactivado, la unidad TAOS agota el tiempo de espera en PPP y envía unos indicadores de inicio de sesión y contraseña como los siguientes:

```
Login:  
Password:
```

El software de cliente visualiza el indicador de inicio de sesión, que permite al usuario conectarse manualmente, o ejecuta una secuencia de comandos Expect-Send como la siguiente:

```
expect "Login:" send $username expect "Password:" send $password
```

Una vez recibida toda la información de autenticación necesaria, la unidad TAOS la autentica comparándola con la información contenida en el perfil del emisor. Los detalles sobre lo que sucede después de una autenticación correcta de la sesión dependen de una serie de factores que se indican en la cabecera de la *autorización*. Si desea obtener información detallada, consulte el Apéndice B, “Opciones de autorización”.



## Modo de seguridad del servidor de terminales

Los parámetros siguientes (que aparecen con los ajustes predeterminados) se utilizan para proteger con contraseña la línea de comandos del servidor de terminales:

```
[in TERMINAL-SERVER]
security-mode = none

[in TERMINAL-SERVER:terminal-mode-configuration]
system-password = ""
```

Parámetro	Especifica
Security-Mode	Requisito de introducir una contraseña para acceder al servidor de terminales.
System-Password	Contraseña (de un máximo de 15 caracteres) para acceder al servidor de terminales.

Si Security-Mode está establecido en None (el valor predeterminado), los usuarios reciben inmediatamente un indicador de servidor de terminales cuando se conectan mediante una interfaz asíncrona. Por ejemplo:

```
ATDT961234
CONNECT 115200
** unidad TAOS Terminal Server **

ascend%
```

Si Security-Mode está establecido en Partial, se solicita a los usuarios su nombre y contraseña propios, como están configurados en el perfil del emisor.

Si Security-Mode está establecido en Full, se solicita a los usuarios que especifiquen una contraseña del sistema y su nombre y contraseña propios antes de que aparezca el indicador del servidor de terminales.

Los comandos siguientes especifican una seguridad completa de contraseñas en el servidor de terminales y establecen la contraseña del sistema en secret:

```
admin> read terminal-server
TERMINAL-SERVER read

admin> set security-mode = full

admin> set terminal system-password = secret

admin> write
TERMINAL-SERVER written
```

Con estos ajustes, los usuarios deben responder a los indicadores siguientes para conectarse al servidor de terminales:

```
System Password:

Name:
Password:
```

## Personalización de la secuencia de conexión

Los parámetros siguientes (que aparecen con los ajustes predeterminados) definen las cadenas que se envían a un usuario de llamada de entrada y las cadenas que se esperan de éste durante el proceso de conexión:

```
[in TERMINAL-SERVER:terminal-mode-configuration]
banner = "*** unidad TAOS Terminal Server ***"
login-prompt = "Login: "
password-prompt = "Password: "
third-login-prompt = ""
third-prompt-sequence = last
prompt = "ascend% "
login-timeout = 300
```

Parámetro	Especifica
Banner	Primera línea enviada al usuario de llamada de entrada. La cabecera predeterminada es <code>*** unidad TAOS Terminal Server ***</code> .
Login-Prompt	Segunda línea enviada al usuario de llamada de entrada, que solicita un nombre de usuario. El sistema utiliza el nombre proporcionado en este indicador para autenticar el perfil del emisor.
Password-Prompt	Tercera línea enviada al usuario de llamada de entrada, que solicita una contraseña. El sistema utiliza la contraseña proporcionada en este indicador para autenticar el perfil del emisor.
Third-Login-Prompt	Tercer indicador de inicio de sesión, obligatorio en algunos servidores RADIUS y algunas secuencias de conexión del proveedor.
Third-Prompt-Sequence	Dónde debe aparecer el tercer indicador de inicio de sesión dentro de la secuencia de conexión (en primer lugar o en último lugar).
Prompt	Cadena que se debe utilizar como indicador de línea de comandos en la interfaz del servidor de terminales.
Login-Timeout	Número de segundos durante los que aparece el indicador de inicio de sesión antes de agotarse el tiempo de espera para la conexión. Cuando un usuario se conecta al servidor de terminales en modo de terminal, aparece un indicador de inicio de sesión. Si el usuario no realiza ninguna acción desde el indicador de inicio de sesión en menos de 300 segundos, la conexión agota el tiempo de espera. Si establece el parámetro Login-Timeout en cero, la conexión nunca agota el tiempo de espera.

### *Especificación de la cabecera y los indicadores*

A continuación se muestra un ejemplo de configuración de la cabecera, los indicadores de inicio de sesión, el indicador de la línea de comandos y el tiempo de espera de conexión:

```
admin> read terminal-server
TERMINAL-SERVER read
admin> set terminal banner = "ABC Corp. Terminal Server"
```

```
admin> set terminal login-prompt = "Name:"
admin> set terminal password-prompt = "Password:"
admin> set terminal prompt = "ABC: "
admin> write
TERMINAL-SERVER written
```

Con estos ajustes, un usuario de llamada de entrada que se conecte a la línea de comandos del servidor de terminales recibe la siguiente secuencia de indicadores:

```
ABC Corp. Terminal Server
System Password:
Name:
Password:
```

Si modifica los ajustes predeterminados del indicador de inicio de sesión y de la línea de comandos, asegúrese de que las secuencias de comandos Expect-Send de los usuarios se han grabado para esperar a recibir las cadenas que especifica. Por ejemplo:

```
expect "Name:" send username expect "Password:" send password
expect "ABC Corp. Terminal Server" send "" expect "ABC: " send "telnet
10.1.1.3"
```

### *Cuándo debe utilizarse el tercer indicador*

Algunos servidores RADIUS requieren un indicador de inicio de sesión adicional (tercero), definido por el atributo Ascend-Third-Prompt (213). Si la llamada ha sido autenticada por RADIUS y el perfil especifica un valor para este atributo, debe configurar el servidor de terminales para que muestre el indicador necesario. Si RADIUS espera un tercer indicador, siempre lo espera en último lugar, después de la secuencia de inicio de sesión normal.

Algunos ISP utilizan un servidor de terminales que sigue una secuencia de inicio de sesión distinta a la utilizada por Lucent Technologies (por ejemplo, una que incluya una selección de menú antes de la conexión). Si éste es el caso en su entorno, debe configurar el servidor de terminales para que muestre el indicador necesario y debe especificar que se muestre en primer lugar, con lo que se minimiza el otro servidor de terminales y se conserva la compatibilidad con el software de cliente que utilizan los abonados.

En el ejemplo siguiente se muestra cómo configurar los parámetros Third-Login-Prompt y Third-Prompt-Sequence para que un servidor RADIUS espere un tercer indicador:

```
admin> read terminal-server
TERMINAL-SERVER read

admin> set terminal third-login-prompt = third-prompt>
admin> set terminal third-prompt-sequence = last
admin> write
TERMINAL-SERVER written
```

En el ejemplo siguiente se muestra cómo configurar los parámetros Third-Login-Prompt y Third-Prompt Sequence para imitar a otro servidor de terminales que espera que los usuarios seleccionen un servicio antes de conectarse:

```
admin> read terminal-server
TERMINAL-SERVER read
```

```
admin> set terminal third-login-prompt = service?  
admin> set terminal third-prompt-sequence = first  
admin> write  
TERMINAL-SERVER written
```

## ***Autenticación por tarjeta de testigo***

Una unidad TAOS permite la autenticación por tarjeta de testigo utilizando un servidor RADIUS como intermediario entre la unidad TAOS que responde a la llamada y un servidor de autenticación externa (EAS), como un servidor Security Dynamics ACE/Server o un servidor Enigma Logic SafeWord.

## **Seguridad ampliada con tarjetas de testigo**

Las tarjetas de testigo protegen frente a ataques pasivos y ataques de repetición, en los que un usuario no autorizado registra información válida de autenticación intercambiada entre sistemas y, posteriormente, la repite para obtener acceso. Como las tarjetas de testigo proporcionan contraseñas de un solo uso, éstas cambian muchas veces al día, con lo que la repetición resulta imposible.

Una tarjeta de testigo es un dispositivo de hardware, generalmente parecido a una calculadora del tamaño de una tarjeta de crédito, con una pantalla LCD que proporciona al usuario el testigo (contraseña) de un solo uso actual que le permitirá acceder a una red segura. El testigo cambia muchas veces al día. Las tarjetas de testigo actualizan de forma continua esta información de autenticación manteniendo un reloj sincronizado con un EAS, como un servidor ACE/Server o SafeWord. Los usuarios autorizados deben poseer la tarjeta de testigo para poder acceder a una red segura.

Si el EAS es un servidor ACE/Server, el usuario tiene una tarjeta de testigo SecurID que muestra un código de acceso generado aleatoriamente que cambia cada 60 segundos.

Si el EAS es un servidor SafeWord, el usuario puede tener uno de los tipos siguientes de tarjeta de testigo:

- ActivCard
- CryptoCard
- DES Gold
- DES Silver
- SafeWord SofToken
- SafeWord MultiSync
- DigiPass
- SecureNet Key
- WatchWord

Una unidad TAOS permite las tarjetas de testigo sólo a través de RADIUS. El servidor RADIUS debe estar configurado para interactuar con los módulos EAS, que generalmente se ejecutan en el mismo sistema físico que el servidor RADIUS.

**Nota:** Mientras se utiliza la autenticación RADIUS, el propio servidor RADIUS actúa como EAS. Mientras se utiliza la autenticación por tarjeta de testigo, el servidor RADIUS transmite la petición de autenticación a un servidor ACE/Server o SafeWord, y se hace referencia a este sistema como EAS. Este detalle no afecta a la configuración del perfil External-Auth de la unidad TAOS, que aún debe especificar RADIUS como servidor externo.

## **Método sencillo de autenticación de llamadas por tarjeta de testigo**

Una unidad TAOS puede dar soporte a la autenticación por tarjeta de testigo desde dispositivos que no ejecutan el software TAOS. Para ello, la unidad autentica las llamadas en el software de servidor de terminales utilizando la autenticación PAP normal para efectuar los intercambios de testigo de desafío-respuesta. Por ejemplo, el perfil RADIUS siguiente especifica la autenticación desde un servidor ACE/Server:

```
carlos Password = "ACE"  
    Service-Type = Framed-User,  
    Framed-Protocol = PPP,  
    Framed-IP-Address = 10.2.3.78,  
    Framed-IP-Netmask = 255.255.255.255
```

El servidor RADIUS descarta la respuesta del usuario al indicador Password inicial del servidor de terminales, de modo que el usuario puede introducir cualquier valor. El servidor RADIUS genera un paquete Access-Challenge con un indicador de desafío (normalmente un indicador Passcode para la autenticación ACE) y utiliza la respuesta a este paquete de desafío para autenticar el usuario con el EAS.

Si el perfil del emisor especifica el par atributo-valor siguiente, el sistema no requiere un intercambio de desafío-respuesta:

<b>Atributo</b>	<b>Valor</b>
Ascend-Token-Immediate (200)	Elude el procedimiento de desafío-respuesta necesario para algunos métodos de autenticación por tarjeta de testigo. Los valores válidos son Tok-Imm-No (0), que es el valor predeterminado, y Tok-Imm-Yes (1). Si se utiliza, debe ser un elemento de verificación en el perfil RADIUS.  <b>Nota:</b> Si se establece este atributo en Tok-Imm-Yes, el perfil será incompatible con la autenticación PAP-TOKEN, PAP-TOKEN-CHAP y CACHE-TOKEN (consulte “Autenticación de conexiones de tarjeta de testigo desde unidades TAOS” en la página A-28).

Cuando los usuarios tienen una tarjeta de testigo que no requiere un intercambio de desafío-respuesta (como es el caso de ACE), puede utilizar Ascend-Token-Immediate para simplificar el proceso de autenticación. Los usuarios responden al indicador Password inicial con el testigo actual. El servidor RADIUS no descarta esta respuesta inicial, sino que la utiliza para autenticar la llamada a través de EAS.

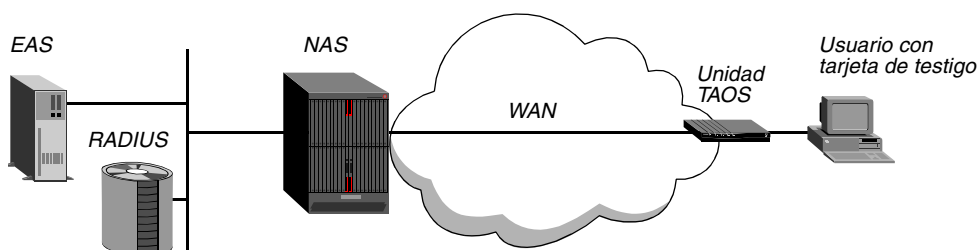
A continuación se muestra un ejemplo de perfil RADIUS que aplica el atributo Ascend-Token-Immediate:

```
robin Password = "ACE", Ascend-Token-Immediate = Tok-Imm-Yes
Service-Type = Framed-User,
Framed-Protocol = PPP,
Framed-IP-Address = 10.3.4.5,
Framed-IP-Netmask = 255.255.255.255
```

## Autenticación de conexiones de tarjeta de testigo desde unidades TAOS

En la Figura A-5 se muestra una conexión de llamada de entrada con una unidad TAOS en una red segura. El usuario remoto debe utilizar una tarjeta de testigo para poder acceder a la red segura.

*Figura A-5. Autenticación por tarjeta de testigo para conexiones de llamada de entrada*



En una disposición como la que se muestra en la Figura A-5, un usuario con una tarjeta de testigo inicia una conexión con la unidad TAOS (el servidor de acceso de red o NAS).

El NAS envía un paquete Access-Request al servidor RADIUS para autenticar la llamada de entrada y el servidor RADIUS envía la petición de conexión al EAS (un servidor ACE/Server o SafeWord).

El EAS devuelve un paquete Access-Challenge a través del servidor RADIUS y la unidad TAOS al usuario que realiza la llamada de entrada. El usuario ve el mensaje de desafío, obtiene la contraseña actual de su tarjeta de testigo e introduce la contraseña en respuesta al mensaje de desafío. La contraseña vuelve al EAS a través del NAS y del servidor RADIUS.

El EAS envía una respuesta al servidor RADIUS en que se especifica si el usuario ha introducido el testigo correcto. Si el usuario introduce un testigo incorrecto, el EAS devuelve otro desafío y el usuario puede volver a intentarlo, pero sólo un total de tres veces.

Como último paso de la autenticación, el servidor RADIUS envía una respuesta de autenticación a la unidad TAOS. Si la autenticación no es correcta, la unidad TAOS recibe un paquete Access-Reject y desconecta la llamada. Si la autenticación es correcta, la unidad TAOS recibe un paquete Access-Accept que contiene una lista de pares atributo-valor del perfil de usuario de la base de datos del servidor RADIUS. La unidad TAOS utiliza los pares atributo-valor para crear la conexión.

### Configuración de una unidad TAOS como un NAS

Para configurar la unidad TAOS de modo que funcione como el NAS, debe configurar el perfil Answer-Defaults para permitir el método de autenticación apropiado. Por ejemplo, puede

establecer el parámetro Receive-Auth-Mode en Any-PPP-Auth, como se describe en “Autenticación de sesiones de protocolo entramado” en la página A-6.

También debe configurar el perfil External-Auth para que autentique las conexiones a través de RADIUS (consulte “Perfil External-Auth” en la página 1-6).

### *Especificación del tipo de servicio por conexión*

Puede especificar un servicio digital o analógico para cada conexión mediante el atributo NAS-Port-Type de RADIUS (atributo 61) o mediante el perfil local. A continuación se muestra el parámetro pertinente con su ajuste predeterminado:

```
[in CONNECTION/"":telco-options]  
nas-port-type = any
```

Nas-Port Type	Tipo de servicio de la sesión. El ajuste predeterminado permite un servicio sin restricciones. Si se establece este parámetro en digital o analog se restringe el servicio al tipo especificado.
---------------	--

En la tabla siguiente se muestran los ajustes del perfil local correspondientes a los pares atributo-valor de RADIUS para el atributo NAS-Port-Type de RADIUS:

Ajustes de RADIUS	Ajustes del perfil local correspondientes
NAS-Port-Type = Async	nas-port-type = analog or: nas-port-type = any
NAS-Port-Type = Sync	nas-port-type = digital or: nas-port-type = any
NAS-Port-Type = ISDN_Sync	nas-port-type = digital or: nas-port-type = any
NAS-Port-Type = ISDN_Async_V120	nas-port-type = digital or: nas-port-type = any
NAS-Port-Type = ISDN_Async_V110	nas-port-type = digital or: nas-port-type = any
NAS-Port-Type = Virtual	nas-port-type = any

### *Modo de visualización y respuesta del usuario de llamada de entrada a los desafíos*

El usuario debe poder visualizar el desafío y responder a éste desde el EAS. La utilidad APP Server puede ejecutarse en una computadora accesible para el usuario, o el usuario puede poner en modo de contraseña la unidad TAOS de extremo distante ejecutando el comando Set Password en la interfaz del servidor de terminales de la unidad. Por ejemplo:

```
ascend% set password  
Entering Password Mode...  
  
[^C to exit] Password Mode>
```

Estos dos métodos para gestionar los desafíos se explican en la documentación de Pipeline y MAX.

## *Configuración de perfiles RADIUS para la autenticación por tarjeta de testigo*

TAOS da soporte a las siguientes modalidades de autenticación por tarjeta de testigo:

- PAP-TOKEN
- PAP-TOKEN-CHAP
- CACHE-TOKEN

### *Utilización de la autenticación PAP-TOKEN*

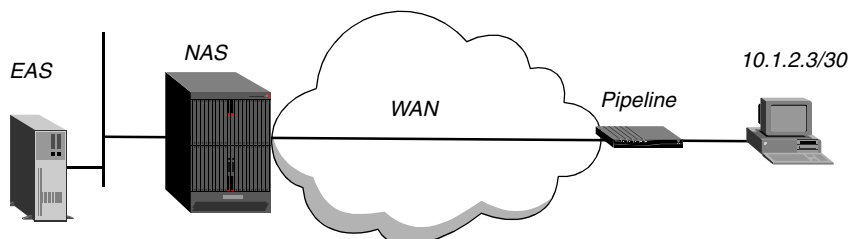
PAP-TOKEN es una extensión de la autenticación PAP. No resulta práctica para las llamadas multicanal, puesto que si los requisitos de ancho de banda motivan la conexión de otro canal, la unidad TAOS debe interrumpir la sesión para desafiar al usuario y solicitarle otro testigo.

Con PAP-TOKEN, el valor Send-Password del emisor se envía como parte de la negociación inicial de sesión, con lo que se activa un desafío desde el EAS. El EAS devuelve un desafío y en él el usuario escribe el testigo actual obtenido de la tarjeta de testigo. El testigo se envía como texto explícito (a través de PAP), pero esta ausencia de cifrado no debe considerarse un riesgo grave de seguridad dado que el testigo sólo se utiliza una vez.

La respuesta al desafío inicial autentica el canal base de la llamada. Si los requisitos de ancho de banda motivan la conexión de otro canal, el usuario recibe un desafío para que especifique una contraseña.

En la Figura A-6 se muestra un usuario de una computadora con una tarjeta de testigo SecurID que realiza una llamada de entrada a la unidad TAOS a través de una unidad Pipeline. El EAS es un host UNIX que ejecuta el software Security Dynamics ACE/Server y RADIUS.

*Figura A-6. PAP-TOKEN con un ACE/Server*



Cuando el EAS devuelve un paquete Access-Challenge a través del servidor RADIUS y la unidad TAOS al usuario que realiza la llamada de entrada, éste ve el mensaje de desafío, obtiene el testigo actual e introduce la contraseña en respuesta al mensaje de desafío. La contraseña vuelve a través del NAS y del servidor RADIUS al EAS, donde se autentica.

A continuación se muestra un perfil RADIUS para el usuario de una computadora:

```
Connor Password = "ACE"
Service-Type = Framed-User,
Framed-Protocol = PPP,
Framed-IP-Address = 10.1.2.3,
Framed-IP-Netmask = 255.255.255.252
```

A continuación se muestra un perfil Connection de extremo distante en la unidad Pipeline:

```
Station=Connor
Active=Yes
```



```
Dial #=18005551212
Encaps=PPP
Route IP=Yes
Encaps options...
    Send Auth=PAP-TOKEN
    Send PW=localpw
IP options...
    LAN Adrs=10.1.2.3/30
```

### *Utilización de la autenticación PAP-TOKEN-CHAP*

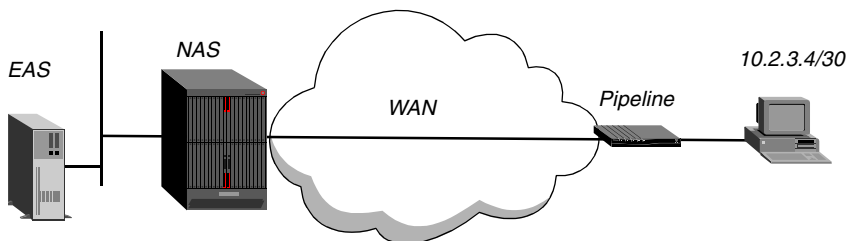
PAP-TOKEN-CHAP resulta apropiada para la autenticación por testigo de llamadas multienlaces. La autenticación de un canal base utiliza PAP-TOKEN. Si se agregan canales a la llamada, éstos se autentican mediante CHAP y la contraseña Aux Send PW del emisor. Para informar al NAS del valor de Aux Send PW que debe esperar para los canales subsiguientes, el servidor RADIUS envía este valor como valor Ascend-Receive-Secret al autenticarse la llamada inicial.

Además del requisito de que el atributo Password debe especificar ACE o SAFEWORD, la autenticación PAP-TOKEN-CHAP requiere el par atributo-valor siguiente:

Atributo	Valor
Ascend-Receive-Secret (215)	Cadena de texto de hasta 20 caracteres que debe coincidir con la contraseña Aux Send PW enviada por el extremo distante para autenticar los canales agregados. El servidor RADIUS entrega el secreto de recepción al NAS cuando se autentica la llamada inicial. El NAS almacena el secreto de recepción como valor Recv-Password para el emisor y lo utiliza para crear la síntesis que se envía al servidor RADIUS a través de CHAP.

En la Figura A-7 se muestra un usuario con una tarjeta de testigo que realiza una llamada a la unidad TAOS a través de una unidad Pipeline. El EAS es un host UNIX que ejecuta el software de servidor Enigma Logic SafeWord y RADIUS. Tras la autenticación, el usuario puede abrir una sesión multienlaces.

*Figura A-7. PAP-TOKEN-CHAP con un servidor SafeWord*



A continuación se muestra un ejemplo del perfil de usuario:

```
Raoul Password = "SAFEWORD"
Service-Type = Framed-User,
Framed-Protocol = MPP,
Framed-IP-Address = 10.2.3.4,
Framed-IP-Netmask = 255.255.255.252,
Ascend-Receive-Secret = "aux-send",
```

```
Ascend-Base-Channel-Count = 2,  
Ascend-Maximum-Channels = 2
```

A continuación se muestra un perfil Connection de extremo distante en la unidad Pipeline:

```
Station=Raoul  
Active=Yes  
Dial #=18005551212  
Encaps=MPP  
Route IP=Yes  
Encaps options...  
    Send Auth=PAP-TOKEN-CHAP  
    Send PW=localpw  
    Aux Send PW=aux-send  
    Base Ch Count=2  
IP options...  
    LAN Adrs=10.2.3.4/30
```

### ***Utilización de la autenticación CACHE-TOKEN***

CACHE-TOKEN es otra forma de autenticar por testigo las llamadas multienlaces. El servidor RADIUS guarda en la caché una versión cifrada del testigo durante un número especificado de minutos. Si el emisor marca canales adicionales, el servidor RADIUS recibe la petición del NAS, verifica que el testigo no ha caducado y lo utiliza en la caché para autenticar los canales. Si el testigo ha caducado, la petición debe autenticarse a través del EAS con otro testigo de desafío.

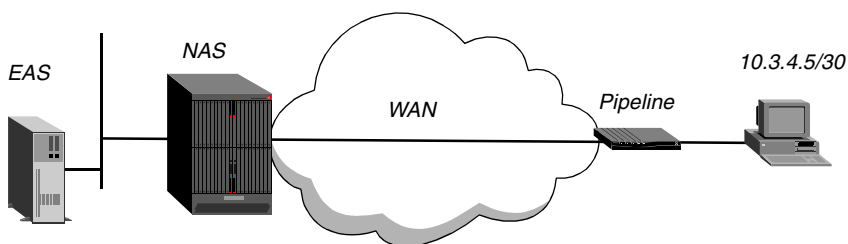
Además del requisito de que el atributo Password debe especificar ACE o SAFEWORD, la autenticación CACHE-TOKEN utiliza los pares atributo-valor siguientes:

<b>Atributo</b>	<b>Valor</b>
Ascend-Receive-Secret (215)	Cadena de texto de hasta 20 caracteres que debe coincidir con el valor Send PW enviado por el extremo distante para autenticar la llamada inicial. El servidor RADIUS utiliza este valor para descifrar la síntesis hash enviada por el NAS utilizando una forma de intercambio CHAP. La síntesis hash se deriva del testigo enviado por el emisor y el valor Send PW normal en el perfil de extremo distante.
Ascend-Token-Expiry (204)	<p>Número de minutos durante los que el testigo de la caché es válido. El valor predeterminado cero significa que no se permite guardar el testigo en la caché. Debe ser un elemento de verificación.</p> <p>La caducidad del testigo se produce exclusivamente en el servidor RADIUS. El NAS envía peticiones de autenticación y, si el testigo ha caducado, el servidor RADIUS envía la petición al EAS, que devuelve otro desafío al extremo distante.</p>

Atributo	Valor
Ascend-Token-Idle (199)	Número de minutos durante los que un testigo en la caché es válido si una llamada está desocupada. De forma predeterminada, el testigo sigue siendo válido hasta que se alcanza el valor del atributo Ascend-Token-Expiry. Debe ser un elemento de verificación.  Este atributo es útil para aplicar la autenticación cuando una conexión vuelve a activarse después de un período de inactividad. Si no especifica este atributo, el testigo de la caché sigue siendo válido hasta que el valor de Ascend-Token-Expiry hace que caduque. Normalmente el valor de Ascend-Token-Idle es más bajo que el valor de Ascend-Token-Expiry.

En la Figura A-8 se muestra un usuario que realiza una llamada de entrada utilizando una Pipeline y que se autentica mediante un EAS, que es un host UNIX que ejecuta el software de servidor Enigma Logic SafeWord y RADIUS.

*Figura A-8. CACHE-TOKEN con un servidor SafeWord*



A continuación se muestra un perfil de usuario RADIUS para el usuario de llamada de entrada:

```
Aydin Password="SAFWORD", Ascend-Token-Expiry=30, Ascend-Token-Idle=10,  
    Service-Type = Framed-User,  
    Framed-Protocol = MPP,  
    Framed-IP-Address = 10.3.4.5,  
    Framed-IP-Netmask = 255.255.255.252,  
    Ascend-Receive-Secret = "chap-val",  
    Ascend-Base-Channel-Count = 2,  
    Ascend-Maximum-Channels = 2
```

A continuación se muestra un perfil Connection de extremo distante en la unidad Pipeline:

```
Station=Aydin  
Active=Yes  
Dial #=18005551212  
Encaps=MPP  
Route IP=Yes  
Encaps options...  
    Send Auth=CACHE-TOKEN  
    Send PW=localpw  
    Aux Send PW=chap-val  
    Base Ch Count=2  
IP options...  
    LAN Adrs=10.3.4.5/30
```

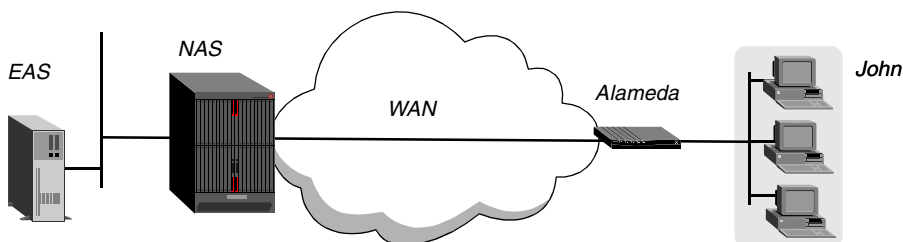
### *Utilización de la autenticación ACE para usuarios de la red*

Si el EAS es un servidor Secure Dynamics ACE/Server, se puede conceder el acceso de llamada de entrada a varios usuarios de una red remota mediante un único perfil que especifique el nombre del ruteador remoto. Para realizar una llamada de entrada, un usuario debe introducir el testigo con el formato siguiente:

```
token.username
```

El servidor RADIUS presenta el argumento *username*, y no el nombre del ruteador, al servidor ACE/Server. El almacenamiento del testigo en la caché sigue funcionando con normalidad. Todos los usuarios comparten el mismo perfil RADIUS y la contabilidad RADIUS utiliza el nombre del ruteador en lugar del nombre real del usuario. En la Figura A-9, varios usuarios remotos están conectados a una unidad TAOS llamada Alameda.

*Figura A-9. Autenticación ACE para usuarios de ruteador remoto*



El perfil de usuario especifica el nombre de sistema del Pipeline y la contraseña para la autenticación ACE. Por ejemplo:

```
Alameda Password = "ACE"  
Service-Type = Framed-User,  
Framed-Protocol = PPP,  
Framed-IP-Address = 10.72.138.1,  
Framed-IP-Netmask = 255.255.255.0
```

Un usuario de la red llamado John responde de la forma siguiente a un desafío de contraseña:

```
From: hostname  
0-Challenge: challenge  
Enter next password: newtoken.John
```

## ***Autenticación de túnel***

Tanto ATMP como L2TP permiten la autenticación de túnel. Cuando la autenticación de túnel es necesaria, el agente externo (o controlador de acceso L2TP) que inicia una petición de túnel debe proporcionar una contraseña para que el agente local (o servidor de red L2TP) permita el registro del túnel.

### **Autenticación de túneles ATMP**

El perfil ATMP del agente local contiene un parámetro Password. Si éste no es nulo, los perfiles de cliente móvil deben proporcionar la contraseña para iniciar un túnel. Si el agente externo proporciona la contraseña correcta al solicitar un túnel, el agente local devuelve un mensaje RegisterReply con un número que identifica el túnel y se establece el túnel del cliente móvil. Si la contraseña no coincide, el agente local rechaza el túnel, y el agente externo registra

un mensaje y desconecta el cliente móvil. Los comandos siguientes configuran el perfil ATMP del agente local para que precise la autenticación de túnel:

```
admin> read atmp
ATMP read

admin> set password = tunnel-password

admin> write
ATMP written
```

El perfil Connection del cliente móvil debe incluir el mismo valor para el parámetro Password del subperfil Tunnel-Options. Por ejemplo:

```
admin> read connection mobile-client
CONNECTION/mobile-client read

admin> set tunnel profile-type = mobile-client

admin> set tunnel primary-tunnel-server = 3.3.3.3:8877

admin> set tunnel password = tunnel-password

admin> write
CONNECTION/mobile-client written
```

A continuación se muestra un perfil RADIUS equivalente:

```
mobile-client Password = "my-password",
  Service-Type = Framed-User
  Tunnel-Type = ATMP,
  Tunnel-Server-Endpoint = "3.3.3.3:8877",
  Tunnel-Password = "tunnel-password"
```

Muchos servidores RADIUS cifran las contraseñas de túnel antes de enviarlas al agente local si el perfil del cliente móvil utiliza el atributo Tunnel-Password (69) para especificar la contraseña. Si el perfil especifica Tunnel-Password y el servidor RADIUS no cifra la contraseña, la autenticación de túnel fallará.

Si, por el contrario, el perfil de cliente móvil utiliza el atributo Ascend-Home-Agent-Password (184) para especificar la contraseña, el servidor RADIUS no realiza ningún cifrado antes de enviar la contraseña al agente local. Esta opción puede ser necesaria si se utiliza un servidor RADIUS que no cifra el valor de Tunnel-Password.

**Nota:** A menos que utilice un servidor RADIUS que no permita el cifrado de Tunnel-Password (o que el cifrado no sea necesario), se recomienda utilizar el atributo Tunnel-Password en lugar de Ascend-Home-Agent-Password como protección frente a programas de exploración de paquetes locales que detecten contraseñas de túnel.

## Autenticación de túneles L2TP

Los túneles L2TP pueden autenticarse si en ambos extremos de la conexión se utiliza el mismo valor de secreto (un secreto compartido).

Si utiliza perfiles locales para la autenticación de clientes móviles en el LAC (la unidad TAOS), puede especificar un único secreto compartido para autenticar todos los túneles configurados localmente. Los comandos siguientes especifican un único secreto compartido para toda la configuración del servidor de túnel de LAC:

```
admin> read tunnel-server l2tp-1
TUNNEL-SERVER/l2tp-1 read
```

```
admin> set enabled = yes
admin> set shared-secret = tunnel-secret
admin> write
TUNNEL-SERVER/l2tp-1 read
```

Si el LAC utiliza RADIUS para autenticar clientes móviles, los perfiles RADIUS de los clientes pueden especificar un secreto compartido mediante el atributo Tunnel-Password (69).

**Nota:** Para que la autenticación de túnel no falle, el servidor RADIUS debe cifrar el atributo Tunnel-Password.

El perfil siguiente autentica el túnel del perfil RADIUS del cliente que realiza la llamada:

```
l2tp-client Password = "my-password"
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Framed-IP-Address = 10.50.1.1,
  Framed-IP-Netmask = 255.255.0.0,
  Tunnel-Type = L2TP,
  Tunnel-Medium-Type = IP,
  Tunnel-Server-Endpoint = "lns-sys.domain.org"
  Tunnel-Password = "tunnel-secret"
```

Si lo prefiere, puede eliminar el atributo Tunnel-Password de los perfiles de los clientes que realizan una llamada y crear un perfil cuyo único propósito sea autenticar túneles L2TP. Esto hace necesaria una búsqueda RADIUS adicional la primera vez que se crea un túnel, pero simplifica la administración cuando los secretos compartidos cambian. El perfil RADIUS para la autenticación de túnel debe especificar el nombre del homólogo L2TP, una contraseña nula ("") y el ajuste Outbound-User de Service-Type. Por ejemplo:

```
lns-sys.domain.org Password = "", Service-Type = Outbound-User
  Tunnel-Password = "tunnel-secret"
```

Cuando se establece inicialmente un túnel L2TP, el LNS y el LAC emiten una búsqueda RADIUS basada en el nombre del homólogo. Si el sistema encuentra un perfil como el que se muestra en el ejemplo anterior, utiliza el valor de Tunnel-Password para autenticar el túnel.

**Nota:** La contraseña del perfil de pseudousuario debe ser nula (""). Como la contraseña nula representa un riesgo para la seguridad, *el perfil debe especificar el ajuste Outbound-User para Service-Type.*

## ***Autenticación previa (CLID o DNIS)***

El ID de línea de llamada (CLID) es el número de teléfono de un dispositivo que realiza llamadas. Puede utilizar el CLID para la autenticación sólo si la información de llamada está disponible de extremo a extremo y si se aplica la identificación de número automática (ANI) a la llamada. En algunas áreas, puede ser que el proveedor de WAN no pueda proporcionar los CLID o que un emisor desee que su CLID se mantenga en secreto. Normalmente, la gente utiliza el CLID como protección frente a la situación en la que un usuario no autorizado obtiene el nombre, la contraseña y la dirección IP de un usuario autorizado y llama desde otra ubicación.

El servicio de información de número de marcación (DNIS) es el número al que se llama, que es un elemento informativo del protocolo de señalización ISDN Q.931. Es el número de

teléfono al que llama el dispositivo remoto para conectarse a la unidad TAOS, pero sin especificación de prefijo de marcación ni grupo de línea troncal. Cuando el perfil precisa la autenticación del número marcado, éste debe coincidir con un número de teléfono en un perfil Connection local o un perfil de usuario RADIUS.

La verificación CLID o DNIS se produce antes de que la unidad TAOS acepte una llamada e inicie el proceso de autenticación de una contraseña.

## **Configuración de una unidad TAOS para que extraiga y utilice información de una llamada**

Para que una unidad TAOS pueda extraer y utilizar información CLID o DNIS, se debe establecer el parámetro CLID-Auth-Mode en el perfil Answer-Defaults. Por ejemplo, los comandos siguientes especifican que el sistema utilice información CLID si ésta está disponible, pero que si la autenticación CLID falla por el motivo que sea, el sistema siga intentando realizar la autenticación de la contraseña para la llamada:

```
admin> read answer
ANSWER-DEFAULTS read

admin> set clid-auth-mode = clid-prefer

admin> write
ANSWER-DEFAULTS written
```

Puede establecer CLID-Auth-Mode en uno de los valores siguientes:

- **Ignore:** La información de ID de emisor y número marcado no se tiene en cuenta a menos que se haya especificado como elemento de verificación en un perfil de usuario RADIUS. Es el valor predeterminado. Consulte el apartado “Ejemplo de utilización del ID de emisor como elemento de verificación (sólo RADIUS)” en la página A-39.
- **CLID-Prefer o DNIS-Prefer:** El sistema realiza una autenticación previa mediante el número CLID o DNIS respectivamente, si el número aparece en la llamada. Tras la autenticación previa, la llamada puede pasar a una segunda fase de autenticación de contraseña o puede establecerse la conexión inmediatamente. Sin embargo, si el conmutador telco no presenta el CLID ni el DNIS, no se desconecta la llamada. En efecto, si el número aparece, el sistema actúa como si CLID-Auth-Mode tuviera el valor CLID-Require o DNIS-Require. Si el número no aparece, actúa como si CLID-Auth-Mode tuviera el valor Ignore.
- **CLID-First o DNIS-First:** Si el conmutador telco ha enviado el ID de línea de llamada (CLID) o el número marcado (DNIS), la unidad TAOS lo utiliza para autenticar la llamada. Si este nivel de autenticación falla por el motivo que sea, o si el conmutador telco no proporciona el ID de línea de llamada ni el número marcado, la unidad TAOS no descarta la llamada, sino que permite que las negociaciones procedan a la autenticación de contraseña.
- **CLID-Require o DNIS-Require:** La llamada debe autenticarse previamente o fallará. Si el número CLID o DNIS coincide con un perfil, la llamada puede pasar a una segunda fase de autenticación de contraseña o puede establecerse la conexión inmediatamente. Si no hay ningún perfil coincidente, o si no aparece el número CLID ni DNIS, nunca se responde a la llamada y, por lo tanto, nunca se factura como llamada al usuario.

- **Fallback (sólo para CLID):** El CLID es obligatorio, pero sólo si la llamada se autentica con RADIUS. Si el servidor RADIUS no responde, el sistema pasa a realizar la autenticación de contraseña en lugar de descartar la llamada.

**Nota:** Para algunos tipos de señalización E1, el sistema debe solicitar explícitamente información CLID del conmutador. Para estos métodos de señalización, debe establecer el parámetro Caller-ID en el perfil E1 con el valor Get-Caller-ID.

## Especificación del elemento causante de una desconexión (sólo RADIUS)

Si la autenticación CLID o DNIS falla, un servidor RADIUS puede bien devolver el valor predeterminado, Normal Call Clearing (decimal 16), como elemento causante en paquetes de desconexión ISDN, o bien enviar User Busy (decimal 17), según el ajuste de los parámetros siguientes (que aparecen con los ajustes predeterminados):

```
[in EXTERNAL-AUTH:rad-auth-client  
auth-id-fail-return-busy = no  
auth-id-timeout-return-busy = no
```

Parámetro	Especifica
Auth-ID-Fail-Return-Busy	Activa y desactiva el envío de la causa de desconexión User Busy (17) cuando falla la autenticación CLID o DNIS. El ajuste predeterminado, No, hace que el sistema envíe la causa Normal Call Clearing (decimal 16).
Auth-ID-Timeout-Return-Busy	Activa y desactiva el envío de la causa de desconexión User Busy (17) cuando la autenticación CLID o DNIS agota el tiempo de espera. El ajuste predeterminado, No, hace que el sistema envíe la causa Normal Call Clearing (decimal 16).

Por ejemplo, para devolver el elemento causante User Busy al agotarse el tiempo de espera:

```
admin> read external-auth  
EXTERNAL-AUTH read  
  
admin> set rad-auth-client auth-id-timeout-return-busy = yes  
  
admin> write  
EXTERNAL-AUTH written
```

## Configuración de perfiles para la autenticación CLID o DNIS

Si el perfil de un emisor especifica un número de ID de emisor, la unidad TAOS puede comparar ese número con el proporcionado por el conmutador telco a fin de verificar que la llamada procede de una ubicación conocida.



### *Ajustes de los perfiles Connection*

A continuación se muestran los parámetros (con los ajustes predeterminados) para especificar números CLID y DNIS en un perfil Connection:

```
[in CONNECTION/""]  
clid = ""  
calledNumber = ""
```

<b>Parámetro</b>	<b>Especifica</b>
CLID	Número de teléfono del dispositivo que realiza la llamada. Cuando un usuario realiza una llamada de entrada mediante MP o MP+, el dispositivo que llama puede tener más de un número de teléfono asociado. En ese caso, el CLID es el número de teléfono asociado al canal que está en uso.
CalledNumber	Número al que se llama, que es un elemento informativo del protocolo de señalización ISDN Q.931. Es el número de teléfono al que llama el dispositivo remoto para conectarse a la unidad TAOS, pero sin especificación de prefijo de marcación ni de grupo de línea troncal

### *Ajustes de los perfiles RADIUS*

RADIUS utiliza los pares atributo-valor siguientes para especificar números CLID y DNIS:

<b>Atributo</b>	<b>Valor</b>
Caller-Id (31)	Número de teléfono del dispositivo que realiza la llamada (el valor de cadena). Cuando un usuario realiza una llamada de entrada mediante MP o MP+, el dispositivo que llama puede tener más de un número de teléfono asociado. En ese caso, el CLID es el número de teléfono asociado al canal que está en uso.
Client-Port-DNIS (30)	Número al que se llama, que es un elemento informativo del protocolo de señalización ISDN Q.931. Es el número de teléfono al que llama el dispositivo remoto para conectarse a la unidad TAOS, pero sin especificación de prefijo de marcación ni grupo de línea troncal (valor de cadena).
Ascend-Require-Auth (201)	Especifica si el perfil requiere una autenticación adicional después de la autenticación del número al que se llama. Los valores válidos son Not-Require-Auth (0), que es el valor predeterminado, y Require-Auth (1).

### *Ejemplo de utilización del ID de emisor como elemento de verificación (sólo RADIUS)*

Para las conexiones autenticadas con RADIUS, si el número Caller-Id o Client-Port-DNIS es conocido, se incluye en el paquete Access-Request dirigido al servidor RADIUS. Si se ha especificado el número de ID de emisor como elemento de verificación en el perfil de usuario RADIUS (si se ha especificado en la primera línea del perfil), como se muestra en el ejemplo siguiente, se rechaza el paquete Access-Request si el número de ID de emisor entregado al servidor no coincide con el valor del atributo Caller-Id.

```
emma Password = "test", Caller-Id = "5551213"  
Service-Type = Framed-User,  
Framed-Protocol = PPP,  
Ascend-Assign-IP-Pool = 1,  
Ascend-Route-IP = Route-IP-Yes
```

En el ejemplo anterior se muestra un perfil de usuario normal, pero el usuario está limitado a un número de teléfono específico. Esta limitación puede utilizarse para evitar conexiones de varios usuarios. A menos que el usuario posea una PBX u otro servicio que siempre proporcione el mismo número para varias líneas telefónicas, sólo un usuario podrá conectarse. La limitación de número de teléfono único se suele utilizar por motivos de seguridad para evitar que se abuse de un administrador del sistema u otra cuenta importante.

### *Ejemplo de utilización del nombre de usuario para la autenticación DNIS de primer nivel*

En versiones anteriores, si sólo se efectuaba una autenticación DNIS de primer nivel, no se disponía de ninguna información de nombre de usuario para los registros contables de SNMP, Syslog o RADIUS. En la versión actual del software, si sólo se efectúa una autenticación DNIS de primer nivel y el perfil contiene un par atributo-valor User-Name, el servidor RADIUS devuelve el valor del atributo User-Name en su respuesta DNIS Auth. Si se efectúa una autenticación de contraseña de usuario de segundo nivel, la información de nombre de usuario se toma del nombre de inicio de sesión, igual que en las versiones anteriores.

A continuación se muestra un ejemplo de perfil RADIUS autenticado por DNIS que incluye el atributo User-Name:

```
3735 Password = "Ascend-DNIS"  
User-Name = "johnfan",  
Service-Type = Login-User,  
Ascend-Require-Auth = Not-Require-Auth,  
Login-Service = TCP-Clear,  
Login-Host = 10.40.40.36,  
Login-TCP-Port = 7,  
Ascend-Idle-Limit = 0
```

### *Ejemplos en los que es preferible el CLID*

El perfil Connection siguiente valida el número CLID si está presente en la llamada. Si el número CLID presentado por la llamada no coincide, se descarta la llamada. Si el número CLID no aparece en la llamada, el perfil procede a la autenticación de contraseña.

```
admin> read conn edgar  
CONNECTION/edgar read  
  
admin> set ppp recv-password = test  
  
admin> set ip-options address-pool = 1  
  
admin> set clid = 5551234  
  
admin> write  
CONNECTION/edgar written
```

Si CLID-Auth-Mode está establecido en CLID-Prefer, la unidad TAOS envía un paquete Access-Request al servidor RADIUS con el número de ID de emisor como nombre de usuario, Ascend-CLID como contraseña y con Outbound-User especificado para Service-Type. Si la unidad encuentra una entrada de usuario RADIUS coincidente, como la que se muestra en el

ejemplo siguiente, la llamada se autentica y puede iniciar inmediatamente el servicio configurado:

```
5551234 Password = "Ascend-CLID", Service-Type = Outbound-User
Ascend-Require-Auth = Not-Require-Auth
```

Si no se encuentra ninguna entrada coincidente, el paquete Access-Reject no provoca la interrupción de la llamada. En lugar de ello, el usuario aún tiene permiso para conectarse, pero debe pasar por una autenticación de usuario normal. De forma similar, si el sistema encuentra una entrada coincidente en la que Ascend-Require-Auth está establecido en Require-Auth, valida el número CLID y, a continuación, procede a autenticar la contraseña de la llamada. Por ejemplo, los perfiles siguientes permiten al usuario realizar una llamada de entrada desde cualquiera de los números CLID especificados:

```
5551234 Password = "Ascend-CLID", Service-Type = Outbound-User
Ascend-Require-Auth = Require-Auth
5551235 Password = "Ascend-CLID", Service-Type = Outbound-User
Ascend-Require-Auth = Require-Auth
edgar Password = "test"
Service-Type = Framed-User,
Framed-Protocol = PPP,
Ascend-Assign-IP-Pool = 1,
Ascend-Route-IP = Route-IP-Yes
```

El perfil siguiente limita el usuario al número CLID especificado:

```
edgar Password = "test", Caller-Id = "5551235"
Service-Type = Framed-User,
Framed-Protocol = PPP,
Ascend-Assign-IP-Pool = 1,
Ascend-Route-IP = Route-IP-Yes
```

**Nota:** El perfil de usuario para la segunda fase de autenticación puede ser bien una entrada de usuario normal, como la que se muestra en el ejemplo anterior, o bien cualquier otro tipo de perfil de usuario válido. Por ejemplo, puede especificar la autenticación por tarjeta de testigo o la autenticación de contraseña UNIX.

## *Ejemplos en los que es preferible el DNIS*

El perfil Connection siguiente valida el número DNIS si éste aparece en la llamada. Si el número DNIS presentado por la llamada no coincide, se descarta la llamada. Si el número DNIS no aparece en la llamada, se autentica la contraseña del perfil.

```
admin> read conn edgar
CONNECTION/edgar read
admin> set ppp recv-password = test
admin> set ip-options address-pool = 1
admin> set callednumber = 1212
admin> write
CONNECTION/edgar written
```

Si CLID-Auth-Mode está establecido en DNIS-Prefer, la unidad TAOS envía un paquete Access-Request al servidor RADIUS con el número Client-Port-DNIS como nombre de usuario, Ascend-DNIS como contraseña y Outbound-User establecido en Service-Type. Si la unidad encuentra una entrada de usuario RADIUS coincidente, como la que se muestra en el

ejemplo siguiente, la llamada se autentica y puede iniciar inmediatamente el servicio configurado:

```
1212 Password = "Ascend-DNIS", Service-Type = Outbound-User
    Ascend-Require-Auth = Not-Require-Auth
```

Si no se encuentra ninguna entrada coincidente, el paquete Access-Reject no provoca la interrupción de la llamada. En lugar de ello, el usuario aún tiene permiso para conectarse, pero debe pasar por una autenticación de usuario normal. De forma similar, si el sistema encuentra una entrada coincidente en la que Ascend-Require-Auth está establecido en Require-Auth, valida el número DNIS y, a continuación, procede a autenticar la contraseña de la llamada. Por ejemplo, los perfiles siguientes permiten al usuario utilizar cualquiera de los números DNIS especificados:

```
1212 Password = "Ascend-DNIS", Service-Type = Outbound-User
    Ascend-Require-Auth = Require-Auth

1217 Password = "Ascend-DNIS", Service-Type = Outbound-User
    Ascend-Require-Auth = Require-Auth

edgar Password = "test"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Ascend-Assign-IP-Pool = 1,
    Ascend-Route-IP = Route-IP-Yes
```

El perfil siguiente limita el usuario al número DNIS especificado:

```
edgar Password = "test", Client-Port-DNIS = "1217"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Ascend-Assign-IP-Pool = 1,
    Ascend-Route-IP = Route-IP-Yes
```

**Nota:** El perfil de usuario para la segunda fase de autenticación puede ser bien una entrada de usuario normal, como la que se muestra en el ejemplo anterior, o bien cualquier otro tipo de perfil de usuario válido. Por ejemplo, puede especificar la autenticación por tarjeta de testigo o la autenticación de contraseña UNIX.

### *Ejemplos en los que el CLID es obligatorio*

Si CLID-Auth-Mode está establecido en CLID-Require, la autenticación previa de la llamada telefónica es obligatoria. Para los perfiles Connection locales, esto significa que cada perfil debe especificar el número CLID necesario. Si se recibe una llamada que no presenta la información necesaria, la unidad TAOS ni siquiera responde a la llamada.

Para las llamadas autenticadas por RADIUS, el ajuste CLID-Require significa que debe existir una entrada de usuario para cada ID de emisor válido. Si un usuario realiza una llamada de entrada desde un número de teléfono que no posee una entrada Ascend-CLID, la unidad TAOS no responde a la llamada. El usuario no tiene oportunidad de ser autenticado y no se le factura la llamada.

Los comandos siguientes configuran un perfil Connection local con un número CLID. Si el perfil Answer-Defaults especifica que el CLID es obligatorio, la llamada debe presentar un ID de emisor coincidente.

```
admin> read conn aydin
CONNECTION/aydin read
```

```
admin> set ppp recv-password = test
admin> set ip-options address-pool = 1
admin> set clid = 5551212
admin> write
CONNECTION/aydin written
```

Las entradas RADIUS siguientes identifican todos los ID de línea de llamada que son aceptables cuando el CLID es obligatorio:

```
5551212 Password = "Ascend-CLID", Service-Type = Outbound-User
      Ascend-Require-Auth = Require-Auth
5551213 Password = "Ascend-CLID", Service-Type = Outbound-User
      Ascend-Require-Auth = Require-Auth
5551214 Password = "Ascend-CLID", Service-Type = Outbound-User
      Ascend-Require-Auth = Require-Auth
5551215 Password = "Ascend-CLID", Service-Type = Outbound-User
      Ascend-Require-Auth = Require-Auth
5551216 Password = "Ascend-CLID", Service-Type = Outbound-User
      Ascend-Require-Auth = Require-Auth
```

Una llamada que llegue de cualquier otro número será rechazada. Dado que es necesaria una autenticación adicional, cada llamada requiere también su propio perfil de usuario, que puede o no limitar ese usuario en concreto a un único ID de emisor. En el ejemplo siguiente se permite al usuario realizar una llamada de entrada desde cualquiera de los números CLID especificados:

```
aydin Password = "test"
      Service-Type = Framed-User,
      Framed-Protocol = PPP,
      Ascend-Assign-IP-Pool = 1,
      Ascend-Route-IP = Route-IP-Yes
```

### *Ejemplos en los que el DNIS es obligatorio*

Si CLID-Auth-Mode está establecido en DNIS-Require, la autenticación previa de la llamada telefónica es obligatoria. Para los perfiles Connection locales, esto significa que cada perfil debe especificar el número DNIS necesario. Si se recibe una llamada que no presenta la información necesaria, la unidad TAOS no responde a la llamada.

Para las llamadas autenticadas por RADIUS, el ajuste DNIS-Require significa que debe existir una entrada de usuario para cada número DNIS válido. Por ejemplo, si se recibe una llamada de un número que no posee una entrada Ascend-DNIS, la unidad TAOS no responde a la llamada. El usuario no tiene oportunidad de ser autenticado y no se le factura la llamada.

Los comandos siguientes configuran un perfil Connection local con un número DNIS. Si el perfil Answer-Defaults especifica que el CLID es obligatorio, la llamada debe presentar un ID de emisor coincidente.

```
admin> read conn aydin
CONNECTION/aydin read
admin> set ppp recv-password = test
admin> set ip-options address-pool = 1
```

```
admin> set calledNumber = 1234
admin> write
CONNECTION/aydin written
```

Las entradas siguientes identifican todos los ID de línea de llamada que son aceptables cuando se requiere un DNIS:

```
1234 Password = "Ascend-DNIS", Service-Type = Outbound-User
    Ascend-Require-Auth = Require-Auth
2345 Password = "Ascend-DNIS", Service-Type = Outbound-User
    Ascend-Require-Auth = Require-Auth
3456 Password = "Ascend-DNIS", Service-Type = Outbound-User
    Ascend-Require-Auth = Require-Auth
4567 Password = "Ascend-DNIS", Service-Type = Outbound-User
    Ascend-Require-Auth = Require-Auth
5678 Password = "Ascend-DNIS", Service-Type = Outbound-User
    Ascend-Require-Auth = Require-Auth
```

Una llamada que llegue desde otro número será rechazada. Dado que es necesaria una autenticación adicional, cada llamada requiere su propio perfil de usuario, que puede o no limitar ese usuario en concreto a un único ID de emisor. En el ejemplo siguiente se permite al usuario realizar una llamada de entrada desde cualquiera de los números DNIS especificados:

```
aydin Password = "test"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Ascend-Assign-IP-Pool = 1,
    Ascend-Route-IP = Route-IP-Yes
```

El perfil siguiente limita el usuario al número DNIS especificado:

```
aydin Password = "test", Client-Port-DNIS = "5678"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Ascend-Assign-IP-Pool = 1,
    Ascend-Route-IP = Route-IP-Yes
```

## Devolución de llamada

Una devolución de llamada es una función en la que la unidad A realiza una llamada a la unidad B, la cual cuelga y vuelve a llamar a la unidad A. La función de devolución de llamada ayuda a garantizar que el emisor de origen no pague por la llamada y que la unidad TAOS establezca una conexión con un emisor conocido. El hecho de colgar y volver a llamar aporta un nivel de certeza de que la conexión se realiza con un usuario fiable, porque la unidad TAOS devuelve la llamada inmediatamente después de verificar el nombre y la contraseña del usuario. Para dar soporte a la devolución de llamada, la unidad TAOS debe permitir tanto las llamadas de entrada como las de salida.

La unidad TAOS da soporte a los tres modos de devolución de llamada siguientes:

- Devolución de llamada CLID o DNIS (anteriormente denominada devolución de llamada CLID/DNIS Ascend). La unidad TAOS detecta la devolución de llamada mientras suena el timbre de una llamada de entrada mediante el elemento informativo CLID o DNIS. La

unidad TAOS no responde a la llamada (es decir, no descuelga) y no se cobra por ella al emisor de origen.

- **Devolución de llamada Ascend.** Este modo es parecido al de la devolución de llamada CLID o DNIS, excepto que la unidad TAOS detecta la devolución de llamada durante la fase de autenticación (después de descolgar) mediante el nombre de usuario y la contraseña del perfil Connection. La llamada *inicial* se cobra al emisor de origen.
- **Protocolo de control de devolución de llamada (CBCP).** Este modo fue desarrollado por Microsoft para cubrir la necesidad de una mayor seguridad en las conexiones PPP. La opción de devolución de llamada definida en el documento RFC 1570 no es tan segura como otras formas de devolución de llamada, ya que la autenticación se efectúa sólo durante la llamada inicial y *no* durante la devolución de llamada. La devolución de llamada CBCP, igual que la devolución de llamada Ascend, permite una conexión más segura, porque la devolución de llamada se produce *después* de la autenticación.

CBCP ofrece unas funciones que no están disponibles con la devolución de llamada estándar definida en el documento RFC 1570. El extremo del cliente permite un retardo configurable para que los usuarios tengan tiempo de inicializar los módems o activar el software de soporte antes de que la unidad TAOS llame al cliente. La unidad TAOS no permite que un perfil Connection o un perfil RADIUS CBCP sea compartido por más de un cliente Windows.

La unidad TAOS detecta y negocia la devolución de llamada CBCP mediante el protocolo CBCP durante la negociación PPP. Puede configurar la unidad TAOS para que el usuario pueda negociar el número de teléfono de la devolución de llamada. La devolución de llamada CBCP ocupa el lugar del servidor de acceso remoto (RAS) para devolver la llamada al cliente RAS (Windows 95).

## Características de la devolución de llamada

La devolución de llamada en la unidad TAOS presenta las características siguientes:

- **Autenticación local o externa:** Los perfiles Connection para configurar la autenticación pueden ser locales o externos (en el servidor RADIUS). Para cada realización de devolución de llamada, la unidad TAOS accede a RADIUS una sola vez durante la autenticación externa. La unidad TAOS no solicita atributos RADIUS durante el proceso de devolución de llamada.
- **Conexiones permanentes, de relé de trama o X.25:** La unidad TAOS no da soporte a la devolución de llamada a través de conexiones permanentes, de relé de trama o X.25.
- **Seguridad que implica rutas y filtros externos:** La unidad TAOS da soporte a la devolución de llamada, así como a filtros externos y rutas externas, pero las conexiones están limitadas a un máximo de 16 filtros externos y 10 rutas externas por perfil Connection.
- **Seguridad de túnel ATMP:** La unidad TAOS da soporte al protocolo de gestión de túneles de Ascend (ATMP) y a los tres tipos de modos de devolución de llamada. La unidad TAOS no crea el túnel durante la llamada inicial, sino cuando la unidad TAOS (agente externo) devuelve la llamada al origen móvil.
- **Seguridad:** Puede utilizar la devolución de llamada para ampliar la seguridad, y la unidad TAOS desconecta todas las llamadas de entrada que tienen la devolución de llamada activada. Si la unidad TAOS no puede registrar la conexión de la devolución de llamada (por ejemplo, debido a una falta de recursos internos), la unidad TAOS desconecta la llamada.
- **Espera de devolución de llamada:** Esta función proporciona una devolución de llamada a la inversa en la unidad TAOS. La unidad TAOS llama a una unidad remota, que devuelve

la llamada a la unidad TAOS. Cuando la unidad TAOS rechaza la llamada, la unidad TAOS desactiva el proceso de llamada de salida (para la unidad a la que se ha llamado) hasta que la unidad vuelve a llamar o cuando han transcurrido 90 segundos.

- *Mensajes de registro de devolución de llamada creados:* Hay cinco nuevos mensajes de registro que proporcionan información acerca de los procesos de devolución de llamada. (Consulte la publicación *Guía de administración de APX 8000/MAX TNT/DSLNT*.)
- *Códigos de causa de desconexión:* Las llamadas de entrada registradas para la devolución de llamada se desconectan con el código de causa 6 o 102. (Consulte la publicación *Guía de administración de APX 8000/MAX TNT/DSLNT*.)
- *Comandos de depuración de devolución de llamada:* La unidad TAOS da soporte a un nuevo comando de devolución de llamada para proporcionar información de diagnóstico. (Consulte la publicación *Guía de administración de APX 8000/MAX TNT/DSLNT*.)
- *Ruteo especial:* La unidad TAOS puede rutear una devolución de llamada a través de un tipo de recurso diferente a la llamada inicial. Por ejemplo, la unidad TAOS puede aceptar la llamada inicial de una tarjeta de módem y la unidad TAOS puede realizar la llamada de salida a través de una tarjeta de acceso mixto.

## Información general sobre la configuración de la devolución de llamada

Si bien es posible combinar los modos de devolución de llamada para una plataforma concreta, no lo es combinar tipos de devolución de llamada dentro de un mismo perfil Connection. Si selecciona más de un tipo de devolución de llamada, la unidad TAOS realiza la devolución de llamada siguiendo este orden: devolución de llamada CLID o DNIS, devolución de llamada Ascend y, finalmente, devolución de llamada CBCP. La unidad TAOS permite la autenticación CLID o DNIS en combinación con la devolución de llamada CBCP. Las funciones de devolución de llamada y espera de devolución de llamada no pueden mezclarse en un mismo perfil, ya que no es posible esperar y efectuar simultáneamente una devolución de llamada para un perfil determinado.

Para cada modo de devolución de llamada, puede seleccionarse un índice de agrupaciones de direcciones IP en lugar de una dirección IP estática. El índice de agrupaciones permite al usuario obtener una dirección IP dinámica de una agrupación. La unidad TAOS asigna la dirección IP cuando devuelve la llamada al usuario.

## Configuración de la devolución de llamada CLID o DNIS

Con CLID, se recibe una llamada y la unidad TAOS recupera el perfil coincidente con la información Calling-Station-ID del paquete de configuración de ISDN. La unidad TAOS desconecta la llamada de entrada sin responderla e inicia la devolución de llamada. Los dispositivos negocian el PPP. Con DNIS, la unidad TAOS recupera el perfil coincidente con el Called-Station-ID. El emisor de origen no puede detectar que la razón de la desconexión de la llamada es la devolución de llamada pendiente, a menos que haya activado la función de espera de devolución de llamada. La función de espera de devolución de llamada le permite hacer que el emisor de origen espere 90 segundos antes de volver a marcar la conexión.



### *Configuración de parámetros globales*

Debe realizar una configuración global para la devolución de llamada CLID o DNIS dentro del perfil Answer-Defaults:

<b>Parámetro de Answer-Defaults</b>	<b>Ajustes obligatorios</b>
CLID-Auth-Mode	CLID-Require o DNIS-Require son ajustes obligatorios.

### *Configuración del perfil Connection local*

Puede establecer una configuración local a través del perfil Connection. A continuación se muestran algunos ajustes habituales (y obligatorios, si se indica) del perfil Connection para una devolución de llamada CLID o DNIS para un usuario concreto:

<b>Parámetro del perfil Connection</b>	<b>Ajuste habitual</b>
Active	Yes.
Encapsulation-Protocol	PPP. Como alternativa, puede seleccionar MP o MPP.
Dial-Number	Número que debe marcarse durante la fase de devolución de llamada.
CLID	Número CLID. Para dar soporte a la devolución de llamada CLID, debe especificar un valor válido para CLID.
Telco-Options>Callback	Yes.
Telco-Options>Data-Service	Por ejemplo, Modem.
Telco-Options>Dialout-Allowed	Yes.
Telco-Options>Delay-Callback	Por ejemplo, 10. Este ajuste indica el número de segundos que deben transcurrir antes de que la unidad TAOS vuelva a llamar al usuario.
CalledNumber	Número DNIS. Para dar soporte a la devolución de llamada DNIS, debe especificar un valor válido para CalledNumber.

### *Configuración del perfil Connection externo*

A continuación se muestran algunos ajustes habituales (y obligatorios, si se indica) del perfil Connection de RADIUS para una devolución de llamada CLID o DNIS.

<b>Atributo RADIUS</b>	<b>Ajuste habitual</b>
Password (2)	Contraseña para el número CLID. Por ejemplo, Ascend-CLID.
User-Service (6)	Dialout-Framed-User (5).
Ascend-Require-Auth (201)	Require-Auth (1).
Ascend-Callback (246)	Callback-Yes (1).

## Métodos de autenticación

### Devolución de llamada

---

Atributo RADIUS	Ajuste habitual
Caller-Id (31)	Especifica el número que realiza la llamada para la autenticación de ID de línea de llamada (CLID). Indica el número de teléfono del usuario que desea conectarse a la unidad TAOS.
Framed-Protocol (7)	PPP (1), MP o MPP (256).
Framed-Address (8)	Dirección IP de un emisor. RADIUS puede autenticar un emisor de entrada haciendo coincidir la dirección IP del usuario con la especificada en el perfil de usuario. Por ejemplo, 192.168.143.2
Framed-Netmask (9)	Máscara de subred para el emisor en Framed-Address. Por ejemplo, 255.255.255.255.
Ascend-Dial-Number (227)	Número de teléfono que marca la unidad TAOS.
Ascend-Data-Svc (247)	Switched-Modem (42). Especifica el tipo de servicio de datos que utiliza el enlace para las llamadas de salida.
Ascend-Send-Auth (231)	Send-Auth-PAP (1).
Ascend-Send-Passwd (232)	Contraseña que el servidor RADIUS envía al extremo remoto de una conexión en una llamada de salida. Por ejemplo, Ascend.
Ascend-Route-IP (228)	Route-IP-Yes (1) o Route-IP-No (0). Si se establece este atributo en Route-IP-Yes (el valor predeterminado), el ruteo IP se activa para el perfil. Si se establece en Route-IP-No, el ruteo IP se desactiva para el perfil.

Dado que la unidad TAOS realiza una única petición RADIUS, todos los parámetros deben estar presentes en el perfil.

### Configuración de la espera de devolución de llamada

Con la devolución de llamada CLID o DNIS, la unidad TAOS cuelga la llamada entrante de un emisor e inicia inmediatamente una devolución de llamada. La devolución de llamada asegura que una conexión se realiza con un destino conocido. Para las llamadas de salida, puede configurarse el emisor de la llamada para que espere una devolución de llamada de la máquina a la que llama. La función de espera de devolución de llamada evita que el emisor de la llamada tenga que realizar una llamada de salida más de una vez antes de que se le devuelva la llamada.

Por ejemplo, una unidad TAOS inicia una llamada a una unidad Pipeline. La unidad Pipeline recibe un mensaje ISDN de configuración de entrada, reconoce el CLID y rechaza la llamada de entrada con un mensaje de desconexión. Si la unidad TAOS tiene activada la función de espera de devolución de llamada, espera durante 90 segundos a que la unidad Pipeline devuelva la llamada. Si esta función no está activada, la unidad TAOS puede determinar que la llamada no se ha conectado y volver a efectuarla inmediatamente.

Si establece Expect-Callback en Yes en el dispositivo que llama, todas las llamadas de salida que no se conecten por la razón que sea se colocan en una lista que no permite más llamadas a ese destino durante 90 segundos. Este retardo proporciona al dispositivo al que se llama la oportunidad de completar la devolución de llamada.

Para configurar la devolución de llamada CLID o DNIS para la espera de devolución de llamada, hay dos parámetros de conexión local que requieren configuración:

**Parámetro del perfil Connection Ajuste**

Telco-Options>Callback	No
Telco-Options>Expect-Callback	Yes

A continuación se muestran algunos ajustes habituales del perfil Connection externo para la espera de devolución de llamada:

<b>Atributo RADIUS</b>	<b>Ajuste habitual</b>
Password (2)	Ascend.
User-Service (6)	Dialout-Framed-User (5).
Ascend-Dial-Number (227)	Número de teléfono que marca la unidad TAOS.
Framed-Protocol (7)	PPP (1).
Ascend-Data-Svc (247)	Switched-64K (2). Especifica el tipo de servicio de datos que utiliza el enlace para las llamadas de salida.
Ascend-Dialout-Allowed (131)	Dialout-Allowed (1).
Framed-Address (8)	Dirección IP de un emisor. RADIUS puede autenticar un emisor de entrada haciendo coincidir la dirección IP del usuario con la especificada en el perfil de usuario. Por ejemplo, 4.5.6.7.
Framed-Netmask (9)	Máscara de subred para el emisor en Framed-Address. Por ejemplo, 255.255.255.0.
Ascend-Metric (225)	Número entero que especifica el recuento de saltos virtuales de una ruta IP. El ajuste predeterminado es 7.
Ascend-Send-Auth (231)	Send-Auth-PAP (1).
Ascend-Send-Passwd (232)	Contraseña que el servidor RADIUS envía al extremo remoto de una conexión en una llamada de salida. Por ejemplo, Ascend.
Ascend-Expect-Callback (149)	Expect-Callback-Yes (1).
Ascend-Route-IP (228)	Route-IP-Yes (1) o Route-IP-No (0). Si se establece este atributo en Route-IP-Yes (el valor predeterminado), el ruteo IP se activa para el perfil. Si se establece en Route-IP-No, el ruteo IP se desactiva para el perfil.

## **Configuración de la devolución de llamada Ascend**

La unidad TAOS efectúa una devolución de llamada Ascend después de negociar por completo la conexión PPP. Cuando una unidad TAOS es el dispositivo al que se llama, la llamada llega y se produce una autenticación normal. A continuación, la unidad TAOS desconecta la llamada e inicia la devolución de llamada, se desconecta la llamada y la llamada negocia el PPP. Cuando una unidad TAOS es el dispositivo que llama, espera una devolución de llamada si la conexión se desarrolla normalmente y se desconecta antes de que se transmita algún dato. La unidad TAOS no vuelve a marcar durante un número especificado de segundos.

### *Configuración de parámetros globales*

La configuración global de la devolución de llamada Ascend se realiza en el perfil Answer-Defaults. A continuación se muestran algunos ajustes habituales de configuración global para la devolución de llamada Ascend:

<b>Parámetro de Answer-Defaults</b>	<b>Ajuste habitual</b>
CLID-Auth-Mode	No puede establecerse en CLID-Require ni DNIS-Require. Si se establece el parámetro en uno de estos ajustes, se efectúa una devolución de llamada CLID o DNIS en lugar de una devolución de llamada Ascend.
PPP-Answer > Enable	Yes.
PPP-Answer > Receive-Auth-Mode	Any-PPP-Auth.
PPP-Answer > CBCP-Enable	Este ajuste no es obligatorio para la devolución de llamada Ascend.

### *Configuración del perfil Connection local*

La configuración local se establece en el perfil Connection. A continuación se muestran ejemplos de ajustes habituales del perfil Connection para una devolución de llamada Ascend:

<b>Parámetro del perfil Connection</b>	<b>Ajuste habitual</b>
Active	Yes.
Encapsulation-Protocol	PPP. Encapsulation-Protocol también puede establecerse en MP o MPP.
Dial-Number	Este parámetro representa el número que se debe marcar durante la fase de devolución de llamada de salida.
Telco-Options>Callback	Yes. Si especifica CBCP-Enable, tiene prioridad Telco Options > Callback.
Telco-Options > Data-Service	Modem.
Telco-Options > Dialout-Allowed	Yes.
Telco-Options > Delay-Callback	Por ejemplo, 10. Este ajuste indica el número de segundos que deben transcurrir antes de que la unidad TAOS vuelva a llamar al usuario.
PPP-Options > Send-Auth-Mode	Pap-PPP-Auth. Puede utilizarse otra autenticación PPP (o ninguna), según el extremo remoto.
PPP-Options > Send-Password	Por ejemplo, Ascend.
PPP-Options > Recv-Password	Por ejemplo, Ascend.
PPP-Options > CBCP-Enabled	Este parámetro no es obligatorio para la devolución de llamada Ascend.

### *Configuración del perfil Connection externo*

A continuación se muestran configuraciones RADIUS habituales para una devolución de llamada Ascend. Las configuraciones visualizadas asumen la utilización de filtros externos.

<b>Atributo RADIUS</b>	<b>Ajuste habitual</b>
Password (2)	Contraseña del usuario. Por ejemplo, Ascend.
User-Service (6)	Framed-User (2).
Ascend-Callback (246)	Callback-Yes (1).
Framed-Protocol (7)	PPP (1), MP o MPP (256).
Framed-Address (8)	Dirección IP de un emisor. RADIUS puede autenticar un emisor de entrada haciendo coincidir la dirección IP del usuario con la especificada en el perfil de usuario. Por ejemplo, 4.5.6.7.
Framed-Netmask (9)	Máscara de subred para el emisor en Framed-Address. Por ejemplo, 255.255.255.255.
Ascend-Dial-Number (227)	Número de teléfono que marca la unidad TAOS.
Ascend-Data-Svc (247)	Switched-64K (2). Especifica el tipo de servicio de datos que utiliza el enlace para las llamadas de salida.
Ascend-Send-Auth (231)	Por ejemplo, Send-Auth-PAP (1). Ajuste optativo.
Ascend-Send-Passwd (232)	Por ejemplo, Ascend. Ajuste optativo. Contraseña que el servidor RADIUS envía al extremo remoto de una conexión en una llamada de salida. Si el valor no coincide con el valor del extremo remoto (en Connection > PPP Options > Recv-Password o en el perfil de usuario RADIUS), el sistema remoto rechaza la llamada.
Ascend-Data-Filter (242)	<p>Ajuste optativo. El parámetro Ascend-Data-Filter especifica las características de un filtro de datos en un perfil de usuario RADIUS. La unidad TAOS utiliza el filtro sólo cuando realiza o recibe una llamada asociada al perfil que incluye la definición del filtro.</p> <p>IP Out Forward. Este ajuste optativo especifica un filtro IP para filtrar los paquetes que salen de la unidad TAOS y determina que la unidad TAOS debe enviar los paquetes que coincidan con el filtro.</p> <p>Generic Out Forward 12 ffff 0806. Este ajuste optativo especifica un filtro genérico para filtrar los paquetes que salen de la unidad TAOS y determina que la unidad TAOS debe enviar los paquetes que coincidan con el filtro. El desplazamiento, la máscara y el valor se especifican a continuación.</p> <p>Generic Out Drop 0 0 0. Este ajuste optativo especifica un filtro genérico para filtrar los paquetes que salen de la unidad TAOS y determina que la unidad TAOS debe descartar los paquetes que coincidan con el filtro. El desplazamiento, la máscara y el valor se especifican a continuación.</p>
Ascend-Route-IP (228)	Route-IP-Yes (1) o Route-IP-No (0). Route-IP-Yes (el valor predeterminado) activa el ruteo IP para el perfil. Route-IP-No desactiva el ruteo IP para el perfil.

## Configuración de una devolución de llamada CBCP

CBCP es una opción que se negocia durante la fase de protocolo de control de enlaces (LCP) de la negociación PPP. Aunque se configure el soporte para el CBCP en todo el sistema de la unidad TAOS, no todas las conexiones deben negociar la devolución de llamada CBCP. Esta opción se realiza mediante los parámetros del perfil Answer-Defaults y de cada perfil Connection. El extremo al que se llama y el extremo que realiza la llamada en una sesión PPP inician la autenticación una vez que se les comunica que se va a utilizar el CBCP.

La unidad TAOS utiliza el nombre de usuario y la contraseña para enlazar un emisor con un perfil Connection o un perfil de usuario RADIUS específicos. Los parámetros de CBCP configurados en el perfil Connection especifican variables para la devolución de llamada. Si, en cualquier punto, el cliente y la unidad TAOS están en desacuerdo acerca de algún parámetro de CBCP, la unidad TAOS puede descartar la conexión. La unidad TAOS no permite que un perfil Connection o un perfil RADIUS CBCP se comparta por varios clientes Windows.

Según la configuración, bien el cliente o bien la unidad TAOS pueden proporcionar el número de teléfono al que se devuelve la llamada.

En la devolución de llamada CBCP, un emisor se conecta a la unidad TAOS y se inician las negociaciones LCP. La unidad TAOS verifica que se ha activado el modo CBCP en el perfil. Si el emisor y la unidad TAOS negocian satisfactoriamente la opción LCP para el CBCP, éste se iniciará después de la autenticación. El emisor se autentica a sí mismo para la unidad TAOS. Si la autenticación falla, la unidad TAOS interrumpe la conexión. Durante el CBCP, el cliente también proporciona a la unidad TAOS el número de segundos (un valor configurable) que debe esperar antes de iniciar la devolución de llamada y, si procede, el número de teléfono. La unidad TAOS retarda la devolución de la llamada basándose en la negociación anterior. La unidad TAOS marca el número del cliente aplicando la información del mismo perfil utilizado durante la negociación.

### *Configuración de parámetros globales*

Los parámetros globales se encuentran en el perfil Answer-Defaults. El parámetro CBCP-Enable y dos atributos RADIUS análogos, Ascend-CBCP-Enable y Ascend-CBCP-Mode, dan soporte a la devolución de llamada CBCP. El parámetro CBCP-Enable activa el protocolo CBCP para las llamadas PPP de entrada.

A continuación se muestran algunos ajustes habituales de configuración global para la devolución de llamada CBCP:

<b>Parámetro de Answer-Defaults</b>	<b>Ajuste habitual</b>
CLID-Auth-Mode	CLID-Require o DNIS-Require no son ajustes obligatorios.
PPP-Answer > Enable	Yes.
PPP-Answer > Receive-Auth-Mode	Any-PPP-Auth.
PPP-Answer > CBCP-Enable	Yes es obligatorio.

### *Configuración del perfil Connection local*

La configuración local se especifica en el perfil Connection. A continuación se muestran ejemplos de ajustes habituales del perfil Connection para una devolución de llamada CBCP para un usuario concreto:

<b>Parámetro del perfil Connection</b>	<b>Ajuste</b>
--	---------------

Active	Yes.
Encapsulation-Protocol	PPP. Encapsulation-Protocol también puede establecerse en MP o MPP.
Dial-Number	Si el modo CBCP está establecido en CBCP-User-Number o CBCP-All, puede proporcionarse el número de teléfono de devolución de llamada durante la negociación de la devolución de llamada. Este ajuste puede dejarse en blanco.
Telco-Options > Callback	No.
Telco-Options > Data-Service	Por ejemplo, Modem.
Telco-Options > Dialout-Allowed	Yes.
PPP-Options > Send-Auth-Mode	El ajuste No es obligatorio. Se utiliza con Windows 95, Windows 98 y Windows NT.
PPP-Options > Recv-Password	Por ejemplo, Ascend.
PPP-Options > CBCP-Enabled	Yes.
PPP-Options > Trunk-Group-Callback-Control	Por ejemplo, 9. Si el emisor proporciona el número de teléfono, establezca este parámetro con el valor que la unidad TAOS agrega al principio del número proporcionado por el usuario al devolver la llamada.
PPP-Options > Mode-Callback-Control	CBCP-User-Number. Este parámetro tiene los siguientes valores posibles: CBCP-No-Callback, CBCP-User-Number, CBCP-Profile-Num y CBCP-All.

### *Configuración del perfil Connection externo*

A continuación se muestran las configuraciones RADIUS habituales para una devolución de llamada CBCP:

<b>Atributo RADIUS</b>	<b>Ajuste habitual</b>
Password (2)	Contraseña para el usuario CBCP. Por ejemplo, Ascend.
User-Service (6)	Framed-User (2).
Framed-Protocol (7)	PPP (1), MP (2) o MPP (256).
Ascend-Dial-Number (227)	Número de teléfono que utiliza la unidad TAOS para volver a llamar cuando el modo CBCP está establecido en CBCP-Profile-Num o CBCP-All.
Ascend-Data-Svc (247)	Normalmente Switched-Modem (42), para CBCP. Especifica el tipo de servicio de datos que utiliza el enlace para las llamadas de salida.

<b>Atributo RADIUS</b>	<b>Ajuste habitual</b>
Ascend-Send-Auth (231)	Por ejemplo, Send-Auth-None (0). No se trata de un ajuste obligatorio.
Ascend-CBCP-Enable (112)	CBCP-Enabled (1).
Ascend-CBCP-Mode (113)	CBCP-Profile-Callback (3).
Ascend-Assign-IP-Pool (218)	1 (el valor predeterminado). Número entero que corresponde a una agrupación de direcciones. Con el ajuste 0, RADIUS selecciona una dirección de cualquier agrupación que tenga una dirección disponible.
Ascend-Route-IP (228)	Route-IP-Yes (1) o Route-IP-No (0). Route-IP-Yes (el valor predeterminado) activa el ruteo IP para el perfil. Route-IP-No desactiva el ruteo IP para el perfil.

El ajuste Ascend-CBCP-Trunk-Group no es obligatorio. Este ajuste resulta útil cuando el emisor introduce el número de devolución de llamada y se utilizan grupos de línea troncal.

### *Ejemplos de configuración de una devolución de llamada tras la autenticación CLID*

Los comandos siguientes definen un perfil Connection que utiliza CLID para la autenticación previa y que, a continuación, vuelve a llamar al extremo distante:

```
admin> read conn clara-w95
CONNECTION/clara-w95 read
admin> set clid = 5105551234
admin> set dial-number = 95551212
admin> set encaps = ppp
admin> set ppp send-auth-mode = pap-ppp-auth
admin> set ppp send-password = test
admin> set ip-options remote-address = 10.10.11.12
admin> set session callback = yes
admin> write
CONNECTION/clara-w95 written
```

A continuación se muestra un perfil RADIUS equivalente:

```
5105551234 Password = "Ascend-CLID"
User-Name = "clara-w95",
Service-Type = Framed-User,
Framed-Protocol = PPP,
Framed-IP-Address = 10.10.11.12,
Ascend-Dial-Number = "95551212",
Ascend-Send-Auth = Send-Auth-PAP,
Ascend-Send-Secret = "test",
Ascend-Callback = Callback-Yes
```



### *Ejemplos de configuración de una devolución de llamada tras la autenticación*

Los comandos siguientes definen un perfil Connection que efectúa una autenticación PPP y que, a continuación, vuelve a llamar al extremo distante:

```
admin> read conn clara-w95
CONNECTION/clara-w95 read
admin> set dial-number = 95551212
admin> set encaps = ppp
admin> set ppp recv-password = test
admin> set ppp send-auth-mode = pap-ppp-auth
admin> set ppp send-password = test
admin> set ip-options remote-address = 10.10.11.12
admin> set session callback = yes
admin> write
CONNECTION/clara-w95 written
```

A continuación se muestra un perfil RADIUS equivalente:

```
clara-w95 Password = "test"
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Framed-IP-Address = 10.10.11.12,
  Ascend-Dial-Number = "95551212",
  Ascend-Send-Auth = Send-Auth-PAP,
  Ascend-Send-Secret = "test",
  Ascend-Callback = Callback-Yes
```



# Opciones de autorización

## B

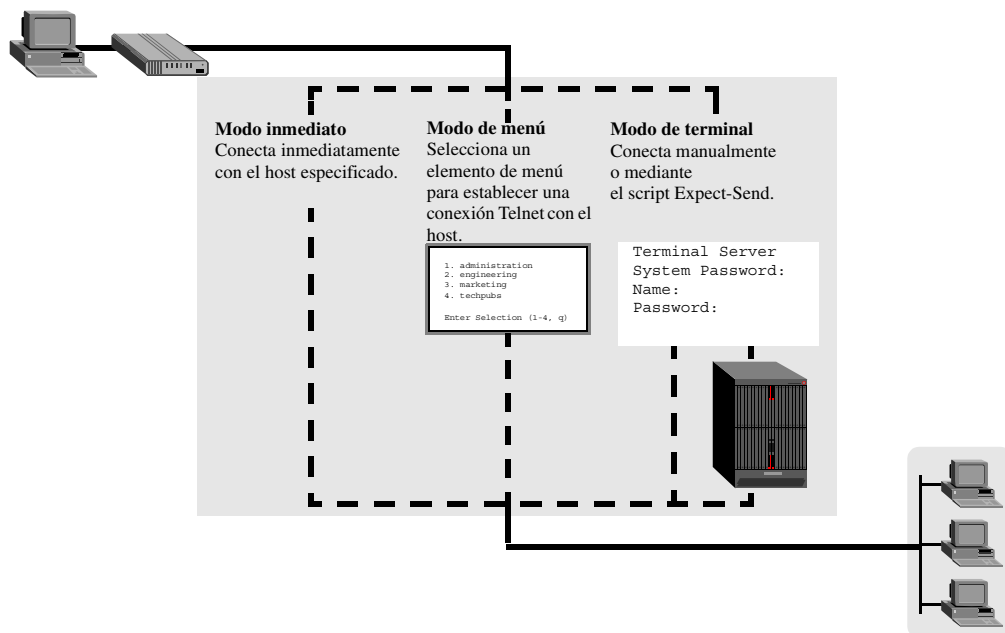
Introducción .....	B-1
Autorización de un servicio de conexión de modo inmediato .....	B-2
Autorización del acceso en modo de menú .....	B-4
Autorización de conexiones en modo de terminal .....	B-10
Autorización del acceso a la gestión SNMP .....	B-16

## ***Introducción***

Los procedimientos de autorización definen las acciones que puede efectuar un usuario una vez que obtiene el acceso a su red. La autorización tiene lugar *después* de que se haya completado la autenticación. Los usuarios de llamada de entrada acceden a la red mediante el software de servidor de terminales o mediante el software SNMP (Protocolo de gestión de red simple). Si desea obtener información detallada acerca del acceso SNMP, consulte “Autorización del acceso a la gestión SNMP” en la página B-16.

En la mayoría de los casos, el servidor de terminales se utiliza como paso intermedio hacia el acceso a un host de red, en lugar de como interfaz por derecho propio. Admite tres modos de acceso por llamada de entrada, cada uno de los cuales autoriza acciones específicas, como se muestra en la Figura B-1.

Figura B-1. Modos de acceso mediante el servidor de terminales



El *modo inmediato* redirige la corriente de datos de entrada hacia un host de conexión especificado. Para ello, según el servicio especificado, puede utilizar una sesión Telnet, TCP o Rlogin del tipo BSD.

El *modo de menú* visualiza un menú de las acciones autorizadas. Si la llamada está autenticada según RADIUS, un administrador puede configurar un menú personalizado de comandos autorizados. En el caso de las llamadas autenticadas localmente, el menú se limita a algunos hosts de conexión.

El *modo de terminal* accede a la línea de comandos del servidor de terminales. Hay muchos entornos que no autorizan el acceso por llamada de entrada al indicador de línea de comandos, debido al posible riesgo de seguridad. Sin embargo, puede incluir un comando de servidor de terminales, como SLIP o PPP, en la secuencia de comandos Expect-Send del módem para que ejecute automáticamente el comando autorizado e invoque una sesión de modo de paquete como parte de la secuencia de conexión (en el caso de otros comandos, como Telnet, TCP o Rlogin del tipo BSD, el modo inmediato proporciona una manera más segura de redirigir la corriente de datos de entrada).

## Autorización de un servicio de conexión de modo inmediato

En el modo inmediato, el servidor de terminales utiliza TCP, Rlogin o Telnet para enviar la corriente de datos de las llamadas de entrada directamente a un host para una sesión de conexión.

## Utilización del perfil Terminal-Server

A continuación se muestran los parámetros (con ajustes de ejemplo) necesarios para configurar el modo inmediato:

```
[in TERMINAL-SERVER:immediate-mode-options]
service = telnet
telnet-host-auth = no
host = 10.2.3.4
port = 56
```

Parámetro	Especifica
Service	Activa y desactiva el modo inmediato. También especifica el servicio que se debe utilizar para conectar con el host especificado. El ajuste predeterminado None desactiva el modo inmediato. Otros valores son Telnet, Raw-TCP y Rlogin.
Telnet-Host-Auth	Activa y desactiva el manejo de las llamadas PPP asíncronas en modo inmediato. Con el ajuste No, las llamadas PPP asíncronas fallan. Con el ajuste Yes, el servidor de terminales dirige las llamadas PPP asíncronas al host especificado en lugar de al software del ruteador.
Host	Nombre de host o dirección IP a los que los usuarios estarán conectados en el modo inmediato de servidor de terminales.
Port	Número de puerto TCP que se va a utilizar para las conexiones.

Por ejemplo, los comandos siguientes permiten conexiones Telnet inmediatas a la dirección de host 10.2.3.4 para conexiones del servidor de terminales, incluidas las conexiones PPP asíncronas:

```
admin> read terminal-server
TERMINAL-SERVER read

admin> set immediate service = telnet

admin> set immediate telnet-host-auth = yes

admin> set immediate host = 10.2.3.4

admin> set immediate port = 23

admin> write
TERMINAL-SERVER written
```

Si la llamada de entrada es TCP-Clear (no encapsulada) o V.120, la llamada se autentica en el servidor de terminales de la forma habitual y, a continuación, se dirige al host Telnet, en que el usuario se conecta de acuerdo con la secuencia de conexión utilizada en ese host.

Si la llamada de entrada utiliza la encapsulación PPP, la unidad TAOS deberá autenticar la llamada mediante PAP o CHAP y, a continuación, utilizar el software del ruteador para establecer una sesión PPP asíncrona. Para evitar que se redirija la llamada al ruteador, de modo que el usuario pueda conectarse con el host Telnet, debe establecer el parámetro Telnet-Host-Auth en el valor Yes.

## Utilización de perfiles Connection

Puede activar conexiones TCP inmediatas de forma general en el perfil Terminal-Server utilizando el servicio TCP en el modo inmediato, como se describe en esta sección. De forma alternativa puede configurar TCP-Clear para una conexión específica, como se describe en “Conexiones TCP-Clear” en la página 1-25.

## Uso de perfiles RADIUS

RADIUS utiliza los pares atributo-valor siguientes para especificar una conexión en modo inmediato:

Atributo	Valor
Login-Service (15)	Tipo de servicio de conexión permitido al emisor. Los valores válidos son Telnet (0), Rlogin (1) y TCP-Clear (2).
Login-Host (14)	Dirección IP del host de conexión.
Login-TCP-Port (16)	Puerto TCP de destino en el host de conexión especificado (un número entero del 1 al 65535). El valor predeterminado es 23.
Service-Type (6)	Especifica si el enlace puede utilizar servicios entramados o no entramados. Los valores válidos son Login-User (1), Framed-User (2) y Outbound-User (5).

Si establece el atributo Login-Service en Telnet o TCP-Clear y no especifica ningún valor para el atributo Login-Host, la respuesta de la unidad TAOS dependerá del valor del parámetro Auth-TS-Secure en el subperfil Rad-Auth-Client del perfil External-Auth. Si Auth-TS-Secure tiene el valor Yes (el valor predeterminado), unidad TAOS descarta la llamada. Si Auth-TS-Secure tiene el valor No, unidad TAOS permite que el usuario acceda a la interfaz del servidor de terminales. Para obtener información detallada acerca del parámetro Auth-TS-Secure, consulte la publicación *APX 8000/MAX TNT/DSLNT Reference (Referencia de APX 8000/MAX TNT/DSLNT)*.

A continuación se muestra un perfil RADIUS que especifica una sesión Telnet inmediata para el usuario:

```
joel Password = "localpw"  
  Service-Type = Login-User,  
  Login-Service = Telnet  
  Login-Host = 10.2.3.4,  
  Login-TCP-Port = 56
```

## Autorización del acceso en modo de menú

En el modo de menú, el servidor de terminales visualiza un menú de hosts autorizados o, si la llamada está autenticada por RADIUS, un menú de los comandos autorizados u otros elementos. Los usuarios inician una sesión Telnet seleccionando un host del menú.

## Ajustes del perfil Terminal-Server

A continuación se muestran los parámetros que le permiten describir hasta cuatro hosts a los que podrán acceder los usuarios en modo de menú. Los ajustes que aparecen son los valores predeterminados.

```
[in TERMINAL-SERVER:menu-mode-options]
start-with-menus = no
toggle-screen = no
remote-configuration = no
text-1 = ""
host-1 = ""
text-2 = ""
host-2 = ""
text-3 = ""
host-3 = ""
text-4 = ""
host-4 = ""
```

Parámetro	Especifica
Start-With-Menus	Activa y desactiva el modo de menú después de la autenticación. El comando Menu en modo de terminal puede invocar un modo de menú independientemente de este ajuste.
Toggle-Screen	Activa y desactiva la alternancia entre el modo de menú y el modo de terminal. Con el ajuste Yes, los usuarios pueden pulsar 0 (la tecla con el cero) en el menú para pasar a la línea de comandos del servidor de terminales. Consulte “Autorización del acceso a la gestión SNMP” en la página B-16 para ver cuestiones relacionadas.
Remote-Configuration	Activa y desactiva la recuperación de la definición del menú desde RADIUS.
Text- <i>N</i>	Texto descriptivo relativo a un host (normalmente, un nombre de host o una descripción del host).
Host- <i>N</i>	Direcciones IP de hasta cuatro hosts. El servidor de terminales asigna un número a cada entrada. Cuando el usuario selecciona un número, el servidor de terminales inicia una sesión Telnet con el host en la dirección IP especificada.

## Ajustes de un perfil initial-banner RADIUS

Un perfil `initial-banner` es un perfil de pseudousuario cuya primera línea tiene el formato siguiente:

```
initial-banner-name-N Password = "ascend", Service-Type = Outbound-User
```

El argumento *name* optativo es el nombre de sistema de la unidad TAOS (especificado por el parámetro Name en el perfil System) y *N* es un número de una serie secuencial que empieza por 1. Asegúrese de que no faltan números en la serie especificada por *N*. Si existe un espacio vacío en la secuencia de números, la unidad TAOS deja de recuperar los perfiles cuando encuentra dicho espacio.

## Opciones de autorización

### Autorización del acceso en modo de menú

---

El par atributo-valor siguiente puede utilizarse para definir un perfil de pseudousuario `initial-banner`:

Atributo	Valor
Reply-Message (18)	Texto descriptivo relativo a un host. El texto puede ser un nombre de host o puede contener instrucciones u otra información útil.

**Nota:** El parámetro Remote-Configuration en Terminal-Server Menu-Mode-Options debe tener el valor Yes para que el servidor de terminales utilice la definición de menú remota.

## Ejemplos de creación de un menú de hosts

Los comandos siguientes configuran el menú mostrado en la Figura B-2 y especifican que el menú debe visualizarse al establecer la sesión inicial:

```
admin> read terminal
TERMINAL-SERVER read

admin> set menu start-with-menus = yes

admin> set menu text-1 = administration
admin> set menu text-2 = engineering
admin> set menu text-3 = marketing
admin> set menu text-4 = techpubs
admin> set menu host-1 = 10.2.3.4
admin> set menu host-2 = 10.2.3.57
admin> set menu host-3 = 10.2.3.121
admin> set menu host-4 = 10.2.3.224

admin> write
TERMINAL-SERVER written
```

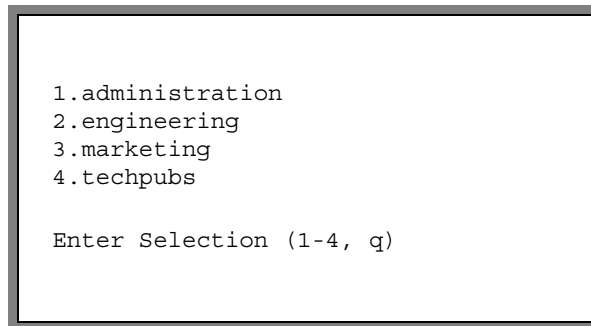
A continuación se muestra un perfil de pseudousuario banner de RADIUS equivalente:

```
banner-tnt01 Password = "ascend", Service-Type = Outbound-User
  Ascend-Host-Info = "10.2.3.4 administration",
  Ascend-Host-Info = "10.2.3.57 engineering",
  Ascend-Host-Info = "10.2.3.121 marketing",
  Ascend-Host-Info = "10.2.3.22 techpubs"
```

Con una de estas configuraciones, la unidad TAOS visualiza el menú en cuanto haya autenticado el nombre y la contraseña de inicio de sesión del usuario.



Figura B-2. Modo de menú del servidor de terminales



Los usuarios pueden bien establecer una conexión Telnet con el host especificado pulsando 1, 2, 3 o 4, o bien abandonar el menú pulsando Q. Al abandonar el menú, se interrumpe la conexión. Si el parámetro Toggle-Screen tiene el valor Yes, los usuarios pueden pulsar 0 para salir del modo de menú y entrar en el modo de línea de comandos del servidor de terminales.

## Creación de un menú personalizado de comandos (sólo RADIUS)

En perfiles RADIUS, puede configurar un menú personalizado de elementos de entre los que el usuario puede elegir y puede especificar un indicador de entrada de datos. Puede especificar hasta 20 atributos Ascend-Menu-Item por perfil. Los elementos de menú se visualizan en el orden de aparición en el perfil RADIUS.

Si especifica un menú personalizado en un perfil RADIUS, el usuario no tiene acceso al modo de menú normal ni a la línea de comandos del servidor de terminales.

RADIUS utiliza los pares atributo-valor siguientes para crear un menú de inicio de sesión personalizado:

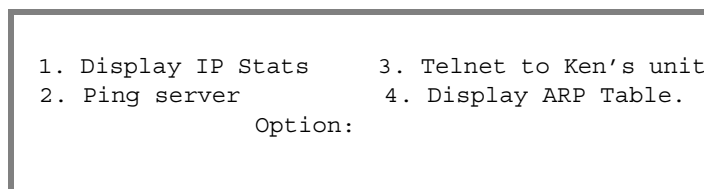
Atributo	Valor
Ascend-Menu-Item (206)	<p>Elemento de menú que aparece en lugar del indicador del servidor de terminales. Cada elemento puede incluir un comando, una cadena de texto y un patrón que el usuario debe escribir para seleccionar el elemento de menú, separados por punto y coma. El formato es el siguiente:</p> <pre>"comando;texto;[coincidencia]"</pre> <p>El <i>comando</i> es una cadena que se envía al servidor de terminales cuando se selecciona el elemento. Debe ser un comando de servidor de terminales válido.</p> <p>El <i>texto</i> es una cadena que aparece en la pantalla del usuario (hasta 31 caracteres).</p> <p>La <i>coincidencia</i> (optativa) es un patrón de hasta 10 caracteres que el usuario debe escribir para seleccionar el elemento. La unidad TAOS considera los espacios en blanco como parte del patrón de coincidencia.</p>

Atributo	Valor
Ascend-Menu-Selector (205)	Indicador para la entrada de datos del usuario en la interfaz del menú personalizado. La cadena predeterminada es:  Enter Selection (1-n, q)  donde <i>n</i> es el número de instancias de atributos Ascend-Menu-Item en el perfil.

Por ejemplo, el perfil RADIUS siguiente define la pantalla de inicio de sesión personalizada que se muestra en la Figura B-3:

```
Emma Password = "m2dan", Service-Type = Login-User
  Ascend-Menu-Item = "show ip stats;Display IP Stats",
  Ascend-Menu-Item = "ping 1.2.3.4;Ping server",
  Ascend-Menu-Item = "telnet 10.2.4.5;Telnet to Ken's unit",
  Ascend-Menu-Item = "show arp;Display ARP Table",
  Ascend-Menu-Selector = "                Option:"
```

*Figura B-3. Pantalla de inicio de sesión personalizada para un usuario RADIUS*



```
1. Display IP Stats      3. Telnet to Ken's unit
2. Ping server          4. Display ARP Table.
                        Option:
```

Con la pantalla de inicio de sesión que se muestra en la Figura B-3, el usuario dispone únicamente de cuatro opciones. Si selecciona la opción 3, por ejemplo, el usuario establece una conexión Telnet con un host local. Si selecciona la opción 2, el usuario realiza una operación Ping para un servidor.

Para modificar la pantalla de modo que visualice una cadena exclusiva (un patrón de coincidencia) en lugar de un número para cada opción, agregue las definiciones Ascend-Menu-Item para los patrones de coincidencia. Por ejemplo, el perfil siguiente define la pantalla de inicio de sesión personalizada que se muestra en la Figura B-4:

```
Emma Password = "m2dan", Service-Type = Login-User
  Ascend-Menu-Item = "show ip stats;ip=Display IP Stats;ip",
  Ascend-Menu-Item = "ping 1.2.3.4;p=Ping server;p",
  Ascend-Menu-Item = "telnet 10.2.4.5;t=Telnet to Ken's unit;t",
  Ascend-Menu-Item = "show arp;dsp=Display ARP Table;dsp",
  Ascend-Menu-Selector = "                Option:"
```

Figura B-4. Pantalla de inicio de sesión personalizada con patrones de coincidencia

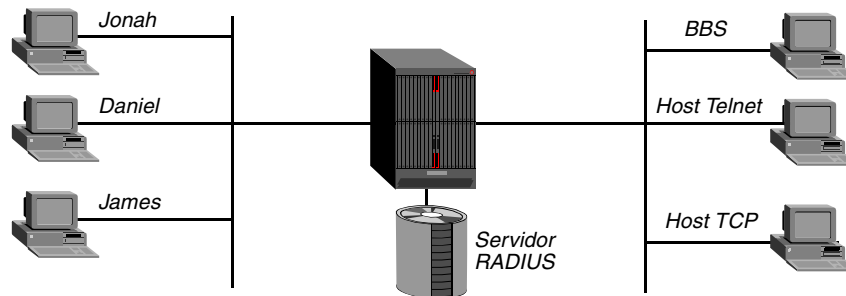
```
ip=Display IP Stats      t=Telnet to Ken's unit
p=Ping server           dsp=Display ARP Table.
                        Option:
```

**Nota:** No combine selecciones de menú numéricas con la coincidencia de patrones. El primer ajuste del atributo Ascend-Menu-Item determina si la ventana visualiza selecciones numeradas o patrones.

## Ejemplo ampliado de modo de menú y RADIUS

En la Figura B-5, un administrador de la red debe establecer un menú de servidor de terminales que proporcione al usuario la posibilidad de conectarse a un BBS o de iniciar PPP, SLIP o CSLIP. RADIUS se ejecuta en un servidor UNIX.

Figura B-5. Ejemplo ampliado de servidor de terminales



El servidor RADIUS utiliza el perfil DEFAULT para determinar el tipo de acceso que concede a los usuarios que no aparecen en el archivo users. Sólo es posible configurar un único perfil DEFAULT en el archivo users. Asegúrese de que el perfil DEFAULT sea el último de la línea. RADIUS no tiene en cuenta los perfiles que siguen al perfil DEFAULT.

La primera línea del perfil de usuario permite a un usuario del servidor de terminales conectarse con su contraseña o nombre de cuenta UNIX. El atributo Reply-Message proporciona un texto de mensaje introductorio. Los atributos Ascend-Menu-Selector y Ascend-Menu-Item proporcionan las líneas del texto del menú. En este ejemplo, debería configurar el perfil de usuario del modo siguiente:

```
DEFAULT Password = "UNIX"
  Ascend-Idle-Limit = 1800,
  Framed-Routing = None,
  Framed-Compression = Van-Jacobson-TCP-IP,
  Ascend-Link-Compression = Link-Comp-None,
  Ascend-Assign-IP-Pool = 1,
  Ascend-Route-IP = Route-IP-Yes,
  Reply-Message = "Welcome to ABCNet's Terminal Server."
  Ascend-Menu-Selector = "Press q to Quit>>",
  Ascend-Menu-Item = "rlogin bbs.net;BBS",
  Ascend-Menu-Item = "ppp;Start PPP",
```

## Opciones de autorización

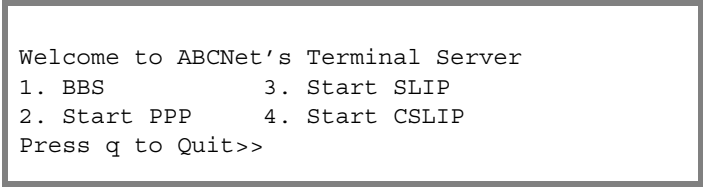
### Autorización de conexiones en modo de terminal

---

```
Ascend-Menu-Item = "slip;Start SLIP",  
Ascend-Menu-Item = "cslip;Start CSLIP"
```

En la Figura B-6 se muestra el texto que aparece en la pantalla del servidor de terminales.

*Figura B-6. Menú que se visualiza cuando se utiliza el perfil DEFAULT*



```
Welcome to ABCNet's Terminal Server  
1. BBS          3. Start SLIP  
2. Start PPP    4. Start CSLIP  
Press q to Quit>>
```

En lugar de utilizar el perfil DEFAULT, puede configurar perfiles individuales para restringir el acceso de los usuarios a determinados servicios. Por ejemplo, si desea que el usuario Jonah establezca una sesión Rlogin con `bbs.net` inmediatamente después de la autenticación, puede configurar el perfil de usuario siguiente:

```
Jonah Password = "UNIX"  
Service-Type = Login-User,  
Login-Host = bbs.net,  
Login-Service = Rlogin
```

Para permitir que se registren nuevos usuarios, puede configurar un perfil como el siguiente:

```
Guest Password = "UNIX"  
Service-Type = Login-User,  
Login-Host = unix.bbs.net,  
Login-Service = Rlogin
```

Si un usuario accede como invitado, se conecta a la máquina UNIX inmediatamente. La máquina UNIX posee una secuencia de comandos de shell en `/usr/local/bin/guest`, como la siguiente:

```
#!/bin/sh  
echo Welcome to BBS.NET.  
signup
```

La línea `signup` hace referencia a una secuencia de comandos de shell interactiva que se puede escribir para reunir información introductoria, configurar una cuenta temporal para la verificación y efectuar cualquier tarea pertinente.

## Autorización de conexiones en modo de terminal

Por lo general, los administradores establecen el modo de terminal para negociar una sesión usuario-host como parte de la secuencia de comandos Expect-Send de llamada de entrada. En lugar de proporcionar únicamente el nombre de conexión y la contraseña necesarios para autenticar un perfil Connection, la secuencia de comandos también incluye el indicador del servidor de terminales y un comando, como PPP, SLIP, Telnet o Rlogin. De este modo, la sesión con un host se invoca como parte del proceso de conexión, de forma que el usuario nunca ve realmente el indicador de línea de comandos.

## Conexiones TCP, Rlogin o Telnet en modo de terminal

De forma predeterminada, el perfil Terminal-Server desactiva la utilización de los comandos TCP, Rlogin y Telnet, ya que el modo inmediato ofrece estos comandos de una forma más segura. Sin embargo, puede activarlos en modo de terminal para permitir que los usuarios se conecten y realicen una secuencia de inicio de sesión desde la línea de comandos o que inicien la sesión como parte de una secuencia de comandos Expect-Send, como la siguiente:

```
expect "Login:" send $username expect "Password:" send $password
expect "ascend%" send "telnet 10.1.2.3"
```

Para obtener información acerca de la utilización del modo inmediato en lugar del modo de terminal, consulte “Autorización de un servicio de conexión de modo inmediato” en la página B-2.

### *Autorización para utilizar los comandos*

Los parámetros Terminal-Server siguientes (que aparecen con los ajustes predeterminados) desactivan el inicio de conexiones TCP, Rlogin y Telnet en modo de terminal:

```
[in TERMINAL-SERVER:terminal-mode-configuration]
tcp = no
rlogin = no

[in TERMINAL-SERVER:terminal-mode-configuration:rlogin-options]
rlogin = no

[in TERMINAL-SERVER:terminal-mode-configuration:telnet-options]
telnet = no
```

Parámetro	Especifica
TCP	Activa y desactiva el comando TCP, que inicia una sesión TCP con un host especificado. De forma predeterminada, este comando está desactivado.
Rlogin	Activa y desactiva el comando Rlogin, que inicia una sesión remota con un host especificado. De forma predeterminada, este comando está desactivado.
Telnet	Activa y desactiva el comando Telnet, que inicia una sesión Telnet con un host especificado. De forma predeterminada, este comando está desactivado.

Los comandos siguientes activan la utilización de los comandos Telnet y Rlogin desde el indicador del servidor de terminales:

```
admin> read terminal-server
TERMINAL-SERVER read

admin> set terminal telnet telnet = yes
admin> set terminal rlogin rlogin = yes

admin> write
TERMINAL-SERVER written
```

### *Configuración del rango de puertos de origen Rlogin*

Los administradores pueden configurar el rango de puertos Rlogin utilizando los parámetros siguientes (que aparecen con los ajustes predeterminados):

```
[in TERMINAL-SERVER:terminal-mode-configuration:rlogin-options]
max-source-port = 1023
min-source-port = 128
```

Parámetro	Especifica
Max-Source-Port	Puerto de origen Rlogin más alto. Su valor debe estar comprendido entre 128 y 1023, y debe ser mayor o igual que el valor de Min-Source-Port. El valor predeterminado es 1023.
Min-Source-Port	Puerto de origen Rlogin más bajo. Su valor debe estar comprendido entre 128 y 1023, y debe ser menor o igual que el valor de Max-Source-Port. El valor predeterminado es 128. Para utilizarlo con BSD Rlogin, establezca este valor en 512.

Por ejemplo, los comandos siguientes configuran un rango de puertos de origen válidos de 512 a 1023:

```
admin> read terminal-server
TERMINAL-SERVER read

admin> set terminal rlogin min-source-port = 512

admin> write
TERMINAL-SERVER written
```

El comando Slot notifica que los puertos no están disponibles o que un rango está configurado de forma incorrecta. El mensaje siguiente indica que todos los puertos del rango configurado están en uso:

```
"no connection: no port available, connection was refused."
```

Los mensajes siguientes indican que el rango de puertos de origen se ha configurado incorrectamente:

```
"error: max-source-port should be greater than or equal to min-source-port"
"error: Value (1024) out of range [128 - 1023]"
```

### *Definición de ajustes predeterminados para sesiones Telnet*

Además del parámetro Telnet, que permite sesiones Telnet en modo de terminal, los parámetros siguientes establecen valores predeterminados para sesiones Telnet. Los ajustes no anulan las selecciones que puede realizar un usuario para cada sesión cuando se ejecuta el comando Telnet.

```
[in TERMINAL-SERVER:terminal-mode-configuration]
terminal-type = vt100
clear-call = no
buffer-chars = yes

[in TERMINAL-SERVER:terminal-mode-configuration:telnet-options]
telnet-mode = ascii
```

```
auto-telnet = no
local-echo = no
```

Parámetro	Especifica
Terminal-Type	Tipo de terminal, como VT100, para la sesión Telnet.
Clear-Call	Activa y desactiva la interrupción de la conexión cuando un usuario termina una sesión Telnet.
Buffer-Chars	Activa y desactiva el mantenimiento de caracteres de entrada en un búfer durante 100 milisegundos antes de enviarlos al host. La alternativa es enviar los caracteres de entrada a medida que se reciben.
Telnet-Mode	Modo binario, ASCII o transparente.
Auto-Telnet	Activa y desactiva el inicio de una sesión Telnet cuando un usuario especifica un nombre de host en el indicador de línea de comandos. Como efecto secundario, cuando Auto-Telnet tiene el valor Yes, el sistema interpreta una cadena de comando desconocida como el nombre de un host para una sesión Telnet.
Local-Echo	Activa y desactiva el eco de caracteres localmente. Los usuarios pueden cambiar el ajuste del eco dentro de una sesión Telnet individual.

A continuación se muestra un ejemplo en el que un administrador configura algunos de los parámetros de sesión:

```
admin> read terminal-server
TERMINAL-SERVER read
admin> set clear-call = yes
admin> set telnet auto-telnet = yes
admin> set telnet local-echo = yes
admin> write
TERMINAL-SERVER written
```

## Sesiones PPP y SLIP en modo de terminal

De forma predeterminada, el perfil Terminal-Server desactiva la utilización del comando PPP, dado que los emisores suelen utilizar el software de llamada de entrada PPP para una sesión de protocolo entramado. Sin embargo, puede permitir que los emisores que no posean el software PPP inicien una sesión PPP como parte de una secuencia de comandos Expect-Send. Por ejemplo:

```
expect "Login:" send $username expect "Password:" send $password
expect "ascend% " send "PPP"
```

## Opciones de autorización

### Autorización de conexiones en modo de terminal

---

Algunas aplicaciones requieren SLIP en lugar de PPP. La unidad TAOS no admite una llamada de entrada SLIP directa, dado que SLIP no admite la autenticación. Sin embargo, si se ha activado SLIP en el servidor de terminales, los usuarios pueden iniciar una sesión SLIP y, a continuación, ejecutar una aplicación, como FTP, en dicha sesión. Para iniciar SLIP, el usuario debe invocar una sesión en modo de terminal. Por ejemplo:

```
expect "Login:" send $username expect "Password:" send $password
expect "ascend% " send "SLIP"
```

### Autorización para utilizar los comandos

Los parámetros siguientes (que aparecen con los ajustes predeterminados) autorizan sesiones PPP y SLIP en modo de terminal:

```
[TERMINAL-SERVER:ppp-mode-configuration]
ppp = no

[in TERMINAL-SERVER:slip-mode-configuration]
slip = no
```

Parámetro	Especifica
PPP	Activa y desactiva el comando PPP, que inicia una sesión PPP. De forma predeterminada, este comando está desactivado.
SLIP	Activa y desactiva el comando SLIP, que inicia una sesión SLIP. De forma predeterminada, este comando está desactivado.

Por ejemplo, los comandos siguientes activan sesiones PPP y SLIP:

```
admin> read terminal-server
TERMINAL-SERVER read

admin> set ppp ppp = yes

admin> set slip slip = yes

admin> write
TERMINAL-SERVER written
```

### Definición de ajustes predeterminados para sesiones PPP

Además del parámetro PPP, que activa sesiones PPP en modo de terminal, los parámetros siguientes establecen valores predeterminados para sesiones PPP:

```
[TERMINAL-SERVER:ppp-mode-configuration]
delay = 5
direct = no
info = session-ppp
```

Parámetro	Especifica
Delay	Número de segundos de retardo antes de pasar del inicio de sesión al proceso de modo de paquete.
Directo	Activa y desactiva la negociación PPP directa después de utilizar el comando PPP. De forma predeterminada, el servidor de terminales espera a recibir un paquete PPP antes de iniciar la negociación PPP.



Parámetro	Especifica
Info	Activa y desactiva la visualización de un mensaje informativo cuando el usuario entra en el modo PPP. Con el ajuste <code>Session-PPP</code> , el sistema visualiza <code>PPP Session</code> . Con el ajuste <code>Mode-PPP</code> , el sistema visualiza <code>PPP Mode</code> .

Los comandos siguientes configuran el sistema para que inicie la negociación PPP inmediatamente después de la ejecución del comando PPP:

```
admin> read terminal-server
TERMINAL-SERVER read

admin> set ppp ppp = yes

admin> set ppp direct = yes

admin> write
TERMINAL-SERVER written
```

### *Definición de ajustes predeterminados para sesiones SLIP*

Además del parámetro SLIP, que activa sesiones SLIP en modo de terminal, los parámetros siguientes establecen valores predeterminados para sesiones SLIP:

```
[in TERMINAL-SERVER:slip-mode-configuration]
slip-bootp = no
info = basic-slip
```

Parámetro	Especifica
SLIP-BOOTP	Activa y desactiva la respuesta a BOOTP durante sesiones SLIP. Con el ajuste <code>Yes</code> , un usuario que inicie una sesión SLIP puede obtener una dirección IP de la agrupación de direcciones IP mediante BOOTP. Con el ajuste <code>No</code> , el servidor de terminales no ejecuta BOOTP. En lugar de ello, el sistema solicita al usuario que acepte una dirección IP al iniciarse la sesión SLIP.
Info	Activa y desactiva la visualización de un mensaje informativo cuando el usuario entra en el modo SLIP. Con el ajuste <code>Basic-SLIP</code> , se visualiza un mensaje de inicio predeterminado. Con el ajuste <code>Advanced-SLIP</code> , el mensaje incluye la máscara de subred del emisor y la dirección IP del gateway.

Los comandos siguientes permiten que el servidor de terminales responda a BOOTP durante sesiones SLIP:

```
admin> read term
TERMINAL-SERVER read

admin> set slip slip-bootp = yes

admin> write
TERMINAL-SERVER written
```

## Autorización a los usuarios para el acceso a la interfaz del servidor de terminales

Algunos entornos permiten a los emisores acceder a la línea de comandos del servidor de terminales y limitan los comandos que son accesibles. Si decide permitir el acceso a la línea de comandos del servidor de terminales, asigne al servidor de terminales su propia contraseña a fin de proteger la línea de comandos frente a accesos no autorizados.

**Nota:** Para obtener información detallada acerca del acceso a la línea de comandos del servidor de terminales, consulte “Autenticación de inicios de sesión de usuario” en la página A-22.

## Autorización del acceso a la gestión SNMP

El software de gestión SNMP, que utiliza la MIB Ascend Enterprise y que tiene conectividad IP con la unidad TAOS, puede realizar tareas administrativas, incluida la reconfiguración de la unidad TAOS. Es importante restringir este tipo de acceso a las estaciones de gestión fiables. A continuación se muestran los parámetros SNMP pertinentes (con los ajustes predeterminados):

```
[in SNMP]
enabled = no
read-community = public
read-write-community = write
enforce-address-security = no
read-access-hosts = [ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 ]
write-access-hosts = [ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 ]
contact = ""
location = ""
```

Parámetro	Especifica
Enabled	Activa y desactiva el acceso a SNMP. El valor predeterminado No impide a los administradores SNMP acceder a la unidad.
Read-Community	Contraseña (de hasta 32 caracteres) que debe solicitarse para el acceso de lectura por parte de un administrador SNMP. El acceso de lectura permite la utilización del comando GET de SNMP. La contraseña predeterminada es la cadena conocida públicamente <code>public</code> .
Read-Write-Community	Contraseña (de hasta 32 caracteres) que debe solicitarse para el acceso de lectura y escritura por parte de un administrador SNMP. El acceso de lectura y escritura permite la utilización de los comandos Get y Set de SNMP. El valor predeterminado es la cadena conocida públicamente <code>write</code> .
Enforce-Address-Security	Activa y desactiva la seguridad de dirección, que excluye la gestión SNMP a menos que se inicie desde una dirección IP especificada.
Read-Access-Hosts	Matriz de hasta cinco direcciones IP desde las que los gestores SNMP pueden acceder a la unidad con permiso de lectura (Get).
Write-Access-Hosts	Matriz de hasta cinco direcciones IP desde las que los gestores SNMP pueden acceder a la unidad con permiso de lectura y escritura (Get o Set).

Parámetro	Especifica
Contact	Nombre de la persona con la que se debe contactar en referencia a la unidad TAOS (legible y configurable por SNMP).
Location	Dónde está ubicada la unidad (legible y configurable por SNMP).

Por ejemplo, los comandos siguientes permiten el acceso mediante utilidades de gestión SNMP:

```
admin> read snmp
SNMP read

admin> set enabled = yes

admin> write
SNMP written
```

## Definición de cadenas de comunidad

Una vez activado el acceso mediante administradores SNMP, debe establecer una cadena secreta de comunidad de lectura y escritura o debe restringir el acceso mediante la seguridad de dirección. *En caso contrario, las estaciones de gestión no autorizadas podrán reconfigurar la unidad.*

Los comandos siguientes asignan una cadena Read-Write-Community confidencial:

```
admin> read snmp
SNMP read

admin> set read-write-community = secret

admin> write
SNMP written
```

## Configuración y aplicación de la seguridad de dirección

Si el parámetro Enforce-Address-Security tiene el valor No (el valor predeterminado), a los administradores SNMP que presenten el nombre de comunidad correcto se les concederá el acceso. Si el valor es Yes, la unidad TAOS comprueba la dirección IP de origen del administrador SNMP y permite el acceso únicamente a las direcciones IP que aparecen en las matrices Read-Access-Host y Write-Access-Host.

Los comandos siguientes aplican la seguridad de dirección y especifican las direcciones fiables para el acceso de lectura y escritura:

```
admin> read snmp
SNMP read

admin> set enforce-address-security = yes

admin> set read-access-hosts 1 = 10.2.3.1
admin> set read-access-hosts 2 = 10.2.3.2
admin> set read-access-hosts 3 = 10.2.3.3
admin> set write-access-hosts 1 = 10.1.1.1
admin> set write-access-hosts 2 = 10.1.1.2
admin> set write-access-hosts 3 = 10.1.1.3
```

## Opciones de autorización

### *Autorización del acceso a la gestión SNMP*

---

```
admin> set write-access-hosts 4 = 10.1.1.4
admin> set write-access-hosts 5 = 10.1.1.5
admin> write
SNMP written
```

# Índice alfabético

## A

- acceso como invitado, conexiones ARA, 8-5
- Adaptador de terminal (TA). *Consulte* TA (Adaptador de terminal)
- adyacencias OSPF, 3-4
- agente BOOTP-Relay, 2-54
- agente externo, ATMP, 4-11
- agente local de gateway, ATMP, 4-23
- agente local de ruteador, ATMP, 4-25
- agente local. *Consulte* ATMP
- agrupaciones
  - alineación de red, reglas para la, 2-72
  - configuración, ejemplos, 2-71
  - definidas en RADIUS, 2-69
  - direcciones, asignadas dinámicamente desde, 2-74
  - globales, gestionadas por RADIPAD, 2-69
  - RADIPAD, especificar host, 2-70
  - RADIUS ejemplos, 2-71
  - resumidas, 2-72
  - resumidas de OSPF, importar, 3-17
  - rutas a resumidas, 2-73
  - ruteador virtual, definición, 6-4
  - ruteador virtual, ejemplo, 6-7
- agrupaciones de direcciones globales RADIPAD, 2-69
- agrupaciones, RADIUS, 2-69
- AH de IPSec, información general, 5-9
- algoritmo de Dijkstra OSPF, 3-9
- algoritmos
  - árbol de trayectoria más corta (Dijkstra), 3-9
  - ruteo de estado de enlace, 3-8
  - utilización de la línea, calcular la, 1-21
- alineación de red. *Consulte* agrupación
- ancho de banda
  - agregar, 1-21
  - algoritmo para calcular la utilización de la línea, 1-21
  - atributos RADIUS para, 1-22
  - controlar la utilización, 1-21
  - fax IP, asignar, 10-3
  - incrementos, 1-21
  - objetivo de utilización, 1-22
  - picos en la utilización de la línea, 1-20
  - tarifas de telecomunicaciones, 1-20
- anuncios de estado de enlace (LSA). *Consulte* base de datos de estado de enlace
- AppleTalk
  - agrupación de llamada de entrada para clientes, 8-2
  - controlador de módulo, requisito, 8-1
  - direcciones, 8-1
  - ejemplos de configuración, 8-8
  - IP, 8-9
  - lista de zonas, explicación, 8-3
  - rangos de red, 8-1
  - ruteador no raíz, definición, 8-3
  - ruteador raíz, definición, 8-3
- AppleTalk Remote Access (ARA). *Consulte* ARA
- ARA
  - acceso como invitado, permitir, 8-5
  - configuración, ejemplo, 8-6
  - controlador de módulo, requisito, 8-1
  - direcciones, AppleTalk, 8-1
  - IP, 8-10
  - tiempo máximo de conexión, 8-5
- áreas OSPF, 3-6
- áreas stub, 3-7
- ARP
  - interfaces virtuales, con, 2-10
  - modo de proxy en LAN, 2-8
  - proxy en Ethernet, 2-8
- Ascend-Data-Rate (197)
  - descripción y utilización de, 1-11
- asignación dinámica de ancho de banda (DBA).
  - Consulte* DBA
- ataques de denegación del servicio, 2-11
- ATMP
  - agente local
    - contraseña, A-35
    - gateway y ruteador, comparación, 4-18
    - temporizador para túneles inactivos, 4-19
  - agente local de gateway, 4-23
  - agente local de ruteador, 4-25
  - componentes del túnel, 4-1
  - conexión FA a HA, 4-12
  - documentos RFC relacionados, 4-1
  - ejemplos, 4-13
  - enlace con la red interna, 4-20
  - flexibilidad, agentes locales primario y secundario, 4-22
  - IPX, 4-31
  - límites de reintento de túnel, 4-4

- nombre de la red interna, 4-12
  - peticiones de túneles, 4-11
  - reinicios necesarios, 4-2
  - respuestas RIP para clientes móviles, 4-21
  - rutas entre agentes, 4-3
  - ruteador local, 4-21
  - túnel local, 4-27
  - atributos de caducidad de la contraseña, A-4
  - autenticación
    - ACE, A-34
    - ajustes del perfil Connection, 1-7
    - CACHE-TOKEN, A-32
    - CHAP, A-9
    - cifrado en el servidor RADIUS, A-6
    - CLID, A-36, A-37
    - conexiones PPP, A-6
    - contraseña del sistema, A-23
    - contraseña para llamadas de salida PPP, 1-45
    - contraseña para PPP de llamada de entrada, 1-13
    - elegir método, A-1
    - externa, A-26
    - información de llamada, utilizar, A-37
    - modo de recepción, A-7
    - modo de seguridad del servidor de terminales, B-16
    - modo global para direct-access, 1-47
    - MS-CHAP, A-9
    - número llamado, A-38
    - OSPF, MD5 (RFC 2178), 3-4
    - PAP, A-8
    - PAP-TOKEN, A-30
    - PAP-TOKEN-CHAP, A-31
    - RADIUS, 1-6, 1-8, A-2
    - requerir de los emisores, 1-4
    - seguridad de usuario para llamadas de salida, 1-50
    - tarjeta de testigo, A-2, A-26
    - tercer indicador, A-25
    - testigos, cómo configurar, A-26
    - túnel, A-35
    - túneles, A-35
    - túneles L2TP, 5-5
    - túneles PPTP, 5-28
    - Windows NT, para, 1-14
  - autenticación ACE, A-34
  - autenticación de contraseña
    - túneles L2TP, abrir, 5-6
  - autenticación de contraseñas
    - túneles PPTP, abrir, 5-29
  - autenticación de modo Global para llamadas de salida de módem, 1-47
  - autenticación del número llamado, A-37, A-38
  - autenticación DNIS, A-37, A-38, A-40
  - autenticación externa
    - métodos, 1-6
    - servidores, 1-6, A-26
  - autenticación para OSPF MD5 (RFC 2178), 3-4
  - autenticación por tarjeta de testigo, A-2, A-26
    - configurar Cache-Token, A-32
    - configurar PAP-Token-CHAP, A-31
    - ejemplo, A-28
    - RADIUS, A-26
  - autorización
    - acceso SNMP al sistema, B-16
    - ajustes predeterminados de Telnet, B-12
    - inicios de sesión en hosts, B-11
    - inicios de sesión interactivos del servidor de terminales, B-11
    - modo de menú, B-2, B-4
    - modo de terminal, B-10
    - modo inmediato, B-2
    - restricción del acceso al servidor de terminales, B-1
    - sesiones PPP, B-13
    - sesiones SLIP, B-15
- 
- B**
  - BACP, 1-24
  - base de datos de estado de enlace
    - actualización, 3-8
    - adyacencias, 3-4
    - áreas, 3-6
    - ASE, 3-2
    - comandos para visualizar, 3-3
    - creación, 3-8
    - descripción, 3-2
    - ejemplo, 3-9
  - BOOTP
    - activar, 2-52
    - activar BOOT-Relay, 2-54
    - direcciones de servidor, 2-54
    - sesiones SLIP, B-15
  - búfer, datos TCP-Clear, 1-25
- 
- C**
  - cabeceras, A-24
  - caché de ruta
    - cachés de puerto, 2-50
  - caché. *Consulte* caché de ruta
  - cachés de puerto, 2-49
  - cachés de ruta, 2-50
  - CACHE-TOKEN, autenticación, A-32
  - cadena de comunidad, B-16
    - establecer, B-17
    - Read-Community, B-16
    - Read-Write-community, B-16
  - calidad del servicio (QOS). *Consulte* TOS (Tipo de servicio)

- 
- canales básicos, 1-16
  - canales máximos, 1-17
  - canales mínimos, 1-17
  - CBCP. *Consulte* Protocolo de control de devolución de llamada.
  - CHAP, autenticación, A-9
  - CHAP bidireccional
    - perfiles locales, configurar, A-10
    - utilización de RADIUS, A-15
  - cifrado
    - contraseña, A-2
    - IPSec, para, 5-11
  - CLID
    - autenticación, A-36, A-37
    - definición, A-36
    - devolución de la llamada, A-44
    - devolución de la llamada, configurar, A-46
    - túneles L2TP, abrir, 5-5
    - túneles PPTP, abrir, 5-28
  - clientes
    - aplicaciones TCP, 1-29
    - ARA, 8-4
    - clientes móviles ATMP, 4-9
    - conexiones Telnet, 1-47
    - inicio de sesión, servidor de terminales, 1-6
    - ISDN, 1-5, 1-16
    - LAN Manager, 1-45
    - Macintosh, software IP, 8-9
    - Netmanage Pacer, 8-4
    - NetWare, 7-4
    - software desfasado y fragmentación, 4-6
    - unidades TAOS de entrada, 1-19
    - UNIX, 2-53
    - Windows 95, 1-14
    - Windows NT, 1-14, 1-45
  - clientes de transacciones
    - SDTN, 11-5
  - cola por prioridad (proxy), 2-24
  - colas
    - cola por prioridad (proxy), 2-24
    - limitar el tamaño de, 2-48
  - compartir perfiles, 1-7
  - compresión
    - cabeceras VJ, 2-13
    - enlace, en túneles, 4-5
    - enlaces de PPP, en, 1-14
    - MS-Stac, 1-14
    - MTU, 4-5
    - Stac, 1-14
    - Stac-9, 1-14
  - compresión del enlace, 1-13
  - compresión del enlace, PPP, 1-13
  - conexiones asíncronas
    - descripción, 1-1
    - secuencias de comandos de inicio de sesión
      - Expect-Send, A-22
    - servidor de terminales, 1-5
    - sesiones entramadas, A-22
    - velocidades de conexión multicanal, 1-19
  - conexiones de entrada conmutadas, ejemplos, 1-12
  - conexiones de entrada, ejemplos, 1-12
  - conexiones de llamada de entrada Visa-II, 11-5
  - conexiones de salida por módem, 1-47
  - conexiones de WAN
    - asíncronas, 1-1
    - duración máxima, 1-9
    - opciones de telecomunicaciones, 1-34
    - protocolos de encapsulación, 1-2
    - síncronas, 1-1
    - temporizador de inactividad, 1-9
  - conexiones del protocolo multienlace (MP). *Consulte* MP
  - conexiones del protocolo multienlace Plus (MP+). *Consulte* MP+
  - conexiones MP
    - BACP, utilización con, 1-24
  - conexiones permanentes
    - ajustes de telecomunicaciones, 1-34
    - ejemplo, 1-36
    - grupos y, 1-34, 1-35
    - interfaces de reserva para, 1-40
    - MP+, 1-37
    - perfiles Connection, 1-34
    - RADIUS, 1-35
    - volver a cargar RADIUS, 1-35
  - conexiones síncronas
    - descripción, 1-1
    - PPP de entrada, 1-15
  - conexiones Visa-II, configurar, 11-8
  - conexiones X.75, 1-32
    - longitud máxima de las tramas, 1-33
  - Configuración de NAS (Servidor de acceso de red), A-28
  - configuración horaria universal (UTC), 2-55
  - conmutador GRF
    - conexión vía ATMP, 4-16
    - temas relativos a la fragmentación, 4-5
  - conmutador GRF y OSPF, 3-13
  - perfil Connection
    - Consulte también* RADIUS
  - consultas Finger, 2-53
    - de cliente UNIX, 2-53
  - contiguos, OSPF, 3-5
  - contraseña
    - indicador, A-24
    - secretos compartidos, A-5
    - Telnet, A-6
-

contraseña de Telnet, 2-40  
contraseñas  
  ACE, A-30  
  caducidad (RADIUS), A-4  
  cambiar no caducadas, A-4  
  cifrado, A-2  
  cifrado para llamada de salida, A-6  
  conexiones PPP de entrada, para, 1-13  
  conexiones PPP de salida, para, 1-44  
  conexiones TCP-Clear para, 1-26  
  especificar la caducidad, A-3  
  llamada de salida direct-access, para, 1-48  
  modo Global para direct-access, 1-47  
  RADIUS, A-2  
  SAFEWORD, A-30  
  sistema, A-23  
  Tunnel-Password, Ascend-Home-Agent-Password,  
    A-35  
control de calidad de enlaces  
  conexiones PPP, para, 1-14  
  descripción, 1-13  
  soporte de número mágico, 1-14  
control de pulso, ejemplo, 2-84  
costes de OSPF, ejemplo, 3-20

**D**

DBA, 1-19  
  algoritmo para calcular la utilización de la línea, 1-21  
  atributos RADIUS, 1-22  
  incrementos, 1-21  
  objetivo de utilización, 1-22  
  período de tiempo para calcular la utilización de la  
    línea, 1-21  
  persistencia del grado de utilización, 1-22  
  reducciones, 1-21  
definiciones de agrupación de direcciones, ejemplo,  
  2-71  
desencadenar, actualizaciones RIP, 2-47  
devolución de la llamada  
  Ascend, A-45  
  Ascend, configurar, A-49  
  CBCP, configurar, A-52  
  CLID, configurar, A-46  
  DNIS, configurar, A-46  
devolución de la llamada Ascend, A-45  
  configurar, A-49  
devolución de la llamada CBCP, configurar, A-52  
devolución de la llamada Expect, A-45  
dial query, IPX, 7-3, 7-10  
difusiones dirigidas, desactivar, 2-11  
dirección de difusión, pasar por alto peticiones de eco,  
  2-44

dirección IP del sistema, 2-40  
  ATMP, recomendación, 4-2  
  ruteadores virtuales, para, 6-4  
dirección local, interfaz numerada, 2-20  
dirección remota, 2-18  
direcciones  
  AppleTalk, 8-1  
  conexiones TCP-Clear, 1-26  
  difusión y RIP, 2-7  
  dinámicas, que requieren aceptación, 2-41  
  DNS, 2-59  
  filtrado, 9-15, 9-26  
  interfaces numeradas, para, 2-20  
  IP del sistema, 2-39  
  IP en IP, 5-33  
  puertos Ethernet, 2-6  
  ruteadores virtuales, efecto en, 6-2  
  servidores NetBIOS, 2-58, 2-66  
  verificación de la dirección de origen, 2-23  
  *Consulte también* agrupaciones

direcciones IP  
  aislamiento de la red, 4-6  
  asignación dinámica, ejemplo, 2-74  
  dirección del sistema, 2-39  
  evitar la simulación de locales, 9-16  
  filtrado, 9-15  
  interfaces numeradas, 2-20  
  interfaces virtuales, 2-10  
  para la interfaz de LAN, 2-7  
  ruteadores del extremo remoto, 2-18  
  verificación de la dirección de origen, 2-23

direcciones IPX  
  clientes NetWare de entrada, para, 7-5  
  filtrado, 9-26  
  para la interfaz de LAN, 7-7  
  servidores NetWare, 7-15

DNIS  
  actualización automática, 2-62  
  definición, A-36  
  devolución de la llamada, A-44  
  devolución de la llamada, configurar, A-46  
  túneles L2TP, abrir, 5-5  
  túneles PPTP, abrir, 5-28  
  túneles PPTP, autenticación, 2-62, 5-28

DNS  
  conexiones TCP-Clear, 1-26  
  intento de lista, 2-59  
  servidores cliente, 2-63  
  servidores cliente específicos de la conexión, 2-65,  
    2-67  
  servidores cliente generales del sistema, 2-65  
  servidores locales, 2-58  
  tabla local en RAM, configurar, 2-60  
  tabla local, ejemplo, 2-61  
duración máxima de una llamada, 1-9



**E**

Emplear trayectoria más corta primero (OSPF).  
*Consulte* OSPF

encadenamiento de agrupaciones IP  
 definición, 2-75  
 perfiles locales, configurar en, 2-76  
 RADIUS, configurar en, 2-78

encapsulación de ruteo genérica (GRE), 4-1

entrada, llamadas de  
 autenticar, 1-4  
 contraseñas, 1-45  
 MP+, 1-34, 1-37  
 PPP, 1-45

envío de difusión múltiple  
 ajustes globales, 2-81  
 clientes de difusión multiple, LAN, 2-86  
 clientes de difusión multiple, WAN, 2-86  
 control de pulso, configurar, 2-83  
 interfaz MBONE, especificar, 2-84  
 interfaz MBONE, LAN, 2-84  
 interfaz MBONE, WAN, 2-84  
 limitaciones para ruteadores virtuales, 6-6  
 límite de velocidad, especificar para clientes, 2-88  
 ruta a la interfaz mcast, 2-2  
 tiempo de espera de miembro de grupo IGMP, 2-82

ESP de IPSec, 5-11  
 TCP-Clear, 1-31

ESP. *Consulte* protocolo de carga útil de seguridad de la encapsulación

estadísticas de protocolo, 6-5

interfaz Ethernet  
*Consulte también* interfaces IPX, interfaces de LAN

extensión Microsoft de CHAP (MS-CHAP). *Consulte* autenticación

extensiones TAOS en IPX, 7-3

**F**

fax de entrada  
 configurar, 10-6

fax de salida  
 configurar, 10-8

fax IP  
 asignar ancho de banda, 10-3  
 configurar, 10-5  
 definición, 10-1  
 entrada y salida, 10-1  
 faxes de entrada, configurar, 10-6  
 faxes de salida, configurar, 10-8  
 parámetros, 10-2

filtro TOS (Tipo de servicio)  
 aplicar a interfaces, 9-38

filtros  
 acción de reenvío (IP, IPX, genéricos), 9-7  
 cómo se procesan paquetes, 9-3  
 comparaciones satisfactorias, definición, 9-3  
 dirección del tráfico que debe controlarse, 9-6  
 especificaciones del perfil Connection, 1-7  
 filtro de datos, aplicar, 9-2  
 filtro de llamadas, aplicar, 9-3, 9-37  
 filtro TOS, aplicar, 9-38  
 gestión de sesiones, aplicar para, 9-37  
 persistencia, 9-35  
 remotos dinámicos, 9-30  
 SAP IPX, 7-17  
 tipos, 9-1  
*Consulte también* filtros genéricos, filtros IP, filtros IPX, filtros de ruta, filtros TOS

filtros de datos, aplicar, 9-2

filtros de llamadas, aplicar, 9-3, 9-37

filtros de paquetes. *Consulte* filtros

filtros de ruta  
 acción que realizar cuando existen coincidencias, 9-6  
 aplicar a interfaces, 9-34, 9-39  
 cambiar la métrica de una ruta, 9-29  
 contenido de los paquetes, cómo se comparan, 9-5  
 paquetes RIP de una dirección especificada, 9-28  
 rutas específicas, filtrado, 9-29

filtros genéricos  
 acción (reenviar o descartar), 9-4  
 aplicar a interfaces, 9-34  
 bytes que deben probarse, 9-10  
 contenido de los paquetes, cómo se comparan, 9-4  
 desplazamiento del contenido de los paquetes, 9-10  
 ejemplo, 9-12  
 valor de máscara antes de la comparación, 9-11

filtros IP  
 acción (reenviar o descartar), 9-4  
 aplicar a interfaces, 9-34, 9-36  
 contenido de los paquetes, cómo se comparan, 9-4  
 evitar la simulación de direcciones, ejemplo, 9-16  
 filtrado de direcciones de destino, 9-15  
 filtrado de direcciones de origen, 9-15  
 filtrado de números de puerto, 9-16  
 utilizaciones de seguridad, 9-18

filtros IPX  
 acción (reenviar o descartar), 9-5  
 aplicar a interfaces, 9-34  
 contenido de los paquetes, cómo se comparan, 9-5  
 ejemplos, 9-27  
 filtrado de direcciones de destino, 9-26  
 filtrado de direcciones de origen, 9-26  
 filtrado de números de zócalo, 9-27

filtros TOS (Tipo de servicio)  
 acción (establecer bits de precedencia), 9-19  
 acción realizada cuando existen coincidencias, 9-5  
 aplicar a interfaces, 9-34

## Índice alfabético

### G

contenido de los paquetes, comparación, 9-4  
cuándo utilizarlos, 9-19  
ejemplo, 9-24  
flexibilidad, ATMP, 4-22  
fragmentación  
ATMP, evitar entre agentes, 4-5  
hacer que los clientes realicen, 4-6  
prefragmentación en el software de cliente, 4-6  
software de cliente desfasado, 4-6  
túneles, 4-5  
fragmentación y reensamblaje de paquetes, 4-4  
Framed-Route, número máximo por perfil, 2-27  
función del ruteador de frontera de área (ABR), 3-2

### G

global-pools, RADIUS, 2-70  
grado de utilización  
persistencia, 1-22  
solicitud de ancho de banda, 1-22  
grupos  
canales permanentes de, 1-34  
IGMP, 2-82, 2-88  
permanentes, 1-35

### H

HDLC-modo de respuesta normal  
con SDTN, 11-5  
configurar, 11-6  
hint-zone, 8-4  
hora media de Greenwich (GMT), 2-55  
host  
coincidencias con DNS, 2-61  
conexión IP-Direct a local, 2-21  
dirigir llamadas asíncronas de entrada al, B-2  
local, conexión de TCP-Clear con, 1-28  
nombres en el menú Terminal-Server, B-7

### I

ICMP  
pasar por alto la difusión eco, 2-44  
pasar por alto redirecciones, 2-44  
ID de filtro, RADIUS, 9-36  
IGMP  
control de pulso de difusión múltiple, 2-83  
paquetes de rastreo de difusión múltiple, 2-80  
reenvío de difusión múltiple  
retardo para la eliminación de grupos, 2-88  
versión 1 o versión 2, 2-80

indicadores  
contraseña, A-24  
inicio de sesión, A-24  
tercero, A-25  
información de llamada, configuración de la seguridad, A-37  
inicios de sesión  
autorización de interactivos, B-11  
indicador, A-24  
servidor de terminales, B-1, B-11  
Telnet, 2-43  
tiempo de espera, A-24  
intentos de lista  
L2TP, 5-15  
intercambio de paquetes interredes (IPX). *Consulte* IPX  
interfaces  
blackhole (bh0), 2-4  
cliente de difusión múltiple, 2-88  
IPX de WAN, 7-7  
IPX, LAN, 7-5  
local, 2-2  
loopback (lo0), 2-3  
mcast, 2-2  
numeradas, ejemplo, 2-20  
reject (rj0), 2-4  
ruteador virtual, pertenecientes al, 6-8  
soft IP (sip0), 2-4  
tabla de, 2-3  
tunnel, 2-4  
vr0\_main, 2-4  
WAN, active, 2-4  
wanabe, 2-4  
interfaces AppleTalk de LAN  
hint-zone, 8-4  
petición ZipGetNetInfo para la configuración, 8-4  
ruteador no raíz, configurar, 8-4  
ruteador raíz, configurar, 8-3  
zona predeterminada, 8-3  
interfaces AppleTalk de WAN  
acceso como invitado de ARA, permitir, 8-5  
AppleTalk PPP, 8-8  
clientes ARA, 8-6  
filtros, aplicar, 9-2, 9-36  
IP, 8-9  
ruteador AppleTalk, 8-8  
software de cliente, 8-4  
tipos de conexión, 8-4  
interfaces de OSPF, ejemplo, 3-13  
interfaces de reserva, 1-39  
Interfaces de WAN AppleTalk  
dispositivo remoto, modo homólogo, 8-6  
interfaces de WAN de relé de trama  
filtros, aplicar, 9-2, 9-36  
interfaces IP de LAN  
ajustes de IP-Interface, 2-6

- hr/>
- clientes de difusión múltiple, 2-89
  - difusiones dirigidas, desactivar, 2-11
  - dirección física, 2-6
  - filtrar paquetes RIP, 9-39
  - filtros de ruta, 9-39
  - MBONE, 2-84
  - opciones de OSPF, 3-10
  - proxy ARP, activar, 2-8
  - RIP, activar, 2-9
  - ruteador virtual, asignar al, 6-7
  - sólo de gestión, 2-12
  - virtual
    - OSPF, 3-3
    - proxy ARP, 2-10
  - virtuales, 2-10
  - interfaces IP de WAN
    - ajustes del perfil Connection, 2-13
    - AppleTalk, 8-9
    - atributos RADIUS, 2-15
    - clientes de difusión múltiple, 2-89
    - compresión VJ, 2-13
    - conexión de interfaz numerada, 2-20
    - de host a host, 2-21
    - de ruteador a ruteador, 2-18
    - filtrar paquetes RIP, 9-39
    - filtros de datos, aplicar, 9-2, 9-36
    - filtros de llamadas, aplicar, 9-3
    - IP Direct, 2-21
    - MBONE, 2-84
    - opciones de OSPF, 3-10
    - privadas, 2-22
    - ruta del host, 2-19
    - ruta predeterminada específica del cliente, 2-23
    - ruteador virtual, asignar al, 6-7
    - túnel ATMP, 4-7, 4-13
    - túnel L2TP, 5-3
    - túnel PPTP, 5-27
  - interfaces IPX de LAN
    - ajustes de IPX-Interface, 7-5
    - información general, 7-6
    - paquetes de tipo 20, 7-7
    - requisito Ethernet del controlador de módulo, 7-5
    - ruteo y simulación, 7-6
    - tipo de trama, 7-6
  - interfaces IPX de WAN
    - ajustes del perfil Connection, 7-8
    - ajustes del perfil RADIUS, 7-9
    - autenticación, 7-7
    - consulta de SAP, marcación de la conexión, 7-10
    - dial query, 7-10
    - dispositivo remoto, modo homólogo, 7-9
    - filtros, aplicar, 9-2, 9-36
    - net-number y net-alias, 7-11
    - proxy del servidor local, 7-11
    - RIP IPX, activar, 7-10
    - SAP IPX, activar, 7-10
  - interfaces MBONE
    - Consulte también* envío de difusión múltiple
    - ejemplos, 2-85
  - interfaces numeradas, 2-20
    - ejemplo, 2-21
  - interfaces OSPF de LAN
    - autenticación, 3-4, 3-12
    - costes, 3-12
    - intervalos de paquetes hello, 3-11
    - manejo de ASE, 3-12
    - manejo de LSA, 3-12
    - número y tipo de área, 3-6, 3-11
    - prioridad del ruteador designado, 3-5, 3-11
  - interfaces OSPF de WAN
    - autenticación, 3-4, 3-12
    - costes, 3-12
    - intervalos para paquetes hello, 3-11
    - manejo de ASE, 3-12
    - manejo de LSA, 3-12
    - número y tipo de área, 3-6, 3-11
    - prioridad del ruteador designado, 3-5, 3-11
  - interfaces virtuales de LAN, 2-9
  - interfaces virtuales IP, ejemplo, 2-10
  - interfaz blackhole (bh0), 2-4
  - interfaz de cliente de difusión múltiple, ejemplo, 2-88
  - interfaz Ethernet
    - configuración IP, 2-7
    - controlador de módulo, IPX, 7-5
    - de sólo de gestión, 2-12
    - desactivar difusiones dirigidas, 2-11
    - filtros, aplicar, 9-39
    - interfaces virtuales IP, 2-9
    - RIP, 2-9
    - sólo de gestión, 2-12
    - tabla de interfaces, 2-3
    - varias direcciones IP para, 2-10
  - interfaz IP software
    - ejemplo, 2-10
    - interfaz sip0, 2-4
    - ruta, 2-10
    - sip#, crear, 2-10
  - interfaz local, 2-4
  - interfaz loopback (lo0), 2-3
  - interfaz reject (rj0), 2-4
  - interfaz tunnel, 2-4
  - interfaz virtual router (vr0\_main), 2-4
  - interfaz wanabe, 2-4
  - Internet Group Membership Protocol (IGMP). *Consulte* IGMP
  - IP
    - dirección de interfaz software, 2-10
    - notación de subred, 2-5
    - ruteos de host, 2-6
-

## Índice alfabético

### L

IP de línea serie (SLIP). *Consulte* SLIP  
(IP de línea serie)

IP direct, ejemplo, 2-21

IP en IP

ejemplo, 5-34

implantación actual, 5-33

tamaño de la MTU, 5-33

IPSec

cifrado, 5-11

L2TP, configurar, 5-6

modo de transporte, 1-30, 5-7

modo de túnel, 1-30, 5-7

perfil para AH de IPSec, 5-9

perfil, aplicar a LNS, 5-8

protocolos, 5-6

servidor del túnel, aplicar, 5-7

interfaces IPX de WAN

IPX

en ATMP, 4-31

extensiones TAOS para el ruteo de WAN, 7-2

marcar conexiones para consultas SAP, 7-3

números de zócalo, 7-16

red virtual para clientes de entrada, 7-3, 7-5

requisito del controlador de módulo, 7-5

rutas estáticas, 7-13

software de cliente NetWare, 7-4

*Consulte también* interfaces IPX de LAN

IPX rutas estáticas, ejemplo, 7-17

ipxroute, RADIUS, 7-12

IPXWAN, soporte para la negociación, 7-2

### L

L2F

perfiles de cliente, configurar, 5-22

L2TP

autenticación del túnel

CLID o DNIS, 5-5

PPP, 5-6

autenticación del túnel, IPSec, 5-6

ejemplo, 5-3

enlaces de control y de datos, 5-1

función de concentrador de acceso (LAC), 5-1

intentos de lista, 5-15

nombre del sistema, 5-18

opciones del temporizador, 5-14

puntos finales múltiples, 5-15

ruteadores virtuales, utilización con, 6-14

servidor de red (LNS), conexión con el, 5-3

túnel con LNS, 5-2

líneas arrendadas, conexiones en, 1-34

lista DNS, 2-59

llamada de salida direct-access

configurar, 1-47

contraseñas para, 1-48

ejemplo con contraseña de usuario, 1-50

ejemplo con contraseña global, 1-48

seguridad, 1-48

llamadas

autenticación, 1-2

de salida, iniciar, 1-3

perfil Answer-Defaults, 1-2

perfiles configurados, 1-2

ruteo, 1-2

salida, configurar, 1-44

llamadas analógicas y MP, 1-18

llamadas de entrada, 1-6

autenticar, 1-4

contraseñas, 1-45

MP+, 1-34, 1-37

perfil Answer-Defaults, 1-3

PPP, 1-45

responder, 1-34, 1-37, 1-38

SDTN, 11-5

TCP-Clear, B-3

llamadas de salida

contraseñas, 1-13

ejemplo, 1-43

iniciar, 1-3, 1-34, 1-37, 1-38

PPP, 1-13

protocolo de autenticación, A-6

llamadas de transacciones de módem, SDTN, 11-9

LNS

conexiones, configurar, 5-3

*Consulte también* servidor de red L2TP

perfil IPSec, aplicar a, 5-8

LSA de tipo 5, 3-7

LSA de tipo 7, 3-7, 3-19

LSA, intervalo de retransmisión, 3-12

### M

máscara de red. *Consulte* máscara de subred

máscaras de subred de longitud variable (VLSM), 3-4

métrica, 2-14, 3-1, 3-6

módems

ajustes recomendados, A-22

autenticación y secuencias de comandos Expect-Send,  
A-22

ISDN, 1-4

llamada de salida direct access, 1-48

llamadas PPP, 1-16

módems analógicos. *Consulte* módems

módems ISDN

descripción, 1-4

servidor de terminales, 1-5

modo de bloqueo de adición de ancho de banda, 1-20

modo de menú  
 autorizar el acceso, B-4  
 configurar el texto del menú, B-6  
 descripción, B-2

modo de seguridad (servidor de terminales), A-23

modo de terminal  
 autorizar, B-10  
 descripción, B-10

modo de transporte, IPSec, 1-30, 5-7

modo de túnel, IPSec, 1-30, 5-7

modo inmediato, B-2  
 autorización del acceso, B-2  
 PPP, B-3

modos, acceso al servidor de terminales  
 inmediato, B-2  
 menú, B-2  
 seguridad, B-16

modos, acceso del servidor de terminales  
 terminal, B-10

MP  
 atributos RADIUS, 1-17  
 canales básicos, 1-16  
 canales máximos, 1-17  
 canales mínimos, 1-17  
 configurar, 1-16  
 ejemplo, 1-18  
 número de canales que se utiliza, 1-17  
*Consulte también* PPP

MP+  
 agregar ancho de banda, 1-20  
 configurar, 1-19  
 conmutado, ejemplo, 1-23  
 controlar la utilización de ancho de banda, 1-21  
 DBA, 1-20  
 directrices de ancho de banda, 1-20  
 grado de utilización de la línea para agregar ancho de banda, 1-22  
 incrementos de ancho de banda, 1-21  
 modo de bloqueo de adición de ancho de banda, 1-20  
 permanente, ejemplo, 1-37  
 persistencia del grado de utilización, 1-22  
 picos en la utilización de la línea, 1-20  
 RADIUS, 1-22  
 tarifas de telecomunicaciones, 1-20  
 umbral para solicitar ancho de banda, 1-22  
*Consulte también* MP, PPP

MS-CHAP, autenticación, A-9

multiacceso de no difusión, 3-21

## N

NBMA. *Consulte* multiacceso de no difusión, 3-21

NetBIOS

direcciones IP de host, 2-72  
 paquetes IPX de tipo 20, 7-7  
 servidores, especificar, 2-58

Net-Number y Net-Alias, 7-10

NetWare. *Consulte* IPX  
 ejemplos, 7-11

nombre del sistema  
 L2TP, 5-18

nombres  
 dispositivo remoto, del, 1-13  
 DNS, 1-26  
 host, 1-26  
 inicio de sesión, 1-3, 1-5, 1-49

notación de subred, 2-5

NSSA de OSPF, ejemplo, 3-19

número de índice de parámetro de seguridad (SPI), 5-9

números de zócalo, IPX, 7-16

## O

objetivo de utilización, solicitar ancho de banda y, 1-22

opciones de ASE de OSPF, ejemplo, 3-17

opciones de contabilidad para sesiones, 1-11

opciones del temporizador, L2TP para, 5-14

OSPF  
 adyacencias, formación, 3-4  
 ajustes de la ruta estática, 3-18  
 algoritmo de ruteo de estado de enlace, 3-8  
 áreas normales, 3-7  
 áreas NSSA (not-so-stubby area), 3-7  
 áreas stub, 3-7  
 áreas y ABR, 3-6  
 autenticación MD5 (RFC 2178), 3-4  
 cálculos ASBR, 3-2  
 comunicaciones entre ruteadores, 2-3  
 contiguos, 3-5  
 costes, 3-6  
 costes, configurar, 3-6  
 definición de AS, 3-3  
 desactivar globalmente, 3-25  
 función ABR, 3-2  
 GRF conmutador, y, 3-13  
 importar rutas de agrupaciones de direcciones, 3-17  
 interfaces IP de LAN, configurar, 3-13  
 interfaces virtuales, limitación, 3-3  
 LSA de tipo 5, 3-7  
 LSA de tipo 7, 3-7  
 LSA de tipo 7, configurar, 3-19  
 opciones de ASE, configurar, 3-17  
 paquetes hello, 3-11  
 RIP, comparación, 3-1  
 RIP, importar como ASE, 3-16  
 rutas de terceros, 3-20

ruteador designado, 3-4  
ruteador designado de reserva, 3-4  
soporte multiacceso de no difusión (NBMA), 3-21  
soporte para máscaras de subred de longitud variable (VLSM), 3-4  
tabla de ruteo, creación, 3-9  
tipos de área, 3-7  
OSPF y RIP, ejemplo, 3-15

**P**

PAP, autenticación, descripción, A-8  
PAP-TOKEN, autenticación, A-30  
PAP-TOKEN-CHAP, autenticación  
para llamadas de entrada, A-31  
paquetes  
redirección de puertos, 2-55  
paquetes de ruta de origen, descartar, 2-44  
paquetes en el búfer  
descripción, 1-25  
ejemplo, 1-28  
paquetes hello OSPF, 3-5  
parámetro VRouter para L2TP, 6-15  
patrón de final de paquete, 1-27  
perfil Answer-Defaults  
acceso como invitado de ARA, 8-4  
ajustes predeterminados, 1-4  
autenticación PPP, requerir, 1-4  
cómo el sistema responde llamadas, 1-3  
filtros, RADIUS, 9-36  
llamadas de entrada, 1-2, 1-3  
modo homólogo IPX, 7-10  
predeterminados RADIUS, 1-4  
V.120, 1-4  
perfil Atalk-Global, 8-1  
perfil Atalk-Interface, 8-2  
perfil ATMP  
agente externo, 4-8  
agente local, 4-17, A-34  
agente local y externo, 4-28  
perfil Connection, 1-7  
ajustes de MP, 1-16  
ajustes de MP+, 1-7, 1-21, 1-24, 2-42  
ajustes de OSPF, 3-10  
ajustes de PPP, 1-12  
ajustes del cliente móvil ATMP, 4-9  
ARA, 8-5  
asignación dinámica de direcciones, 2-74, 2-78, 2-80  
envío de difusión múltiple, 2-87  
filtros, aplicar, 9-34  
Frame Relay Direct, 2-33, 9-31  
gestión de sesiones, 1-9  
llamada de salida, 1-44

llamada de salida por módem, 1-49  
opciones de IPX, 7-8  
opciones DNS de cliente, 2-64  
opciones IP, 2-13  
permanente, 1-34  
ruteo AppleTalk, 8-5  
servidor de red L2TP, conexión con el, 5-3  
servidor de red PPTP, 5-26  
TCP-Clear, 1-25  
túnel IP en IP, 5-33  
X.75, 1-33  
perfil External-Auth, 1-6  
perfil Filter  
acción de reenvío, 9-7  
dirección, A-20, A-21, A-38, A-39, B-15  
genérico, 9-7  
IP, 9-12  
IPX, 9-25  
ruta, 9-28  
tipo de servicio, 9-19  
TOS, 9-19  
tráfico, dirección filtrada, 9-6  
perfil IP-Global, 2-39  
agrupaciones de direcciones, 2-68  
dirección del sistema, 2-39  
envío de difusión múltiple, 2-81  
opciones de caché de ruta, 2-49  
opciones de protocolo, 2-51  
opciones de ruteo del sistema, 2-43  
opciones de seguridad del ruteador, 2-40  
opciones DNS, 2-58  
opciones DNS de cliente, 2-64  
opciones RIP, 2-45  
OSPF, 3-16  
perfil IP-Interface, 2-6  
ajustes, 2-7  
direcciones de ranuras, 2-6  
ejemplos, 2-7  
envío de difusión múltiple, 2-87  
filtros de ruta, 9-34  
OSPF, 3-10  
perfil IP-Route  
ajustes, 2-26  
ejemplos, 2-29  
OSPF, 3-18  
rutas de varios trayectos, 2-32  
perfil IPX-Global, 7-4  
perfil IPX-Interface, 7-5  
perfil IPX-Route, 7-14  
perfil IPX-SAP-Filter, 7-17  
perfil L2-Tunnel-Global  
L2TP, 5-2  
PPTP, 5-25  
perfil RADIUS predeterminado, 1-4  
perfil SNMP, B-16

- hr/>
- Perfil Terminal-Server, A-23
  - perfil Terminal-Server, 1-5
    - ajustes predeterminados de sesiones Telnet, B-12
    - autorización de inicios de sesión interactivos, B-11
    - autorización de sesiones PPP, B-14
    - autorización para, B-2
    - establecer tercer indicador, A-24
    - llamada de salida por módem, 1-47
    - restricción del acceso, B-1
  - perfil Transaction-Server, 11-2
  - perfil Tunnel-Server
    - L2TP, 5-2
    - PPTP, 5-25
  - perfil VRouter, 6-3
  - perfiles
    - agrupaciones RADIUS, 2-69
    - Answer-Defaults, 1-3
      - autenticación, requerir, 1-4
      - configuración de V.12, 1-4
      - predeterminados RADIUS, 1-4
    - Atalk-Global, 8-1
    - Atalk-Interface, 8-2
    - ATMP
      - agente externo, 4-8, A-34
      - agente local, 4-17
    - compartir, 1-7, 2-41
    - Connection, 1-7
      - ARA, 8-5
      - clientes móviles ATMP, 4-9
      - DNS cliente, 2-64
      - envío de difusión múltiple, 2-87
      - filtros, aplicar, 9-34
      - Frame Relay Direct, 2-33, 9-31
      - gestión de sesiones, 1-9
      - llamada de salida, 1-44
      - llamada de salida por módem, 1-49
      - opciones de IPX, 7-8
      - opciones IP, 2-13
      - OSPF, 3-10
      - permanente, 1-34
      - PPP, 1-13
      - ruteo AppleTalk, 8-5
      - TCP-Clear, 1-25
      - túnel IP en IP, 5-33
      - X.75, 1-33
    - External-Auth, 1-6
    - Filter
      - acción de reenvío, 9-7
      - dirección, A-20, A-21, A-38, A-39, B-15
      - genérico, 9-7
      - IP, 9-12
      - IPX, 9-25
      - ruta, 9-28
      - TOS, 9-19
    - global-pools RADIUS, 2-70
    - IP-Global, 2-39
      - agrupaciones de direcciones, 2-68
      - dirección del sistema, 2-39
      - envío de difusión múltiple, 2-81
      - opciones de caché de ruta, 2-49
      - opciones de protocolo, 2-51
      - opciones de ruteo del sistema, 2-43
      - opciones de seguridad del ruteador, 2-40
      - opciones DNS, 2-58
      - opciones DNS de cliente, 2-64
      - opciones RIP, 2-45
      - OSPF, 3-16
    - IP-Interface, 2-6, 2-87
      - filtros de ruta, 9-34
      - OSPF, 3-10
    - IP-Route, 2-26
      - OSPF, 3-18
    - IPX-Global, 7-4
    - IPX-Interface, 7-5
    - IPX-Route, 7-14
    - IPX-SAP-Filter, 7-17
    - L2-Tunnel-Global
      - L2TP, 5-2
      - PPTP, 5-25
    - RADIUS
      - acción de filtro, 9-7
      - agente local de gateway ATMP, 4-14
      - agente local del ruteador ATMP, 4-14
      - ARA, 8-6
      - clientes móviles ATMP, 4-10
      - dirección del filtro, 9-6
      - DNS cliente, 2-65, 2-66
      - filtros genéricos, 9-9
      - filtros IP, 9-14
      - filtros TOS, 9-22
      - filtros, aplicar, 9-35
      - gestión de sesiones, 1-9, 1-11
      - IPX ATMP, 4-33, 4-35
      - llamada de salida, 1-45
      - llamada de salida por módem, 1-49
      - LNS, conexión con, 5-3, 5-26
      - opciones de IPX, 7-9
      - opciones IP, 2-15
      - permanente, 1-35
      - PPP, 1-13
      - PPP, multienlace, 1-17
      - rutas estáticas privadas, 2-29
      - ruteo AppleTalk, 8-6
      - TCP-Clear, 1-28, B-4, B-6
      - túnel IP en IP, 5-34
    - RADIUS ipxroute, 7-15
    - rutas RADIUS, 2-27
    - SNMP, B-16
    - Terminal-Server, 1-5, A-24, B-1
      - autorización, B-2
      - modo de seguridad, A-23
      - PPP-Mode-Configuration, B-14
      - Terminal-Mode-Configuration, B-11, B-12
    - Tunnel-Server
      - L2TP, 5-2
      - PPTP, 5-25
    - VRouter, 6-3
  - perfiles de llamada de salida, RADIUS, 1-43
  - perfiles de pseudousuario de ruta RADIUS, 2-27
-

- hr/>
- perfiles de pseudousuario. *Consulte* RADIUS
  - perfiles de usuario, RADIUS. *Consulte* RADIUS
  - peticiones de eco, pasar por alto la difusión, 2-44
  - Ping, pasar por alto la difusión, 2-44
  - política RIP de horizonte dividido, 2-47
  - política RIP de veto de rutas inverso, 2-47
  - políticas de ruteo
    - calidad del servicio, 2-24
    - descartar paquetes de ruta de origen, 2-44
    - dirección IP del sistema, 2-40
    - generales del sistema, 2-43
    - opciones de caché, 2-49
    - opciones de protocolo, activar, 2-51
    - RIP, 2-45
    - seguridad, ruteador, 2-40
    - tipo de servicio, 2-24
    - unidades redundantes, 2-48
  - PPP
    - atributos RADIUS, 1-13
    - autenticación, B-3
    - autenticación de contraseñas, A-6
    - autorización, B-13
    - compresión del enlace, 1-13
    - configuración, ejemplo, 1-15, 1-16, 1-46
    - configurar, 1-12
    - control de calidad de enlaces, 1-14
    - control de la calidad del enlace, 1-13
    - enviar contraseña (llamada de salida), 1-45
    - MRU, 1-13
    - recibir contraseña (llamada de entrada), 1-13
    - requerir autenticación, 1-4
    - síncrono, ejemplo, 1-15
  - PPTP
    - autenticación del túnel
      - CLID o DNIS, 5-28
      - PPP, 5-29
    - enlace de datos GRE, 5-25
    - enlaces de control y de datos, 5-25
    - función de concentrador de acceso (PAC), 5-24
    - servidor de red (PNS), conexión con el, 5-24
    - túnel con el PNS, 5-26
  - precedencia, Tipo de servicio, 2-15, 2-18
  - predicción de cabeceras VJ, 2-13
  - preferencias, 2-45
    - ajustes predeterminados, 2-45
    - RIP, 2-47
    - rutas estáticas, 2-45
  - prioridad para ruteadores designados, 3-11
  - protocolo AH. *Consulte* protocolo de cabecera de autenticación (AH)
  - protocolo Boot (BOOTP). *Consulte* BOOTP
  - protocolo de autenticación
    - especificar, A-6
    - RADIUS, utilización, A-7
  - protocolo de autenticación de contraseñas (PAP).
    - Consulte* autenticación
  - protocolo de autenticación de establecimiento de enlace con desafío (CHAP). *Consulte* autenticación
  - protocolo de cabecera de autenticación (AH), 5-6
  - protocolo de carga útil de seguridad de la encapsulación (ESP), 5-6
  - protocolo de control de asignación de ancho de banda
    - Consulte* BACP, 1-24
  - protocolo de control de devolución de llamada (CBCP), A-45
  - protocolo de control de transmisiones (TCP). *Consulte* TCP
  - protocolo de datagramas de usuario (UDP). *Consulte* UDP
  - protocolo de gestión de túneles de Ascend (ATMP).
    - Consulte* ATMP
  - protocolo de gestión del control de Internet (ICMP).
    - Consulte* ICMP
  - protocolo de hora de red simple (SNTP). *Consulte* SNTP
  - protocolo de información de ruteo (RIP). *Consulte* RIP
  - protocolo de resolución de direcciones (ARP). *Consulte* ARP
  - protocolo de transacción rápida (QTP), 11-1
  - protocolo de túnel de capa 2 (L2TP). *Consulte* L2TP
  - protocolo de túnel de capa 2 (L2TP). *Consulte* L2TP
  - protocolo de túnel punto a punto (PPTP). *Consulte* PPTP
  - protocolo punto a punto (PPP). *Consulte* PPP
  - protocolo simple de gestión de red. *Consulte* SNMP
- protocolos
- AppleTalk, 8-1
  - ARP, 2-8
  - ATMP, 4-1
  - autenticación, A-7
  - BOOTP, 2-52
  - cabecera de autenticación (AH), 5-6
  - CCP, 1-14
  - CHAP, 1-45
  - estadísticas para, 6-5
  - GRE, 4-1, 5-25
  - ICMP, 2-44
  - IGMP, 2-80
  - IP en IP, 5-33
  - IPSec, 5-6
  - IPX, 7-2
  - IPXWAN, 7-2
  - L2TP, 5-1
  - Microsoft/STAC, 1-14
  - MP+, 1-19
  - MS-CHAP, 1-45
  - opciones de ruteador, activar, 2-51



OSPF, 3-1  
 PAP, 1-45  
 PPP, 1-13, 1-17  
 PPTP, 5-24  
 protocolo de carga útil de seguridad de la  
   encapsulación (ESP), 5-6  
 protocolo de transacción rápida (QTP), 11-1  
 RIP, 2-9  
 RIP IPX, 7-2  
 SAP IPX, 7-1  
 SLIP, B-15  
 SNTP, 2-55  
 Stac LZS, 1-14  
 TCP, 2-53  
 Telnet, B-3  
 UDP, 2-48  
 V.120, 1-5  
 X.75, 1-32  
 protocolos de encapsulación, 1-2  
   ARA, 8-4  
   Framed-Protocol en RADIUS, 1-13  
   GRE, 4-1  
   IP en IP, 5-33  
   MP, 1-17  
   MP+, 1-19  
   PPP, 1-13  
 proxy ARP, 2-8  
 puertos  
   destino para conexiones TCP-Clear, B-4  
   destino TCP-Clear, 1-26, 1-28  
   direct-access, para, 1-47  
   TCP, para acceso al módem, 1-47  
 puntos finales múltiples, para L2TP, 5-15

## Q

QOS de proxy, ejemplos, 2-25  
 QTP, 11-3

## R

RADIPAD para la gestión centralizada de agrupaciones,  
   2-69  
 radipa-hosts, RADIUS, 2-70  
 RADIUS  
   acción de reenvío, 9-7  
   agente local de gateway ATMP, 4-14  
   agente local del ruteador ATMP, 4-14  
   agrupaciones resumidas, 2-73  
   ajustes de MP, 1-17

ajustes de MPP, 1-22  
 ajustes de PPP, 1-13  
 ARA, 8-6  
 asignación dinámica de direcciones, 2-74, 2-78, 2-80  
 atributos de clientes móviles ATMP, 4-10  
 atributos de telecomunicaciones, 1-35  
 atributos DNS de cliente, 2-65, 2-66  
 atributos IP de la conexión, 2-15  
 CHAP bidireccional, configurar, A-15  
 clientes de difusión múltiple, 2-87  
 conexiones permanentes, 1-35  
 dirección del filtro, 9-6  
 filtros genéricos, 9-9  
 filtros IP, 9-14  
 filtros predeterminados en Answer-Defaults, 9-36  
 filtros TOS, 9-22  
 filtros, aplicar, 9-35  
 gestión de contraseñas, A-2  
 gestión de sesiones, 1-9, 1-11  
 información general, 1-8  
 interfaz wanabe, 2-4  
 IPX de ATMP, 4-33, 4-35  
 llamada de salida, 1-45  
 llamada de salida por módem, 1-49  
 LNS, conexión con, 5-3, 5-26  
 modo homólogo IPX predeterminado, 7-10  
 opciones de IPX, 7-9  
 perfil External-Auth, 1-6  
 perfiles de agrupaciones, 2-69  
 perfiles de pseudousuario de agrupaciones, 2-69  
 perfiles de ruta, 2-27  
 perfiles global-pools, 2-69  
 perfiles ipxroute, 7-15  
 PPP, 1-13  
 PPP, multienlace, 1-17  
 predeterminados, 1-4  
 protocolo de autenticación, especificar, A-7  
 pseudo-usuario  
   ipxroute, 7-15  
 pseudousuario  
   agrupaciones, 2-27, 2-69  
   global-pools, 2-70  
 rutas estáticas privadas, 2-29, 2-38  
 rutas privadas, configurar, 2-33  
 ruteo AppleTalk, 8-6  
 secretos compartidos, A-5  
 servidor de tarjetas de testigo, A-26  
 TCP-Clear, 1-28, B-4, B-6  
 temporizador de inactividad, 1-10  
 túnel IP en IP, 5-34  
 volver a cargar perfiles permanentes, 1-35  
*Consulte también* perfiles  
 rango de puertos de origen Rlogin configurable, B-12

- 
- rangos de red, AppleTalk, 8-1
  - Read-Community, B-16
  - Read-Write-Community, B-16
  - red troncal de difusión múltiple (MBONE), 2-80
  - red virtual IPX para clientes de entrada, 7-3
  - redes de transacciones, 11-1
  - redes de transacciones de corta duración. *Consulte* STDN
  - redes virtuales privadas. *Consulte* túneles, ruteadores virtuales
  - redes virtuales privadas. *Consulte* túneles, ruteadores virtuales
  - redirección de puerto, 2-55
  - reenvío de capa 2 (L2F), 5-18
  - reinicio del sistema
    - requisitos de ATMP, 4-2
  - reloj, configurar mediante SNTP, 2-55
  - resumen. *Consulte* agrupación
  - retardo de tránsito LSA, 3-12
  - Reverse-ARP (RARP). *Consulte* RARP
  - RIP
    - actualizar solamente las rutas cambiadas (desencadenamiento), 2-47
    - agentes locales ATMP, 4-19
    - ASE de OSPF, 3-15
    - ATMP, entre agentes, 4-3
    - desencadenar, 2-47
    - dirección de difusión múltiple, 2-7
    - dirección del sistema, anunciada, 4-3
    - filtros de ruta, definición, 9-28
    - interfaces de LAN, utilizar en, 2-9
    - métrica, 2-14
    - OSPF, comparación, 3-1
    - paquetes, número en la cola, 2-48
    - pasar por alto la ruta predeterminada en las actualizaciones, 2-49
    - propagación de rutas recibidas, 2-46
    - ruteador virtual, definición, 6-4
    - Consulte también* RIP IPX, 7-2
  - RIP IPX
    - interfaces de WAN, 7-10
    - rutas estáticas IPX, 7-14
    - unidades TAOS, entre, 7-2
  - RIP y OSPF, 3-15
  - RIP, desencadenar, 2-47
  - Rlogin, rango de puertos de origen, B-12
  - ruta de subred, ejemplo, 2-31
  - ruta del host, ejemplo, 2-19
  - ruta predeterminada
    - cómo utilizarla, 2-25
    - configuración de ejemplo, 2-29
    - ejemplo, 2-29
    - específica del cliente, definición, 2-23
    - protección frente a actualizaciones, 2-49
    - tabla de interfaces, 2-2
    - varios trayectos, 2-32
  - ruta, RADIUS, 2-27
  - rutas de host
    - resumidas en anuncios, 2-72
    - supresión de anuncios, 2-49
  - rutas de terceros, 3-20
  - rutas directas, 2-2
  - rutas estáticas
    - agrupaciones resumidas, a, 2-73
    - ajustes de OSPF, 3-18
    - ajustes del perfil IP-Route, 2-26
    - atributos RADIUS, 2-27
    - clientes móviles ATMP a, 4-22
    - dirección de software, 2-11
    - IPX al servidor NetWare, 7-13
    - perfil de usuario RADIUS, en, 2-28
    - perfiles para definir, 2-1
    - preferencias, 2-45
    - privadas por conexión (RADIUS), 2-29, 2-38
    - razones para definir las, 2-25
    - ruta predeterminada, ejemplo, 2-29
    - ruteador virtual, definir para un, 6-10
    - subred remota, a una, 2-31
    - terceros, OSPF, 3-20
    - varios trayectos, 2-32
  - rutas estáticas privadas en RADIUS, 2-38
  - rutas privadas, 2-22
    - ejemplo, 2-22
    - específicas de la conexión, 2-38
  - rutas privadas (RADIUS), ejemplo, 2-38
  - rutas RADIUS en perfiles de usuarios, 2-28
  - ruteador designado (DR), 3-4
  - ruteador designado de reserva (BDR), 3-4
  - ruteador no raíz, 8-4
  - ruteador raíz, AppleTalk, 8-3
  - ruteadores virtuales
    - agrupaciones de direcciones para, 6-4
    - asignación de interfaces a, 6-7
    - comandos de red modificados, 6-2
    - definición, 6-1
    - definición, ejemplo, 6-4
    - dirección del sistema para, 6-4
    - eliminar, 6-12
    - estadísticas de protocolo, 6-5
    - interfaces, visualización, 6-9
    - L2TP, soporte para, 6-14
    - políticas de RIP, 6-4
    - rutas estáticas, definición, 6-10
    - rutas estáticas, visualización, 6-11
    - tabla de ruteo, 6-5
  - ruteadores virtuales, ejemplo, 6-4
  - ruteo IP, ejemplo, 2-18
-

ruteo IPX, ejemplo, 7-11  
ruteo privado, tablas, 2-32

## S

salida, cómo se inician llamadas de, 1-3

### SAP IPX

dial query, 7-3  
filtro, ejemplos, 7-18  
paquetes de respuesta, servicios de filtrado, 7-17  
tabla SAP, cómo utilizarla, 7-1  
tabla SAP, servicios de filtrado, 7-17

### SDNT

servidor de transacciones, definición, 11-3

### SDTN

clientes de transacciones, 11-5  
conexiones VISA II, configurar, 11-8  
HDLC-modo de respuesta normal, 11-5  
licencia, verificar, 11-1  
National Institute of Standards and Technology, 11-1  
perfiles, 11-2  
protocolo de red sin conexiones (CLNP), 11-1  
retardos de ajuste, evitar, 11-9  
terminales Visa, 11-1

secretos compartidos, A-5

secuencias de comandos de inicio de sesión, A-22

Expect-Send, A-22

### seguridad

ajustes predeterminados de Telnet, B-12  
autenticación CLID, A-36, A-37  
autenticación del número llamado, A-38  
autenticación por tarjeta de testigo, A-2, A-26  
autorización de inicios de sesión interactivos del ser,  
B-11  
autorización de sesiones SLIP, B-15  
autorización del modo inmediato, B-2  
autorizar el modo de menú, B-4  
contraseña del sistema, A-23  
contraseñas para conexiones PPP, A-6  
desactivar difusiones dirigidas, 2-11  
dirección de origen, verificación, 2-23  
dirección SNMP, B-16  
dirección, aplicar, B-17  
información de llamada, utilizar, A-37  
llamada de salida direct-access, para, 1-48  
modo de menú, B-2  
modo de terminal, B-10  
modo del servidor de terminales, B-16  
modo inmediato, B-2  
pasar por alto peticiones de eco ICMP de difusión  
general, 2-44  
políticas del ruteador, 2-40  
restricción del acceso al servidor de terminales, B-1  
sesiones PPP, B-13

tarjetas de testigo, utilizar, A-26

tercer indicador, A-25

verificación de la dirección de origen, 2-23

servicio analógico, especificar en una conexión, A-29

servicio digital, especificar en una conexión, A-29

### servidor de terminales

ajustes predeterminados de Telnet, B-12  
autorización de inicios de sesión interactivos, B-11  
autorización de sesiones SLIP, B-15  
autorización del modo inmediato, B-2  
autorizar el modo de menú, B-4  
cabeceras, A-24  
conexiones asíncronas, 1-5  
contraseña del sistema, A-23  
indicador de contraseña, A-24  
indicador de inicio de sesión, A-24  
modo de menú, B-2  
modo de seguridad, B-16  
modo de terminal, B-10  
modo inmediato, B-2  
protección de contraseña, A-22  
restricción del acceso, B-1  
secuencias de comandos de inicio de sesión  
Expect-Send, A-22  
tercer indicador, A-25

servidor de transacciones, definición, 11-3

servidor Microsoft WINS, asignar, 2-66

### servidores

autenticación externa, 1-6, A-26  
BOOTP, 2-54  
DNS, cliente, 2-63  
DNS, local, 2-59  
Enigma Logic SafeWord, A-26  
NetBIOS, 2-58  
NetWare, rutas hacia, 7-14  
proxy del servidor local NetWare, 7-11  
RADIUS, ejecutar RADIPAD, 2-69  
Security Dynamics ACE/Server, A-26  
SNTP, 2-55

servidores DNS, configuración de ejemplo, 2-65

servidores locales de proxy IPX, 7-11

servidores locales de proxy, IPX, 7-11

### sesiones

ajustes de los perfiles Connection, 1-9  
ajustes en RADIUS, 1-9  
ajustes predeterminados de Telnet, B-12  
control, 1-3  
duración máxima, 1-9  
framed-protocol, establecer, 1-3  
opciones de contabilidad, 1-11  
servicio login-service, establecer, 1-3

sesiones de Login-Service, 1-3, 1-6

sesiones Framed-Protocol, 1-3

simulación de direcciones locales, evitar, 9-16

simulación de tipos de trama IPX, 7-6  
 sistema autónomo (AS)  
     definición, 3-3  
     función de ruteador de frontera (ASBR), 3-2  
 sistema de nombre de dominio (DNS). *Consulte* DNS  
 sistema de nombres de dominio (DNS). *Consulte* DNS  
 SLIP (IP de línea serie)  
     *Consulte también* autorización  
     dirección de BOOTP, B-15  
 SNMP  
     activar, B-17  
     aplicar la seguridad de direcciones, B-17  
     autorización, B-16  
     cadenas de comunidad, B-16  
     captura de alarma para control de pulso, 2-83  
     limitaciones para ruteadores virtuales, 6-3  
     paquetes, número en la cola, 2-48  
     seguridad de direcciones, B-16  
 SNTP  
     desplazamiento de UTC, especificar, 2-55  
     servidores, especificar, 2-55  
 soporte de ID de filtro RADIUS, 9-36  
 soporte de número mágico LQM, 1-15  
 soporte para varios destinos para TCP-Clear, 1-25  
 soporte Proxy-QoS y TOS, 2-24  
 sumas de comprobación, UDP, 2-52  
 supresión de anuncios de ruta de host, 2-49

## T

TA (Adaptador de terminal) V.120, 1-5  
 tabla de interfaces IP, visualización, 2-3, 6-5  
 tabla de ruteo IP  
     campos, explicación, 2-2  
     convergencia, RIP, 3-2  
     crear, 2-1  
     OSPF comunicaciones entre ruteadores, 2-3  
     preferencias, 2-45  
     ruta a la interfaz local, 2-2  
     ruta a la interfaz mcast, 2-2  
     ruta predeterminada, 2-2  
     rutas dinámicas, 2-2  
     rutas directas, 2-2  
     rutas estáticas, 2-1  
     ruteador virtual, para, 6-5  
     ruteadores virtuales y direcciones, 6-2  
     visualización, 2-2  
     *Consulte también* base de datos de estado de enlace  
 tabla de ruteo privado, 2-32  
 tabla de ruteo. *Consulte* tabla de ruteo IP  
 tabla DNS local, ejemplo, 2-60  
 tarjeta Hybrid Access

longitud máxima de las tramas, 1-33  
 tarjetas de ranura, utilización en llamadas de entrada, 1-1  
 tarjetas de testigo, A-26, A-28  
     desafíos de acceso, A-28  
     ejemplo para llamada de entrada, A-28  
 TCP  
     enlace de control del túnel PPTP, 5-25  
     puerto para servicio inmediato de llamada de salida, 1-47  
     valor de tiempo de espera, 2-53  
 TCP-Clear, 1-25  
     ajustes necesarios, 1-25  
     atributos RADIUS, 1-28  
     autenticación de, B-3  
     contraseñas, 1-26  
     corrientes de datos en el búfer, 1-25  
     dirección IP del host, 1-26  
     ESP de IPSec, 1-31  
     mejoras de rendimiento, 1-25  
     mensajes de estado, desactivar, 1-28  
     nombre DNS del host, 1-26  
     patrón de final de paquete, 1-27  
     protocolo de encapsulación, 1-26, 1-28, B-4  
     puerto TCP de destino, 1-26, 1-28, B-4  
     varios destinos, 1-25  
 TCP-Raw. *Consulte* TCP-Clear  
 telecomunicaciones  
     ajustes de los perfiles Connection, 1-7  
     atributos RADIUS, 1-35  
     conexiones permanentes, opciones, 1-34  
     información CLID o DNIS, 5-5, 5-28  
     información de llamada, A-36  
     tarifas, 1-20  
 Telnet  
     ajustes predeterminados de modo de terminal, B-12  
     contraseña, A-6  
     inicios de sesión, 2-43  
     perfil User predeterminado, 2-42  
 temporizador de salida, 1-43  
 temporizador de salida configurable, 1-43  
 temporizadores  
     definir un valor absoluto en las conexiones, 1-10  
     para túneles inactivos, 4-19  
     RADIUS, en, 1-10  
     sesiones PPP, para, 1-8  
 temporizadores de inactividad  
     RADIUS, en, 1-10  
     túneles ATMP, 4-19  
 tercer indicador, A-25  
 testigos, A-28  
 tiempo de espera, inicio de sesión, A-24  
 tipo de llamada para las conexiones, 1-34

tolerancia a fallos  
 dirección IP del controlador, 2-10

TOS (Tipo de servicio)  
 ajustes, 2-15, 2-17  
 ejemplos, 2-25  
 información general, 2-24  
 niveles de prioridad, 2-15, 2-18

tramas, tipos IPX, 7-6

túnel ATMP conectado con conmutador GRF, 4-16

túneles  
 autenticación ATMP, A-35  
 autenticación del túnel L2TP, 5-5, 5-6  
 autenticación del túnel PPTP, 5-28, 5-29  
 compresión del enlace, 4-5  
 configuraciones de clientes móviles, 4-9  
 conmutador GRF, 4-5, 4-16  
 DDP-IP, 8-10  
 información general de ATMP, 4-1  
 información general de L2TP, 5-1, 5-14  
 información general de PPTP, 5-24  
 IP en IP, 5-33  
 IPX en ATMP, 4-31  
 L2TP, configurar el túnel, 5-2  
 límite de MTU, explícito, 4-4  
 límites de reintento de ATMP, 4-4  
 perfiles de L2TP, 5-2  
 perfiles PPTP, 5-25  
 petición de túnel ATMP  
   agente externo, 4-11  
   respuesta del agente local, 4-18, 4-20  
 PPTP, configuración del túnel, 5-25  
 puerto UDP para la información de control de ATMP, 4-3  
 temas relativos a la fragmentación, 4-5  
 temporizador de inactividad ATMP, 4-19

túneles DDP-IP, 8-10

túneles L2F  
 autenticación, 5-19

## U

UDP  
 ATMP, puerto para el control del túnel, 4-3  
 colas de paquetes, reducción de la carga útil, 2-48  
 puerto para el enlace de control del túnel L2TP, 5-2  
 sumas de comprobación, activar, 2-52

unidad máxima de recepción (MRU), 1-13, 4-5

unidad máxima de transmisión (MTU), 4-4, 5-33

utilización de la línea  
 algoritmo dinámico para calcular, 1-21  
 atributos RADIUS, 1-22  
 objetivo de utilización y, 1-22  
 período de tiempo para calcular, 1-21  
 picos, 1-20

utilización de los canales  
 ancho de banda, 1-21  
 llamadas multienlace, 1-17  
 máximo permitido, 1-17  
 mínimo para establecer una sesión, 1-17  
 número básico, 1-16  
 permanentes, 1-34

utilización media de la línea (ALU). *Consulte*  
 utilización de la línea

## V

V.120 TA (Adaptador de terminal), 1-5  
 ajustes para llamadas de entrada, 1-4  
 autenticación, B-3  
 servidor de terminales, 1-5

velocidad de recepción, 1-11

velocidad de transmisión, 1-11

verificación de la dirección de origen, 2-23

verificación de la dirección de origen por sesión, 2-23

vetar rutas de salida, 2-48

vinculación de llamadas analógicas mediante MP, 1-18

VISA-II, conexiones de llamada de entrada, 11-5

VRouters. *Consulte* ruteadores virtuales, 6-1

## Z

ZipGetNetInfo, enviar al ruteador raíz petición, 8-4

zona predeterminada, AppleTalk, 8-3

zonas  
 hint-zone, 8-4  
 lista de, 8-3  
 predeterminada, 8-3

